CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY OF
THE PRIME MINISTER

CYBERSECURITY STRATEGIE BELGIË 2.0 2021-2025

MEI 2021

.be


Security

Synopsis

De Belgische bevolking en organisaties beschikken over verschillende ontwikkelingsmogelijkheden dankzij de aanwezigheid en de groei van digitale diensten en technologieën. De overheid, burgers en organisaties krijgen echter ook meer en meer te maken met (geavanceerde) cyberdreigingen, die de risico's kunnen verhogen en de opportuniteiten van de digitale diensten en technologieën in gevaar brengen. Het doel van deze geactualiseerde nationale Cybersecurity Strategie is om de mogelijkheden van diensten, goederen, mensen en kapitaal over de grenzen te vrijwaren.

Deze strategie wil een toekomstgerichte visie presenteren van een open, vrije en veilige cyberruimte die een antwoord biedt op mogelijke cyberdreigingen waar België mee geconfronteerd wordt of mee kan geconfronteerd worden. Dit document identificeert de verschillende belanghebbenden, de belangrijkste dreigingen, draagt een duidelijke missie uit en schuift op basis hiervan strategische doelstellingen en prioriteiten naar voren voor de komende jaren, alsook de nodige middelen om hieraan invulling te kunnen geven. Vermits cyberveiligheid bij uitstek een gedeelde verantwoordelijkheid is, worden de verschillende rollen van de betrokken actoren omschreven. Het Centrum voor Cybersecurity België (CCB) staat in voor de coördinatie van cyberveiligheid, daarom heeft zij een sleutelrol in de verwezenlijking van deze Cybersecurity Strategie 2.0.

Centrum voor Cybersecurity België, Brussel, mei 2021

Inhoudstafel

1. Inleiding

Onze samenleving en economie zijn in constante verandering, een proces dat versneld wordt door de digitale transformatie. Mensen, organisaties, apparaten, data en processen connecteren en interageren steeds meer via online kanalen zoals het internet, mobiele apparaten, Internet of Things (IoT), of het gebruik van cloud voor de opslag van (persoonlijke) bestanden en foto's. Deze groei in het gebruik van nieuwe technologieën gaat gepaard met de toename in cyberaanvallen, maar ook met de toename van de ernst en de impactgraad van deze aanvallen. Gevoelige gegevens, waaronder persoonlijke data, klantengegevens en politiek gevoelige gegevens (e.g.: militaire inlichtingen) lopen steeds meer het risico om openbaar gemaakt te worden. Daarom is het van uiterste belang om deze gegevens te beschermen door de digitale omgeving te beveiligen.

1.1 Beleidscontext

In 2012 tekende België zijn eerste Cybersecurity Strategie uit, die focuste op het erkennen van de cyberdreiging, het verbeteren van de veiligheid en het opstellen van maatregelen om gepast te kunnen reageren op incidenten. Door de continue verandering in het cyberlandschap is er nood aan een nieuwe Belgische cyberveiligheidsstrategie, die inspeelt op de huidige en toekomstige risico's en dreigingen.

De Cybersecurity Strategie 2.0 geeft het Belgische beleid vorm en doelt op het beveiligen van het cyberlandschap op alle niveaus, voor alle stakeholders. De opvolging en coördinatie van en toezien op de uitvoering van de Belgische Cybersecurity Strategie is de verantwoordelijkheid van het Centrum voor Cybersecurity België (CCB). De Cybersecurity Strategie 2.0 stelt doelstellingen tegen 2025 op en zal periodiek herzien of bijgestuurd worden.

Deze Strategie kadert ook in een internationale context. Zo werkt de Europese Unie aan een aantal initiatieven om de cyberweerbaarheid binnen de EU te promoten en te verbeteren. In juli 2016 werd de NIS richtlijn (*Network and Information Security*) aangenomen, die in België werd omgezet in de Wet van 7 april 2019: *Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid*. Artikel 7 van deze richtlijn (overgenomen in artikel 10 van de Belgische wet) schrijft de lidstaten voor om een nationale

strategie uit te tekenen in het kader van de veiligheid van netwerk- en informatiesystemen.

Daarnaast werd in juni 2019 de Cybersecurity Act van kracht, welke o.a. het mandaat van ENISA uitbreidt tot Agentschap van de Europese Unie voor cyberbeveiliging. Deze verordening benadrukt bovendien de nood aan een Europees Informatie en Communicatie Technologie cybersecurity certificaat, met het oog op het verhogen van het vertrouwen in en de beveiliging van producten en diensten, cruciaal voor de digitale interne markt.

Tot slot moeten de nationale engagementen inzake weerbaarheid in het kader van de NAVO *Cyber Defence Pledge* voor ogen gehouden worden.

1.2 Cybersecurity

Cybersecurity is het resultaat van een geheel aan beveiligingsmaatregelen die het risico op verstoring van of ongeoorloofde toegang tot informatie en communicatie (ICT) systemen minimaliseren.

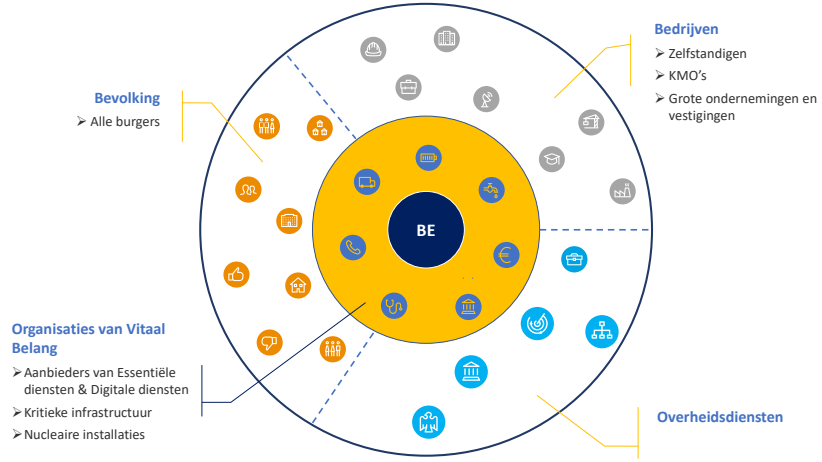
Cybersecurity, of cyberveiligheid, omvat alle redelijke en aanvaardbare maatregelen om de ICT van burgers, bedrijven, organisaties en de overheid te beschermen tegen cyberdreigingen. Het gaat om het beschermen van systemen (zoals hardware, software en gerelateerde infrastructuur), netwerken, alsook de gegevens die ze bevatten. De maatregelen tegen het gebruik van ICT om bijvoorbeeld fraude te plegen, om op te ruien of om terroristen te rekruteren vallen strikt genomen buiten de scope van deze strategie.

Dit vereist het ontwikkelen en versterken van technische en organisatorische maatregelen. Allereerst moeten de juiste doelstellingen geïdentificeerd worden alsook de gepaste bewustzijnscampagnes rond cyberveiligheid voor alle stakeholders. Er moet tevens gekeken worden naar het implementeren van preventieve maatregelen om gevoelige gegevens te beschermen tegen cyberdreigingen en -incidenten, zodat ongeautoriseerde toegang tot deze gegevens onmogelijk wordt. Het is eveneens noodzakelijk om eventuele dreigingen te monitoren en te analyseren. Wanneer een incident dan toch plaatsvindt, is het belangrijk dat men voorbereid is om er op een efficiënte manier op te reageren en op te lossen.

Het identificeren van een cyberveiligheid 'governancekader' is van belang voor het behalen van de cyberveiligheidsdoelstellingen. Bijgevolg is het cruciaal om rollen en taken te bepalen, alsook de verantwoordelijkheid van alle betrokken stakeholders te verduidelijken. Het opzetten van een nationaal governancekader maakt dialoog en coördinatie van de verschillende activiteiten mogelijk.

De Algemene Verordening Gegevensbescherming, en 'Privacy' in het algemeen, vormen geen onderdeel van Cybersecurity *strictu sensu*, maar ze leunen uiteraard sterk aan bij de opdracht van het CCB om incidenten en dreigingen te detecteren. Een goede samenwerking met de Belgische Gegevensbeschermingsautoriteit is bijgevolg noodzakelijk. Ook het bestrijden van online desinformatie campagnes is geen daadwerkelijk deel van cyberveiligheid, maar het is er aan verbonden. Ook in dit kader is een samenwerking met de bevoegde inlichtingen- en veiligheidsdiensten onontbeerlijk.

1.3 Doelgroepen



Cybersecurity is niet enkel de verantwoordelijkheid van de overheid. Het is een gezamenlijke inspanning, waar alle betrokken stakeholders aan kunnen bijdragen. Dankzij ieders inspanning zal het de algemene veiligheid ten goede komen.

i. Bevolking

Burgers zijn in eerste instantie zelf verantwoordelijk voor de bescherming van hun bezittingen. Hieronder vallen smartphones, laptops, tablets, maar ook de applicaties die erop staan (zoals bijvoorbeeld banking applicaties) en dus ook de gegevens die ze bevatten. Door de eigen apparaten en applicaties te beschermen en door ze op gepaste wijze te gebruiken, wordt het voor dreigingsactoren minder evident om cyberaanvallen uit te oefenen. Met steun van de overheid en de media, zoals onder meer Safeonweb.be en risico-info.be, kan de bevolking zich bewust zijn/worden van de voornaamste cyberdreigingen en voelt zij zich betrokken bij het beveiligen van de cyberomgeving.

ii. Bedrijven

Bedrijven spelen een grote rol in het beschermen van de eigen infrastructuur en de gegevens van hun werknemers. Kleine en Middelgrote Ondernemingen (KMO's, minder dan 250 werknemers) hebben hierin een belangrijke plaats, daar zij meer dan 99 % van de Belgische bedrijven omvatten. Onder deze groep van stakeholders worden ook de onderwijsinstellingen begrepen en leveranciers van beveiligingsproducten. Beveiligingsproducten zoals firewalls, virusscans, encryptie of andere soft- en hardwareproducten maken de IT-systemen heel wat veiliger en maken de kans op incidenten kleiner. Het investeren in deze beveiligingsproducten, het ondersteunen van leveranciers ervan en het faciliteren van de gebruikers van IT-systemen in het gebruik van deze producten is van belang. Het uitwerken van een basis cyberveiligheid-certificatie die aan de onderneming toelaat aan te tonen dat deze de nodige aandacht vestigt op de meest voorkomende cyberbedreigingen vormt een niet onbelangrijk aspect van deze aanpak en kan ook dienen als een competitief voordeel. In 2019 lanceerde de Europese Unie in deze optiek ook een cybersecurity certificatie kader.

iii. Overheidsdiensten

België heeft een complexe overheidsstructuur wat een gecoördineerd cyberveiligheidsbeleid voor overheidsdiensten niet eenvoudig maakt. De federale overheid beschikt over horizontale, verticale en programmatorische diensten. Gewesten en Gemeenschappen hebben ministeries en directies.

