Cyber Security Strategy

BELGIUM BELGIQUE BELGIE BELGIEN

23-11-2012	Securing Cyberspace

Erkennen van de cyberdreiging
Verbeteren van de veiligheid
Kunnen reageren op incidenten

SAMENVATTING

Onze maatschappij en economie zijn zeer afhankelijk geworden van informatie- en communicatietechnologie die actueel de basis vormt voor de werking van vele bedrijfsprocessen, ook in vitale sectoren. Daarom zijn de beschikbaarheid en een goede, integere werking van deze informaticasystemen cruciaal.

België als kennismaatschappij is door de snelle technologische evolutie zeer kwetsbaar geworden. Economische en politieke spionage in cyberspace vormen een gevaar voor het wetenschappelijke en economisch potentieel van ons land. Maar ook de continuïteit van de maatschappelijke activiteiten in cyberspace komt in het gedrang bij onrechtmatig binnendringen, zich handhaven of buiten werking stellen van ICT-infrastructuur.

De cyberdreiging is reëel. Geld en macht blijven het voornaamste oogmerk van de criminelen. De mogelijkheden om hun objectief te realiseren nemen echter elke dag toe. De vereiste kennis en tools worden toegankelijker met als gevolg dat het aantal cyber security incidenten zorgwekkend toeneemt.

Met een nationale cyber security strategie stelt België drie strategische objectieven voorop om de cyberveiligheid in België te garanderen:

- streven naar een veilige en betrouwbare cyberspace met respect voor de fundamentele rechten en waarden van de moderne samenleving;
- streven naar een optimale beveiliging en bescherming van de kritieke infrastructuren en overheidssystemen tegen de cyberdreiging;
- ontwikkelen van eigen cyber security capaciteiten voor een onafhankelijk veiligheidsbeleid en een gepaste reactie op veiligheidsincidenten.

De aanpak om de drie bovenstaande strategische objectieven te realiseren, vertaalt zich in verschillende actielijnen.

Cyber security moet gecentraliseerd en geïntegreerd worden aangepakt door een centraal orgaan. Dit vereist duidelijke afspraken tussen en een belangrijk engagement van de verschillende nationale partners die zich situeren bij zowel overheid, private sector als academische wereld. Alle aspecten van de veiligheid dienen aan bod te komen in een optimale nationale en internationale samenwerking.

Vertrekkend van de bestaande wetgeving, dient een wettelijk kader gecreëerd te worden met aandacht voor een evenwicht tussen de rechten en vrijheden van de burger en de noodzakelijke tussenkomsten van de overheid.

De cyberdreiging in het algemeen, maar ook deze specifiek gericht tegen de overheidssystemen en kritieke infrastructuren, dient permanent te worden opgevolgd. Veiligheidsincidenten dienen consequent en gecoördineerd te worden behandeld. De capaciteit moet hiertoe worden versterkt.

Standaard veiligheidsnormen en –richtlijnen zullen worden opgesteld om de bescherming van ICT-systemen te verbeteren. Informatie en sensibilisering van zowel burgers, bedrijven, nationale belangrijke infrastructuren als de overheid zijn een must.

Ook bij incidenten van criminele aard of cybercriminaliteit is een gezamenlijke actie van verschillende actoren vereist om op die manier de impact van het incident zo beperkt mogelijk te houden, alsook de daders te kunnen traceren en voor het gerecht te brengen.

Aan de hand van de nodige opleidingen en informatiecampagnes moet de expertise en kennis rond cyber security vergroot worden bij de verschillende actoren die vertoeven in cyberspace. De technologische ontwikkeling dient te worden gestimuleerd om zo veilige toegang te kunnen bieden tot cyberspace.

INHOUD

1 DE CYBERDREIGING

1.1 Onze maatschappij en onze economie zijn afhankelijk van ICT

Onze maatschappij en economie zijn zeer afhankelijk geworden van informatie- en communicatietechnologie (ICT). De afhankelijkheid van ICT neemt toe omdat er voor bedrijfsprocessen vaak **geen wisseloplossingen** meer bestaan **buiten cyberspace**.

Naast de **opslag en administratieve verwerking** van data worden ook steeds meer **industriële processen** gecontroleerd en aangestuurd via ICT. Deze SCADA[1]-systemen worden onder andere gebruikt in vitale sectoren en zijn steeds vaker verbonden met het internet. Ook de opmars van 'the Internet of things' of 'machine-to-machine'[2]-toepassingen in onder andere transport-, luchtvaart- en gezondheidssector vergroot de ICT-afhankelijkheid, alsook de daarmee gepaard gaande kwetsbaarheid.

