DOC 55 **2169/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

1er septembre 2021

# LES CYBERATTAQUES MENÉES CONTRE LES SYSTÈMES IT DE L'ÉTAT ET DES SERVICES PUBLICS

**Audition**

## RAPPORT

FAIT AU NOM DE LA COMMISSION
DE L'INTÉRIEUR, DE LA SÉCURITÉ,
DE LA MIGRATION ET
DES MATIÈRES ADMINISTRATIVES
PAR
M. **Michael FREILICH**

---

**SOMMAIRE** Pages



BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

1 september 2021

# DE CYBERAANVALLEN OP HET IT-SYSTEEM VAN DE STAAT EN DE OVERHEIDSDIENSTEN

**Hoorzitting**

## VERSLAG

NAMENS DE COMMISSIE
VOOR BINNENLANDSE ZAKEN, VEILIGHEID,
MIGRATIE EN
BESTUURSZAKEN
UITGEBRACHT DOOR
DE HEER **Michael FREILICH**

---

**INHOUD** Blz.



05220

**Composition de la commission à la date de dépôt du rapport/**
**Samenstelling van de commissie op de datum van indiening van het verslag**
Président/Voorzitter: Ortwin Depoortere

**A. — Titulaires / Vaste leden:**

| | |
|---|---|
| N-VA | Sigrid Goethals, Yngvild Ingels, Koen Metsu |
| Ecolo-Groen | Julie Chanson, Simon Moutquin, Eva Platteau |
| PS | Hervé Rigot, Daniel Senesael, Eric Thiébaut |
| VB | Ortwin Depoortere, Dries Van Langenhove |
| MR | Philippe Pivin, Caroline Taquin |
| CD&V | Franky Demon |
| PVDA-PTB | Nabil Boukili |
| Open Vld | Tim Vandenput |
| Vooruit | Bert Moyaers |

**B. — Suppléants / Plaatsvervangers:**

| |
|---|
| Christoph D'Haese, Joy Donné, Darya Safai, Yoleen Van Camp |
| Wouter De Vriendt, Claire Hugon, Cécile Thibaut, Stefaan Van Hecke |
| Khalil Aouasti, Hugues Bayet, André Flahaut, Ahmed Laaouej |
| Frank Troosters, Tom Van Grieken, Hans Verreyt |
| Denis Ducarme, Philippe Goffin, Florence Reuter |
| Jan Briers, Nahima Lanjri |
| Gaby Colebunders, Greet Daems |
| Katja Gabriëls, Marianne Verhaert |
| Ben Segers, Anja Vanrobaeys |

**C. — Membres sans voix délibérative / Niet-stemgerechtigde leden:**

| | |
|---|---|
| cdH | Vanessa Matz |
| INDEP | Emir Kir |
| ONAFH | Emir Kir |

| | | |
|---|---|---|
| *N-VA* | : | *Nieuw-Vlaamse Alliantie* |
| *Ecolo-Groen* | : | *Ecologistes Confédérés pour l'organisation de luttes originales – Groen* |
| *PS* | : | *Parti Socialiste* |
| *VB* | : | *Vlaams Belang* |
| *MR* | : | *Mouvement Réformateur* |
| *CD&V* | : | *Christen-Democratisch en Vlaams* |
| *PVDA-PTB* | : | *Partij van de Arbeid van België – Parti du Travail de Belgique* |
| *Open Vld* | : | *Open Vlaamse liberalen en democraten* |
| *Vooruit* | : | *Vooruit* |
| *cdH* | : | *centre démocrate Humaniste* |
| *DéFI* | : | *Démocrate Fédéraliste Indépendant* |
| *INDEP-ONAFH* | : | *Indépendant - Onafhankelijk* |

| *Abréviations dans la numérotation des publications:* | | *Afkorting bij de numering van de publicaties:* | |
|---|---|---|---|
| *DOC 55 0000/000* | *Document de la 55e législature, suivi du numéro de base et numéro de suivi* | *DOC 55 0000/000* | *Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer* |
| *QRVA* | *Questions et Réponses écrites* | *QRVA* | *Schriftelijke Vragen en Antwoorden* |
| *CRIV* | *Version provisoire du Compte Rendu Intégral* | *CRIV* | *Voorlopige versie van het Integraal Verslag* |
| *CRABV* | *Compte Rendu Analytique* | *CRABV* | *Beknopt Verslag* |
| *CRIV* | *Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)* | *CRIV* | *Integraal Verslag, met links het defi nitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)* |
| *PLEN* | *Séance plénaire* | *PLEN* | *Plenum* |
| *COM* | *Réunion de commission* | *COM* | *Commissievergadering* |
| *MOT* | *Motions déposées en conclusion d'interpellations (papier beige)* | *MOT* | *Moties tot besluit van interpellaties (beigekleurig papier)* |

MESDAMES, MESSIEURS,

Votre commission a consacré ses réunions des 22 et 29 juin 2021 à des auditions relatives aux cyberattaques commises contre les systèmes IT de l'État et des services publics.

## I. — **PROCÉDURE**

Conformément à l'article 32 du Règlement de la Chambre, la commission a décidé à l'unanimité d'organiser cette audition lors de sa réunion du 17 mai 2021. Au cours de sa réunion du 25 mai 2021, la commission a examiné les propositions des groupes concernant les personnes et organisations à entendre.

Les personnes et organisations suivantes ont été entendues lors de la réunion du 22 juin 2021:

— M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité Belgique (CCB);

— M. Peter Lanssens, représentant de la Sûreté de l'État (VSSE);

— M. Frédéric Van Leeuw, procureur fédéral;

— Mme Leen Depuydt et M. Piet Pieters, représentants du Centre de Crise National (NCCN);

— M. Michaël De Laet, représentant de la *Federal Computer Crime Unit* (FCCU) de la police fédérale.

La réunion du 29 juin 2021 a été consacrée à l'audition des personnes et organisations suivantes:

— M. Philipp Amann, *Head of Expertise and stakeholder management*, et M. Fernando Ruiz, *Head of Operations*, représentants de la *European Cybercrime Centre d'Europol*;

— M. Bart Preneel, professeur à la KU Leuven, cellule "*Computer Security and Industrial Cryptography*" (COSIC);

— M. Dirk Haex, codirecteur de Belnet;

— M. Geert Baudewijns, CEO de Secutec.

Conformément à l'article 32 du Règlement de la Chambre, la commission a décidé, au début de l'audition

DAMES EN HEREN,

Uw commissie heeft haar vergaderingen van 22 en 29 juni 2021 gewijd aan hoorzittingen over de cyberaanvallen op het IT-systeem van de Staat en de overheidsdiensten.

## I. — **PROCEDURE**

Overeenkomstig artikel 32 van het Kamerreglement heeft de commissie tijdens de vergadering van 17 mei 2021 eenparig beslist tot het organiseren van deze hoorzitting. Tijdens de vergadering van 25 mei 2021 heeft de commissie de voorstellen van de fracties over de te horen personen en instanties besproken.

Tijdens de vergadering van 22 juni 2021 werden de volgende personen en organisaties gehoord:

— de heer Miguel De Bruycker, directeur van het *Center for Cybersecurity Belgium* (CCB);

— de heer Peter Lanssens, vertegenwoordiger van de Veiligheid van de Staat (VSSE);

— de heer Frédéric Van Leeuw, federaal procureur;

— mevrouw Leen Depuydt en de heer Piet Pieters, vertegenwoordigers van het Nationaal Crisiscentrum (NCCN);

— de heer Michaël De Laet, vertegenwoordiger van de *Federal Computer Crime Unit* (FCCU) van de Federale Politie.

De vergadering van 29 juni 2021 was gewijd aan een hoorzitting met de volgende personen en organisaties:

— de heer Philipp Amann, *Head of Expertise and stakeholder management*, en de heer Fernando Ruiz, *Head of Operations*, vertegenwoordigers van het *European Cybercrime Centre van Europol*;

— de heer Bart Preneel, professor aan de KU Leuven, research group "*Computer Security and Industrial Cryptography*" (COSIC);

— de heer Dirk Haex, codirecteur van Belnet;

— de heer Geert Baudewijns, CEO van Secutec.

Overeenkomstig artikel 32 van het Kamerreglement heeft de commissie bij aanvang van de hoorzitting van

du 22 juin 2021, que la réunion ferait l'objet d'un rapport de commission.

## II. — **AUDITION DU 22 JUIN 2021**

### A. **Exposés introductifs**

#### 1. ***Exposé introductif de M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité Belgique (CCB)***

*M. Miguel De Bruycker* ne souhaite pas détailler un incident en particulier, mais fournir avant tout un cadre général qui permette de mieux comprendre la cybermenace. Il indique que nous nous trouvons en pleine transformation numérique. Notre vie tout entière, qu'il s'agisse des aspects sociétaux, sociaux ou professionnels, est désormais tournée vers le numérique. La pandémie de COVID-19 a davantage renforcé ce phénomène et nous a rendus complètement dépendants des technologies numériques, d'internet ou encore du cloud. En effet, tout le monde effectue des achats en ligne, fait des rencontres ou entretient des contacts sociaux avec des amis en ligne, les entreprises utilisent toutes le cloud, et cetera. La transformation numérique figure donc parmi les priorités à l'ordre du jour.

Par conséquent, nous assistons à l'émergence de nouvelles formes de criminalités. Les criminels sévironT dès lors également dans le monde du numérique. L'intervenant évoque, par exemple, le *phishing* (hameçonnage), le *smishing* (hameçonnage par SMS) et le *vishing* (hameçonnage vocal). Les victimes sont contactées par des soi-disant entreprises technologiques qui veulent les "aider", mais qui vont en réalité leur extorquer des dizaines de milliers d'euros.

Nous assistons ainsi à l'émergence de nombreuses nouvelles techniques d'extorsion. L'intervenant évoque le phénomène de *ransomware* (rançongiciels), des entreprises qui se font pirater, mais également au phénomène de *sextortion* où les criminels obtiennent des images qui leur permettent ensuite d'extorquer leurs victimes. Le bitcoin joue également un rôle de premier plan dans le développement de tels phénomènes. En effet, les criminels peuvent plus facilement organiser le transfert de cet argent virtuel.

Les *Ransomware* ne sont certainement pas sans danger. M. De Bruycker prend l'exemple d'une personne en Allemagne qui n'a pas pu être transportée à l'hôpital parce que le système informatique était paralysé, rendant impossible le traitement de sa demande. Son transfert vers un autre hôpital a dès lors été organisé, mais le

22 juni 2021 beslist dat van de vergadering een commissieverslag wordt opgesteld.

## II. — **HOORZITTING VAN 22 JUNI 2021**

### A. **Inleidende uiteenzettingen**

#### 1. ***Inleidende uiteenzetting van de heer Miguel De Bruycker, directeur van het "Center for Cybersecurity Belgium" (CCB)***

*De heer Miguel De Bruycker* wenst niet dieper in te gaan op één specifiek incident, maar wil in de eerste plaats een algemeen kader meegeven om zo beter de cyberdreiging te begrijpen. Hij geeft aan dat we volop in een digitale transformatie zitten. Zowel onze maatschappij, als ons sociaal en professioneel leven migreert helemaal richting de digitale wereld. De COVID-19-pandemie heeft ervoor gezorgd dat dit nog versterkt, waardoor we helemaal afhankelijk worden van die digitale wereld, het internet of "*the clouds*". We kopen allemaal online, daten online, hebben sociale contacten met vrienden online, bedrijven gaan helemaal in de cloud, enzovoort. De digitale transformatie staat dus heel hoog op de agenda.

Zo zien we ook nieuwe vormen van criminaliteit ontstaan. Criminelen zullen zich naar die digitale wereld verplaatsen. De spreker verwijst bijvoorbeeld naar phishing, smishing (via sms) en *vishing*. De mensen worden gebeld door zogenaamde techbedrijven die hen willen helpen maar op het einde van de dag zijn ze tienduizenden euro kwijt.

Hierdoor worden we geconfronteerd met heel wat nieuwe vormen van afpersing. Zo verwijst de spreker naar het fenomeen van ransomware, bedrijven die worden gehijacked, maar ook sextortion waarbij beelden worden genomen en mensen hiermee worden afgeperst. Bitcoin speelt hierin ook een belangrijke rol. Het is immers virtueel cash geld, waardoor de illegale wereld dit geld op een gemakkelijker manier kan transfereren.

Ransomware is zeker niet onschuldig. Zo haalt de heer De Bruycker het voorbeeld aan van iemand in Duitsland die niet naar het ziekenhuis kon worden gebracht omdat het hele systeem niet meer in staat was om haar vraag administratief te verwerken. Zij moest worden afgeleid naar een ander ziekenhuis en de hulp kwam daardoor

délai de prise en charge s'est avéré fatal. Par ailleurs, un *ransomware* a paralysé le principal réseau de distribution de carburant aux États-Unis pendant plusieurs jours.

Autre exemple: les appels en absence provenant de numéros étrangers. Les victimes rappellent un numéro qui a tenté de les joindre et finissent par payer plusieurs dizaines d'euros chaque mois, car elles se retrouvent en contact avec un numéro surtaxé qu'elles n'ont jamais demandé à joindre (une escroquerie appelée fraude "Wangiri"). La technique du *sim-swapping* est également utilisée dans notre pays. Le pirate tente de faire activer le numéro de la victime sur une nouvelle carte SIM grâce à des personnes qui ont accès à la base de données de l'entreprise pour laquelle elles sont employées. Elles attribuent alors un numéro temporaire à cette carte, ce qui permet de contourner l'authentification à deux facteurs. Le pirate peut ensuite disposer de données sur des personnes ou des entreprises. Les violations de données sont également de plus en plus récurrentes, ce qui entraîne une augmentation exponentielle du vol de données.