Het Centrum voor Cybersecurity België (CCB) ontwikkelt adviezen en richtlijnen die voor alle overheidsdiensten ter beschikking zijn.

Veiligheid en cyberveiligheid in het bijzonder zijn federale materie en worden op nationaal niveau behandeld.

iv. Organisaties van Vitaal Belang

De Organisaties van Vitaal Belang (OVI) voor ons land dienen optimaal beschermd te worden tegen cyberaanvallen, aangezien incidenten ten aanzien van deze organisaties een grootschalige, nationale impact kunnen hebben.

Met Organisaties van Vitaal Belang worden in dit kader bedoeld de publieke en private entiteiten die een essentiële dienst verlenen ten aanzien van de Belgische bevolking, en die daarvoor gebruik maken van netwerk- en informatiesystemen. Men begrijpt hieronder minstens de exploitanten van Kritieke Infrastructuren, de Aanbieders van Essentiële Diensten en digitaledienstverleners, en de nucleaire inrichtingen (zoals bedoeld in hun respectievelijke wettelijke kaders)[1].

A priori bepalen de sectorale overheden in overleg met het Nationaal Crisiscentrum (NCCN) en met het CCB wie de Organisaties van Vitaal Belang zijn. De term is evolutief bedoeld en omvat de sectoren van energie, mobiliteit, telecom, de financiële sector, drinkbaar water, volksgezondheid, digitale dienstverleners en de overheid.

1.4 Visie

België pleit voor een open, vrije en veilige cyberruimte waar burgers en ondernemingen zich volledig kunnen ontplooien, waar ze zich internationaal kunnen engageren en waar fundamentele rechten gevrijwaard en beschermd worden. Om het essentiële vertrouwen van de samenleving in de cyberruimte op te bouwen en te garanderen, is cyberveiligheid van noodzakelijk en doorslaggevend belang. Dit is een gedeelde verantwoordelijkheid van alle belanghebbenden en vergt een breed gedragen aanpak.

1 Hoewel het Wetenschappelijk en Economisch Potentieel van het land en de organisaties die essentiële diensten leveren binnen de overheidssector binnen de beoogde scope van 'Organisaties van Vitaal Belang' vallen, moet eerst een duidelijk governance kader op gebied van cyber voor deze sectoren ontwikkeld worden.

1.5 Missie

Tegen 2025 moet België in het cyberdomein één van de minst kwetsbare landen van Europa zijn.

De Cybersecurity Strategie 2.0 heeft tot doel van België tegen 2025 een van de minst kwetsbare landen van Europa te maken in het Cybersecurity domein. Dit zal onderbouwd worden met het uittekenen van actieplannen om alle stakeholders te beschermen, van de algemene bevolking over private organisaties tot organisaties van vitaal belang. De strategie is in lijn met investeringsstrategieën van de regering en van de private sector voor toekomstige ontwikkelingen en waarborgt deze investeringen en de creatie van nieuwe opportuniteiten en jobs. Bovendien maken de strategische doelstellingen het mogelijk om voorbereid te zijn op nieuwe technologische ontwikkelingen en de mogelijke risico's.

2. Risicobeoordeling

De Belgische Nationale Risicobeoordeling 2018-2023 van het Nationale Crisiscentrum beschouwt cyber als één van de belangrijkste risicoclusters waarmee ons land de komende jaren geconfronteerd zal worden. Binnen deze cluster worden cybercriminaliteit en hacktivisme ten aanzien van bedrijven en kritieke infrastructuren geïdentificeerd als nationale prioritaire risico's.

In 2017 zagen we hoe de WannaCry-ransomware zich verspreidde naar meer dan 150 landen en bedrijfsactiviteiten onderbraken, en hoe de NotPetya-malware in een flits uitgroeide tot het duurste cyberincident ooit.

Bovendien is de evolutie van de cyberdreiging van financieel gedreven naar geopolitiek gemotiveerd uiterst zorgwekkend. Westerse landen worden geconfronteerd met een dreiging in cyberspace die het gevaar van fysieke aanvallen overstijgt. Deze cyberbedreigingen kunnen ernstige directe gevolgen hebben op bijvoorbeeld onze elektriciteitsdistributie, onze banksystemen of op de beschikbaarheid van alle online diensten. Door aanhoudende berichtgeving over cyberincidenten, zelfs minder ernstige, kan de bevolking het vertrouwen in de digitale omgeving en diensten verliezen, wat nefaste economische gevolgen kan hebben.

De cyberdreiging kan als onderdeel van de hybride dreiging aangewend worden om de effecten van andere aanvalsmethodes te versterken. Bij deze dreiging kan een combinatie van bijvoorbeeld een fysieke aanslag met een reeks cyberaanvallen de uitwerking ernstig versterken en tijdelijk een sfeer van chaos veroorzaken.

Deze strategie omschrijft de nationale doelstellingen voor de periode 2021-2025 om tegemoet te komen aan dit voortdurend veranderend cyberlandschap. Teneinde de juiste prioriteiten neer te zetten bij het opstellen van deze doelstellingen, is het noodzakelijk een duidelijk beeld te hebben van de verschillende cyberrisico's en –dreigingen waarmee België in deze periode geconfronteerd kan worden. Dit hoofdstuk biedt een bondig overzicht van de belangrijkste dreigingsactoren en technologische risico's.

Er moet evenwel vermeld worden dat de risicobeoordeling een continu proces is. Geijkte overlegplatformen, zoals het Coördinatie Comité voor Inlichting en Veiligheid en haar Platform 4 Cyber, zullen daarom de genomen maatregelen blijven evalueren, de cybertrends opvolgen en de

doelstellingen indien nodig bijsturen. Het opstellen van een Belgische bijdrage aan de Europese 5G risicoanalyse in 2019 is hiervan een voorbeeld.

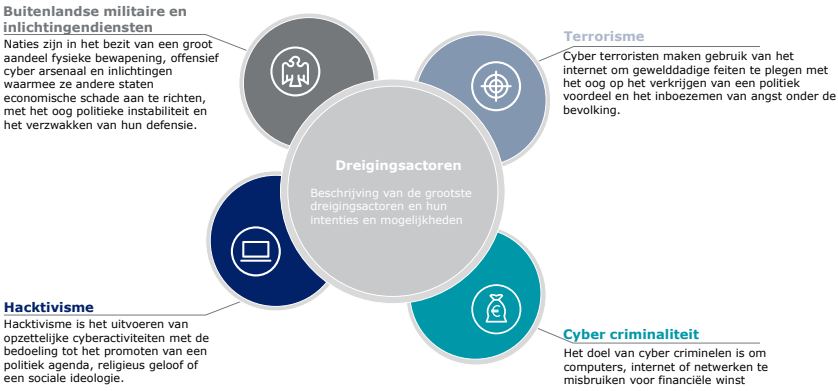
Daarnaast voorziet het Nationale Crisiscentrum als vervolgtraject op de Belgische Nationale Risicobeoordeling 2018-2023 een diepgaandere analyse met alle betrokken actoren van de belangrijkste risicoclusters (waarvan cyber deel uitmaakt). Deze heeft als doel de achterliggende oorzaken en gevolgen beter in kaart te brengen om zo een duidelijk overzicht te kunnen bieden aan besluitvormers bij het behandelen van het risico.

Ten slotte vinden er op het Belgisch grondgebied regelmatig evenementen plaats die een verhoogd cyberrisico inhouden (een internationale top, verkiezingen, …). Voor dit soort evenement kan het nodig blijken een uitzonderlijke risicobeoordeling uit te voeren om verhoogde risico's te identificeren en gepaste maatregelen aan te bevelen.

2.1 Dreigingsactoren

Omdat de motivaties en mogelijkheden van dreigingsactoren voortdurend wijzigen, is het van groot belang om te begrijpen wie de grootste dreigingsactoren zijn en om deze te monitoren. Dit maakt het ook mogelijk te begrijpen hoe het cyberlandschap zich verder ontwikkelt. België beschouwt de volgende actoren als grootste dreiging voor de Belgische staat en de bevolking: cybercriminelen, buitenlandse militaire- en inlichtingendiensten, terroristische groeperingen en hacktivisten.

Dreigingsactoren



2.1.1 Cybercriminaliteit

De (potentiële) impact van cyberdreigingen uitgaande van cybercriminelen is de laatste jaren steeds duidelijker geworden. Het gaat hierbij niet alleen om dreigingen die onze infrastructuur kunnen verstoren, maar ook om dreigingen ten aanzien van de integriteit, de beschikbaarheid en de vertrouwelijkheid van de informatie die wij digitaal vastleggen, analyseren en uitwisselen. De digitalisering van zaken of goederen (Internet of Things) impliceert dat deze 'hackbaar' zijn. Dit heeft een directe impact op de algemene veiligheid van elke burger, maar het betekent ook dat ze mogelijk digitale sporen bevatten die van belang kunnen zijn in criminaliteitsonderzoek.

Het hoofddoel van criminele actoren, zowel individuen als in het kader van georganiseerde criminaliteit, is veelal het generen van geld en winst, bijvoorbeeld via phishing, datadiefstal of ransomware. In sommige gevallen kunnen zij daarnaast ook destructieve doeleinden voor ogen hebben, bijvoorbeeld datasabotage of cyberaanvallen. Cybercriminelen specialiseren zich in specifieke diensten, die ze vervolgens op het Dark Web aanbieden tegen betaling. Een crimineel kan hierdoor een abonnement nemen op bijvoorbeeld een Exploit Kit, waarmee hij zonder enige technische kennis gebruik kan maken van de laatste digitale inbraaktechnieken.

Cybercriminelen bieden hun diensten aan om het even wie er voor wil betalen aan. Naast cyberterrorisme dienen daarom ook criminele organisaties (of individuen) die materiële en/of fysieke schade willen berokkenen te worden ingecalculeerd als potentiële dreigingsactor op nationaal niveau.

De mogelijke impact van cyberaanvallen op kritieke infrastructuren kan immers dermate zijn dat de stabiliteit van de staatsinstellingen onder druk komt te staan.

2.1.2 Buitenlandse militaire en inlichtingendiensten

Naties en staten bezitten heel wat kennis en fysieke bewapening, alsook een offensief cyberarsenaal. Het is echter steeds mogelijk dat ze deze voor andere doeleinden wensen te gebruiken dan het beschermen van de eigen burgers. Zo kunnen de militaire en inlichtingendiensten deze kennis en bewapening uitbuiten om andere staten economische schade aan te richten, om er politieke instabiliteit teweeg te brengen en/of om er de defensie te verzwakken. Buitenlandse militaire en inlichtingendiensten voeren niet enkel meer cyberaanvallen uit met het oog op het halen van een competitief voordeel op vlak van inlichtingen: meer en meer wordt gebruik gemaakt van geavanceerde technieken om de werking van organisaties te verstoren - en indirect zo ook van de landen waarin deze gevestigd zijn -, bijvoorbeeld door confidentiële informatie bloot te leggen.