De **beschikbaarheid** en de **goede, integere werking** van al deze systemen zijn cruciaal. Ze vormen immers de basis voor de werking van vitale sectoren zoals energievoorziening, watervoorziening, vervoer, de financiële sector, gezondheidszorg en de overheid. Indien de ICT-infrastructuur van deze sectoren of delen ervan worden verstoord of buiten werking gesteld, hetzij moedwillig, hetzij onopzettelijk, kan dit enorme schade veroorzaken en zelfs levensbedreigend zijn.

Een veilig en beschikbaar **internet is de ruggengraat van onze economie**. Economische digitale spionage is een directe bedreiging voor de concurrentiekracht van onze bedrijven. Onze economie heeft behoefte aan betrouwbare communicatiesystemen om performant te kunnen zijn.

1.2 Ons land is kwetsbaar

België is steeds meer een **kennismaatschappij** waar het kapitaal net wordt gevormd door de informatie (strategische beleidsinformatie, industriële procedés, patenten en brevetten).

In de voorbije jaren hebben diverse incidenten aangetoond dat gerichte besmetting van bedrijven en organisaties met kwaadaardige software de basis vormt van economische en politieke spionage waardoor het **wetenschappelijke en economisch potentieel** van ons land in het gedrang komt.

Diverse **factoren** bepalen de kwetsbaarheid van België:

(1) Vooreerst is er de **bereikbaarheid** van alle belangrijke ICT-systemen over internet met grote bandbreedte. Dit economisch belangrijk voordeel vormt tevens een kwetsbaarheid omdat deze grote bandbreedte ook kan worden aangewend om andere servers te bestoken en buiten werking te stellen tijdens zogenoemde DDoS-aanvallen[3].

---

[1] SCADA of Supervisory Control And Data Acquisition is het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines of toestellen in industriële procescontrolesystemen. Deze SCADA-systemen zijn vaak direct of indirect (dmv bijvoorbeeld USB-sticks) verbonden met het internet.

[2] 'The Internet of things' of 'machine-to-machine' (m2m) is het gebruik van sensoren en aanstuurmodules om apparatuur (vb. smartmeters, huishoud-elektro, containers, vrachtwagens, medische toezichtapparatuur) via draadloze datacommunicatie te controleren en eventueel bij te sturen.

[3] DDoS of Distributed Denial of Service is de benaming voor een type aanval waarbij een bepaalde dienst onbereikbaar wordt voor de gebruikelijke afnemers van de dienst. Het is een aanvalstechniek, waarbij de normale werking van het aangevallen systeem ernstig wordt verstoord door een groot aantal aanvragen.

(2) Organisaties wenden voor hun informatiesystemen in de meeste gevallen **standaard commerciële technologie** aan. Voortdurend worden er van deze technologieën nieuwe kwetsbaarheden gevonden en gepubliceerd. Cybercriminelen spelen hierop sneller in dan de meeste systeembeheerders.
(3) De concentratie van data en toepassingen van diverse bedrijven en organisaties in gemeenschappelijke datacenters in de '**Cloud**' maakt deze datacenters en de netwerken tot de achillespezen van onze cybermaatschappij. Bovendien bevinden deze infrastructuren zich vaak niet meer op Belgisch grondgebied waardoor het niet steeds meer mogelijk is om als Belgische overheid de veiligheid van Belgische bedrijven en organisaties te garanderen.
(4) Door de grote databanken met persoonsgegevens komt ook de **privacy** van de burgers in het gedrang.
(5) Vaak ontbreekt het bedrijven, overheden en organisaties nog aan adequate **beveiligings- en detectiemaatregelen** waardoor niet gepast kan worden gereageerd op incidenten die hun infrastructuur treffen.
(6) Ten slotte is het zo dat bestaande internationale allianties ter bescherming van de veiligheid van het land niet noodzakelijk gelden of toepasbaar zijn in cyberspace. De focus in deze cyber security strategie zal dan in de eerste plaats ook liggen op het **nationale aspect**.

Door deze kwetsbaarheden is er dus enerzijds gevaar voor onrechtmatig binnendringen en gebruiken van ICT-infrastructuur, anderzijds voor buiten werking stellen van deze infrastructuur. Hiermee komt naast het wetenschappelijke en economisch potentieel ook de **bescherming van essentiële en vitale belangen** in het gedrang.

1.3 De cyberdreiging is reëel

De **intenties** van criminelen zijn **onveranderd**: rijk worden en hun economische, wetenschappelijke, politieke of militaire macht uitbreiden. De **mogelijkheden** om dit te realiseren zijn echter sterk **toegenomen**. De internetrevolutie faciliteert met beperkte middelen spionage, sabotage, subversie, terrorisme, sturing en bevelvoering, propaganda en militaire cyberoperaties.

Sinds de lente 2012 worden in België duizenden PC's, voornamelijk van particulieren, geblokkeerd door een kwaadaardige 'ransomware virus' waarbij de slachtoffers wordt gevraagd te betalen om hun PC te deblokkeren.