Ensuite, l'intervenant souligne la fraude croissante dont sont victimes les entreprises. Il cite plusieurs techniques qui consistent essentiellement à tromper des entreprises avec de faux messages afin de les escroquer. On peut également citer les attaques DDoS (*Distributed Denial-of-Service*) dont Belnet a été victime. Il s'agit d'un vaste réseau de systèmes qui, rassemblés dans un "*botnet*", sont tous contrôlés en même temps pour envoyer des messages à destination d'une même cible.

Les attaques de la chaîne d'approvisionnement sont relativement récentes. Les criminels infiltrent les systèmes qui ont été achetés en y insérant un code avant qu'ils soient distribués, ce qui leur permet ensuite d'accéder à des dizaines de milliers d'autres appareils. Il s'agit de nouvelles formes d'espionnage. De cette manière, le pirate peut facilement s'introduire à distance dans l'ordinateur ou le smartphone d'une personne et accéder aux données, à la caméra, au micro, au système GPS, etc.

M. De Bruycker souligne que ces phénomènes se multiplient à un rythme alarmant. CERT.be constate que le nombre de signalements d'incidents passe pratiquement du simple au double chaque année et le nombre de messages transférés à *suspect@safeonweb.be* ne cesse d'augmenter également. Jusqu'à présent, on estime déjà à plus de 2 millions le nombre de messages transférés cette année, soit plus de 12 500 messages en moyenne par jour calendrier. Cette année, 500 000 URL malicieuses ont été bloquées et plus de 23 000

te laat. In de Verenigde Staten heeft men gedurende dagen het distributienetwerk voor brandstoffen lamgelegd door middel van ransomware.

Een ander voorbeeld is het bellen vanuit het buitenland. Mensen bellen terug naar een nummer dat poogde hen te bereiken, het gevolg is dat zij maandelijks tientallen euro betalen aan een abonnement bij Wangiri dat zij nooit hebben gevraagd. Ook *sim-swapping* komt voor in ons land. Dit is door mensen die toegang hebben tot een databank van een bedrijf omdat zij er werken om zo telefoonnummers toe te kennen aan simkaarten. Zij zullen tijdelijk een nummer op die kaart zetten waardoor de *two-factor*-identification wordt omzeild. Op die manier krijgen ze toegang tot gegevens van personen of bedrijven. Ook data *breaches* komt meer en meer voor waardoor de diefstal van informatie exponentieel toeneemt.

Verder wijst de spreker ook op toenemende fraude bij bedrijven. Hij geeft een aantal voorbeelden van technieken waarbij voornamelijk bedrijven met valse berichten om de tuin worden geleid om hen op te lichten. Zo was er ook de aanval op Belnet met DDoS-aanvallen (*Distributed-Denial-of-Service-attacks*). Dit betreft een heel grote hoeveelheid aan systemen die in een botnetwerk zitten en die allemaal op hetzelfde moment worden aangestuurd om netwerkberichten te sturen naar één zelfde punt.

Relatief nieuw zijn de *supply chain attacks*. Aan de systemen die men aankoopt, worden nog voor de distributie een code toegevoegd waardoor criminelen zich toegang kunnen verschaffen tot tienduizenden andere toestellen. Dit zijn nieuwe vormen van spionage. Op die manier kan men vanop afstand eenvoudig binnenbreken in iemands computer of smartphone en toegang krijgen tot informatie, camera, microfoon, GPS-systeem, enzovoort.

De heer De Bruycker benadrukt dat deze fenomenen zorgwekkend snel toenemen. CERT.be ziet elk jaar bijna een verdubbeling van het aantal incidentmeldingen, alsook het aantal berichten die "*verdacht@safeonweb.be*" ontvangt neemt steeds meer toe. Zo stelt men op dit moment reeds meer dan 2 miljoen berichten voor dit jaar. Dat is een gemiddelde van meer dan 12 500 per kalenderdag. Dit jaar werden 500 000 kwaadaardige URL's geblokkeerd en meer dan 23 000 virussen werden in deze berichten gedetecteerd. Dit geeft een gemiddelde

virus ont été détectés dans ces messages. Cela correspond, en moyenne, à 2 900 liens malicieux par jour pour notre pays et ces chiffres ne reflètent que le nombre de signalements reçus par ce service.

L'intervenant détaille les systèmes de prévention des cyberattaques. L'attaque par amplification est la technique qui été utilisée pour amplifier la puissance de l'attaque contre Belnet. Cela consiste à inciter des dizaines de milliers de serveurs à envoyer le contenu de leur base de données. De cette façon, Belnet a été mis complètement hors service. Outre cette technique, de nombreuses autres techniques peuvent être utilisées pour réaliser cette amplification.

En matière de prévention, il est primordial de savoir que le cybercriminel choisit la technique qu'il va utiliser, la taille du contenu qu'il va envoyer, le moment où il va lancer l'attaque, ainsi que sa victime. C'est précisément là que réside le problème, car il est impossible d'anticiper le moment, la technique, la puissance et la future cible de la prochaine attaque. Il n'est pas facile de protéger l'ensemble du pays en permanence et contre tous les types d'attaques.

M. De Bruycker souligne également les nouveaux problèmes auxquels nous sommes confrontés. Cela a commencé avec l'apparition de la smart TV, la télévision connectée à internet. Un nombre croissant d'appareils que nous utilisons au quotidien sont connectés à internet. Cependant, aucun système n'est prévu pour envoyer des mises à jour de sécurité à ces appareils. Un smartphone effectue automatiquement une mise à jour de sécurité s'il n'est pas éteint. Ce n'est pas le cas pour l'IdO (l'internet des objets). Ainsi, dans quelques années, nous disposerons d'un nombre incalculable d'appareils connectés et faciles à pirater.

L'intervenant recommande d'instaurer une réglementation au niveau européen afin que chaque système pouvant être connecté à internet à l'avenir reçoive automatiquement les correctifs de sécurité de son fournisseur. Dans le cas contraire, nous finirons par perdre le contrôle de ces systèmes d'ici quelques années.

Il montre ensuite, via la courbe de Microsoft Exchange, que le taux de vulnérabilité, en pourcentage, des serveurs de notre pays était en moyenne plus élevé que celui de l'Union européenne et du Benelux début mars (au moment de l'incident au SPF Intérieur). L'intervenant en conclut tout d'abord que nous ne sommes pas encore suffisamment sensibles à la sécurité informatique en Belgique. Par ailleurs, le système de spear warning dont nous disposons permet d'envoyer une alerte ciblée en fonction de la vulnérabilité des systèmes concernés.

van 2 900 kwaadaardige links per dag voor ons land en dit betreft dan enkel wat aan deze dienst wordt gemeld.

De spreker gaat dieper in op de mogelijkheden om cyberaanvallen te voorspellen. De techniek die gebruikt werd om de kracht van de aanval op Belnet te versterken, heet amplification. Dit bestaat erin dat men tienduizenden servers aanzet tot het sturen van de inhoud van hun databank. Op die manier is Belnet volledig onderuitgehaald. Naast deze techniek kunnen nog heel wat andere technieken gebruikt worden om die amplificatie uit te voeren.

In de voorspelling is het belangrijk te weten dat de tegenpartij zelf kiest welke techniek hij gaat gebruiken, het volume dat hij gaat inzetten, het tijdstip wanneer hij de aanval uitvoert, alsook wie hij gaat aanvallen. Dit vormt precies het probleem omdat het niet te voorspellen valt welke de volgende aanval zal zijn, welke techniek, welke kracht en wie het doelwit zal zijn. Het hele land beschermen op alle momenten, en op alle punten is niet evident.

De heer De Bruycker wijst ook op nog andere problemen die op ons afkomen. Dit is begonnen met de smart-tv, de televisie die verbonden is met het internet. Steeds meer toestellen die we dagelijks gebruiken zijn verbonden met het internet. Er is echter in geen enkel mechanisme voorzien om *security updates* naar die systemen te sturen. Een smartphone zal automatisch een security update uitvoeren wanneer men dit niet uitschakelt. Dit is niet het geval voor de IOT's (*Internet of Things*). Op die manier zitten we binnen enkele jaren met ontelbare toestellen die toegang hebben tot het internet en gemakkelijk te hacken zijn.

De spreker beveelt aan om op Europees niveau een regel in te voeren zodat elk systeem dat in de toekomst met het internet verbonden kan worden, standaard veiligheidspatches van zijn leverancier moet kunnen ontvangen. Zo niet verliezen we in de toekomst de controle over deze systemen.

Hij toont verder via de Microsoft exchange curve aan dat ons land begin maart (het moment van het incident bij de FOD Binnenlandse Zaken) procentueel gemiddeld meer kwetsbare exchange servers had in vergelijking met de Europese Unie en de Benelux. Een eerste conclusie die de spreker hieraan verbindt, is dat we in België nog steeds weinig "*security aware*" zijn. Anderzijds hebben we een concept als spear warning, het gericht waarschuwen van mensen met kwetsbare systemen. Op die manier kan men vaststellen dat ons land het op enkele

Cela nous permet de constater que notre pays a pu se hisser au-delà de la moyenne européenne en quelques jours et même figurer parmi les plus performants en quelques semaines.

Le CCB a également élaboré un plan stratégique, approuvé par le gouvernement, qui vise à renforcer l'environnement numérique. L'objectif est d'armer les utilisateurs de réseaux informatiques. En concertation avec des partenaires tels que le NCCN et les services de police, le CCB a développé le concept d'"organisations d'intérêt vital" qui regroupe les infrastructures critiques, les opérateurs de services essentiels et les organismes travaillant dans le cadre de la loi NIS et de la loi AFCN. Des stratégies spécifiques sont prévues pour ces organisations. Il est notamment question de disposer d'une capacité de réaction. La coopération entre les secteurs public, académique et privé, ainsi qu'un engagement international fort, figurent également parmi ces objectifs stratégiques. Ce plan stratégique ambitionne de faire de la Belgique l'un des pays les moins vulnérables dans un avenir proche.

### 2. ***Exposé introductif de M. Peter Lanssens, représentant de la Sûreté de l'État (VSSE)***

*M. Peter Lanssens* souligne que si la cybermenace n'est pas spécifiquement mentionnée dans la loi organique réglementant le fonctionnement de la VSSE, cette menace fait, dans une certaine mesure, tout de même l'objet d'un suivi. Plus précisément, la VSSE s'y intéresse dans le cadre des sept menaces sur lesquelles elle est tenue d'enquêter conformément à cette loi (l'espionnage, l'ingérence, le terrorisme, l'extrémisme, la prolifération, les organisations criminelles et les organisations sectaires nuisibles).

Dans le cas des cyberattaques disruptives, l'on distingue différents groupes d'auteurs potentiels en fonction de l'origine de la menace: les acteurs étatiques, s'ils sont contrôlés par un État, et les acteurs non étatiques, s'ils ne sont pas sous le contrôle d'un État.

Concernant les acteurs étatiques, plusieurs pays sont considérés comme les acteurs les plus importants en matière de cyberattaques disruptives (et d'autres types): la Russie, la Chine et, dans une moindre mesure, l'Iran et la Corée du Nord. Ces pays ont à la fois l'intention, les moyens et les compétences pour développer une cybercapacité offensive afin de l'exploiter.

L'intervenant indique qu'il est très difficile de déterminer avec fiabilité l'origine de ces cyberattaques, ce qui constitue un avantage pour les auteurs de celles-ci. Cependant, par rapport au cyberespionnage, par

dagen tijd beter deed dan het Europese gemiddelde en na enkele weken één van de betere posities innam.

Het CCB heeft ook een strategisch plan, dat is goedgekeurd door de regering, waarbij men de digitale omgeving wil versterken. Zij willen de gebruikers van computernetwerken wapenen. In samenwerking met de partners zoals het NCCN en de politiediensten werd een concept ontwikkeld waarbij kritieke infrastructuur, aanbieders van essentiële diensten en instanties die werken met de NIS-wet en de FANC-wet groeperen onder organisaties van vitaal belang en daar diensten voor aanbieden. Dit houdt onder meer in het hebben van een responscapaciteit. Verder hoort ook de samenwerking tussen de publieke, academische en private sector tot deze strategische doelstellingen samen met een sterk internationaal engagement. De bedoeling is alvast om van België binnen afzienbare tijd één van de minst kwetsbare landen te maken.

### 2. ***Inleidende uiteenzetting van de heer Peter Lanssens, vertegenwoordiger van de Veiligheid van de Staat (VSSE)***

*De heer Peter Lanssens* benadrukt dat cyberdreiging niet specifiek wordt vermeld in de organieke wet die de werking van de VSSE reguleert, maar toch wordt deze dreiging er in zekere mate opgevolgd. De VSSE doet dit meer bepaald binnen het kader van de zeven dreigingen die de VSSE volgens die wet dient op te volgen (spionage, inmenging, terrorisme, extremisme, proliferatie, georganiseerde misdaad en schadelijke sektarische organisaties).

Uitgaande van de bron van de dreiging worden – in het geval van disruptieve cyberaanvallen – verschillende mogelijke dadergroepen onderscheiden en ingedeeld naargelang ze al dan niet staatsgestuurd zijn. We spreken dan van *state* of *non-state actors*.

Wat betreft de state actors zijn er een aantal landen die worden beschouwd als de belangrijkste actoren voor disruptieve (en andere) cyberaanvallen: Rusland, China en in mindere mate Iran en Noord-Korea. Deze landen hebben zowel de intentie, de middelen als de knowhow om een offensieve cybercapaciteit te ontwikkelen en te gebruiken.

De spreker geeft aan dat deze cyberaanvallen voor de dader als intrinsiek voordeel hebben dat een betrouwbare attributie ervan heel moeilijk is. Er is echter meer risico verbonden aan het uitvoeren van een grootschalige

exemple, où les auteurs “se contentent” de voler des informations, une attaque disruptive à grande échelle comporte davantage de risques parce qu’elle peut faire des victimes. Une réponse internationale de grande ampleur peut effectivement être envisagée. En cas d’attaque disruptive contre un État membre de l’OTAN – comme la Belgique –, il n’est pas exclu d’invoquer l’article 5 du traité de l’OTAN. Compte tenu des potentielles répercussions auxquelles ils s’exposent, les acteurs étatiques ne mèneront probablement des cyberattaques disruptives que lorsqu’il sera question de nécessité impérieuse pour défendre leurs intérêts stratégiques.