De capaciteiten van verschillende nationale militaire en inlichtingendiensten worden steeds meer geavanceerd. Daarom wordt het steeds moeilijker om zulke cyberaanvallen op te sporen en om zich er preventief tegen te verweren. Bijgevolg is de feitelijke activiteit van deze dreigingsactoren veel frequenter dan statistieken laten blijken.

2.1.3 Hacktivisme

Hacktivisme is het uitvoeren van verschillende opzettelijke cyberactiviteiten met het oog op het promoten van een politieke agenda, religieus geloof of een sociale ideologie. Het kan een politiek gemotiveerde beweging zijn die deze activiteit uitvoert. Momenteel zijn hierbij de meest gebruikte aanvalsmethoden Doxing[2], DDoS[3], Web defacement[4] en het onrechtmatig overnemen van identiteiten en sociale mediakanalen.

2.1.4 Terrorisme

Cyberterrorisme is het uitvoeren van gewelddadige activiteiten met behulp van het internet, met als achterliggend doel om politiek voordeel te

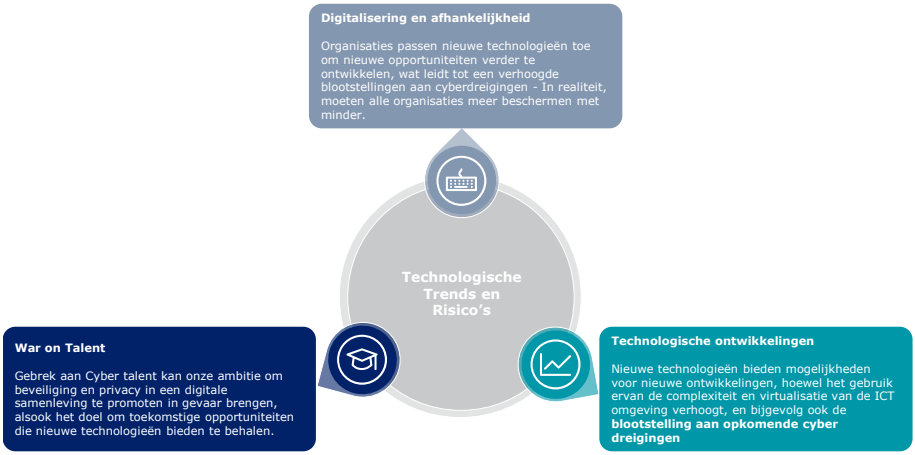
2 Doxing is het meestal onrechtmatig publiek verspreiden van informatie of documenten van een iemand.
3 DDoS staat voor distributed-denial-of-service aanvallen waarbij een groot volume aan data naar één specifiek systeem wordt gestuurd om de normale werking ervan te verstoren.
4 Een web defacement is het onrechtmatig wijzigen van de inhoud van een web site of pagina

halen door intimidatie en het inboezemen van angst. Deze daden kunnen resulteren in verwoesting, het verlies van mensenlevens en/of lichamelijke schade. De meest voor de hand liggende doelwitten van cyberterroristen zijn publieke diensten, industrieën, kritieke infrastructuren, etc.

Zo gebruiken bijvoorbeeld sommige terroristische groeperingen de onlinewereld als propaganda- en wervingskanaal voor terrorisme, maar sinds 2016 is er een duidelijke overgang in het gebruik van Twitter en Facebook naar meer geëncrypteerde communicatiekanalen. De huidige ontwikkelingen wijzen ook op een toenemend gebruik van cyberinstrumenten voor de financiering van terrorisme, bv. via ransomware, cryptomining of zelfs crowdfunding. Er bestaat in deze context grote bezorgdheid dat terroristische organisaties ook meer cyberaanvallen zouden uitvoeren. Echter lijkt het dat deze aanvalstechnieken redelijk beperkt blijven. Voor de uitvoering van DDOS aanvallen schaffen groeperingen nog steeds domein hostingdiensten aan, downloaden ze software en huren botnets, in plaats van het ontwikkelen van hun eigen cyberwapens.

2.2 Technologische trends en risico's

Het technologische landschap staat niet stil en er komen steeds meer nieuwe producten op de markt. Organisaties passen deze nieuwe technologieën toe om competitief te blijven en om nieuwe opportuniteiten te ontwikkelen. Echter zijn aan deze technologische ontwikkelingen ook risico's verbonden, eveneens omdat ze de vaardigheden van de dreigingsactoren verder helpen ontwikkelen. Het is daarom cruciaal om steeds bewust te zijn van ontwikkelingen in technologieën en om de daaraan verbonden risico's te beseffen.



2.2.1 Afhankelijkheid

Organisaties passen nieuwe technologieën toe om nieuwe opportuniteiten te ontwikkelen en om hun productiviteit of efficiëntie te verhogen. De toename van het gebruik van deze technologieën zorgt daarom voor een steeds grotere afhankelijkheid van ICT. Dit gaat gepaard met een verhoogde blootstelling aan cyberdreigingen. Men kan algemeen ook vaststellen dat de ingebruikname van technologieën sneller stijgt dan de beveiliging ervan.

Organisaties zullen meer inzetten op het verschaffen en gebruiken van nieuwe technologieën dan op het toekennen van budgetten voor de beveiliging ervan. Vaak wordt over het hoofd gezien dat nieuwe technologieën niet altijd meteen extensief getest worden. Het is dan ook een groot risico om aan te nemen dat er nog geen aanvallen bestaan of dat het veilig lijkt om de technologie te implementeren en te beveiligen op de gebruikelijke manieren. Het duurt immers vaak een paar maanden of jaren voor de meeste aanvallen en vectoren op een bepaalde technologie publiek worden en voor er goed tegen kan beveiligd worden. Secure Development – met aandacht voor veiligheid – dient daarom opgenomen te worden in het ontwikkelingsproces van nieuwe software en technologieën.

Er is ook een steeds toenemende afhankelijkheid van zogenaamde Third Party Providers in elke stap van het ontwikkelings-, productie-, onderhouds-, en verwerkingsproces. Hierdoor verhoogt het risico en de mogelijke kritieke impact van 'supply chain attacks'.

De interconnectie van producten kan ook aanleiding geven tot 'hazardization'. Dit is de situatie die ontstaat wanneer een product veilig is wanneer het door een consument wordt verkregen, maar wanneer het wordt aangesloten op een netwerk, gevaarlijk wordt door kwaadwillige, onjuiste of onzorgvuldige wijzigingen in de operationele code.

2.2.2 Technologiespecifieke risico's

Nieuwe toepassingen die het gevolg zijn van opkomende technologieën bieden vaak grote voordelen tegenover traditionele methodes; bijvoorbeeld op gebied van efficiëntie en schaalvoordeel. Hier zijn echter soms specifieke veiligheidsrisico's aan verbonden.

Een goed voorbeeld is Cloud Computing. Het grote voordeel is dat de infrastructuur niet meer moet onderhouden worden en dat alles mee schaalt met het tempo waarmee de organisatie groeit. Een centrale Cloud infrastructuur kan daarom professioneel goed beveiligd worden. Het risico is echter dat een ongeoorloofde toegang ineens het compromitteren van een heel grote hoeveelheid aan informatie betekent.

Hierbij zijn ook twee economische dreigingen te formuleren. Ten eerste wordt de wereld van de cloud-based toepassing gekenmerkt door de aanwezigheid van een beperkt aantal mondiale spelers, waarbij schaalvoordelen kunnen worden uitgespeeld, wat een concentratierisico met zich meebrengt. Anderzijds wordt innovatie in deze markt vaak door nieuwe, veel kleinere spelers aangeboden. Deze jonge organisaties staan vaak niet op hetzelfde niveau qua performantie en maturiteit van processen. Dit kan leiden tot misplaatst vertrouwen in deze toepassingen.
Steeds toenemende technologische ontwikkeling in nieuwe (soorten) ICT-gebaseerde producten en diensten in vele economische deelgebieden vergen ook van de toezichthoudende overheden een snelle evolutie in markttoezicht en inspectiecapaciteiten. Anderzijds bieden deze technologieën natuurlijk soms ook voordelen om markttoezicht efficiënter uit te bouwen.

Autoriteiten besteden reeds veel aandacht aan persoonsgerichte aspecten rond 'security' en 'privacy'. De product gebonden aspecten van deze thema's, zoals reglementering en controle, zijn daarentegen nog niet of nauwelijks gedekt door de toezichthoudende autoriteiten. Er is dus nood aan een aanpassing van het bestaande wettelijke kader. Dit moet voornamelijk vanuit een Europees/internationaal kader gebeuren. De Europese

Cybersecurity Act is hierin een belangrijke stap en vereist een duidelijke Belgische implementatie.

Een ander vaak voorkomend risico is het individueel beschermen van met het internet verbonden apparaten. De grootste recente uitdaging op dit vlak is het Internet of Things (IoT).

Het is van groot belang de risico's in te schatten en de nodige beveiliging op te stellen, alvorens nieuwe technologieën in gebruik te nemen. De snelheid in ontwikkeling en adoptie van nieuwe technologieën zoals Artificiële intelligentie, Quantum Computing, Blockchain, en Smart Meters&Grids maakt een gepaste evaluatie van (en bescherming tegen) alle risico's een hele uitdaging.

2.2.3 War On Talent

Met de digitale transformatie en de toepassing van nieuwe technologieën, is er tevens een stijging in misbruik van deze systemen. Het is daarom belangrijk als organisatie te investeren in het rekruteren van IT-profielen, alsook van IT-security profielen. Er is echter een tekort aan cybersecurity talent op de arbeidsmarkt. Er zijn weinig opleidingen waar cybersecurity een (belangrijk) onderdeel vormt. Vaak wordt het eerder als bijkomend vak onderwezen, waardoor er in de praktijk weinig kennis van wordt opgedaan of overgedragen.

Er is daarom een duidelijk tekort aan cybersecurity professionals. Veel organisaties zullen als gevolg deze functies niet kunnen invullen of vullen ze in met andere profielen. De uitdaging om competente en betrouwbare medewerkers te vinden gaat uiteraard hand in hand met de interne dreiging ("the insider threat").

3. Strategische doelstellingen en aanpak

Het uittekenen van een cyberstrategie heeft de ambitie om in te spelen op de technologische ontwikkelingen en om tegemoet te komen aan de hoge nood om de bevolking, de private en publieke sector en de vitale sectoren te beschermen. De Cyber Strategie 2.0 bevat zes strategische doelstellingen voor de komende vier jaren. Deze strategie schrijft een aantal acties voor teneinde deze strategische doelstellingen te verwezenlijken. Dit zal mede gerealiseerd kunnen worden dankzij de hulp van verschillende stakeholders.