Naast particulieren worden echter ook bedrijven afgeperst. *Zo werd bijvoorbeeld een Belgische bankonderneming in mei 2012 het slachtoffer van cybercriminelen. Als de bank niet met een groot bedrag losgeld over de brug kwam, zouden de gegevens van duizenden klanten die door hacking werden bekomen, op het internet te grabbel worden gegooid.*

In het cyberdomein geldt dat het eenvoudiger, goedkoper en sneller is om binnen te dringen of aan te vallen dan om de systemen daartegen te beschermen.

De **kennis en de tools** om cyberaanvallen uit te voeren zijn algemeen **toegankelijk** op internet. De technologie maakt het bovendien mogelijk dat tegenstanders op een beveiligde manier kunnen communiceren en hierbij hun identiteit kunnen verbergen zodat toezicht door enige overheid moeilijk of zelfs onmogelijk is geworden.

De snelle technologische ontwikkeling maakt dat de **beveiliging** van veel systemen **niet up-to-date** is waardoor deze systemen kwetsbaar zijn voor overname door criminelen.

In hun streven naar puur geldgewin hebben criminele organisaties in het voorbije decennium van de bovenstaande factoren gebruik gemaakt om netwerken van gehackte servers en werkposten op te zetten. Vaak hanteren ze hiervoor kwaadaardige software die ze, zonder medeweten van de gebruiker, als Trojaanse paarden in de systemen binnenbrengen waarna de cybercrimineel de controle neemt. De opgebouwde

netwerken worden ***botnets*** genoemd en worden ingezet voor tal van illegale activiteiten: het verspreiden van spam en kwaadaardige software, het bespioneren van bedrijven en particulieren, het uitvoeren van frauduleuze financiële transacties, het afpersen van bedrijven na sabotage van servers en werkposten en het buiten werking stellen van systemen door ze massaal met data te bestoken (DDoS-aanval).

Sinds 2007 werden in ons land verschillende golven van aanvallen op het online bankieren vastgesteld. In de recentste gevallen in 2012 wordt zowel gebruik gemaakt van Trojaanse paarden en botnets als van phishing-websites en social engineering waarbij de hacker telefonisch onder allerlei voorwendsels het slachtoffer ertoe kan bewegen om onwetend medewerking te geven bij de hacking en de illegale geldtransfers.

De kracht van botnets en Trojaanse paarden is niet ontsnapt aan de aandacht van andere groepen in de maatschappij waardoor **nieuwe drijfveren** de laatste jaren aan de basis liggen van nieuwe dreigingen.

Ten eerste is er het **hacktivisme door de massa**. Dit hacktivisme bestaat uit het plegen van politiek of ideologisch geïnspireerde cybercriminaliteit waarbij regelmatig 'geheime informatie' openbaar wordt gemaakt. De acties treffen zowel de overheid als commerciële bedrijven en monden vaak uit in aanvallen en tegenaanvallen. De aansturing van acties gebeurt via sociale media waardoor er weinig of geen tijd is voor de overheden om op incidenten te reageren, laat staan om ze te voorkomen. De hacktivisten zijn over het algemeen weinig gestructureerd maar krijgen door het hergebruik van 'Anonymous' als merknaam grote media-aandacht.

Een mondiaal bedrijf in de staalindustrie werd begin 2012 het eerste belangrijke slachtoffer van de hackerbeweging 'Anonymous Belgium'. Sindsdien zijn er steeds meer cybercriminelen die onder dezelfde vlag feiten plegen en daarbij zowel overheid als industrie aanvallen.

Ten tweede heeft men georganiseerde groepen en staten die zich schuldig maken aan **cyberspionage** vanuit economische en politieke motieven. Hun bedoeling is om kennis te nemen van strategieën, patenten, voorraden, e.d. zowel bij grote bedrijven (olie- en energiemaatschappijen, financiële instellingen) als bij diverse overheidsdepartementen in alle landen. Vaak blijft deze spionage maanden of zelfs jaren onopgemerkt en is onduidelijk welke informatie in handen van de tegenstander is gekomen.

De in België vastgestelde veiligheidsincidenten verschillen aanzienlijk in omvang en in mate van complexiteit. Zo kunnen bepaalde incidenten op het departement Buitenlandse Zaken zeker worden gekwalificeerd als cyberaanvallen.[4]

Een derde ontwikkeling is het destabiliseren of stilleggen van kritieke en andere essentiële infrastructuren waardoor levensbedreigende situaties kunnen ontstaan. Specifieke malware laat toe om de besturing van bepaalde industriële faciliteiten over te nemen of te saboteren. Deze vorm van **cyberwarfare** is duidelijk staatsgestuurd.

Het hardnekkig Sality.gen computervirus legde in 2012 zowel delen van de centrale administratie als van de controle- en ontvangstkantoren van de FOD Financiën anderhalve week lam. De oorsprong van de besmetting of de doelstellingen ervan blijven onduidelijk.