Néanmoins, certains pays ont déjà mené des attaques disruptives par le passé. Par exemple, le secteur de l’énergie en Ukraine a déjà subi de lourdes attaques de la part de la Russie. L’Iran a mis hors service des dizaines de milliers d’ordinateurs après avoir mené une cyberattaque contre Aramco en Arabie saoudite, ce qui a perturbé la production de pétrole de ce pays pendant un certain temps.

La VSSE enquêtera donc également sur les cybermenaces disruptives que font peser certains acteurs étatiques dans un contexte d’espionnage et d’ingérence.

En ce qui concerne les acteurs non étatiques, M. Lanssens affirme que les cyberattaques disruptives sont désormais malheureusement aussi à la portée des acteurs non étatiques. Il fait ici notamment référence aux organisations criminelles, aux groupes terroristes et aux “hacktivistes”. Bien sûr, ce type d’acteurs ne disposent souvent pas des mêmes moyens et compétences que les acteurs étatiques, mais il a été constaté que les attaques par *ransomware* et DDoS, les plus fréquemment utilisées par ces groupes d’auteurs, peuvent sans aucun doute avoir des effets disruptifs (par exemple, sur les hôpitaux, les pipelines ou Belnet). En comparaison avec les acteurs étatiques, ils adoptent une attitude plus opportuniste. Les analyses de vulnérabilité des réseaux menées à grande échelle fournissent à ces acteurs une source continue de cibles potentielles. Il est même possible d’“acheter” une attaque DDoS sur le darknet.

Dans le cadre de ses missions légales, la VSSE peut également surveiller ces acteurs non étatiques. Dans le cas des groupes terroristes, il n’y a bien sûr aucun doute à ce sujet. Dans ce cas, bien qu’elles aient exprimé l’intention de développer une cybercapacité offensive, ces organisations ne disposent pas (encore) du personnel adéquat ni des moyens de le faire de manière crédible.

La VSSE ne peut enquêter sur des organisations criminelles que si les activités de ces dernières peuvent être reliées à au moins une des autres menaces sur

disruptieve aanval, mogelijk met slachtoffers tot gevolg, dan bijvoorbeeld bij cyberspionage waar er “slechts” informatie wordt gestolen. Een brede internationale reactie is dan immers niet ondenkbeeldig. Bij een disruptieve aanval tegen een NAVO-lidstaat – zoals België – valt zelfs het inroepen van artikel 5 van het NAVO-handvest niet uit te sluiten. Gezien de mogelijke repercussies zullen state actors disruptieve cyberaanvallen waarschijnlijk dus alleen uitvoeren wanneer ze daar een dwingende noodzaak toe zien voor hun strategische belangen.

Desalniettemin hebben in het verleden een aantal landen zich al laten verleiden tot disruptieve aanvallen. Rusland heeft bijvoorbeeld de energiesector in Oekraïne al zwaar bestookt. En Iran heeft bij een cyberaanval tegen Aramco in Saoedi-Arabië enkele tienduizenden computers uitgeschakeld waardoor de olieproductie van Saoedi-Arabië een tijd lang verstoord werd.

Disruptieve cyberdreigingen door statelijke actoren zullen door de VSSE dan ook opgevolgd worden in de context van spionage en inmenging.

Wat betreft de non-state actors stelt de heer Lanssens dat disruptieve cyberaanvallen inmiddels helaas ook binnen het handbereik van niet-statelijke actoren zijn gekomen. Hierbij verwijst hij onder meer naar de georganiseerde misdaad, terroristische groeperingen en “hacktivisten”. Zij beschikken uiteraard vaak niet over dezelfde middelen en knowhow als statelijke actoren maar er kon worden vastgesteld dat *ransomware*- en DDoS-aanvallen, wat typisch is voor deze dadergroepen, zeer zeker disruptieve effecten kunnen hebben (bijvoorbeeld op hospitalen, pijpleidingen of Belnet). In vergelijking met statelijke actoren gaan zij meer opportunistisch te werk. Grootschalige scans naar kwetsbaarheden van netwerken leveren deze actoren een continue aanvoer van potentiële doelwitten op. Een DDoS-aanval kan zelfs op het darknet tegen betaling “besteld” worden.

De VSSE kan binnen haar wettelijk kader ook deze niet-statelijke actoren opvolgen. In het geval van terroristische groeperingen bestaat daar uiteraard geen twijfel over. In dit geval is het zo dat zij weliswaar de intentie hebben geuit om een offensieve cybercapaciteit te ontwikkelen maar deze organisaties beschikken (voorlopig) niet over geschikt personeel noch over de middelen om dat op een geloofwaardige manier te doen.

Georganiseerde misdaad kan de VSSE alleen opvolgen voor zover de activiteiten ervan in verband kunnen gebracht worden met minstens één van de andere dreigingen

lesquelles ce service est chargé d'enquêter. Les attaques par ransomware purement motivées par l'appât du gain ne relèvent donc pas de sa compétence. En revanche, s'il existe des indications que ces organisations criminelles sont contrôlées par un État dans le but de faciliter l'espionnage ou l'ingérence, la VSSE est alors compétente pour mener l'enquête.

Le même raisonnement s'applique à l'"hacktivisme". Pour la VSSE, l'action menée ou le groupe d'auteurs doit pouvoir être relié, par exemple, à des activités terroristes, extrémistes, d'espionnage ou à des pratiques d'ingérence.

En ce qui concerne la lutte contre la menace et le rôle de la VSSE à cet égard, il est important de préciser que la lutte contre les cybermenaces disruptives et d'autres types de cybermenaces sérieuses ne relève pas d'un seul service public. Elle requiert une approche coordonnée de différents services, qui contribuent chacun à cette lutte dans les limites de leur propre domaine de compétence et d'expertise. Pour ce faire, il convient de s'assurer qu'aucun poste ne reste vacant.

La première étape dans cette lutte est la prévention. Le renforcement de la cybersécurité en Belgique a un impact direct sur la prévention des cyberattaques disruptives. Il est possible de prévenir les attaques opportunistes en particulier, car les auteurs de ces dernières exploitent des vulnérabilités auxquelles il est possible de remédier. Le renforcement de la cybersécurité au sens large en Belgique est donc également l'objectif principal de la Stratégie Cybersécurité Belgique 2.0 du Centre pour la cybersécurité (CCB). Cette stratégie met en exergue l'importance de la coopération et le rôle des différents services.

Une bonne coopération en matière de prévention entre les différents acteurs a déjà eu lieu, notamment à l'approche des élections de 2019. La publication du guide "Surfer en toute sécurité pendant la campagne électorale" et les séances d'informations organisées à destination des différents partis politiques en sont des exemples concrets.

Si, malgré des mesures préventives, nous sommes encore confrontés à une attaque disruptive en Belgique, il convient alors de mettre en place un mécanisme permettant de prendre les contre-mesures appropriées de manière coordonnée. La gestion d'une telle crise est prévue dans le cyberplan d'urgence élaboré par le CCB. Il est également prévu que les différents services travaillent de concert.

Dans le cas d'une cyberattaque très grave, il peut s'avérer insuffisant de prendre des mesures uniquement

die deze dienst dient op te volgen. De ransomware aanvallen die puur gericht zijn op geldgewin vallen daarmee buiten hun bevoegdheid. Indien er aanwijzingen zijn dat die misdaadgroepen gestuurd worden door een Staat met het oog op het faciliteren van spionage of inmenging, dan is opvolging door de VSSE uiteraard wel mogelijk.

Dezelfde redenering geldt ook voor "hacktivisme". Voor de VSSE moet de actie of de dadergroep in verband kunnen gebracht worden met bijvoorbeeld terrorisme, extremisme, spionage of inmenging.

Wat betreft de aanpak van de dreiging en de rol hierin voor de VSSE, is het belangrijk om aan te stippen dat de aanpak van disruptieve en andere ernstige cyberdreigingen niet het werk is van één overheidsdienst. Het vergt een gecoördineerde aanpak van verschillende diensten die elk vanuit hun eigen werkveld en expertise een bijdrage leveren. Daarbij moet ervoor gezorgd worden dat er geen posities onbezet worden gelaten.

Een eerste stap in die aanpak stelt zich in preventie. Het verhogen van de cyberveiligheid in België heeft een rechtstreekse impact op het vermijden van disruptieve cyberaanvallen. Vooral de opportunistische aanvallen die vermijdbare kwetsbaarheden exploiteren, kunnen hiermee worden voorkomen. Het verhogen van de algemene cyberveiligheid in België is dan ook het hoofddoel van de Cyberstrategie 2.0 van het Centrum voor Cybersecurity (CCB). In die strategie wordt de samenwerking en de rol van de verschillende diensten benadrukt.

Onder meer in de aanloop naar de verkiezingen van 2019 werd in de context van preventie reeds goed samengewerkt tussen de verschillende actoren. Dit gebeurde bijvoorbeeld door middel van de "veilig online tijdens de verkiezingscampagne" publicatie en presentaties voor de verschillende politieke partijen.

Wanneer we in België ondanks preventieve maatregelen toch geconfronteerd worden met een disruptieve aanval dan moet er een mechanisme voorhanden zijn dat het mogelijk maakt om op een gecoördineerde manier de gepaste tegenmaatregelen te treffen. In dit crisisbeheer wordt voorzien in het cybernoodplan van het CCB. Ook hier werken de verschillende diensten uiteraard samen.

In het geval van een zeer ernstige cyberaanval kan het onvoldoende zijn om alleen bij het slachtoffer van de

en faveur de la victime afin de mettre un terme à l'attaque. Afin d'éviter que la situation ne s'aggrave, il peut être nécessaire d'agir contre les éléments du réseau d'où l'attaque provient. Il s'agit d'une capacité que la Défense souhaite développer dans le cadre de sa stratégie de cyberdéfense.

Enfin, l'intervenant explique le rôle que la VSSE peut jouer dans ce domaine. La VSSE n'a pas reçu la capacité ni la mission de traiter les incidents avec des acteurs externes. À titre d'exception uniquement, la VSSE peut mettre un nombre limité de personnes à la disposition de ses partenaires nationaux à cette fin, ce qui s'est déjà produit dans le passé.

La VSSE doit remplir les tâches qui lui incombent, en tant que service de renseignement, dans la lutte contre la cybermenace. Cet élément constitue indéniablement la principale difficulté. Traditionnellement, la VSSE enquête sur des menaces qui se développent dans un contexte international, mais où les acteurs de la menace sont bel et bien situés sur le territoire belge (par exemple, des terroristes, des extrémistes, des officiers de renseignement, etc.). La préparation et la mise à exécution des cybermenaces peuvent être entièrement réalisées à distance, loin du territoire belge. Les services de renseignement de la VSSE ne sont pas encore capables d'y faire face.

Les cybermenaces font l'objet d'une surveillance intensive dans la plupart des pays européens. Par conséquent, la communauté du renseignement dispose d'une quantité considérable d'informations sur les groupes dits "APT" (*advanced persistent threat*), les logiciels malveillants, l'infrastructure, les techniques, les IOC, etc. La VSSE peut constituer le maillon central entre la communauté internationale du renseignement et les autorités belges. Ce partage d'informations peut viser à prévenir les incidents en Belgique ainsi qu'à contribuer à détecter les attaques en cours et y remédier.

En outre, la Sûreté de l'État – certainement dans le cas d'une menace émanant d'acteurs étatiques – dispose souvent d'informations contextuelles et stratégiques précieuses. Ce service peut notamment décrire le contexte dans lequel un pays tiers déterminé élabore sa cyberstratégie et la manière dont elle s'inscrit dans sa stratégie de politique étrangère au sens large. M. Lanssens rappelle que la cybermenace n'est souvent que le vecteur d'une stratégie plus large d'espionnage ou d'ingérence.

En conclusion, l'intervenant indique que la Sûreté de l'État ne ressent pas le besoin de devenir le service dirigeant en matière de cybersécurité, mais souhaite plutôt jouer un rôle pivot dans le cadre d'une approche pangouvernementale qui mettrait en place

aanval maatregelen te nemen om de aanval te stoppen. Het kan nodig blijken om erger te voorkomen, om actie te ondernemen tegen de netwerkelementen vanwaar de aanval wordt uitgevoerd. Dat is een capaciteit die Defensie wil ontwikkelen in het kader van hun *Cyber Defense*.

Tot slot gaat de spreker dieper in op de rol die de VSSE hierin kan spelen. De VSSE beschikt alvast niet over de capaciteit, noch heeft ze de opdracht, voor incident handling bij externe partijen. Slechts uitzonderlijk kan de VSSE daarvoor een beperkt aantal mensen ter beschikking stellen van haar nationale partners, wat in het verleden reeds is gebeurd.

De VSSE moet haar rol in de aanpak van de cyberdreiging invullen als inlichtingendienst. Daarin stelt zich meteen al de belangrijkste moeilijkheid. Traditioneel werkt de VSSE op dreigingen die zich weliswaar in een internationale context afspelen, maar waarvan de dreigingsactoren zich wel degelijk op Belgisch grondgebied bevinden (bijvoorbeeld terroristen, extremisten, inlichtingenofficieren, enzovoort). Cyberdreigingen kunnen volledig voorbereid en uitgevoerd worden vanaf een grote afstand van België. Het inlichtingeninstrumentarium van de VSSE is daar nog niet op ingesteld.

Cyberdreigingen worden in de meeste Europese landen intens opgevolgd. Daardoor is er binnen de inlichtingengemeenschap behoorlijk wat informatie over APT-groepen (*advanced persistent threat*), *malware tools*, infrastructuur, technieken, IOC's enzovoort aanwezig. De VSSE kan de centrale hub zijn tussen de internationale inlichtingengemeenschap en de Belgische autoriteiten. Die informatiedeling kan zowel tot doel hebben om incidenten in België te voorkomen als om lopende aanvallen te helpen opsporen en remediëren.