3.1 Versterken van de digitale omgeving en het vertrouwen in de digitale omgeving vergroten

3.1.1 Investeren in een veilige netwerkinfrastructuur

Samen met de internet dienstenverleners (ISP) zal gewerkt worden aan een veiligere basis netwerkinfrastructuur. Nieuwe beschermingstechnieken zullen mee de technologische evoluties volgen, zoals Internet of Things (IoT) en nieuwe generaties vaste en mobiele netwerken.

De veiligheid van de netwerkinfrastructuur kan verbeterd worden door het invoeren van veiligere Internetstandaarden (DNS-security, secure routing, encryptie, etc.). Deze standaarden zorgen voor een veilige manier om data uit te wisselen ('safe data transport layer'). Online data uitwisseling is dan over de hele lijn beveiligd. Dit beperkt het risico op een aanval op een zwakke link in de keten.

Dergelijke standaarden kunnen eveneens zorgen voor meer betrouwbare identiteiten en publicaties op het internet. Dit kan bijvoorbeeld door het stimuleren van het gebruik van technologie zoals Itsme en van Extended Validation Certificates op websites.

Ook een testomgeving (*'testbed'*) voor infrastructuur kan uitgebouwd worden. Een testbed is een platform dat toelaat om nieuwe infrastructuur te testen in een betrouwbare, gecontroleerde en veilige omgeving, vooraleer die breed gebruikt wordt.

3.1.2 Oprichten van een Cyber Green House

Het oprichten van een Cyber Green House zal een belangrijke stimulans betekenen voor innovatie in de cybersecurity sector. De oprichting van een innovatiecentrum heeft tot doel om innovatieve cyberoplossingen en businessmodellen te testen in een risicoloze omgeving en om Cybersecurity Guidelines en Best Practices te verspreiden.

3.1.3 Expertise en kennis stimuleren

Om tegemoet te komen aan de nood voor meer beveiliging en de nood voor meer security professionals, is het onvermijdbaar om meer te investeren in expertise en kennis. Onderwijsinstellingen leveren een belangrijke bijdrage aan het cyberveiligheidslandschap. Enerzijds spelen zij een belangrijke rol in het vergroten van de kennis door het voeren van onderzoek. Anderzijds dragen zij bij tot het ontwikkelen en voorzien van relevante opleidingen.

Er zal verder geïnvesteerd worden in Onderzoek & Ontwikkeling (O&O) op vlak van Cyberveiligheid. De private sector en de onderwijsinstellingen zoals universiteiten en hogescholen zullen nauw samenwerken.

Europese initiatieven in dit kader zullen vanuit deze doelstelling worden geëvalueerd.

Beveiligingsmanagers van openbare instellingen moeten opgeleid worden tot een adequaat beveiligingsniveau, door middel van opleidingsprogramma's voor overheidsfunctionarissen.

Om tegemoet te komen aan het gebrek aan informatiebeveiligingsprofessionals, zowel binnen de overheid als binnen de privésector zouden meer jongeren gestimuleerd moeten worden om de STEM richtingen (Science, Technology, Engineering en Mathematics) te volgen. Hiervoor moeten contacten gelegd worden met de gemeenschappen en moet in samenwerking met relevante partners een samenhangend beleid over het onderwerp bepaald worden. Zo kunnen bijvoorbeeld bewustmakings- en informatiematerialen aan scholen verstrekt worden of kan men mentorprogramma's organiseren.

3.1.4 Cybersecurity Certificatie en Labeling van producten, diensten en processen

België zal een kader creëren dat bedrijven moet toelaten om de veiligheid van ICT-producten, -diensten en -processen te evalueren en te certifiëren.

Dit kader zal in lijn worden gebracht met de EU Cybersecurity Act 2019 en met de ontwikkelingen die op Europees niveau gaande zijn. De EU Cybersecurity Act beoogt een Europese erkenning van geleverde certificaten, alsook een maximale afstemming op bestaande Europese en internationale referentiekaders.

Hiervoor zal België, zoals vereist in de EU Cybersecurity Act, een *National Cybersecurity Certification Authority* (NCCA) oprichten. Deze NCCA zal, in overleg met onder meer de markttoezichtautoriteiten, andere sectorale overheden en het NCCN, de nodige expertise in cybersecurity certificering coördineren, certificaten met hoge veiligheidsvereisten toelaten en een nauwe samenwerking met BELAC (de Belgische accreditatieorganisatie) bewerkstelligen door de bestaande processen, procedures en regelgeving maximaal te benutten.

Er zal tevens gewerkt worden aan een cyberveiligheids erkenningsmechanisme voor bedrijven, met een speciale aandacht voor KMO's, die wensen aan te tonen dat basis cyberveiligheidsvereisten, best practices en beleidsmaatregelen minimaal aanwezig zijn. Het is belangrijk om voor strategische sectoren na te denken over een geïntegreerde aanpak die IT-aspecten, fysieke bescherming en de screening van personeel combineert.

Deze initiatieven ondersteunen sterk de visie van deze Cybersecurity Strategie en zullen het vertrouwen van klanten in de veiligheid van de digitale omgeving opkrikken.

3.1.5 Versterken van de cybervaardigheden van inlichtingen- en veiligheidsdiensten

Om een gepast antwoord te kunnen bieden op de snel toenemende dreiging moeten de capaciteiten en de vaardigheden van onze inlichtingen- en veiligheidsdiensten hiermee minstens gelijke tred houden. Het menselijk kapitaal aan technische experten in cyberveiligheid vormt nationaal het beste wapen tegen deze nieuwe dreigingen.

Om onze diensten van de noodzakelijke experten te kunnen voorzien, zullen alternatieve rekruterings- en tewerkstellingsmethodes geëvalueerd en gebruikt worden, waar mogelijk. De behoefte aan jonge en hoogopgeleide computerexperten bestaat immers niet enkel binnen onze veiligheidsdiensten. De "War on talent" wordt uitgevochten tussen gespecialiseerde bedrijven, grote multinationals en alle veiligheidsdiensten in Europa en daarbuiten. Om hun kennis uit te breiden zoeken dergelijke technische experten vaak nieuwe uitdagingen en zijn ze meestal niet op zoek naar een job voor het leven. Een voldoende flexibel rekruteringsysteem en een competitievere verloning moeten onze veiligheidsdiensten in staat stellen om op een meer gedegen manier een dergelijke competitie met de arbeidsmarkt aan te gaan.

Overheidsdiensten moeten hun technische experten cyberveiligheid daarnaast ook voldoende hoogwaardige technische vormingen aanbieden. Dit kan niet enkel tellen als een belangrijke motiverende factor, het garandeert eveneens voldoende technische kennis en expertise.

3.2 Gebruikers en beheerders van computers en netwerken wapenen

Het internet bestaat uit infrastructuur en systemen die quasi volledig in handen zijn van privéeigenaars. Het is dan ook van groot belang dat elke eigenaar van een computersysteem of -netwerk voldoende gewapend is om deze te beschermen tegen cyberdreigingen en –aanvallen.

3.2.1 Bewustmaken en betrekken

Naast het informeren van de burgers over mogelijk dreigingen, streeft de overheid er naar de burgers meer bewust te maken over hoe ze zich beter kunnen beschermen tegen mogelijk cyberrisico's.

Om systemen en computernetwerken te beschermen zijn enerzijds technische beschermingsmaatregelen noodzakelijk, maar anderzijds moet elke gebruiker er verantwoord gebruik van maken. Wie voldoende bewust en waakzaam is, wordt al snel het beste detectiesysteem voor cyberaanvallen. Via de website www.safeonweb.be krijgt de bevolking alle informatie over specifieke dreigingen, hoe die te herkennen en hoe zich te beschermen of te reageren.

Het internet is van en voor iedereen. Ook de veiligheid ervan is een gezamenlijke inspanning. Daarom wordt de bevolking aangespoord om deel te nemen aan de beveiliging. Zo kan bijvoorbeeld iedereen verdachte e-mails doorsturen naar verdacht@safeonweb.be. Dergelijke initiatieven zullen worden uitgebreid.

Het CCB organiseert jaarlijks via de media een bewustzijnscampagne en kadert die in Europese initiatieven. Ook het Europese Agentschap ENISA organiseert elk jaar in oktober de Europese Cybersecurity Month.

Via goede samenwerkingen moet het contact tussen de burger en kwaliteitsvolle dienstverleners in cyberveiligheid in ons land vergemakkelijkt worden. Een dergelijk gestroomlijnde contact moet de burger in staat stellen om veiligheidsincidenten aan te pakken en problemen te neutraliseren.

Het sensibiliseren van de bevolking heeft eveneens in het bedrijfsleven een directe impact en zorgt voor een algemene cultuur van bezorgdheid en veiligheid. Sensibilisatiecampagnes, zoals via webinars, gidsen of de cybersecurity KIT, moeten verder ingezet worden.

3.2.2 Informeren over dreigingen en kwetsbaarheden

Het tijdig waarschuwen over opkomende en belangrijke dreigingen of kwetsbaarheden is cruciaal.

Het CCB analyseert permanent alle beschikbare informatie over cyberdreigingen of kwetsbaarheden en stuurt waar opportuun de nodige waarschuwingen uit. Voor de bevolking beschikt het CCB over de nodige digitale media en onderhoudt het een directe en transparante relatie met de algemene media. BE-Alert van het Nationale Crisiscentrum (NCCN) kan de verspreiding van waarschuwingen ondersteunen en versturen binnen een specifieke regio.

Bedrijven en organisaties worden aangespoord om een "Gecoördineerd bekendmakingsbeleid van kwetsbaarheden" (een *Coordinated Vulnerability Disclosure Policy*) te publiceren. Via Sectorale overheden, beroepsorganisaties en de Cyber Security Coalition Belgium zullen ze geïnformeerd worden over belangrijke dreigingen of kwetsbaarheden. Organisaties van Vitaal Belang zullen eveneens gerichte en niet-publieke waarschuwingen ontvangen via het *Early Warning System* (EWS) van het CCB.

Het CCB heeft met het nationaal *Computer Emergency Response Team* (CERT.be) en als nationaal CSIRT (*Computer Security Incident Response Team*) de opdracht om online veiligheidsproblemen en kwetsbaarheden op te sporen, te analyseren en gebruikers hierover te informeren. Dit kan echter niet zonder de steun van de internet dienstenaanbieders die de waarschuwingen snel moeten doorsturen naar hun kwetsbare of bedreigde klanten.

3.2.3 Verspreiden van cybersecurity-richtlijnen en "best practices"

De cyberdreigingen en de gebruikte aanvalstechnieken evolueren heel snel. Kennisdeling en het delen van "*best practices*" is daarom zeer waardevol. Niet alleen zorgt dit voor kennisverrijking en het voortbrengen van nieuwe ideeën om de dreigingen aan te pakken, het vergemakkelijkt eveneens de besluitvorming. Cyberveiligheidskennis wordt gedeeld via bestaande of op te richten platformen.