In april 2009 slaagden hackers erin om binnen te dringen in het elektriciteitsnet van de Verenigde Staten waardoor ze het netwerk in kaart konden brengen en verstoren. In juni 2010 saboteerde het Stuxnet virus de centrifuges van de Iraanse kerncentrales waardoor hun nucleaire programma 2 jaar vertraging opliep. In mei 2012 werd het superspionagevirus Flame ontdekt. Flame infecteerde meer dan 1000 computers in het Midden-

[4] Antwoord op de schriftelijke vraag nr. 5-4302 van Karl Vanlouwe d.d. 23 december 2011 aan de vice-eersteminister en minister van Buitenlandse Zaken, Buitenlandse Handel en Europese Zaken, 'Cyberaanvallen en cybercrime – Cyberdefensie – EU – NAVO – Specifieke situatie Federale Overheidsdienst Buitenlandse Zaken'.

Oosten en was o.a. in staat om paswoorden te stelen, pc's af te luisteren via de microfoon en Skype- gesprekken op te nemen.

Er zijn aanwijzingen dat buitenlandse hackergroepen, in ruil voor sponsoring, bescherming of tolerantie hun capaciteiten en hun botnets ten dienste stellen van overheden en militaire entiteiten. Bovendien kan de specialisatie en de capaciteit van cybercriminelen gemakkelijk worden ingehuurd via de 'ondergrondse economie'. Men dient rekening te houden met de dreiging dat **terroristen** zich in de toekomst ook van deze middelen en technieken zullen bedienen om hun acties te voeren. Tot op heden is echt cyberterrorisme met gevaar voor mensenlevens uitgebleven.

2 STRATEGISCHE OBJECTIEVEN

België zal streven naar een veilige en betrouwbare cyberspace met respect voor de fundamentele rechten en waarden van de moderne samenleving.

Een **veilige en betrouwbare cyberspace** garandeert de basisprincipes van informatiebeveiliging met name de beschikbaarheid, integriteit, vertrouwelijkheid en onweerlegbaarheid van gegevens en de systemen die gegevens opslaan en/of verwerken.

Het beschermen van onze maatschappij en haar burgers tegen misbruik, ongewenste inhoud en andere dreigingen moet gebeuren met aandacht voor het **evenwicht** tussen het belang van de (nationale) veiligheid en het belang van de kernwaarden van onze moderne samenleving, zoals privacy, tolerantie, vrijheid van meningsuiting, het recht op een open informatievergaring en respect voor anderen.

Dit streven naar meer cyber security is **essentieel** om de kwetsbaarheid van België te verminderen en tegemoet te komen aan de wezenlijke noden van een samenleving en een economie die diep geworteld is in cyberspace.

Aan de bevolking en de bedrijven geeft de overheid **veiligheidsadviezen en tips** hoe de bescherming van hun computers en netwerken te verbeteren en hoe te reageren bij veiligheidsproblemen. Op die manier kunnen burgers en bedrijven blijven genieten van de voordelen en opportuniteiten die een open en veilig internet en een betrouwbare cyberspace te bieden hebben.

België zal streven naar een optimale beveiliging en bescherming van kritieke infrastructuren en overheidssystemen tegen de cyberdreiging.

De kritieke infrastructuren leveren de maatschappij waarden en diensten die zo belangrijk zijn dat verstoring of onderbreking van hun normale werking maximaal moeten worden vermeden.

Door de recente opkomst en constante toename van de cyberdreiging is het doel om de veiligheid van de informaticasystemen van deze kritieke infrastructuren, in overeenstemming met de specifieke dreiging, zo optimaal als mogelijk te verzekeren.

Daarnaast dienen **ICT-systemen van de overheid** voldoende te worden beschermd en gecontroleerd.

België wil eigen cyber security capaciteiten ontwikkelen.

Met eigen cyber security **capaciteiten** kan een onafhankelijk veiligheidsbeleid worden gevoerd en worden gereageerd op veiligheidsincidenten.

De internationale erkenning van een cyberaanval als een gewapende aanval is niet evident waardoor er niet zomaar op externe steun kan worden gerekend. De rol van internationale organisaties voor veiligheid blijft zeer beperkt en de allianties voor cyber security moeten opnieuw worden gedefinieerd. België wil zijn eigen capaciteiten voor cyber security voldoende uitbouwen om ook **internationaal belangrijke samenwerkingen** te kunnen realiseren.

Een respectabel niveau aan cyber security expertise en middelen zal internationale samenwerking bevorderen. België wil de ontwikkeling van nieuwe technologieën in het domein van de cyber security ondersteunen en zo de nationale **academische initiatieven** en de **economische welvaart** stimuleren.

3 AANPAK EN ACTIEDOMEINEN

Om de drie bovenstaande strategische objectieven te realiseren, tekent België een aantal concrete actielijnen uit.