Verder beschikt de Veiligheid van de Staat – zeker in het geval van een dreiging door state actors – vaak over waardevolle contextuele en strategische informatie. Zo kan deze dienst bijvoorbeeld de context schetsen waarin een bepaald derde land haar cyberstrategie ontwikkelt en hoe deze past in haar ruimere buitenlandstrategie. De heer Lanssens herhaalt dat de cyberdreiging vaak gewoon het medium is van een ruimere strategie inzake spionage of inmenging.

Tot besluit geeft de spreker aan dat de Veiligheid van de Staat niet de drang voelt zich op te werpen als de leidende dienst inzake cyberveiligheid, maar kan wel een waardevolle rol op zich nemen in een *whole of government approach* waarin nauw wordt samengewerkt

une coopération étroite entre les différents services concernés, qui assumeraient respectivement certains aspects de cette collaboration. Il est ainsi possible de s'assurer que les moyens dont disposent les services sont utilisés complémentairement, en évitant autant que possible les chevauchements et en garantissant que les services disposent des moyens suffisants pour couvrir tous les aspects à traiter.

### 3. ***Exposé introductif de M. Frédéric Van Leeuw, procureur fédéral***

*M. Frédéric Van Leeuw* souligne tout d'abord qu'il ne peut donner aucun détail sur le contenu des dossiers judiciaires en cours et qu'il formulera donc dans son intervention des considérations générales et des recommandations pour le futur.

Il lui paraît évident, tout d'abord, que la lutte contre la cybercriminalité nécessite un investissement humain et financier. Il ne cache pas que le volet répressif de la chaîne de la cybersécurité mériterait d'être amélioré même si rien n'est plus important dans ce domaine que la prévention. Il se réfère à ce sujet au rapport publié dans le cadre du "*UK Fraud review n° 16*", dans lequel figure le passage suivant: "*An ounce of prevention is worth a pound of cure. A sad feature of many frauds is how easily so many of them could have been avoided if the victims had exercised sensible caution about propositions which in retrospect, were obviously too good to be true*". Cette analyse est certainement valable en matière de cybercriminalité. La prévention coûte en outre moins cher et prend moins de temps que la réparation des dommages causés par des actes de cybercriminalité, que la collecte de preuves ou l'identification des auteurs. Il en veut pour preuve les investissements conséquents qui ont dû être consentis par le SPF Intérieur à la suite de la cyberattaque dont il a fait l'objet. S'il est évident qu'il y a toujours une certaine réticence à investir alors que rien ne se passe, ces investissements peuvent toutefois s'avérer salvateurs par la suite. Il salue dès lors le fait que les auditions organisées par la commission sont de nature à susciter une prise de conscience bienvenue.

La prévention est donc le maître-mot et la priorité absolue comme il ressort d'ailleurs des discussions au sein du Comité de concertation du renseignement et de la sécurité.

M. Van Leeuw souligne en outre l'importance de la réglementation européenne NIS qui tend à assurer la prise de mesures de sécurité techniques et organisationnelles par les opérateurs de services essentiels pour prévenir les incidents ou en limiter l'impact. On a vu par le passé, dans certains dossiers de *hacking* à l'égard

tussen de verschillende betrokken diensten die elk bepaalde aspecten op zich nemen. Op die manier kan erover gewaakt worden dat de middelen van de diensten complementair worden ingezet, waarbij overlap zoveel als mogelijk wordt vermeden maar er tegelijk over gewaakt wordt dat alle aspecten voldoende gecoverd worden.

### 3. ***Inleidende uiteenzetting van de heer Frédéric Van Leeuw, federaal procureur***

*De heer Frédéric Van Leeuw* benadrukt eerst dat hij geen details kan verstrekken over de inhoud van de lopende gerechtelijke onderzoeken en dat hij daarom in zijn uiteenzetting algemene beschouwingen en aanbevelingen voor de toekomst zal formuleren.

In de eerste plaats lijkt het hem voor de hand te liggen dat de strijd tegen de cybercriminaliteit een menselijke en financiële investering vergt. Hij steekt niet weg dat het repressieve gedeelte van de cyberveiligheidsketen zou moete, worden verbeterd, ook al is op dit vlak niets zo belangrijk als preventie. Zo verwijst hij naar de volgende passage uit een rapport dat is verschenen in "*UK Fraud review n° 16*": "*An ounce of prevention is worth a pound of cure. A sad feature of many frauds is how easily so many of them could have been avoided if the victims had exercised sensible caution about propositions which in retrospect, were obviously too good to be true*". Deze analyse gaat zeker op met betrekking tot cybercriminaliteit. Bovendien kost preventie minder geld en tijd dan het herstellen van de door cybercriminaliteit veroorzaakte schade, het verzamelen van bewijsmateriaal of het identificeren van de daders. Als bewijs daarvoor verwijst hij naar de aanzienlijke investeringen die de FOD Binnenlandse Zaken heeft moeten doen naar aanleiding van de tegen die overheidsdienst gerichte cyberaanval. Uiteraard zal men altijd aarzelen te investeren zolang niets aan de hand is, maar dergelijke investeringen kunnen achteraf wel het verschil blijken te maken. Hij juicht het dan ook toe dat de door de commissie georganiseerde hoorzittingen een welgekomen bewustwording zullen teweegbrengen.

Preventie is dus het sleutelwoord en de absolute prioriteit, zoals trouwens blijkt uit de besprekingen in het Coördinatiecomité voor Inlichtingen en Veiligheid.

Daarenboven benadrukt de heer Van Leeuw het belang van de Europese NIS-regelgeving, die inhoudt dat de essentiële-dienstenoperatoren technische en organisatorische maatregelen moeten nemen om incidenten te voorkomen dan wel de impact ervan te beperken. In het verleden is in sommige zaken van hacking tegen

d'institutions bancaires, que le niveau de sécurité était parfois tellement bas que cela faisait peser également un risque pour l'économie. Il n'est donc pas illogique de prévoir des sanctions dans le cas où le système informatique ne respecte pas les mesures de sécurité nécessaires. L'intervenant indique que la réglementation a toutefois des limites et devrait notamment être également appliquée au secteur public. Il cite par ailleurs d'autres textes qui ont leur importance, à savoir la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques ou encore la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

M. Van Leeuw souligne que le parquet fédéral est très favorable aux investissements des cinq dernières années dont il faut reconnaître qu'ils ont permis d'accomplir un mouvement de rattrapage énorme grâce au développement du CCB. Cela étant, il faut être conscient que le budget du CCB est relativement réduit par rapport à son homologue des Pays-Bas, où le budget est de six à sept fois plus important. Le CCB n'en reste pas moins le moteur qui doit mener notre pays et ses citoyens vers une plus grande culture de la sécurité. Le *Computer Emergency Response Team* fédéral, ou CERT.be, qui est le service opérationnel du Centre pour la Cybersécurité Belgique (CCB), joue par ailleurs un rôle crucial dans la gestion des incidents nationaux et pour l'assistance aux victimes. Il est impératif de conserver ces investissements qui sont finalement assez minimes au regard des catastrophes qu'ils permettent d'éviter.

Le renforcement du volet réactif (police/justice) est également important, car la Belgique présente de grandes fragilités.

L'intervenant rappelle que la cybercriminalité revêt plusieurs formes: si elle peut être purement financière et se limiter à frapper des citoyens, les attaques émanent parfois de groupes criminels, parrainés ou non par un État, et visent à désorganiser ou à paralyser des systèmes numériques qui permettent le fonctionnement de la société. Les risques liés à ces attaques seront d'autant plus grands que les objets qui nous entourent seront à l'avenir de plus en plus connectés et gérés de manière centralisée.

La recherche, l'identification et la répression des auteurs se heurtent à des obstacles de taille. Le monde cyber n'a en effet pas de frontières: les auteurs qui se trouvent à l'étranger sont souvent difficilement localisables. Se pose par ailleurs le problème de la volatilité des preuves. Du point de vue de la justice, il peut paraître

bankinstellingen gebleken dat het beveiligingsniveau soms zo laag was dat zelfs de economie gevaar liep. Het is dus niet onlogisch te voorzien in sancties ingeval het informaticasysteem de vereiste beveiligingsmaatregelen niet in acht neemt. De spreker geeft aan dat de regelgeving ook haar limieten heeft en onder meer ook op de overheidssector zou moeten worden toegepast. Voorts somt hij een aantal teksten op die volgens hem ook belangrijk zijn, zoals de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

De heer Van Leeuw benadrukt dat het federaal parket hoogst ingenomen is met de investeringen van de jongste vijf jaar, in verband waarmee moet worden erkend dat ze dankzij de uitbouw van het CCB een enorme inhaalbeweging mogelijk hebben gemaakt. Toch dient men te beseffen dat het budget van het CCB vrij mager uitvalt in vergelijking met zijn Nederlandse evenknie, waarvan het budget zes tot zeven keer zo hoog ligt. Niettemin is het CCB de motor die ons land en de burgers op weg moet helpen naar een grotere veiligheidscultuur. Het federale *Computer Emergency Response Team* (CERT.be), dat de operationele dienst van het Centrum voor Cybersecurity België (CCB) is, speelt voorts een cruciale rol bij het beheren van nationale incidenten en bij het verlenen van bijstand aan de getroffenen. Die investeringen moeten hoe dan ook worden gehandhaafd; uiteindelijk zijn ze een peulschil in vergelijking met de rampen die ze kunnen voorkomen.

Ook de versterking van het reactieve onderdeel (politie/gerecht) is belangrijk, omdat België op bepaalde punten hoogst kwetsbaar is.

De spreker herinnert eraan dat cybercriminaliteit vele gedaanten heeft: ze kan louter financieel zijn en het alleen op burgers gemunt hebben, maar soms zijn de aanvallen het werk van al dan niet door een Staat gesteunde criminele groeperingen, die de digitale systemen waarop een hele samenleving draait, willen verstoren of lamleggen. De gevaren die dergelijke aanvallen meebrengen, zullen des te groter worden naarmate de objecten die ons omringen, in de toekomst almaar meer met elkaar verbonden zullen zijn en gecentraliseerd zullen worden beheerd.

Bij het opsporen, identificeren en bestraffen van daders duiken hinderpalen van formaat op. De cyberwereld heeft immers geen grenzen: van daders in het buitenland is het vaak moeilijk te achterhalen waar ze zich bevinden. Voorts is ook de volatiliteit van het bewijsmateriaal een probleem. Uit het oogpunt van het gerecht kan het

disproportionné d'investir de grosses sommes dans l'organisation, par exemple, de commissions rogatoires, lorsque les montants concernés sont relativement réduits – ce qui est souvent le cas lors du *hacking* d'un compte en banque. Pourtant, si on comptabilise l'ensemble des dommages résultant du *hacking*, ces montants peuvent exploser. Ceci montre la nécessité d'une approche multilatérale et d'une collaboration structurelle pour éviter l'impunité. Alors que la problématique mérite que l'on développe une vision et un plan d'action, le volet policier et judiciaire ne bénéficie pour l'instant que d'une attention limitée. Le mouvement de rattrapage évoqué plus haut reste trop timide et est tardif par rapport à d'autres pays.

D'autre part, certaines cyberattaques ne relèvent pas toujours de la criminalité, mais sont à relier à l'espionnage. M. Van Leeuw cite à titre d'illustration le piratage de Belgacom qui a mobilisé beaucoup de capacité de la police et du parquet fédéral. La question se pose de savoir s'il entre vraiment dans les missions de la justice d'enquêter sur des dossiers qui touchent aux relations entre États. Il est d'ailleurs probable que ces dossiers n'aboutissent jamais à une condamnation. Pourtant, l'intervention de la justice reste nécessaire, car certains actes d'enquête ne peuvent être posés que par un juge d'instruction.

L'intervenant formule ensuite des propositions concrètes pour faire face à ces nouvelles menaces liées à la cybercriminalité.

Il souligne tout d'abord le gros effort de rattrapage à poursuivre au niveau de la police et de la justice pour recruter des spécialistes susceptibles de participer aux enquêtes. Il se réfère à l'opération *Sky* qui démontre que les techniques de *hacking* utilisées par des réseaux criminels peuvent également être mises à profit par les enquêteurs (*hacking* de téléphones cryptés, intrusion dans des systèmes informatiques, etc.). Ce jeu de piste numérique rend nécessaire le recrutement de spécialistes disposant d'un niveau de compétence suffisant pour mener des enquêtes de grande ampleur. Actuellement, il est impossible, au vu des capacités limitées, de participer simultanément à plusieurs opérations de type *Sky* et des accords doivent donc être conclus avec les autorités policières et judiciaires d'autres pays.

La FCCU souffre d'un manque aigu de personnel, d'expertise et de moyens, même si ses membres font preuve d'une créativité qui étonne parfois ses homologues étrangers, dont les moyens sont nettement plus élevés. Une révision des statuts et de l'organisation au

buiten proportie lijken fors te investeren in de organisatie van bijvoorbeeld rogatoire commissies, wanneer bij de aanvallen relatief beperkte bedragen zijn buitgemaakt, wat bij het hacken van een bankrekening vaak het geval is. Tel alle schade als gevolg van hacking bij elkaar op, en dan kunnen die bedragen nochtans gigantisch hoog uitvallen. Een multilaterale benadering en een structurele samenwerking zijn dus noodzakelijk om straffeloosheid te voorkomen. Hoewel met betrekking tot dit vraagstuk een visie en een actieplan aan de orde zijn, gaat er momenteel slechts beperkte aandacht uit naar het politionele en het gerechtelijke aspect. De eerder aangehaalde inhaalbeweging is nog altijd te aarzelend en werd in andere landen al eerder ingezet.