Het CCB onderhoudt een Online Cybersecurity Referentiegids, om organisaties te ondersteunen in het ontwikkelen van een cyberveiligheidsstrategie. De gids biedt "basis" en meer "geavanceerde aanbevelingen" aan op vlak van planning, risicobeheer, veiligheidsmaatregelen en evaluaties op vlak van het gebruik van computers en computernetwerken. De identificatie en beheer van risico's is hierin van cruciaal belang. De aangeboden richtlijnen zijn gebaseerd op internationale standaarden en worden permanent door het CCB geactualiseerd. Bedrijven worden dan ook sterk aangemoedigd deze richtlijnen te hanteren in hun cyberbeveiligingsbeleid.

3.3 Organisaties van Vitaal Belang beschermen tegen alle cyberdreigingen

De Organisaties van Vitaal Belang worden wereldwijd geconfronteerd met een sterk toenemende en meer geavanceerde cyberdreiging. Gezien cyberaanvallen tegen deze organisaties een aanzienlijke impact kunnen hebben op onze maatschappij en op de nationale veiligheid is het cruciaal hen op gepaste wijze te ondersteunen in hun bescherming.

3.3.1 Informatie-uitwisseling optimaliseren en waarschuwingen uitsturen

Het CCB ontvangt als nationale autoriteit voor cyberveiligheid alle pertinente dreigingsinformatie van haar partners. Ze analyseert deze ontvangen

informatie permanent en stuurt via haar 'Early Warning System' (EWS) of via andere kanalen waarschuwingen uit.

De Organisaties van Vitaal Belang zullen op die manier (via het 'Early Warning System' (EWS) van het CCB) permanent geïnformeerd worden over relevante cybersecurity dreigingen, kwetsbaarheden of incidenten.

In België dragen sectorale overheden een cruciale verantwoordelijkheid bij het identificeren, reguleren en controleren van de Organisaties van Vitaal Belang. Een overlegplatform tussen deze sectorale overheden (Cyber Security Sectoral Authorities Platform – CySSAP) moet het beheer van informatie-uitwisselingen met Organisaties van Vitaal Belang helpen optimaliseren; ook met het oog op grensoverschrijdende afhankelijkheden.

3.3.2 Bescherming verbeteren voor internationale instellingen

In België zijn er heel wat internationale instellingen gevestigd, waaronder de NAVO (Noord-Atlantische Verdragsorganisatie) en instellingen van de Europese Unie. De Belgische Organisaties van Vitaal Belang die deze instellingen ondersteunen zullen geïdentificeerd worden zodat er voor een gepaste bescherming gezorgd kan worden.

Bovendien is een goede dialoog en samenwerking met de Internationale instellingen in ons land van belang en noodzakelijk om de effectiviteit van bescherming en de reactie op cyberaanvallen te verhogen.

3.3.3 Incidenten met nationale impact kunnen behandelen

Het Nationaal Cybernoodplan wordt verder geoperationaliseerd. Door een optimale samenwerking tussen het nationaal *Computer Emergency Response Team* (CERT.be) van het CCB, de Geïntegreerde Politiediensten en het Nationaal Crisiscentrum (NCCN) worden incidenten snel en effectief aangepakt en wordt het juridische onderzoek onmiddellijk geïntegreerd.

Incidenten met een nationaal impact worden naar het gepaste niveau geëscaleerd en gehandeld door *ad hoc* samengestelde *Rapid Reaction Teams* waarbij eveneens andere diensten en partners efficiënt worden ingeschakeld.

3.3.4 Oefeningen

Het Belgische Cybernoodplan werd in 2017 goedgekeurd door de ministerraad en beschrijft de procedures die de verschillende diensten moeten volgen bij een cyber gebeurtenis. Dit plan moet elk jaar geëvalueerd en

indien nodig bijgestuurd worden. Het CCB speelt hierin een coördinerende rol. Het regelmatig houden van oefeningen is belangrijk voor het opbouwen van weerbaarheid tegen incidenten en om de effectiviteit van het Noodplan te testen. De geleerde lessen uit deze oefeningen kunnen vervolgens de jaarlijkse evaluaties van dit plan informeren.

De deelname van de Belgische veiligheidsdiensten, andere overheidsdiensten en Organisaties van Vitaal Belang in zowel internationale als nationale oefeningen is dan ook sterk wenselijk. De coördinatie van de Belgische deelnames aan dergelijke oefeningen wordt verzekerd door overleg tussen het CCB, de FOD Buitenlandse Zaken, NCCN en Defensie.

3.4 Reageren op de cyberdreiging

Om de toenemende cybercriminaliteit en overheidsdreigingen snel te kunnen aanpakken moet er worden geïnvesteerd in de snelle identificatie van, en reactie op, gevaar voor onze bevolking, voor onze economie of voor Organisaties van Vitaal Belang.

3.4.1 De internationale dreiging in kaart brengen

Het permanent opvolgen en inschatten van de internationale cyberdreiging is van cruciaal belang om het risico op cyberaanvallen en incidenten te beperken. Het is de eerste stap van elke verdediging.

De cyberintenties en de mogelijkheden van "actoren" tegen onze essentiële en vitale belangen moeten in kaart worden gebracht en de potentiele bronnen moeten opgevolgd worden. Om onze computernetwerken te kunnen beschermen moet de evolutie van hun technische tactieken, technieken en procedures zo goed als mogelijk gekend zijn en moeten onze beschermingsmiddelen ten opzichte van deze worden geëvalueerd.

3.4.2 Criminele cyberinfrastructuur ontwrichten

Cybercriminelen specialiseren zich en hergebruiken de aanvalstechnieken en -software die circuleert op het *Dark Web*. Om hun hoogtechnologische of grootschalige cyberaanvallen te kunnen uitvoeren en tevens anoniem te blijven, maken ze gebruik van eigen alsook van gecompromitteerde computersystemen op het internet.

Door deze criminele cyberinfrastructuur te ontwrichten wordt het business model van de criminelen deels onderuit gehaald. Dit kan onder meer door:

- Opsporen en via juridische weg neutraliseren van de infrastructuur
- Opsporen van gecompromitteerde systemen en notifiëren van de eigenaar
- Beschermen van de communicatie van de bevolking en de bedrijven tegen gekende kwaadaardige infrastructuur
- Nationaal en internationaal delen van informatie

Hiervoor zullen alle inlichtingen en veiligheidsdiensten nauw moeten samenwerken.

3.4.3 Een gepaste repressieve capaciteit ontwikkelen

Om de kwetsbaarheid van België in het cyberdomein te reduceren, zijn preventieve maatregelen de sleutel. Goed geïnformeerde en weerbare burgers, bedrijven en overheden zullen cybercriminelen afweren en ontmoedigen voor de toekomst. De instroom van strafdossiers vermindert met elke investering in preventie. Hierdoor zullen politie en justitie niet langer enkel aan symptoombestrijding moeten doen, maar ten gronde de oorzaken moeten kunnen aanpakken.

Tegelijk is duidelijk dat cybercriminaliteit zal blijven bestaan. Een performant en deskundig repressief sluitstuk blijft dan ook nodig om de restcategorie van gepleegde informaticamisdrijven optimaal aan te pakken. Daders van informaticacriminaliteit moeten geïdentificeerd en gevat worden, de bewijzen van hun aandeel moeten verzameld worden, zoals hoger gesteld moet de criminele infrastructuur in kaart gebracht en ontmanteld worden, het illegale vermogen moet in beslag genomen en verbeurd verklaard worden, de verdachten moeten vervolgd en correct bestraft worden. Aangezien cybercriminelen bij uitstek in een internationale context opereren, moet ook hierbij afgestemd worden met andere, betrokken landen.

Dit strategisch plan heeft de ambitie om de ontwikkeling van een gepaste repressieve capaciteit te ondersteunen. Dergelijke repressieve capaciteit moet in staat zijn om cybercriminaliteit adequaat en deskundig te detecteren, onderzoeken, vervolgen en sanctioneren.

Het objectief hierbij is vooreerst om op alle niveaus van de geïntegreerde politie (zowel de lokale politie als de gedeconcentreerde diensten en centrale diensten van de federale politie) de gepaste capaciteit en expertise op te bouwen, zodat de van elk niveau verwachte beeldvormings- en onderzoekscapaciteiten in een digitale omgeving effectief en snel kunnen verricht worden.

Het opzet is vervolgens te verzekeren dat de parketten en de rechtscolleges van alle gerechtelijke arrondissementen en ressorten beschikken over voldoende parketmagistraten, onderzoeksrechters en zetelende magistraten met een interesse voor cyberveiligheid en cybercriminaliteit die hiertoe een afgestemd opleidingstraject volgen. Deze magistraten worden ondersteund door gespecialiseerde interne netwerken waarbinnen ze ervaringen, problemen en *best practices* kunnen uitwisselen en bespreken. De opsporings- en vervolgingsactiviteiten van justitie moeten daarbij worden gestuurd door een uitgewerkt strafrechtelijk beleid in het cyberdomein.

3.4.4 Een gepast Defensie capaciteit ontwikkelen

Het internet wordt alsmaar meer een doelwit en een middel bij internationale conflicten.

Alle staatshoofden en regeringsleiders van NAVO hebben verklaard dat cyberspace beschouwd moet worden als een nieuw operationeel domein (naast de klassieke land, lucht en maritieme domeinen) waarin militaire en inlichtingen operaties gevoerd kunnen worden.

Tegenstanders gebruiken elke opportuniteit in en doorheen cyberspace om hun informatiepositie te versterken, om onze civiele en militaire systemen te ontregelen en om het vertrouwen te ondermijnen in de informatie welke onze operaties ondersteunen. De verdere uitbouw van de cybercapaciteit binnen ADIV en Defensie is daarom een van dé prioriteiten in de beleidsnota van de minister van Defensie en in het strategisch plan van Defensie. Het moet op termijn ook leiden tot de oprichting van een vijfde component die zich specifiek op de cyberdreiging zal richten. Het objectief is tweeledig: een beter begrip van en een betere bescherming tegen de cyberdreiging, maar ook een beter begrip van de opportuniteiten. De cyberstrategie van Defensie zet deze doelstellingen concreet uiteen. Deze capaciteit zal bovendien een belangrijk duaal karakter hebben in steun van de maatschappij in geval van (hybride) crisissen.

3.4.5 Attributie

Het identificeren en toewijzen van een cyberaanval aan een bepaalde persoon, groep of staat speelt een steeds belangrijkere rol in de wereldpolitiek. De discussie rond de nood en mogelijke internationale coördinatie van de attributie van een cyberaanval staat internationaal hoog op de agenda van onder meer NAVO, EU en VN. Attributie blijft echter een politieke en soevereine beslissing met een grote impact op het buitenlands beleid. Een mogelijke attributie zal daarom via een gecoördineerde nationale procedure grondig geanalyseerd en besloten worden. Hiervoor is capaciteitsopbouw cruciaal.