3.1 Cyber security gecentraliseerd en geïntegreerd aanpakken

Werken aan veiligheid in cyberspace betekent nationaal en internationaal zeer goed samenwerken.

Het vergt van **alle partijen** (overheid, bedrijven, ICT-dienstenleveranciers, netwerkoperatoren en het individu) onderling vertrouwen, gestructureerde informatie-uitwisseling en een **belangrijk engagement** waarbij duidelijke afspraken nodig zijn over de rol van alle belanghebbenden en over de manier van samenwerken met elkaar.

Het is inderdaad maar als alle aspecten van de veiligheid aan bod komen in een nationale strategie dat er een kans op slagen is. Het is bovendien noodzakelijk dat de verschillende aspecten op een **geïntegreerde manier** worden benaderd. Elke partij moet in zijn acties rekening houden met de rol en de bevoegdheden van de andere partijen. Door concrete afspraken hierover te maken, wordt gegarandeerd dat elke partij zijn rol effectief kan opnemen.

Heel wat beschermingsmaatregelen zullen maar efficiënt zijn als ze **internationaal** kunnen worden ingepast. Zowel bilaterale samenwerkingen als een actieve deelname aan initiatieven van internationale organisaties zijn onontbeerlijk. In de eerste plaats kan worden samengewerkt binnen de Europese Unie (bvb. aan de Digitale Agenda[5]) of de NAVO, maar er moet ook mondiaal met partners worden afgestemd. Tevens moeten de **verschillende bestuursniveaus in ons staatsbestel** in rekening worden gebracht. Zowel de federale, de regionale als de lokale besturen dienen in de uitwerking van de strategie te worden betrokken.

Meer dan ooit dient deze strategie te worden ontwikkeld in een **nauw publiek-privaat verband**. De te beschermen systemen en de kritieke infrastructuren zijn immers voor een groot deel in handen van private partijen zonder wiens medewerking een effectief veiligheidsbeleid onmogelijk is. Het betrekken van internetoperatoren, netwerkbeheerders, cloud providers en de diverse bedrijfssectoren is dus een conditio sine qua non.

Ook de **academische wereld** dient een belangrijke taak op te nemen, zowel voor het uitvoeren van *research & development* als voor het vormen van bekwame informatici die het cyber security verhaal ook technologisch kunnen uitwerken.

Om de nationale strategie effectief op een integrale en geïntegreerde manier te kunnen uitbouwen en de uitvoering ervan te kunnen opvolgen, is een **centrale aansturing** noodzakelijk. Deze centrale aansturing dient te gebeuren met respect voor de bevoegdheden van elke partij op elk niveau.

---

[5] De Digitale Agenda (Europese Commissie) moet zorgen voor een belangrijke bijdrage tot de economische groei in de EU en voor de verspreiding van de voordelen van het digitale tijdperk over alle groepen van de samenleving.
Er worden zeven prioritaire actiegebieden afgebakend: (1) verwezenlijking van een digitale interne markt, (2) vergroting van de interoperabiliteit, (3) versterking van het vertrouwen in en de beveiliging van het internet, (4) opvoering van de snelheid van de toegang tot het internet, (5) verhoging van de investeringen in onderzoek en ontwikkeling, (6) verbetering van digitale geletterdheid en inclusie, en (7) het gebruik van ICT om maatschappelijke problemen zoals de klimaatverandering en de vergrijzing aan te pakken.

3.2 Creëren van een wettelijk kader

De uitwerking van een nationale strategie voor cyber security dient verankerd te zijn in een helder wettelijk kader dat garant staat voor een **evenwicht** tussen de **rechten en vrijheden** van de burger en noodzakelijke **tussenkomsten van de overheid** om de veiligheid te kunnen garanderen.

De nationale strategie vertrekt vanuit het bestaand nationaal en internationaal wettelijke kader waarin voor elke overheid haar bevoegdheidsdomein, haar verplichtingen en haar mogelijke juridische instrumenten worden vastgelegd. Een **optimale aanwending** van de **reeds beschikbare bevoegdheden** in een geïntegreerde aanpak zijn in eerste instantie voldoende als uitgangspunt.

Voor de **verdere uitbouw** van de nationale strategie zal moeten worden toegezien dat er voor de nieuwe bevoegdheden of verplichtingen ook een wettelijk basis wordt voorzien of dat bestaande bevoegdheden of verplichtingen worden aangepast of uitgebreid.

Nu al is duidelijk dat de **bevoegdheden van politie, justitie en de veiligheidsdiensten** zullen moeten worden aangepast om effectief en efficiënt te kunnen blijven tussenkomen in cyberspace waar de sporen steeds meer wereldwijd in de Cloud verspreid zitten waardoor de territoriale begrenzing van de jurisdictie onder druk komt te staan. De instrumenten die de cyberveiligheid enerzijds beschermen, vormen anderzijds ook de tools die door criminelen worden misbruikt om aan de greep van justitie te ontsnappen. De balans dient ook hier terug in evenwicht te worden gebracht.