Aan de andere kant zijn er cyberaanvallen die niets met criminaliteit van doen hebben maar verband houden met spionage. De heer Van Leeuw verwijst als voorbeeld naar de hacking tegen Belgacom, waarvoor de politie en het federaal parket veel capaciteit hebben moeten inzetten. De vraag rijst of het echt tot de taken van het gerecht behoort om onderzoek te doen in dossiers die verband houden met de betrekkingen tussen Staten. De kans dat dergelijke dossiers ooit tot een veroordeling zullen leiden, is overigens klein. Toch blijft het optreden van het gerecht noodzakelijk, omdat sommige onderzoeksdaden alleen door een onderzoeksrechter mogen worden gesteld.

Vervolgens reikt de spreker concrete voorstellen aan om een antwoord te bieden op die nieuwe cybercriminaliteitsdreigingen.

In de eerste plaats benadrukt hij dat moet worden voortgegaan met de forse inhaalbeweging om bij de politie en het gerecht specialisten in dienst te nemen die aan de onderzoeken kunnen meewerken. Hij verwijst naar operatie-*Sky*, die aantoont dat de door de criminele netwerken gebruikte hackingmethodes eveneens door de speurders kunnen worden gehanteerd (hacken van versleutelde telefoons, inbreken in informaticasystemen enzovoort). Voor dergelijk digitaal spoorzoeken moeten specialisten in dienst worden genomen die over de nodige competenties beschikken om grootschalige onderzoeken uit te voeren. Aangezien het als gevolg van de beperkte capaciteiten vooralsnog onmogelijk is gelijktijdig aan meerdere operaties van het type *Sky* mee te werken, moeten met de politionele en gerechtelijke overheden van andere landen akkoorden worden gesloten.

De FCCU kampt met een acuut tekort aan personeel, knowhow en middelen, al geven de medewerkers soms blijk van een creativiteit die bewondering oogst bij de buitenlandse evenknieën, die over beduidend meer middelen beschikken. Een herziening van de statuten

sein de la police paraît indispensable pour engager du personnel disposant d'un certain niveau d'expertise.

Le retard est surtout révélateur dans les dossiers sensibles (crime organisé, ingérence étatique) pour lesquels il est nécessaire de faire du renseignement afin d'identifier l'origine des attaques et de les prévenir. Il lui paraît qu'à défaut d'un renforcement conséquent de la FCCU, le point de non-retour sera dépassé d'ici cinq ans. L'intervenant rappelle en effet qu'au cours de la précédente législature le nombre de membres du personnel a fondu et est devenu insuffisant compte tenu du nombre d'infrastructures critiques et d'organisations internationales dans notre pays. Il lui paraît en outre nécessaire de se doter d'unités régionales (RCCU) et de disposer d'experts aux profils diversifiés, capables d'analyser les logiciels malveillants ou de s'infiltrer dans le darkweb, ou encore de spécialistes en cryptage, en piratage et en analyse de monnaie virtuelle. Vu la dimension internationale, la FCCU doit également compter des spécialistes en langue slave, chinoise et arabe. L'intervenant plaide dès lors pour le développement urgent d'une politique de recrutement, de formation et de rémunération adéquate. Il faut par ailleurs disposer d'une équipe d'intervention rapide (*quick reaction force*) à même d'intervenir lorsque le *cyberplan* d'urgence est activé et qui est capable de mener simultanément plusieurs enquêtes axées sur les menaces plus sensibles à l'encontre des infrastructures critiques.

En outre, M. Van Leeuw plaide pour la mise sur pied d'équipes communes d'enquête, réunissant des enquêteurs techniques et tactiques, afin d'optimiser l'utilisation des rares capacités disponibles et d'investir dans l'équipe "*intelligence*" de la FCCU qui est presque inexistante à ce jour. Ceci doit évidemment aller de pair avec l'investissement dans des systèmes et matériels informatiques professionnels adaptés. Trop souvent, il a fallu mendier du matériel et des logiciels, les achats ne se faisant que par à-coups, lors de la survenance d'incidents graves.

Concernant les investissements nécessaires en matière de capacité cyber au sein de la justice, il précise que le parquet fédéral, qui est compétent en matière de criminalité organisée, a été invité par le Collège des procureurs généraux à s'occuper en priorité des attaques sur les infrastructures critiques et des *alpha cases*, autrement dit des dossiers impliquant un nouveau *modus operandi*. Le parquet fédéral copréside par ailleurs le réseau d'expertise cybercrime, chargé de rédiger des instructions à destination de la magistrature.

en van de organisatie bij de politie lijkt onontbeerlijk om personeel te kunnen aantrekken dat over een zeker expertiseniveau beschikt.

De achterstand is vooral veelzeggend in de gevoelige dossiers (georganiseerde misdaad, staatsinmenging) waarvoor inlichtingen moeten worden ingewonnen om de oorsprong van de aanvallen te achterhalen en ze te voorkomen. De spreker is van oordeel dat het keergrenspunt binnen de vijf jaar zal worden overschreden indien de FCCU niet aanzienlijk wordt aangescherpt. Er zij immers op gewezen dat het personeelsbestand tijdens de vorige regeerperiode is gedaald en ontoereikend is geworden, gelet op de vele kritieke infrastructuur en internationale organisaties in België. De spreker is voorts van oordeel dat ook gewestelijke eenheden (RCCU's) zouden moeten worden opgezet en dat men zou moeten kunnen beschikken over experts met uiteenlopende profielen, die in staat zijn om malware te analyseren of om in het dark web binnen te dringen, of over specialisten in encryptie, hacking en de analyse van virtuele munten. Gelet op de internationale dimensie moet de FCCU ook kunnen beschikken over specialisten in de Slavische, Chinese en Arabische talen. Derhalve roept de spreker op om dringend een gepast wervings-, opleidings- en loonbeleid uit te werken. Voorts dient men ook te kunnen beschikken over een *quick reaction force* die meteen kan optreden zodra het cybernoodplan in werking treedt en die tegelijkertijd meerdere onderzoeken kan voeren naar de oorsprong van de meer gevoelige bedreigingen van kritieke infrastructuur.

Daarnaast roept de heer Van Leeuw op tot de oprichting van gemeenschappelijke onderzoeksteams, met zowel technische als tactische rechercheurs, teneinde de schaarse beschikbare capaciteit optimaal te benutten en tot investeringen in het team "*intelligence*" van de FCCU, dat thans nagenoeg onbestaande is. Zulks moet uiteraard gepaard gaan met investeringen in geschikte professionele IT-systemen en apparatuur. Al te vaak moest om hardware en software worden gebedeld en werd slechts bij vlagen materiaal aangekocht, nadat zich ernstige incidenten hadden voorgedaan.

Qua noodzakelijke investeringen in capaciteit om cyberzaken te behandelen binnen het gerecht verduidelijkt de spreker dat het federaal parket, dat bevoegd is inzake georganiseerde misdaad, door het College van procureurs-generaal werd verzocht om voorrang te geven aan de aanvallen op kritieke infrastructuur en aan de zogenaamde *alpha cases*, dat zijn de dossiers waarin een nieuwe *modus operandi* wordt gehanteerd. Het federaal parket is overigens medevoorzitter van het expertisenetwerk cybercriminaliteit, dat ermee belast is instructies uit te werken ten behoeve van de magistratuur.

Une *Cyber Unit* a été constituée au sein du parquet fédéral. Elle compte pour l'instant trois magistrats qui ont bénéficié d'une formation avancée et devrait bénéficier d'ici 2022 d'un élargissement de cadre pour 2 magistrats supplémentaires. Dans l'attente de cet élargissement de cadre, deux autres magistrats du parquet fédéral ont été détachés pour renforcer l'unité. Il est évident toutefois que le parquet fédéral ne peut pas tout gérer: il se concentre par conséquent sur les attaques relatives aux infrastructures critiques. Dès lors, l'intervenant plaide pour qu'au moins un magistrat se spécialise au niveau des parquets locaux de manière à gérer les attaques de moindre importance. Ce magistrat, qui doit être formé, devrait – outre ses propres tâches opérationnelles – venir en soutien de ses collègues confrontés à des dossiers plus techniques. Le même effort devrait être fourni au niveau des parquets généraux.

Par ailleurs, l'intervenant – qui dispense une formation en cybercriminalité dans le cadre des formations données au sein de l'Institut de formation judiciaire – constate qu'il y a encore trop peu d'intérêt pour cette matière de la part de la magistrature assise. Ceci est évidemment problématique lorsqu'ils sont amenés à connaître de dossiers complexes. Il insiste également sur la nécessité de disposer de juges d'instruction spécialisés en matière de cybercriminalité.

Compte tenu de la fragmentation des traces et des informations disponibles entre les services de police et de renseignement, il est en outre essentiel d'approfondir la collaboration internationale. Le parquet fédéral est très actif au niveau d'Eurojust au sein duquel un groupe de travail a d'ailleurs été créé.

D'autres pistes de collaboration devraient être poursuivies comme la désignation d'officiers de liaison dédiés à cette problématique et notamment auprès de la *Joint Cybercrime Action Taskforce* (J-CAT) créée en 2014 au sein de Europol.

Enfin, l'intervenant se réfère à la jurisprudence récente de la Cour constitutionnelle et plaide en faveur de l'élaboration d'une loi solide en matière de rétention des données. Il rappelle en effet que dans les enquêtes liées à la cybercriminalité, les seules preuves dont on dispose sont les données. Il lui paraît donc nécessaire de réfléchir à un juste équilibre entre le droit fondamental au respect de la vie privée et l'efficacité de la lutte contre la cybercriminalité et la criminalité de droit commun présentant une composante numérique. Certes, on doit prévoir des contrôles juridictionnels entourant l'utilisation de ces données, mais en limiter l'accès de manière excessive a un impact important sur l'efficacité des recherches et des poursuites. Il ne sert à rien de

Binnen het federaal parket werd een *Cyber Unit* opgericht. Die telt thans drie magistraten met een doorgedreven opleiding in cyberzaken en tegen 2022 zou het personeelsbestand met 2 extra magistraten moeten worden uitgebreid. In afwachting daarvan werden twee magistraten van het federaal parket gedetacheerd om de *Cyber Unit* te versterken. Het ligt evenwel voor de hand dat het federaal parket niet alles kan beheren en daarom spitst het zich toe op de aanvallen op kritieke infrastructuur. Zodoende roept de spreker op om binnen de lokale parketten te voorzien in minstens één gespecialiseerde magistraat om de minder belangrijke aanvallen te behandelen. Die daartoe opgeleide magistraat zou – naast zijn eigen operationele taken – tevens zijn collega's moeten bijstaan wanneer zij te maken hebben met dossiers met een meer technische inslag. Binnen de algemene parketten zou dezelfde inspanning moeten worden geleverd.

Voorts wijst de spreker (die een opleiding cybercriminaliteit verstrekt binnen het Instituut voor gerechtelijke opleiding) erop dat de zittende magistratuur daarvoor nog te weinig interesse toont. Het ligt voor de hand dat dit problemen geeft zodra zij met complexe dossiers te maken zal krijgen. De spreker benadrukt dat men ook over in cybercriminaliteit gespecialiseerde onderzoeksrechters zou moeten kunnen beschikken.

Daar vaak sprake is van versnippering van de beschikbare sporen en informatie tussen de politie- en inlichtingendiensten, komt het er voorts op aan meer in te zetten op internationale samenwerking. Het federaal parket is erg actief binnen Eurojust, waarbinnen trouwens een werkgroep werd opgericht.

Andere mogelijkheden tot samenwerking zouden moeten worden nagestreefd, zoals de aanwijzing van verbindingsofficieren die zich op die aangelegenheid toeleggen, met name bij de in 2014 binnen Europol opgerichte *Joint Cybercrime Action Taskforce* (J-CAT).

Tot slot verwijst de spreker naar de recente rechtspraak van het Grondwettelijk Hof en hij roept op tot de uitwerking van een degelijke wet betreffende het bewaren van gegevens. Hij wijst erop dat in onderzoeken naar cybercriminaliteit gegevens het enige bewijsmateriaal zijn. Zodoende moet worden nagedacht over een redelijk evenwicht tussen het grondrecht op eerbiediging van de persoonlijke levenssfeer en de doeltreffendheid van het bestrijden van cybercriminaliteit en van misdrijven van gemeen recht met een digitale component. Het lijdt geen twijfel dat er gerechtelijke controles moeten zijn op het gebruik van die gegevens, maar de toegang ertoe buitensporig beperken heeft aanzienlijke gevolgen voor de doeltreffendheid van de onderzoeken en van

prévoir que certains crimes sont imprescriptibles, si la justice ne peut accéder aux données nécessaires que pendant une durée extrêmement limitée.

4. ***Exposé introductif de Mme Leen Depuydt et M. Piet Pieters, représentants du Centre de Crise National (NCCN)***

*Mme Leen Depuydt* précise que les travaux du NCCN sont organisés selon le cycle du risque. Il s'agit d'un processus cyclique composé de plusieurs étapes qui se répètent chacune systématiquement.

L'identification des risques potentiels est effectuée par le NCCN sur la base de l'identification nationale des risques. La phase suivante est la phase de prévention, qui a pour but de traiter le plus grand nombre possible de risques préalablement identifiés afin de prendre des mesures pour empêcher les risques de se concrétiser. Dans ce cas, la responsabilité incombe à ceux qui exercent l'activité qui comporte des risques potentiels. Il s'agit des entreprises, des organisations et des secteurs. Il leur incombe dès lors de limiter ou d'éliminer le plus de risques possible lors de cette phase de prévention.

Il est évidemment impossible d'éliminer tous les risques en faisant de la prévention et il est nécessaire de se préparer minutieusement à toute situation qui pourrait encore mal tourner. Cette préparation, qui permet de faire face à ces risques résiduels, s'appelle la planification d'urgence. La planification d'urgence est l'ensemble des mesures, procédures, outils et mécanismes de coordination qui permettent de prendre des mesures cohérentes en cas de situation d'urgence. L'objectif étant de pouvoir mobiliser les moyens humains et matériels nécessaires pour préparer la gestion de cette situation d'urgence. La planification d'urgence va donc bien au-delà de la simple élaboration de plans d'urgence en tant que tels et correspond à tous les systèmes qui l'entourent.