3.5 Publiek, private en academische samenwerkingen verbeteren

In het voorkomen, reduceren, behandelen en monitoren van cyberdreigingen en –incidenten is samenwerking tussen de betrokken stakeholders, zowel op nationaal als op internationaal niveau, een belangrijke succesfactor.

3.5.1 Coördinatie en samenwerking bevorderen

Elke stakeholder die een rol speelt in de cyberveiligheid van België heeft zijn specifieke verantwoordelijkheden. Het is echter cruciaal om alle initiatieven centraal te coördineren. Het CCB staat als nationale autoriteit in voor de coördinatie tussen de betrokken stakeholders, waaronder publieke diensten maar ook de private en de wetenschappelijke sector.

Cybersecuritykennis en de evolutie van de cyberdreiging wordt via bestaande of nieuwe platformen gedeeld tussen de betrokken veiligheidsdiensten, de publieke overheden, de private en wetenschappelijke sector. Periodieke bijeenkomsten laten experten toe om in direct contact informatie en ervaringen te delen en om onderling te netwerken. De open en structurele dialoog moet het CCB toelaten de meest dringende behoeften beter te begrijpen.

3.5.2 Cyber Security Coalition ondersteunen

De Cyber Security Coalition is een uniek partnerschap waarbij spelers uit de academische wereld, openbare instanties en de private sector de krachten bundelen in de strijd tegen cybercriminaliteit. In 2021 zijn meer dan 100 belangrijke organisaties uit drie sectoren actief lid, en dragen bij aan de missie en doelstellingen van de coalitie.

De coalitie biedt een antwoord op de dringende behoefte aan een sector-overschrijdende samenwerking:
- om kennis en ervaring te delen
- om concrete sectoroverschrijdende initiatieven op te starten, te organiseren en te coördineren
- om te sensibiliseren bij burgers en organisaties
- om de ontwikkeling van expertise te bevorderen
- en om aanbevelingen te doen voor meer efficiënte beleidslijnen en regelgeving

De overheid, en het CCB in het bijzonder, zal de Cyber Security Coalition actief steunen en aan de activiteiten deelnemen.

3.6 Een duidelijk internationaal engagement

De cyberdreiging is mondiaal en kan niet enkel op nationaal niveau worden aangepakt. Internationale samenwerking is een belangrijke pijler van een slagkrachtig nationaal cyberveiligheidsbeleid. Cyberveiligheid behoeft een holistisch perspectief dat de verschillende vectoren van de internationale samenwerking (diplomatiek, militair, economisch, …) hanteert. Het is daarom van belang dat de verschillende betrokken autoriteiten, in nauw overleg en in hun afzonderlijke bevoegdheden nauw samenwerken.

België steunt de wetgevende en diplomatieke rol van de EU, NAVO en andere relevante internationale organisaties in hun bijdrage aan een open, vrije en veilige cyberomgeving en zal hier waar mogelijk actief aan deelnemen. Bijzondere aandacht gaat naar het agentschap voor cybersecurity in Europa, ENISA. Sinds de oprichting in 2004, ontwikkelt ENISA een algemene cultuur en bewustwording voor netwerk- en informatieveiligheid in de Unie. Het CCB zal België blijven vertegenwoordigen in de verschillende organen en platformen van ENISA.

Ook bilaterale samenwerkingen tussen alle betrokken autoriteiten in België en hun buitenlandse evenknieën optimaliseren de internationale samenwerking en kunnen de vertrouwensbanden versterken.

4. Verantwoordelijkheden

Samenwerking en het opnemen van een gedeelde verantwoordelijkheid zijn kritische succesfactoren voor het uitwerken van een effectieve cyberveiligheid. Het verdedigen van de digitale omgeving in België tegen (opkomende) dreigingen is niet enkel de verantwoordelijkheid van de overheid. Ook de andere stakeholders kunnen een relevante bijdrage leveren aan de verschillende doelstellingen en gerelateerde actieplannen, waaronder de burgers, bedrijven en Organisatie van Vitaal Belang.

Net zoals in de reële wereld is het de verantwoordelijkheid van iedere eigenaar van een ICT-systeem om zijn systeem correct te beveiligen en het verantwoord te beheren en te gebruiken. Elke burger moet zich informeren en bewust zijn van de voornaamste risico's bij het gebruik van ICT en van het internet en moet de gegeven veiligheidsadviezen in acht nemen. Concreet betekent dit dat elke gebruiker zowel zorg moet dragen voor de technische beveiliging van zijn systemen als die systemen op een verantwoorde wijze moet gebruiken. Bedrijven en publieke instellingen moeten hun omgeving beschermen en begrijpen dat ze verantwoordelijkheden dragen indien zij het slachtoffer zijn van een cyberaanval.

4.1 Het Centrum voor Cybersecurity België (CCB)

Het CCB volgt het Belgisch beleid inzake cybersecurity op, coördineert het en ziet toe op de uitvoering ervan. Vanuit een geïntegreerde en gecentraliseerde aanpak beheert het de verschillende projecten op het vlak van cyberveiligheid en verzekert het de coördinatie tussen de betrokken diensten en overheden, en de publieke overheden en de private of wetenschappelijke sector.

In samenwerking met het Nationaal Crisiscentrum, verzekert het CCB het crisisbeheer bij cyberincidenten. Voor de administraties en publieke instellingen verspreidt het CCB standaarden, richtlijnen en veiligheidsnormen.

Het CCB maakt de bevolking bewust van de voornaamste cyberdreigingen en hoe zich ertegen te beschermen. Specifieke programma's met publieke en private entiteiten moeten de expertise in het cyberveiligheidsdomein vergroten.

Het CCB heeft ook de opdracht om de Belgische vertegenwoordiging in

internationale fora voor cyberveiligheid te coördineren, de internationale verplichtingen op te volgen en het nationale standpunt op dit vlak voor te stellen. Zij doet dit met het oog op een coherent buitenlands optreden in nauw overleg met de FOD Buitenlandse Zaken en Defensie.

Het CCB stelt het Belgische standpunt voor t.o.v. de Europese instellingen, o.a. m.b.t. certificatie en het labelen van producten en diensten.

4.1.1 CERT.BE

Als nationaal CSIRT (*Computer Security Incident Response Team*) heeft het CCB daarnaast een belangrijke detectische en waarschuwende taak. Het *Computer Emergency Response Team* (CERT.be) is, als operationele dienst van het CCB, verantwoordelijk voor het opsporen, het observeren en het analyseren van online veiligheidsproblemen zoals cyberdreigingen, kwetsbaarheden in ICT-systemen of cyberincidenten. CERT.be zal de bevolking, de bedrijven, overheidsdiensten en Organisaties van Vitaal Belang permanent informeren daarover. CERT.be is in die zin de centrale hub voor het uitwisselen van cyberveiligheidsinformatie.

4.2 De Federale Politie

De geïntegreerde politiediensten staan, in samenwerking met haar partners, in voor de bestrijding van de informaticacriminaliteit.

Als eerstelijnspolitie vormt de Lokale Politie het eerste aanspreekpunt voor de burgers, bedrijven en overheidsdiensten. Vanuit deze rol betrekt zij de gespecialiseerde diensten (RCCU/FCCU) wanneer vereist.

Binnen de Federale Gerechtelijke Politie staan de Regionale Computer Crime Units (RCCU's) en de Federale Computer Crime Unit (FCCU) in voor de gerechtelijke aanpak van ICT-criminaliteit.

De RCCU's staan in voor het leveren van gespecialiseerde bijstand bij onderzoeken in een geïnformatiseerde omgeving - met in hoofdzaak een ondersteunende rol inzake forensische analyse van ICT-materiaal (PC's, smartphones) – voor dossiers inzake allerlei criminaliteitsfenomenen, dit voor zowel de Lokale Politie als de Federale Gerechtelijke Politie van het arrondissement waarvan zij deel uitmaakt. Zij behandelt eveneens op autonome wijze de gerechtelijke aanpak van dossiers informaticacriminaliteit gelinkt aan haar arrondissementele werking. Hierbij is het verzamelen van

digitale sporen van belang met als doel de daders op te sporen en voor het gerecht te brengen.

De FCCU maakt als operationele dienst deel uit van de centrale directie voor de bestrijding van zware en georganiseerde criminaliteit. Naast een forensische ondersteunende analyserol, in hoofdzaak als ondersteuning voor de centrale diensten, staat zij op autonome basis in voor de gerechtelijke aanpak van dossiers informaticacriminaliteit die te maken hebben met aanvallen op de ICT-infrastructuur van kritieke infrastructuren of vitale sectoren. Wanneer het gaat om andere complexe aanvallen die niet gelinkt kunnen worden aan een arrondissement of arrondissement-overschrijdend zijn, vervult de FCCU een coördinerende rol. De FCCU vormt eveneens een nationaal contactpunt in het kader van de internationale aanpak van cybercriminaliteit.

4.3 Het Openbaar Ministerie

Het opsporingsonderzoek in het algemeen, maar ook voor cybercriminaliteit in het bijzonder, wordt in elk gerechtelijk arrondissement gevoerd onder leiding van de bevoegde procureur des Konings. Deze geeft de geïntegreerde politiediensten en desgevallend andere opsporingsdiensten de nodige opdrachten teneinde de sporen te verzamelen en de waarheid aan het licht te brengen. Op het einde van de rit is het eveneens de procureur des Konings die de cybermisdrijven al dan niet voor de rechtbank zal brengen. De procureur des Konings heeft hierbij doorgaans één of meerdere referentiemagistraten cybercrime die zich bij voorrang gelasten met het onderzoek naar cybermisdrijven.

De federale procureur maakt deel uit van het Openbaar Ministerie en is in het bijzonder gelast met de uitoefening van de strafvordering voor welbepaalde misdrijven (o.a. terrorisme, schendingen humanitair recht, etc.). Het federaal parket kan ook gevraagd worden om de coördinatie van strafonderzoeken die meerdere rechtsgebieden beslaan of een internationale dimensie hebben, voor zich te nemen in overleg met de procureur des Konings. Het federaal parket heeft een Cyberunit met daarin federale magistraten die zich in het bijzonder bezig houden met het onderzoek naar cybermisdrijven. Hierbij kan gedacht worden aan complexe cybermisdrijven met een grote internationale dimensie, gepleegd door georganiseerde criminele netwerken middels geavanceerde technieken en aan dreigingen tegen Nationale Kritieke ICT-Infrastructuren. Ten slotte

is het federaal parket ook gelast met de bevordering van de internationale operationele samenwerking en vertegenwoordigt zij het Openbaar Ministerie bij EUROJUST en het European Judicial Cybercrime Network. Indien een cybermisdrijf niet meteen gelokaliseerd kan worden in een welbepaald arrondissement, kan het federaal parket de eerste en meest dringende onderzoeken gelasten.