3.3 De cyberdreiging permanent opvolgen

Zowel de **algemene cyberdreiging** tegen de fundamentele waarden en belangen van de staat als de **specifieke cyberdreigingen** tegen belangrijke essentiële en vitale systemen, dienen permanent te worden opgevolgd en geanalyseerd. Informatie moet actief worden gedeeld met diensten die instaan voor de bescherming van de betrokken systemen.

ICT-systemen en netwerken van de overheid en van belang voor de werking en de toekomst van de staat, moeten worden bewaakt en pogingen tot indringing of verstoring dienen centraal te worden gemeld en opgevolgd.

Veiligheidsincidenten zullen consequent en gecoördineerd worden behandeld. Uit deze incidenten zullen lessen worden getrokken en zal de nationale strategie en aanpak worden bijgestuurd.

De nationale beschermingsmaatregelen moeten in **evenwicht** zijn met de reële cyberdreiging. Dit vraagt, zowel nationaal als internationaal, een intensieve samenwerking en uitwisseling van informatie.

3.4 De bescherming verbeteren tegen het verstoren of misbruiken van informatiesystemen

Om de bescherming van **ICT-systemen** te verbeteren zullen voor de verschillende soorten systemen **standaard veiligheidsnormen en –richtlijnen** worden opgesteld.

De **overheid** zal eigen computer- en netwerksystemen **evalueren en goedkeuren** voor gebruik in sterk beveiligde netwerken. Voor netwerken waarmee **geclassificeerde en gevoelige informatie** wordt verwerkt, zorgen **veiligheidsaudits** voor de controle op de conformiteit.

Meer specifiek voor de **kritieke infrastructuren** zal er regelmatig een **evaluatie** worden uitgevoerd van het door de uitbaters voorziene **veiligheidsbeleid**. Dit beleid moet zowel de fysieke veiligheid als de cyberveiligheid van deze infrastructuren integreren. De samenwerking tussen de uitbaters onderling en de diverse

verantwoordelijke autoriteiten in dit domein zal eveneens regelmatig worden geëvalueerd. Hiervoor zal waar nodig het bestaande wettelijke kader worden aangepast of aangevuld.

Zowel de burgers, de bedrijven, de nationaal belangrijke infrastructuren als de overheid moeten op een gepaste wijze worden gewaarschuwd over nieuwe kwetsbaarheden, dreigingen en de mogelijke beschermingsmaatregelen. Alle gebruikers van ICT-systemen zullen correct worden **geïnformeerd en gesensibiliseerd**.

De overheid zal samenwerken met de Internet Service Providers om ervoor te zorgen dat hun gebruikers kunnen beschikken over een **basisset van veiligheidsproducten en –services**. Internet Service Providers zullen zorgen en waken over de veiligheid van hun netwerken, systemen, diensten en hun klanten.

3.5 De capaciteit om te reageren op cyberincidenten versterken

Om beter te kunnen reageren op ernstige cyberincidenten zal in eerste instantie een **inventaris** worden gemaakt van de **bestaande capaciteiten** inzake cyber security in de verschillende overheidsdiensten.

Volgens de gekende algemene cyberdreiging zullen de **processen** voor het behandelen van dergelijke veiligheidsincidenten eveneens **verder** worden **uitgewerkt** en de specifieke taken in kaart worden gebracht. Deze processen werden geïnitieerd onder de procedure 'incident handling'.[6]

Uit deze inventaris en het overzicht van de belangrijke taken zal blijken waar er eventuele overlappingen zijn en waar de diensten moeten worden versterkt. Per departement zullen de **gepaste middelen en voldoende technische experten en onderzoekers** worden voorzien om de cyber security taken en verantwoordelijkheden effectief te kunnen uitvoeren en opnemen.

Bij problemen zijn een gecoördineerde aanpak en een goede onderlinge samenwerking, zowel tussen overheidsdiensten als met private actoren, van primordiaal belang. Een **centraal en bevoegd orgaan** zal alle opdrachten van de verschillende verantwoordelijke partijen coördineren. Zo is het bijvoorbeeld belangrijk dat de operatoren specifieke dreigingen of incidenten onmiddellijk melden aan de competente overheid.

3.6 Cybercriminaliteit effectief aanpakken

Indien de beveiligingsmaatregelen niet hebben kunnen voorkomen dat een **incident** zich voordoet, dan is het in de eerste plaats belangrijk dat die incidenten door het slachtoffer worden **gedetecteerd en gerapporteerd** aan bevoegde en bekwame partners.

Hierna is **gezamenlijke actie** vereist om:

- de sporen van het incident veilig te stellen;
- een correcte diagnose van het incident te maken;
- de schadegenererende oorzaak van het incident weg te nemen of te neutraliseren;
- zo snel mogelijk terug te komen naar een veilige werkbare toestand.