Le NCCN coordonne la planification d'urgence nationale et collabore étroitement avec les différents secteurs à cette fin. En ce qui concerne les incidents télécom et les cyberincidents, le NCCN collabore avec l'Institut belge des services postaux et des télécommunications (IBPT) et le Centre pour la cybersécurité Belgique (CCB).

Un risque qui conduit à une situation d'urgence réelle marque le début de la phase de gestion de crise. Les plans d'urgence sont alors activés et les structures de crise sont mobilisées. De cette manière, on tente de mettre rapidement de l'ordre dans le chaos et de revenir rapidement à une situation normale.

de vervolgingen. Erin voorzien dat bepaalde misdrijven niet voor verjaring vatbaar zijn heeft weinig zin indien het gerecht slechts gedurende een erg korte termijn toegang heeft tot de nodige gegevens.

4. ***Inleidende uiteenzetting van mevrouw Leen Depuydt en de heer Piet Pieters, vertegenwoordigers van het Nationaal Crisiscentrum (NCCN)***

*Mevrouw Leen Depuydt* verduidelijkt dat de werkzaamheden van het NCCN worden georganiseerd aan de hand van de risicocyclus. Dit is een cyclisch proces waarbinnen verschillende stappen telkens opnieuw doorlopen worden.

Het identificeren van mogelijke risico's gebeurt door het NCCN aan de hand van de nationale risico-identificatie. De volgende fase is de preventiefase, waarin zoveel mogelijk van deze geïdentificeerde risico's aangepakt worden en waarbij maatregelen kunnen genomen worden om zoveel mogelijk te vermijden dat risico's zich voltrekken. Hierbij ligt de verantwoordelijkheid bij diegene die de activiteit, die mogelijke risico's inhoudt, uitvoert. Dit zijn dus de bedrijven, de organisaties en de sectoren. Zij zijn dus verantwoordelijk om in deze fase zoveel mogelijk risico's te beperken of weg te nemen.

Uiteraard is het onmogelijk om elk risico door middel van preventie weg te nemen en is er nood aan een gedegen voorbereiding op alles wat alsnog kan foutlopen. Deze voorbereiding op de aanpak van deze restrisico's is de noodplanning. De noodplanning is het geheel van maatregelen, procedures, instrumenten en coördinatiemechanismen die toelaten om tijdens de noodsituatie consequent op te treden. Het doel daarvan is om de menselijke en materiële middelen die noodzakelijk zijn voor het beheer van die noodsituatie voor te bereiden. De noodplanning gaat dus veel verder dan het noodplan zelf. Het zijn al de systemen errond.

Het NCCN coördineert de nationale noodplanning, en werkt hiervoor nauw samen met de verschillende sectoren. Voor wat betreft telecom- en cyberincidenten, gebeurt dit met het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT) en het Centrum voor Cybersecurity België (CCB).

Wanneer een risico toch tot een effectieve noodsituatie leidt, komt men in de fase van het crisisbeheer. Op dat moment worden de noodplannen geactiveerd, en worden de crisisstructuren gemobiliseerd. Zo tracht men snel orde te brengen in de chaos en snel terug te keren naar een normale toestand.

Chaque situation d'urgence et chaque exercice sont ensuite évalués de manière approfondie avec tous les partenaires concernés. Cela permet de tirer les leçons nécessaires afin de les mettre en œuvre par la suite à chaque étape du cycle du risque. Il s'agit donc d'un processus d'amélioration continu qui a pour but de renforcer le système pour mieux affronter la prochaine situation d'urgence.

La dépendance de la société envers les réseaux de télécommunication et les cyber-réseaux ne cesse de croître. Il faut donc s'attendre à être confrontés à des cyberattaques de plus en plus récurrentes à l'avenir. Cependant, en cas d'autres incidents, il conviendra également de vérifier systématiquement si une cyber-attaque n'est pas à l'origine d'une situation d'urgence, surtout dans le cas des incidents télécom.

*M. Piet Pieters* développe ensuite la première phase du cycle du risque: l'identification et l'analyse des risques. Le NCCN est responsable de la coordination de l'analyse des risques nationaux. Dans ce contexte, la *Belgian National Risk Assessment* 2018-2023 a été mise sur pied et compte plus de 100 experts issus de 40 services publics. Cette identification des risques considère la cyberespace comme l'un des principaux groupes à risque auxquels notre pays sera confronté dans les années à venir. En outre, le cyberrisque a été identifié par le NCCN et ses services partenaires comme l'un des vecteurs prioritaires de la menace hybride.

L'évaluation des risques est un processus continu et cyclique. Il est donc essentiel de conserver une vision large et continue de la société et de l'avenir. En effet, la société actuelle est un environnement qui évolue à un rythme effréné, avec de nombreuses incertitudes, et qui est devenu plus complexe que jamais. Les changements sont de moins en moins prévisibles, peuvent engendrer de graves conséquences et se produisent toujours plus rapidement, notamment sous l'influence des évolutions technologiques.

La complexité et les interdépendances inhérentes à un environnement numérique en évolution rapide augmentent sous l'influence des nouvelles technologies, comme la 5G, l'intelligence artificielle, l'Internet des objets, le *cloud computing*, et cetera. Les cyberrisques font bien sûr également partie de la catégorie des nouveaux risques "émergents", qui nécessitent une attention particulière. L'identification et l'analyse des risques potentiels constituent la base des phases suivantes du cycle du risque, telles que la prise ou la recommandation de mesures d'atténuation et de préparation.

Elke noodsituatie en elke oefening wordt vervolgens grondig geëvalueerd met alle betrokken partners. Zo kunnen nadien de nodige lessen getrokken worden om nadien ook geïmplementeerd te worden in elke etappe van de risicocyclus. Dit is dus een continu proces van verbeteringen om zo sterker te staan voor de volgende noodsituatie.

De maatschappelijke afhankelijkheid van telecom en cybernetwerken wordt steeds groter. Het valt dus te verwachten dat we in de toekomst steeds vaker zullen geconfronteerd worden met directe cyberaanvallen. Maar ook bij andere incidenten zal steeds moeten worden nagegaan of een cyberaanval niet aan de oorsprong ligt van een noodsituatie. In het geval van telecomincidenten is dit zeker het geval.

*De heer Piet Pieters* gaat vervolgens verder in op de eerste fase van de risicocyclus. Hierbij gaat het om de identificatie en de analyse van de risico's. Het NCCN staat in voor de coördinatie op het vlak van nationale risicoanalyse. In dit kader werd De Belgische Nationale Risicobeoordeling 2018-2023 uitgevoerd met meer dan 100 experten uit 40 overheidsdiensten. Deze risico-identificatie beschouwt cyber als één van de belangrijkste risicoclusters waarmee ons land de komende jaren geconfronteerd zal worden. Bovendien werd het cyberrisico door het NCCN en zijn partnerdiensten geïdentificeerd als één van de prioritaire vectoren van de hybride dreiging.

De risicobeoordeling is een continu en cyclisch proces. Daarom is het van essentieel belang om een brede en continue blik op de samenleving, en op de toekomst aan te houden. De huidige samenleving is immers een snel veranderende omgeving, met vele onzekerheden, die complexer is dan ooit tevoren. Veranderingen zijn steeds minder voorspelbaar, kunnen ernstige(re) gevolgen met zich meebrengen en stellen zich steeds sneller, mede onder invloed van technologische ontwikkelingen.

De complexiteit en de interdependenties in de snel veranderende digitale omgeving nemen toe onder invloed van nieuwe technologieën zoals 5G, artificiële intelligentie, het *internet of things*, *cloud computing*, enzovoort. Cyberrisico's maken bij uitstek ook deel uit van de categorie nieuwe "*emerging*" risico's, die een bijzondere aandacht vergen. Het identificeren en analyseren van mogelijke risico's is de basis voor de volgende fases van de risicocyclus zoals het nemen of adviseren tot het nemen van mitigerende en voorbereidende maatregelen.

Une attention toute particulière doit être accordée au maintien des organisations d'intérêt vital pour la société. Le NCCN est le coordinateur national pour la protection et la sécurité des infrastructures critiques. À cette fin, il collabore avec le CCB sur la politique en matière de cybersécurité à l'égard des opérateurs de services essentiels.

M. Pieters souligne que, dans les années à venir, il sera primordial d'identifier les interdépendances des secteurs vitaux afin de pouvoir proposer des mesures ciblées permettant d'accroître la résilience de ces derniers. Ces analyses des interdépendances revêtiront une importance capitale compte tenu de la rapidité avec laquelle ces secteurs effectuent leur transformation numérique. En particulier, l'émergence de la 5G, outre les opportunités qu'elle offrira, s'accompagnera également de nombreux défis. L'interdépendance croissante et la dépendance accrue à l'égard de cette technologie augmentent la vulnérabilité des secteurs vitaux, d'où la nécessité d'organiser des analyses de risques sectorielles approfondies. Cela devra permettre d'identifier les conséquences de cette nouvelle technologie.

M. Pieters indique en outre que les mêmes évolutions sociales et la numérisation rapide de la société sont également prises en compte dans les législations internationales. Par exemple, en décembre 2020, la Commission européenne a annoncé sa nouvelle stratégie de cybersécurité. Dans le cadre de cette nouvelle stratégie, deux nouvelles initiatives législatives sont proposées dans le but d'accroître la résilience des entités critiques et essentielles face aux cyberrisques ainsi qu'aux autres types de risques. La directive sur la résilience des entités critiques (CER) et la directive révisée sur la sécurité des réseaux et des systèmes d'information (SRI2) feront évoluer le cadre législatif actuel concernant les infrastructures critiques et les opérateurs de services essentiels en fonction des développements sociétaux tels que l'interdépendance croissante entre le monde physique et le monde numérique. La politique basée sur la sécurité et la protection devra dès lors évoluer vers une politique axée sur la résilience des secteurs et des entités. L'annonce conjointe s'inscrit dans la vision ayant pour but de mettre en place une synergie maximale entre les deux mondes.

Le NCCN accueille favorablement ces initiatives européennes. Ces dernières confirment et renforcent les initiatives que la Belgique avait déjà entreprises. L'évolution annoncée vers une approche fondée sur tous les types de risques a déjà été amorcée en Belgique depuis quelques années. Avec l'arrivée de la directive SRI, la législation relative à la sécurité et la protection des infrastructures critiques a également été modifiée. Nous observons désormais la même tendance au

Bijzondere aandacht dient te worden besteed aan de continuïteit van de vitale dienstverlening ten aanzien van de samenleving. Het NCCN is de nationale coördinator inzake de bescherming en beveiliging van de kritieke infrastructuren. Het werkt hiervoor samen met het CCB voor het beleid op vlak van cyberveiligheid ten aanzien van aanbieders van essentiële diensten.

De heer Pieters benadrukt dat het de komende jaren van belang zal zijn om de onderlinge afhankelijkheden van vitale sectoren in kaart te brengen en zo gerichte maatregelen te kunnen voorstellen ter verhoging van de weerbaarheid. Deze analyses naar interdependenties zullen extra belangrijk zijn gelet op de snelle digitalisering in deze sectoren. Met name de komst van 5G-technologie zal, naast meerdere opportuniteiten, ook vele uitdagingen met zich meebrengen. Een toenemende interdependentie en een hogere afhankelijkheid van deze technologie impliceren een verhoogde kwetsbaarheid in de vitale sectoren en dringen dus de nood op tot het organiseren van grondige sectorale risicoanalyses. Dit zal moeten toelaten om de impact van deze nieuwe technologie in kaart te brengen.

De heer Pieters geeft verder aan dat men ook op het vlak van internationale wetgeving rekening houdt met dezelfde maatschappelijke evoluties en de snelle digitalisering van de samenleving. Zo kondigde de Europese Commissie in december 2020 haar nieuwe cybersecuritystrategie aan. Binnen deze nieuwe strategie worden twee nieuwe wetgevende initiatieven voorgesteld met als doel het verhogen van de weerbaarheid van kritieke en essentiële entiteiten ten aanzien van cyber- en andere risico's. Met de *Critical Entity Resilience* (CER) en de tweede *Network and Informations Systems* (NIS2) richtlijn zal het huidige wetgevende kader inzake kritieke infrastructuur en aanbieders van essentiële diensten mee evolueren met de maatschappelijke ontwikkelingen zoals de steeds grotere verwevenheid van het fysieke en het digitale domein. Dit brengt een evolutie met zich mee van een beleid geënt op beveiliging en bescherming naar een beleid gericht op veerkrachtige sectoren en entiteiten. De gezamenlijke aankondiging kadert binnen de visie om maximale synergie te organiseren voor beide domeinen.

Het NCCN verwelkomt deze Europese initiatieven. Voor België bevestigt en versterkt dit wat eigenlijk reeds op eigen initiatief was ingezet. De aangekondigde evolutie naar een alle risico's benadering werd in België reeds enkele jaren gelden opgestart. Met de komst van de NIS-wet werd ook de wetgeving betreffende beveiliging en de bescherming van de kritieke infrastructuren gewijzigd. Dezelfde tendens krijgen we nu ook op Europees niveau. Het gaat om een coherent en geïntegreerd beleid ten

niveau européen. Il s'agit d'une politique cohérente et intégrée concernant les secteurs critiques et essentiels. L'influence de ces nouveaux cadres législatifs permettra de poursuivre ce changement dans les années à venir.

*Mme Leen Depuydt* indique ensuite que la méthode de travail n'est pas seulement basée sur la législation européenne, mais aussi sur les sept exigences de base de l'OTAN. Il s'agit de sept exigences de base que les États membres de l'OTAN doivent respecter pour accroître la résilience de la société – autorités, citoyens et entreprises – face à des chocs majeurs ou des situations de crise. L'une de ces exigences de base est la nécessité de prévoir la résilience des systèmes de communication civils. Les réseaux de télécommunications et les cyberréseaux doivent également continuer de fonctionner, même en situation de crise. C'est pourquoi il est essentiel de disposer d'une capacité de secours suffisante.