Het Cybernoodplan betrekt het Openbaar Ministerie bij de beheersing van cyberincidenten en –crisissen.

Het strafrechtelijk beleid en de goede algemene en gecoördineerde werking van het openbaar ministerie is de verantwoordelijkheid van het College van procureurs-generaal. Deze kan hierbij onderrichtingen geven, die dwingend zijn voor alle leden van het Openbaar Ministerie. Zij laten zich bijstaan door nationale expertisenetwerken (REN), samengesteld door een veelheid aan relevante partners. Inzake cybercriminaliteit is dit het REN CYBERCRIME, waarvan de hoofdcoördinatie door het parketgeneraal te Antwerpen wordt waargenomen. Inzake beleidsvragen is het REN CYBERCRIME in die zin het aangewezen contactpunt.

4.4 Defensie

Defensie ontwikkelt een cyberstrategie, beleidsplan en de nodige capaciteiten om militaire en inlichtingen operaties te kunnen ondersteunen vanuit, alsook uit te voeren in, het cyberdomein. Deze investeringen zullen België in staat stellen om op lange termijn te beschikken over technische/technologische capaciteiten die toelaten om noodzakelijke infrastructuur te beschermen tegen cyberaanvallen, en indien nodig een tegenaanval uit te voeren.

Defensie zal over een hoogtechnologische cybercapaciteit beschikken om in militaire operaties haar vrijheid van handelen in en via cyberspace te bewaren.

Bijkomend ondersteunt Defensie het nationaal cybersecurity beleid door:

- De verbintenissen die vastgelegd zijn in het nationale cybernoodplan loyaal in te vullen;

- Haar capaciteiten in te schakelen waar nodig als technisch expert ter ondersteuning van specifieke juridische dossiers of als technische ondersteuning van specifieke dossiers van het CERT.be;

- Het aanbieden van een malware analyse senior-expertise level aan nationale stakeholders;

- Het integreren van relevante *cyberthreat intelligence* in het nationale *cyberthreat intelligence platform*;

- Het opvolgen van actoren met intenties en mogelijkheden voor cyberaanvallen op nationale vitale belangen en structuren;

- Het coördineren, waar opportuun in samenspraak met Buitenlandse Zaken en het CCB, van de Belgische deelname aan internationale cybersecurity oefeningen;

- Het beschikbaar stellen van de infrastructuur van het mil.cert als back-up-site voor het Incident Management van het CERT.be, in crisissituaties waarbij de nationale infrastructuur onbeschikbaar is;

- Tijdens nationale crisissituaties haar intrusieve en offensieve capaciteiten in te zetten om met een eigen cyberaanval te reageren om de aanval te neutraliseren en er de daders van te identificeren.

4.5 Het Nationaal Crisiscentrum (NCCN)

Het NCCN verzekert samen met het CCB de organisatie en de coördinatie van het Cybernoodplan op nationaal niveau. Het NCCN en het CCB staan samen in voor het crisisbeheer.

Het beheer van de directe en indirecte maatschappelijke gevolgen van een crisis blijft het prerogatief van het NCCN, de sectorale overheden en de leden van de betrokken overheid. Het NCCN organiseert en stuurt

de communicatie in geval van een nationale cybercrisis (zie Nationaal Cybernoodplan).

De permanentiedienst van het NCCN verzekert 24 uur per dag en 7 dagen per week de bereikbaarheid van CERT.be, dat instaat voor de eerstelijnsondersteuning bij nationale incidenten en crisissen.

Het NCCN verleent juridische en organisatorische steun aan sectorale autoriteiten voor de identificatie van kritieke infrastructuren en aanbieders van essentiële diensten. Ze levert ook een bijdrage aan de uitvoering van cyberrisicoanalyses die de werking van Organisaties van Vitaal Belang of bepaalde evenementen kunnen verstoren (zie hoofdstuk 3).

Het NCCN beheert de lijst van Organisaties van Vitaal Belang en staat in voor de coördinatie van de opvolging en de aanpassing van de betreffende regelgeving.

Ten slotte analyseert het NCCN op continue wijze de belangrijkste nationale risico's (waaronder cyber risico's) en voert het ad-hoc risicoanalyses uit bij speciale aangelegenheden die een verhoogd risico inhouden, in samenwerking met alle betrokken partners.

4.6 De Veiligheid van de Staat (VSSE)

De Dienst voor de Veiligheid van de Staat (VSSE) heeft als opdracht het inwinnen, analyseren en verwerken van inlichtingen over activiteiten die de inwendige veiligheid van de Staat, de uitwendige veiligheid van de Staat of het wetenschappelijk en economische potentieel van het land bedreigen of zouden kunnen bedreigen.

In het kader van die opdracht zal de VSSE de gepaste contacten onderhouden met en inlichtingen verzamelen van buitenlandse nevendiensten en de ontvangen informatie zoveel mogelijk delen met CERT.be en met andere relevante partners.

4.7 De Federale Overheidsdienst Buitenlandse Zaken

Rol van de Federale Overheidsdienst Buitenlandse Zaken in het kader van cyberveiligheid kan omschreven worden als:

- Internationale *Single Point of Contact* op diplomatiek niveau, zowel bilateraal als binnen relevante multilaterale organisaties (o.a. EU, NAVO, OVSE), in het bijzonder op momenten van crisis.

- In samenspraak met de relevante Belgische autoriteiten de vertegenwoordiging van België in internationale onderhandelingen en dialogen bepalen.

- Het informeren van de relevante Belgische autoriteiten over pertinente internationale evoluties.

- In overeenstemming met alle betrokken Belgische autoriteiten een standpunt in internationale dossiers bepalen.

- De al dan niet gecoördineerde internationale attributie van kwaadwillige cyberactiviteiten.

- Ze biedt haar ervaring aan de bevoegde autoriteiten (CCB), alsook de omgeving van een internationaal netwerk voor het observeren en het analyseren van online veiligheidsproblemen, zoals cyberdreigingen, kwetsbaarheden in ICT systemen, of cyberincidenten.

4.8 De Nationale Veiligheidsoverheid (NVO)

De Nationale Veiligheidsoverheid is bij uitstek actief in het domein van informatiebeveiliging, zij het dan de meest gevoelige gegevens of "geclassificeerde" informatie.

De Cybersecurity Strategie in dit document richt zicht tot vier verschillende doelgroepen. Drie van deze doelgroepen behoren ook tot de doelgroepen waar de Nationale Veiligheidsoverheid zich op richt:

· Bedrijven
· Overheidsdiensten
· Organisaties van Vitaal Belang

Voor de bedrijven en overheidsdiensten ontwikkelt de NVO een aantal producten die toelaten om in een cyberomgeving de geclassificeerde informatie beter te beschermen. Het gebruik van de door de NVO ontwikkelde data encryptie kan de beveiliging van geclassificeerde informatie in het cyberdomein naar een hoger niveau tillen, in zowel de private als publieke sfeer. Zo zal het nationaal geclassificeerd netwerk, waarvan de ontplooiing en de organisatie van het gebruik nog moet worden uitgewerkt, de veilige informatie-uitwisseling faciliteren tussen overheidsdiensten met bijgevolg een beperking van de cyberrisco's.

Voor bepaalde vitale organisaties kan de NVO ook veiligheidsverificaties (veiligheidsadviezen of screening van gevoelige beroepen) uitvoeren. Daarvoor verplicht ze deze organisaties eerst een risicoanalyse, dreigingsanalyse en impactanalyse te doorlopen en de beveiligingsmaatregelen van haar informaticasystemen in kaart te brengen. Dit proces sensibiliseert niet alleen, maar versterkt tevens de door deze organisaties genomen maatregelen in het cyberdomein.

4.9 Het Orgaan voor de Coördinatie en de Analyse van de Dreiging (OCAD)

Het Orgaan voor de Coördinatie en de Analyse van de Dreiging is onder meer verantwoordelijk voor het evalueren van de dreiging inzake terrorisme en extremisme. In geval van cyberdreigingen of -incidenten die (potentieel) in verband staan met terroristische of extremistische groeperingen of ideologisch of religieus geïnspireerde hacktivisten, kan het OCAD in samenwerking met haar partnerdiensten een dreigingsanalyse uitvoeren voor het Nationaal Crisiscentrum.

4.10 Sectorale overheden

De NIS-Wet van 7 april 2019 (Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid) en het uitvoerende Koninklijk Besluit van 12 Juli 2019 specifiëren hoe in België sectorale overheden elk verantwoordelijk zijn voor de identificatie, normering en inspecties van Aanbieders van Essentiële Diensten in hun sector. Het CCB en Nationaal Crisiscentrum hebben hierin een belangrijke adviserende rol. De NIS-wet identificeert zes verschillende sectoren van Aanbieders van Essentiële Diensten: Energie,

Transport, Financiën, digitale infrastructuur, gezondheidszorg en drinkbaar water, met daarnaast ook digitale diensten (zoals Cloudcomputerdiensten, online zoekmachines en online marktplaatsen).

4.11 Het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT)

Het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT) waakt over de veiligheid van de elektronische communicatienetwerken en -diensten van de telecomoperatoren. Zo controleert het BIPT de naleving door de operatoren van zowel de wetgeving (bv. de risicoanalyses en bijhorende veiligheidsmaatregelen) als van zijn beslissingen, behandelt het de meldingen van beveiligingsincidenten (inclusief incidenten die een inbreuk op persoonsgegevens uitmaken, samen met de GBA) en beschikt het over verschillende bevoegdheden om zijn werk te doen (inclusief het geven van bindende instructies aan een operator). Het beschikt ook over een Crisis Response Team in geval van voornoemde incidenten.

BIPT is ook de sectorale overheid en inspectiedienst voor de sector digitale infrastructuren (Internet Exchange Points, leveranciers van DNS-diensten en registers van topleveldomeinnamen) in het kader van de NIS-wet en voor de sectoren elektronische communicatie en digitale infrastructuren in het kader van de wet "kritieke infrastructuren".

Het BIPT is eveneens belast met het toezicht op de toepassing van de wetsbepalingen die de radioapparatuurrichtlijn [RED (2014/53/EU)] omzetten, betreffende producten die een radiofunctionaliteit bevatten.

4.12 Federale Overheidsdienst Economie

De Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie heeft als opdracht de voorwaarden te scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België. Gezien de toenemende digitalisering van onze maatschappij en onze bedrijven, is de FOD Economie betrokken in verschillende domeinen van cyberveiligheid.

Ze is de betrokken administratie voor de identificatie, normering en toezicht op de sectoren energie en digitaledienstverleners onder de NIS-wet.