Het is de **taak van politie en justitie** om op basis van het beschikbare bewijsmateriaal de daders op te sporen, hun werkwijze en motieven te achterhalen en hen voor het bevoegde gerecht te brengen. De resultaten van hun onderzoek moeten tevens helpen om beter zicht te krijgen op de dreigingen en op de manieren waarop de maatschappij er zich tegen kan verdedigen.

---

[6] Processen beschreven in een document uitgewerkt door een werkgroep van het overlegplatform voor de informatieveiligheid BelNIS.

Om echter effectief de cybercriminelen te bestrijden in de cybermaatschappij zal de gezamenlijke actie ook meer **anticiperend** moeten worden gevoerd tegen organisaties van cybercriminelen en tegen de criminele ICT-infrastructuur die ze voor hun activiteiten opbouwen. In het bijzonder dient de focus gelegd te worden op acties die het ontstaan van botnets kunnen voorkomen of die botnets ontmantelen of hun werking verstoren.

3.7 Bijdragen tot de uitbreiding van cyber security expertise en kennis

Net zoals verkeersveiligheid niet enkel een verantwoordelijkheid is van de overheid, zijn er heel wat **partijen** betrokken bij de beveiliging van cyberspace: de internetgebruikers, de leveranciers van producten en diensten, de gebruikersorganisaties, de autoriteiten, …

Het is bijgevolg essentieel dat alle partijen **gesensibiliseerd** worden voor de risico's en dat ze over de noodzakelijke kennis beschikken om hun rol op te kunnen nemen.

Voor de verschillende betrokken partijen moeten er **kennisprofielen** worden opgesteld. Vanaf het basisonderwijs tot bij de universitaire studies zullen, in samenspraak met de organiserende instanties, de **noodzakelijke vormingen** worden voorzien. Deze vormingen moeten worden ondersteund door regelmatig terugkerende **sensibiliseringscampagnes** volgens doelpubliek aangepast (via de massamedia, internet service providers, vakliteratuur, …).

3.8 Technologische ontwikkeling stimuleren

Alle economische sectoren hebben behoefte aan performante en betrouwbare producten of diensten waarvan de kwaliteit en de veiligheid door goedgekeurde instanties worden gecertificeerd. Ook de ICT-sector wordt, na meerdere decennia, geconfronteerd met deze fundamentele noodzaak aan gecertificeerde producten.

Om toegang te krijgen tot grote 'high tech' projecten (defensie, ruimtevaart, financiële systemen, medische sector, …) zullen de informaticaleveranciers en de controleorganen in meerdere opzichten kwaliteitsverbeteringen moeten doorvoeren: doorgedreven beheersing van de **methodologie** voor het ontwerpen van software en van **standaard** internationale veiligheidscontroles, in plaats stellen van **diensten voor controle en homologatie**, …

De **samenwerking** tussen alle betrokken partijen is essentieel voor het succes van deze evolutie: academische onderzoekscentra, *research & development* centra, controleorganen, homologatieautoriteiten, de administratie wetenschapsbeleid, …

BIJLAGE 1: DEFINITIES

BOTNET

Een botnet is een verzameling van computers, geïnfecteerd met kwaadaardige software, die centraal en op afstand worden aangestuurd, zonder medeweten van de gebruiker. Deze botnets vormen veelal de infrastructuur voor kwaadwillige acties in cyberspace.

CLOUD

Cloud computing is een op internet gebaseerde dienstverlening voor gegevensoverdracht via een netwerk van over heel de wereld verspreide servers die toegankelijk worden gemaakt voor entiteiten die voor deze diensten ingeschreven zijn.

CYBERCRIMINALITEIT

Cybercriminaliteit of cybercrime is een misdrijf waarbij automatisering en geautomatiseerde gegevens worden misbruikt als middel, maar waarbij tevens de informaticasystemen of de erin opgeslagen gegevens het doelwit kunnen zijn.

CYBER SECURITY

Cyber security is de gewenste toestand waarbij de beveiliging van cyberspace in verhouding staat tot de cyberdreiging en de mogelijke gevolgen van cyberaanvallen. Cyber security is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. De gevolgen door misbruik, verstoring of uitval kunnen bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van informatie of schade aan de integriteit van die informatie (onrechtmatig wijzigen, wissen of toevoegen).

CYBERSPACE

Cyberspace is de globale omgeving die ontstaat door de interconnectie van informatie- en communicatiesystemen. Cyberspace is ruimer dan de informaticawereld en omvat eveneens de fysieke en virtuele computernetwerken, computersystemen, digitale media en digitale gegevens.

CYBERWAR(FARE)

Het gebruik van cybercapaciteiten op een voldoende schaal, gedurende een zekere periode en aan een hoge intensiteit, met als doel het bereiken van bepaalde objectieven of effecten in of door cyberspace, waarbij deze acties als een bedreiging van de nationale belangen van het geviseerde land wordt ervaren.