Dans le cadre de cette exigence, le NCCN assume un rôle de coordination et collabore avec les autorités sectorielles afin de renforcer la résilience belge. En 2019, ces exigences de base ont été mises à jour par l'OTAN et une attention particulière a été accordée à la nécessité de disposer de réseaux 5G robustes. Les 7 exigences de base donnent les grandes orientations en matière de prévention et sont également prises en compte dans l'élaboration des plans d'urgence.

L'intervenante poursuit en évoquant les différents plans d'urgence. Ils dépendent des autorités ou de l'institution responsable de leur élaboration. Concrètement, il existe trois grands niveaux: local, provincial et fédéral. Au niveau fédéral, le NCCN est chargé des plans d'urgence nationaux. À leur niveau, les bourgmestres et les gouverneurs sont chargés d'élaborer les plans d'urgence et d'intervention multidisciplinaires. En outre, les différents services d'intervention disposent également de plans d'urgence monodisciplinaires d'intervention des disciplines. Le plus connu d'entre eux est le plan d'intervention médicale (PIM). Il est important d'assurer la coordination de tous ces plans afin qu'ils puissent être mis en œuvre et fonctionner simultanément.

Outre ces plans d'urgence, des plans d'urgence internes sont également élaborés par les entreprises et les entités dont les activités comportent un risque, ou qui ont un public vulnérable, comme pour les entreprises Seveso.

Le NCCN a également identifié plusieurs nouveaux types de plans d'urgence ces dernières années. Ceux-ci doivent encore être insérés dans le cadre réglementaire, mais leur nécessité a déjà été établie dans la pratique. Cela s'explique notamment par la régionalisation d'un

aanzien van de kritieke en essentiële sectoren. Deze kentering zal ook nog komende jaren kunnen doorgezet worden onder invloed van die nieuwe wetgevende kaders.

*Mevrouw Leen Depuydt* geeft vervolgens aan dat de manier van werken naast de Europese wetgeving ook gebaseerd is op de 7 *baseline requirements* van de NAVO. Dit zijn 7 basisvereisten waaraan de NAVO-lidstaten moeten voldoen om de weerbaarheid van de maatschappij – de overheid, de burgers en de bedrijven – te verhogen bij ontwrichtende gebeurtenissen of crisissituaties. Eén van deze basisvereisten is de vereiste om te voorzien in veerkrachtige civiele communicatiesystemen. Telecommunicatie en cybernetwerken moeten ook onder crisisomstandigheden kunnen functioneren. Hierbij is voldoende back-upcapaciteit cruciaal.

In het kader van deze vereiste neemt het NCCN een coördinerende rol op en werkt het samen met de sectorale overheden om de Belgische weerbaarheid te verhogen. In 2019 werden deze *baseline requirements* nog geactualiseerd door de NAVO en werd bijzondere nadruk gelegd op de nood aan robuuste 5G-netwerken. De 7 *baseline requirements* zijn richtinggevend op vlak van preventie en worden ook meegenomen in de opmaak van de noodplannen.

De spreekster gaat verder in op de soorten noodplannen. Dit is afhankelijk van de overheid of de instelling die verantwoordelijk is voor de opstelling ervan. Concreet zijn er drie grote niveaus: het lokaal, het provinciaal en het federaal niveau. Op federaal niveau is het NCCN verantwoordelijk voor de nationale noodplannen. De burgemeesters en gouverneurs zijn op hun niveau verantwoordelijk voor het opstellen van multidisciplinaire nood- en interventieplannen. Daarnaast zijn er nog de disciplines, de verschillende interventiediensten, die zelf ook monodisciplinaire noodplannen hebben. De bekendste daarvan is het medisch interventieplan (MIP). Het is belangrijk dat al deze plannen op elkaar zijn afgestemd. Ze moeten samen kunnen werken en samen opereren.

Naast deze noodplannen worden er ook interne noodplannen opgesteld door bedrijven en entiteiten waarvan de activiteiten een risico inhouden, of die bijvoorbeeld een kwetsbaar publiek hebben. Een voorbeeld daarvan zijn de Seveso-bedrijven.

Binnen het NCCN werden de afgelopen jaren ook een aantal nieuwe types noodplannen geïdentificeerd. Deze moeten in het regelgevend kader nog worden geconcretiseerd, maar de noodzaak ervan is reeds in de praktijk vastgesteld. Dit onder meer door de regionalisering van

grand nombre de compétences. Il s'agit donc de plans d'urgence sectoriels.

À l'avenir, le NCCN souhaiterait soutenir encore davantage les secteurs en les encourageant à élaborer de tels plans d'urgence afin qu'ils soient mieux préparés à gérer un incident. Ils pourront également mieux contribuer, par ce biais, à la gestion des crises au niveau national.

Mme Depuydt précise également que la planification d'urgence nationale est réalisée sur la base de l'analyse de risques nationale. Cependant, il n'est pas prévu d'élaborer un plan d'urgence spécifique distinct pour chaque risque identifié. Le NCCN a adopté une approche fondée sur tous les types de risques dans le but de gérer les crises nationales en ayant recours autant que possible à la même structure de base. Cette structure de base est actuellement décrite dans l'arrêté royal du 31 janvier 2003 portant fixation du plan d'urgence pour les événements et situations de crise nécessitant une coordination ou une gestion à l'échelon national. Ce cadre réglementaire fera prochainement l'objet d'une réforme.

L'objectif est de développer les automatismes nécessaires, surtout compte tenu du fait qu'il n'est pas toujours évident de déterminer le type de crise dont il s'agit lorsqu'une situation d'urgence éclate. Cependant, il est important d'organiser la gestion de crise différemment pour un nombre déterminé de risques. Un plan particulier d'urgence et d'intervention (PPUI) est élaboré pour la gestion de ce type de risques. Le plan national d'urgence nucléaire ou le cyberplan d'urgence en sont des exemples concrets.

Ce cyberplan d'urgence est particulier, car il ne comporte aucun lien, comme c'est le cas habituellement, avec les autorités locales. Il n'y a pas d'urgence physique, car celle-ci se déroule dans le monde numérique. Par conséquent, aucun lien n'est établi entre le niveau national, le gouverneur et les autorités locales. Ce plan distingue différents niveaux d'incidents.

Au niveau le plus élevé figure la crise nationale de cybersécurité. Il s'agit de tout événement de cybersécurité qui, par sa nature ou ses conséquences, menace les intérêts vitaux du pays ou les besoins essentiels de la population, nécessite une prise de décision urgente et implique le déploiement de différents services et organismes. Citons, par exemple, les cyberattaques sur des systèmes critiques d'infrastructures critiques ou des fuites d'informations classifiées qui mettent en danger les intérêts vitaux du pays.

Le deuxième niveau est l'incident national de cybersécurité. Il s'agit, dans ce cas, d'un événement de

heel wat bevoegdheden. Het gaat dus om sectorale noodplannen.

In de toekomst zou het NCCN nog meer ondersteuning aan sectoren willen geven door hen aan te moedigen zulke noodplannen op te stellen zodat zij beter voorbereid zijn op het beheer van een incident. Op die manier kunnen zijn ook een betere bijdrage leveren aan het nationale crisisbeheer.

Mevrouw Depuydt verduidelijkt verder dat de nationale noodplanning gebeurt op basis van de nationale risicoanalyse. Er wordt echter niet voor elk geïdentificeerd risico een apart specifiek noodplan opgesteld. Het NCCN werkt volgens een all risk approach waarbij het de bedoeling is om nationale crisissen zoveel mogelijk volgens dezelfde basisstructuur te beheren. Deze basisstructuur is momenteel beschreven in het koninklijk besluit van 31 januari 2003 tot vaststelling van het noodplan voor de crisisgebeurtenissen en -situaties die een coördinatie of een beheer op nationaal niveau vereisen. Dit regelgevend kader zal binnenkort worden herzien.

Het is de bedoeling om de nodige automatismen te ontwikkelen, vooral bij aanvang van een noodsituatie is niet altijd duidelijk om welke crisis het gaat. Voor een beperkt aantal risico's is het wel belangrijk om het crisisbeheer anders te organiseren. Voor deze risico's wordt dan een Bijzonder Nationaal Noodplan (BNIP) opgemaakt. Een voorbeeld daarvan is het nationaal nucleair noodplan, of het cybernoodplan.

Dit cybernoodplan is een bijzonder noodplan omdat de normale link met de lokale overheden er niet is. Er is geen fysieke noodsituatie, die speelt zich immers af in de digitale wereld. Er is dus geen link tussen het nationaal niveau, de gouverneur en de lokale overheden. Binnen dit plan worden verschillende niveaus van incidenten geïdentificeerd.

Het hoogste niveau is de nationale cybersecuritycrisis. Dat is elke cybersecuritygebeurtenis die wegens haar aard of gevolgen de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt, die een dringende besluitvorming vereist, en de inzet van verschillende departement en organismen vergt. Een voorbeeld hiervan zijn cyberaanvallen op kritische systemen van kritieke infrastructuren of lekken van geclassificeerde informatie die de vitale belangen van het land in gevaar brengen.

Het tweede niveau is een nationaal cybersecurityincident. In dit geval heeft een cybersecurity gebeurtenis

cybersécurité qui a des conséquences relativement limitées sur les intérêts vitaux du pays ou les besoins essentiels de la population. Il peut s'agir d'événements qui ont un impact négatif sur l'image de notre pays ou d'attaques DDoS de courte durée sur des sites internet publics d'autorités.

En dernier lieu, on retrouve les incidents de cybersécurité à petite échelle. Ce type d'événements ne rentrent pas dans le cadre des définitions données ci-dessus. Il peut s'agir d'une attaque sur les systèmes d'une entreprise qui n'appartient pas aux secteurs vitaux de notre pays.

Ensuite, l'intervenante explique le rôle du NCCN en cas de crise nationale de cybersécurité. Dans un tel cas de figure, la phase fédérale est déclenchée et le NCCN coordonne la gestion de la crise avec le CCB. Le NCCN bénéficie d'un soutien technique du CCB. Plusieurs cellules sont activées lors de cette phase. La cellule d'évaluation (Celeval) est présidée par le CCB avec les experts techniques. La tâche de cette cellule est de mettre en place une évaluation continue de la situation et, sur cette base, de préparer des avis techniques pour le Comité de coordination.

Le Comité de coordination est présidé par le NCCN en collaboration avec le CCB et sa mission principale consiste à prendre les mesures de précaution et de protection nécessaires pour limiter les conséquences et l'impact de la cybercrise sur les autres secteurs. Pour ce faire, ils se fondent sur l'expertise fournie par la cellule d'évaluation.

La troisième cellule est la cellule d'information. Cette dernière est activée pour rationaliser la communication de crise avec les différents porte-paroles de toutes les entités impliquées. Ce travail de communication est coordonné par les porte-paroles du NCCN.

Si un incident n'est pas considéré comme une crise nationale de cybersécurité, mais comme un incident de cybersécurité, le NCCN offre un appui au CCB qui coordonne la gestion de l'incident en question.

Mme Depuydt souligne que l'année écoulée nous a appris que la préparation aux cyberincidents et aux incidents de télécommunication figure, à juste titre, parmi les priorités du NCCN et de ses partenaires. En 2021, nous avons déjà connu deux incidents télécoms et une crise nationale de cybersécurité. Dès qu'un incident télécom survient, il faut aussi avoir le réflexe d'examiner la situation pour savoir si une cyberattaque est potentiellement à l'origine de cette situation d'urgence. Début janvier, un incident s'est produit sur le réseau Proximus, à la suite duquel les centres d'urgence dans plusieurs provinces n'étaient pas accessibles via les numéros d'urgence

eerder beperkte gevolgen voor de vitale belangen van het land of voor de essentiële behoeften van de bevolking. Voorbeelden hiervan zijn gebeurtenissen die een negatieve invloed hebben op het imago van ons land of DDoS-aanvallen van korte duur op publieke websites van overheden.

Tot slot zijn er de kleinschalige cybersecurityincidenten. Dit zijn gebeurtenissen die niet voldoen aan de bovenvermelde definities. Een voorbeeld daarvan is een aanval op de systemen van een bedrijf dat niet behoort tot de vitale sectoren van ons land.

De spreekster gaat dieper in op de rol van het NCCN bij een nationale cybersecuritycrisis. In dat geval wordt de federale fase afgekondigd en coördineert het NCCN samen met CCB het crisisbeheer. Het NCCN wordt daarbij technisch ondersteund door het CCB. Daarvoor worden verschillende cellen geactiveerd. De evaluatiecel (Celeval) wordt voorgezeten door het CCB samen met de technische experten. De taak van deze cel is een continue evaluatie van de situatie organiseren en op basis daarvan technische adviezen voorbereiden voor het coördinatiecomité.

Het coördinatiecomité wordt voorgezeten door het NCCN in samenwerking met het CCB en heeft als belangrijkste opdracht de nodige voorzorgs- en beschermingsmaatregelen te nemen om de gevolgen en de impact van de cybercrisis op andere sectoren te beperken. Zij doen dit op basis van de expertise die door de evaluatiecel wordt gegeven.

De derde cel is de infocel. Deze wordt geactiveerd om de crisiscommunicatie te stroomlijnen met verschillende woordvoerders van alle betrokken organisaties. Die werkzaamheden worden geleid door de woordvoerders van het NCCN.

Wanneer een incident niet wordt bepaald als nationaal cybersecuritycrisis maar als cybersecurityincident, dan biedt het NCCN zijn ondersteuning aan het CCB dat in dat geval het beheer van het incident coördineert.