Slachtoffers van verschillende types van cyberoplichting kunnen cyberbedrog melden bij Meldpunt, een dienst van de FOD Economie, dewelke relevante data rond deze meldingen deelt met het CCB en slachtoffers van cybercrime doorverwijst naar de Politie.

Gegeven het belang van KMO's voor de Belgische economie zal de FOD Economie nauwer samenwerken met het CCB in het verhogen van de cyberveiligheid van deze groep bedrijven.

4.13 Governancekader en overlegplatformen

Naast de verschillende eigen verantwoordelijkheden is samenwerking tussen de betrokken stakeholders een belangrijke succesfactor in het voorkomen, het reduceren, het behandelen en het monitoren van cyberdreigingen en –incidenten. Cybersecuritykennis en de evolutie van de cyberdreiging wordt via bestaande of nieuwe platformen gedeeld tussen de betrokken veiligheidsdiensten, de publieke overheden, de private en wetenschappelijke sector. Periodieke bijeenkomsten laten experten toe om in direct contact, informatie en ervaringen te delen en om onderling te netwerken.

In Platform 4 Cyber van het coördinatiecomité voor inlichting en veiligheid (CCIV) bespreken de inlichtingen- en veiligheidsdiensten het algemene cyberveiligheidsbeleid.

Overleg tussen de toezichthoudende overheden van Organisaties van Vitaal Belang gebeurt via het Cybersecurity Sectoral Authority Platform (CySSAP).

Het Expertise Netwerk (REN) Cybercrime brengt experten uit de overheidsdiensten in het gebied van cybercriminaliteit bijeen voor periodiek overleg. De coördinatie hiervan wordt waargenomen door het parketgeneraal te Antwerpen.

In het CSI/DPO-platform (les Conseillers en Sécurité de l'Information/ Data Protection Officers) komen de veiligheidsadviseurs en databeschermingsverantwoordelijken van elke overheidsdienst bijeen. Een specifieke vergadering rond cyberaspecten vindt hierover elk kwartaal plaats in het kader van het Quarterly Cyber Threat Report van CCB/CERT.

De SIT (Synergy IT) is het platform voor kennisdeling en overleg van ICT-verantwoordelijken van alle federale overheidsdiensten (Federale

Overheidsdiensten, Openbare Instellingen van Sociale Zekerheid en Instellingen van Openbaar Nut). De SIT komt op maandelijkse basis samen, met als doel om gezamenlijke IT-initiatieven, zowel overheidsopdrachten als projecten, te initiëren en op te volgen, alsook om technische input te geven voor G-Cloud initiatieven.

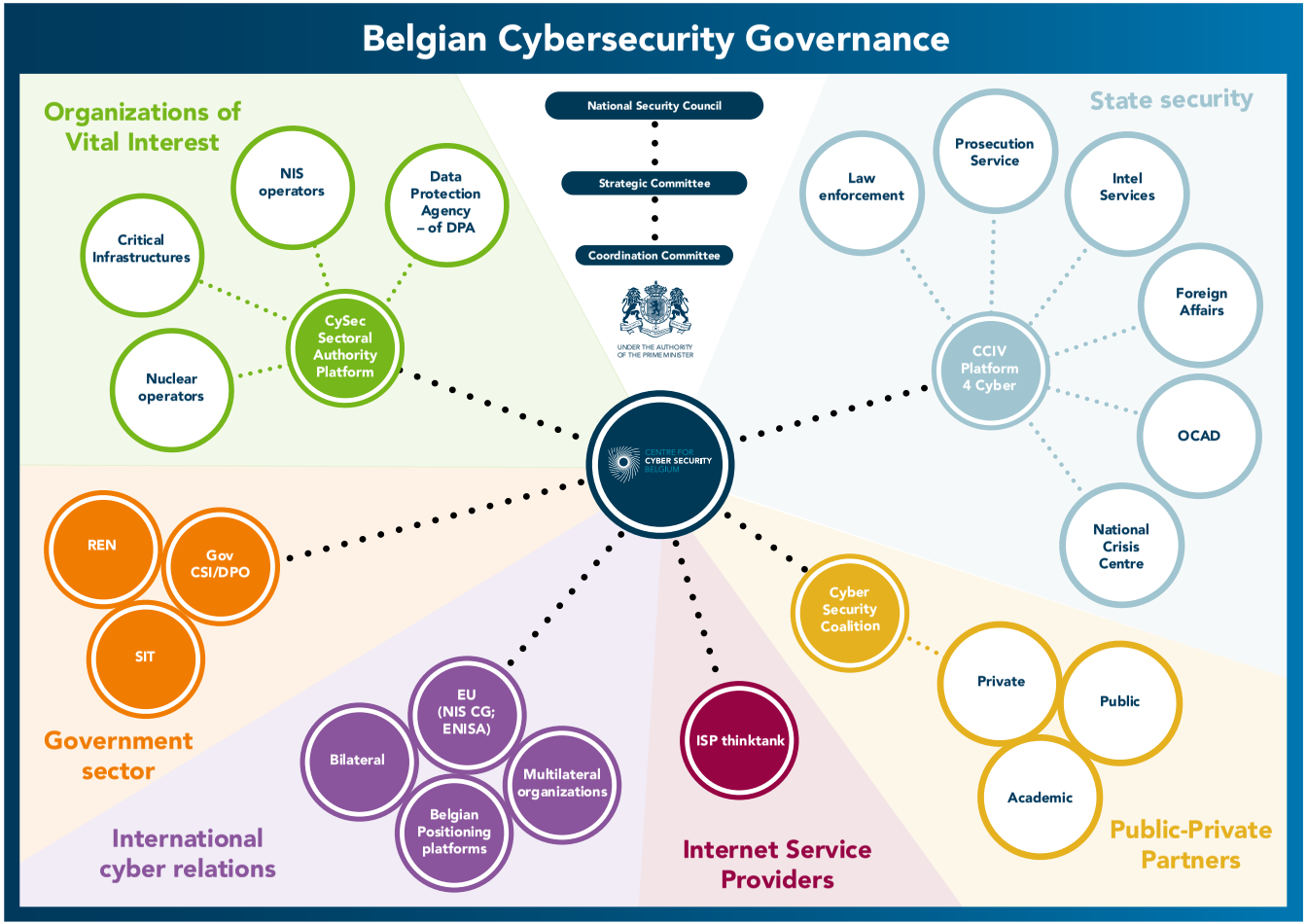
Het uitwerken van formele Belgische standpunten in internationale discussies verloopt via de geijkte kanalen van de FOD Buitenlandse Zaken.

De Interministeriële Economische Commissie (IEC) is een onafhankelijk, flexibel, technisch-administratief coördinatiemechanisme bij de FOD Economie, KMO, Middenstand en Energie dat kan bijstaan om de administratieve standpunten van de federale en gefedereerde autoriteiten in nationale, Europese en Internationale dossiers te bepalen en op elkaar af te stemmen.

In de ISP denktank overlegt het CCB regelmatig met de grootste Internet Service Providers in België omtrent concrete maatregelen en projecten die de cyberveiligheid voor Belgische burgers en bedrijven kunnen verhogen.

De kwartaalrapporteringen van cyberdreigingen, georganiseerd door het CCB en CERT.be, brengen verschillende van deze overlegplatformen samen en informeren alle deelnemers ende Organisaties van Vitaal Belang over de actieve dreigingen.

De Cyber Security Coalition Belgium brengt domeinexperten uit de private, academische en publieke sectoren regelmatig bij elkaar. Dit gebeurt tijdens experience sharing events en in focus groepen waarin best practices, ervaringen of initiatieven besproken worden, rond diverse thematieken (zoals cloud security, NIS, crypto, etc.).


Belgian Cybersecurity Governance
Organizations of Vital Interest
NIS operators
Data Protection Agency – of DPA
Critical Infrastructures
CySec Sectoral Authority Platform
Nuclear operators
National Security Council
Strategic Committee
Coordination Committee
UNDER THE AUTHORITY OF THE PRIME MINISTER
CYBERSECURITY COALITION
State security
Law enforcement
Prosecution Service
Intel Services
Foreign Affairs
CCIV Platform 4 Cyber
OCAD
National Crisis Centre
REN
Gov CSI/DPO
SIT
Government sector
Bilateral
EU (NIS CG; ENISA)
Multilateral organizations
Belgian Positioning platforms
International cyber relations
ISP thinktank
Internet Service Providers
Cyber Security Coalition
Private
Public
Academic
Public-Private Partners

5. Middelen

Om de vooropgestelde visie en de zes strategische doelstellingen van deze ambitieuze strategie uit te voeren, zijn belangrijke, maar essentiële, extra investeringen nodig. Een duidelijk engagement van de Belgische overheid naar deze middelen is zo het elementaire sluitstuk van deze vernieuwde nationale cyberveiligheidsstrategie. Een verhoogde cybercapaciteit is immers cruciaal om onze economie, overheidsdiensten en de Organisaties van Vitaal Belang doeltreffend en haalbaar te wapenen tegen de steeds toenemende cyberdreigingen.

Investeringen in cyberveiligheid hebben daarnaast ook een directe en duidelijke economische impact. Als de overheid erin slaagt het vertrouwen in het "digitaal leven" te inspireren en te garanderen, dan zullen ook bedrijven en burgers geruster investeren in meer digitale toepassingen. Dat zal de productiviteit en de economische groei in ons land stimuleren, en cyberaanvallen zullen nog meer vermeden kunnen worden.

Met dit concrete investeringsengagement volgt België de significante initiatieven in de ons omringende landen. De bedoelde investeringen wekken daarnaast een belangrijk vertrouwen op over de realistische uitvoering van onze doelstellingen, zeker bij onze Europese en internationale partners. Velen onder hen hebben immers net in ons land een belangrijke zetel of vertegenwoordiging.

De missie om van België tegen 2025 één van de minst kwetsbare landen van Europa te maken in het cyberdomein is een collectieve inspanning. Naast het CCB hebben ook andere overheidsdiensten, de inlichtingen- en veiligheidsdiensten, maar ook het bedrijfsleven, de Organisaties van Vitaal Belang zelf, de academische wereld en de burgers elk hun individuele verantwoordelijkheid om de gestelde ambitieuze doelstellingen te bereiken.

De federale overheid heeft hierin een belangrijke verantwoordelijkheid, om de richting aan te geven maar ook om het voorbeeld te stellen. Ze zal daarom een geloofwaardige cybercapaciteit uitbouwen, die gelijke tred kan houden met andere Belgische actoren en aansluiting wil zoeken met de mogelijkheden van onze buurlanden.

Prepress en druk
Centrale drukkerij van de Kamer van Volksvertegenwoordigers

Brussel, mei 2021

Verantwoordelijke uitgever
Centrum voor Cybersecurity België
M. De Bruycker, Directeur
Wetstraat, 16
1000 Brussel

D/2021/14828/001