DDOS-AANVAL

Distributed Denial of Service is de benaming voor een type aanval waarbij een bepaalde dienst onbereikbaar wordt voor de gebruikelijke afnemers van de dienst. Het is een aanvalstechniek, waarbij de normale werking van het aangevallen systeem ernstig wordt verstoord door een groot aantal aanvragen.

HACKER

Een hacker is iemand die, terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft.

SCADA OF ICS (INDUSTRIAL CONTROL SYSTEMS)

Supervisory Control And Data Acquisition is het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines of toestellen in industriële procescontrolesystemen. Deze SCADA-systemen zijn vaak direct of indirect (dmv bijvoorbeeld USB-sticks) verbonden met het internet.

BIJLAGE 2: ACRONIEMEN

ADCC	Algemene Directie Crisiscentrum
ADIV	Algemene Dienst Inlichting en Veiligheid
Belac	Belgische Accredidatie-instelling
Belnet	Belgian national research network
BelNIS	Belgian Network Information Security
BIPT	Belgisch Instituut voor postdiensten en telecommunicatie
CBPL	Commissie voor de bescherming van de persoonlijke levenssfeer
CCSB	Centrum voor Cyber Security België
CERT	Computer Emergency Response Team
ESA	European Space Agency
FCCU	Federal Computer Crime Unit
Fedict	FOD voor Informatie- en Communicatietechnologie
FOD	Federale Overheidsdienst
ICT	Informatie- en communicatietechnologie
KSZ	Kruispuntbank van de Sociale Zekerheid
MCIV	Ministerieel Comité voor inlichting en veiligheid
NAVO	Noord-Atlantische Verdragsorganisatie
NVO	Nationale Veiligheidsoverheid
OCAD	Coördinatieorgaan voor dreigingsanalyse
SCADA	Supervisory Control and Data Acquisition
VSSE	Veiligheid van de Staat, Sûreté de l'Etat

BIJLAGE 3: BESCHERMING VAN KRITIEKE INFRASTRUCTUREN

In het domein van de preventie en de veiligheid voorziet de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren in de gedeeltelijke omzetting van de richtlijn 2008/114/EG van 8 december 2008 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.

Momenteel telt deze wet vier sectoren in haar toepassingsgebied. Het gaat, wat de Europese en nationale kritieke infrastructuren betreft, om de sector energie en de sector vervoer, en wat de nationale kritieke infrastructuren betreft, om de sector financiën en de sector openbare elektronische communicatie.

De wet legt de exploitanten van een kritieke infrastructuur op om een beveiligingscontactpunt aan te duiden, maar ook om een B.P.E. (beveiligingsplan van de exploitant) uit te werken met het oog op het voorkomen, beperken en neutraliseren van de risico's op verstoring van de werking of van de vernietiging van de kritieke infrastructuur door het op punt stellen van interne materiële en organisatorische maatregelen.

Artikel 13 § 2 van de wet preciseert dat dit plan minimum de permanente maatregelen, die in alle omstandigheden van toepassing zijn, en graduele maatregelen, die in functie van de dreiging toegepast moeten worden, bevat. Het OCAD zal de cyberveiligheid in aanmerking nemen bij de analyse van de dreiging, die het uitvoert op vraag van de ADCC, in het kader van de wet betreffende de bescherming van de kritieke infrastructuren.

Deze maatregelen kunnen zowel fysiek zijn, bijvoorbeeld de toegangscontrole of het toezicht op knooppunten, als logisch zijn, d.i. specifiek voor de informaticasystemen of -netwerken van de infrastructuur in kwestie (installatie van software om malware te detecteren, …).

Het is aan de exploitant om op eigen initiatief dergelijke logische maatregelen te nemen, terwijl zijn beveiligingsplan opgesteld is op basis van een risicoanalyse die erin bestaat om de voornaamste scenario's van mogelijke dreigingen, met inbegrip van cyberdreigingen, te identificeren.

Indien echter blijkt dat de exploitanten van een bijzondere sector of deelsector dergelijke maatregelen niet nemen of dat ze onvoldoende zijn, dan blijft het mogelijk om de exploitant te verplichten om specifieke maatregelen op te nemen in zijn beveiligingsplan. Indien de wet inderdaad de minimale inhoud ervan voorziet, laat ze de mogelijkheid voor de Koning om de inhoud ervan, voor een bepaalde sector of deelsector, te detailleren.

Vanuit het oogpunt van de reactie, in geval van een incident met betrekking tot de informaticasystemen of elektronische communicatienetwerken van een kritieke infrastructuur, is voorzien dat de exploitant een bijzondere rol speelt aan de zijde van de overheden die belast zijn met het beheer van de crisis.