Mevrouw Depuydt benadrukt dat het afgelopen jaar ons geleerd heeft dat voorbereiding op cyber- en telecomincidenten terecht één van de prioriteiten is van het NCCN en van de partners. In 2021 kenden we reeds twee telecomincidenten en één nationale cybersecuritycrisis. Bij elk telecomincident moet er ook telkens de reflex zijn om na te gaan of mogelijks een cyberaanval aan de basis ligt van zulke noodsituatie. Begin januari was er een incident op het netwerk van Proximus waardoor de noodcentrales in verschillende provincies op de nacht van 7 en 8 januari 2021 niet bereikbaar waren op de klassieke noodnummers 100-101-112. Het

classiques 100, 101 et 112 dans la nuit du 7 au 8 janvier 2021. Le deuxième incident a eu lieu le 1er avril 2021 et a été causé par l'effondrement partiel du toit d'un centre de données Telenet à Roeselare. Cet incident n'a pas eu d'impact direct sur les clients de Telenet, mais il a représenté malgré tout une menace. Si le toit s'était complètement effondré, les clients résidentiels et professionnels de Telenet dans toute la Flandre occidentale et dans une grande partie de la Flandre orientale auraient pu être fortement touchés.

Enfin, entre le 26 mars et le 27 mai 2021, nous avons été confrontés à la cybercrise lors de laquelle la phase fédérale a été déclenchée en raison de la cyberattaque menée contre le SPF Intérieur. La phase fédérale a été déclenchée afin de faire face à cette situation. Plusieurs réunions du Comité de coordination, de la cellule d'évaluation et de la cellule d'information ont été organisées. Le 27 mai 2021, la phase fédérale a été stoppée après évaluation de la situation, estimant qu'il s'agissait désormais d'un incident national de cybersécurité. Comme le cyberplan d'urgence le prévoit, la gestion de l'incident a ensuite été reprise par le CERT et le CCB.

Le NCCN a coordonné la gestion de crise lors de ces incidents. L'intervenante souligne que le NCCN n'est pas compétent pour résoudre l'origine de la crise, car il ne dispose pas de l'expertise suffisante pour mener à bien cette tâche, qui revient aux autorités sectorielles et aux opérateurs. Dans de tels cas, le NCCN s'efforce de limiter autant que possible l'impact social. Il s'agit de réunir les services adéquats autour de la table, de parvenir ensemble à une compréhension commune de la situation et d'apporter une réponse coordonnée sur cette base. Il s'agit de limiter au mieux les conséquences d'un incident sur le bon fonctionnement des services publics, des infrastructures critiques et de la société au sens large, et de revenir à une situation normale le plus rapidement possible.

Ces incidents font également l'objet d'une évaluation approfondie afin de tirer les leçons nécessaires à appliquer lors d'incidents ultérieurs. Les deux incidents de télécommunications nous ont appris que les services publics vitaux et les infrastructures critiques dépendent fortement du secteur des télécommunications et ne peuvent donc pas dépendre du fonctionnement d'un seul opérateur. À l'avenir, il est donc crucial que chacun de ces services et infrastructures dispose d'une redondance suffisante pour pouvoir assurer leur fonctionnement en cas d'incident télécom, même si les services d'un seul opérateur devaient être momentanément indisponibles.

Nous observons, en second lieu, que le NCCN incitera les secteurs à effectuer des analyses de risque et

tweede incident was op 1 april 2021. Dat kwam door de gedeeltelijke instorting van het dak van een datacenter van Telenet in Roeselare. Dit incident had niet meteen een impact op de klanten van Telenet, maar het was wel een dreiging. Indien het dak verder was ingestort zouden zowel de residentiële klanten als de businessklanten van Telenet in heel West-Vlaanderen en een groot deel van Oost-Vlaanderen potentieel een grote impact hiervan hebben ondervonden.

Ten slotte was er tussen 26 maart en 27 mei 2021 de cybercrisis waarbij de federale fase werd afgekondigd door de cyberaanval op de FOD Binnenlandse Zaken. De federale fase werd afgekondigd om alles in goede banen te leiden. Daarbij werden verschillende vergaderingen georganiseerd van het coördinatiecomité, de evaluatiecel en de infocel. Op 27 mei 2021 werd de fase opgeheven nadat werd geoordeeld dat de situatie was geëvolueerd tot een nationaal cybersecurityincident. Zoals in het cybernoodplan is bepaald werd het beheer op dat moment overgenomen door het CERT-CCB.

Bij deze incidenten werd het crisisbeheer gecoördineerd door het NCCN. De spreekster benadrukt dat het NCCN niet bevoegd is om de oorzaak van de crisis op te lossen, daarvoor hebben zij de expertise niet in huis. Daarvoor blijven de sectorale overheden en de operatoren zelf bevoegd. De focus van het NCCN ligt in dergelijke gevallen op de maatschappelijke impact die zoveel mogelijk wordt beperkt. Dit gebeurt door de juiste diensten rond de tafel te brengen, door samen een gemeenschappelijk beeld te krijgen van de situatie en door op basis daarvan op een gecoördineerde wijze te reageren. Dit om de gevolgen van een incident voor de continuïteit van overheden, kritieke infrastructuren en de maatschappij in zijn geheel zoveel mogelijk te beperken en zo snel mogelijk terug te keren naar een normale toestand.

Dergelijke incidenten worden ook grondig geëvalueerd en hierbij worden achteraf ook de nodige lessen getrokken. De twee telecomincidenten leerden ons dat vitale overheidsdiensten en kritieke infrastructuren erg afhankelijke zijn van telecom en dus onmogelijk kunnen steunen op de werking van één enkele operator. Naar de toekomst toe is het dus cruciaal dat voor elk van deze diensten en infrastructuren voldoende redundantie wordt ingebouwd zodat zijn kunnen blijven functioneren tijdens een telecomincident. Ook wanneer de diensten van één operator niet beschikbaar zouden zijn.

Een tweede vaststelling is dat het NCCN de sectoren zal sensibiliseren om risico- en impactanalyses

d'impact afin d'avoir une meilleure idée des faiblesses de ces secteurs en cas de disponibilité limitée des services de télécommunications. Ainsi, chaque secteur peut prendre des mesures dans les limites de ses propres compétences afin de garantir une meilleure résilience face aux incidents télécoms. En outre, le secteur des télécommunications lui-même doit être mieux préparé à de tels incidents. Un plan d'urgence sectoriel doit être élaboré à cette fin.

Ces incidents ont également montré que les budgets ne prévoient pas les dépenses nécessaires pour assurer le fonctionnement opérationnel du NCCN, en particulier pour la gestion des crises au niveau fédéral. L'intervenante souligne que l'existence même du NCCN dépend de ces ressources opérationnelles, qui sont donc vitales pour la planification d'urgence et la gestion de crise. Dès lors, elle estime qu'il est effectivement nécessaire de prévoir un budget spécifiquement dédié à la gestion de crise.

Ces incidents ont, une fois de plus, prouvé l'utilité et les possibilités qu'offrent les plateformes telles que Be-Alert et ICMS. Ces outils de gestion de crise ont été développés par le NCCN et permettent respectivement d'informer la population et d'échanger des informations entre les différents acteurs de la gestion de crise multidisciplinaire.

En conclusion, *M. Piet Pieters* indique que le NCCN s'inscrit dans la stratégie nationale de cybersécurité, qui a été approuvée très récemment par le Conseil des ministres, et qu'il maintiendra donc à l'avenir son engagement dans le domaine de l'identification et de l'analyse des risques cyber et technologiques actuels et émergents, notamment ceux liés au déploiement de la 5G.

La nouvelle stratégie européenne en matière de cybersécurité et les évolutions de la politique concernant les entités critiques influenceront la poursuite du travail de renforcement de la résilience des services vitaux pour la société, ainsi que des services partenaires dans les secteurs vitaux, face aux risques cyber, technologiques, et autres.

*Mme Leen Depuydt* indique également que le NCCN continuera à aider le secteur des télécommunications en élaborant des préparatifs de gestion des incidents de télécommunication et en intégrant ces préparatifs dans un plan d'urgence sectoriel. Le NCCN sensibilisera également les secteurs à la réalisation d'analyses de risque et d'impact afin de détecter les faiblesses de ces secteurs en matière de disponibilité limitée des services de télécommunications.

uit te voeren om zo een beter zicht te krijgen op de kwetsbaarheden binnen deze sectoren bij een beperkte beschikbaarheid van telecomdiensten. Op die manier kan iedere sector binnen zijn eigen bevoegdheden maatregelen treffen die een grotere weerbaarheid tegen telecomincidenten moet garanderen. Daarnaast moet ook de telecomsector zelf beter voorbereid moeten zijn op dergelijke incidenten. Een sectoraal noodplan moet hiervoor worden opgesteld.

Deze incidenten hebben ook aangetoond dat niet in de budgetten voorzien is voor de noodzakelijke uitgaven voor de operationele werking van het NCCN, in het bijzonder voor het beheer van crisissen op federaal niveau. De spreekster benadrukt dat, aangezien deze operationele uitgaven de kern van het bestaan van het NCCN vormen, en dus van vitaal belang zijn voor noodplanning en crisisbeheer, een specifiek budget voor crisisbeheer echt wel noodzakelijk is.

Door deze incidenten werd nogmaals het nut en de mogelijkheden bewezen van platformen als Be-Alert en ICMS. Deze instrumenten voor crisisbeheer werden ontwikkeld door het NCCN en dienen om respectievelijk de bevolking te informeren of om informatie uit te wisselen tussen de verschillende actoren van het multidisciplinair crisisbeheer.

Tot besluit stelt *de heer Piet Pieters* dat het NCCN zich inschrijft in de nationale cyberstrategie zoals die zeer recent door de Ministerraad werd goedgekeurd, en zich in de toekomst dan ook zal blijven engageren op het vlak van identificatie en analyse van huidige en nieuwe emerging cyber- en technologische risico's zoals met name de risico's verbonden aan de uitrol van 5G.

Onder meer onder invloed van de nieuwe Europese cybersecuritystrategie en van de evoluties van het beleid op het vlak van de kritieke entiteiten, zal worden verder gewerkt op de blijvend verhogen van de weerbaarheid van de maatschappelijke dienstverlening, samen met de partnerdiensten in de vitale sectoren, ten aanzien van cyber-, technologische maar ook andere risico's.

*Mevrouw Leen Depuydt* geeft nog aan dat het NCCN de telecomsector blijvend zal ondersteunen bij het ontwikkelen van het beheer van telecomincidenten en het integreren van deze voorbereidingen in een sectoraal noodplan. Het NCCN zal ook de sectoren sensibiliseren om risico- en impactanalyses uit te voeren en zo de kwetsbaarheden binnen deze sectoren voor beperkte beschikbaarheid van telecomdiensten, te detecteren.

5. ***Exposé introductif de M. Michaël De Laet, représentant de la Federal Computer Crime Unit (FCCU) de la Police Fédérale***

*M. Michaël De Laet* précise que son unité, la FCCU, fait partie de la direction de la lutte contre la criminalité grave et organisée. La cybercriminalité est donc une forme de criminalité organisée. Les missions de l'unité consistent notamment à soutenir les enquêtes d'autres services en menant des enquêtes spécialisées dans les environnements numériques. Cette unité est également le point de contact unique pour l'échange d'informations au niveau international dans ce domaine. Elle développe également une expertise en la matière, en particulier concernant l'Internet des objets, le *darkweb* et les cryptomonnaies, mais aussi la lutte contre la cybercriminalité au sein d'environnements complexes.

L'arrêté royal du 23 juin 2019 exécutant l'article 102, alinéa 2, 4°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux détermine le rôle de cette unité. Il prévoit spécifiquement que la FCCU est chargée de la lutte contre la cybercriminalité organisée.

Outre la FCCU, il existe également 14 RCCU. Chaque arrondissement judiciaire dispose de sa propre *Computer Crime Unit* dont les missions sont similaires, mais destinées à un public cible différent ou pour des faits différents. Elles fournissent également un appui forensique dans le domaine du numérique, mais uniquement pour les services de police qui se trouvent dans leur arrondissement judiciaire. Les RCCU mènent leurs propres enquêtes en matière de cybercriminalité, qui sont soit organisées localement, soit de moindre envergure et moins complexes.

Les cybercrimes qui font l'objet de poursuites figurent dans la loi du 28 novembre 2000 relative à la criminalité informatique. Il s'agit du faux en informatique (article 210*bis* du Code pénal), de la fraude informatique (article 504*quater* du Code pénal), du *hacking* (article 550*bis* du Code pénal) et du sabotage de données (article 550*ter* du Code pénal). Pour les auteurs de ces cybercrimes, les technologies numériques constituent à la fois le moyen et la fin, par opposition à la criminalité informatique au sens large qui utilise les technologies numériques pour commettre d'autres crimes.

L'intervenant précise que l'accent est mis sur la collecte de preuves en vue d'identifier et de poursuivre les auteurs. La police doit jouer un rôle de répression afin de pouvoir attraper les coupables. Cet élément est très important dans l'approche intégrée. Si la prévention et la réparation des dommages revêtent une importance

5. ***Inleidende uiteenzetting van de heer Michaël De Laet, vertegenwoordiger van de Federal Computer Crime Unit (FCCU) van de Federale Politie***

*De heer Michaël De Laet* verduidelijkt dat zijn eenheid, de FCCU, deel uitmaakt van de directie die instaat voor de opvolging van de zware en georganiseerde criminaliteit. Cybercriminaliteit maakt dus deel uit van de georganiseerde criminaliteitsvormen. De taken van de dienst bevatten het leveren van steun voor het onderzoek van andere diensten waarvoor zij dan digitaal onderzoek zullen voeren. De dienst is ook het *single point of contact* (SPOC) voor de internationale informatie-uitwisseling inzake dit domein. Zij doen ook expertiseontwikkeling binnen dit domein, specifiek rond het *internet of things*, het *darknet* en cryptomunten. Maar dus ook de bestrijding van complexe cybercriminaliteit.

Deze rol is hen toebedeeld in het koninklijk besluit van 23 juni 2019 ter uitvoering van artikel 102, tweede lid, 4°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. Daarin wordt specifiek bepaald dat de aanpak van de georganiseerde cybercriminaliteit aan de FCCU wordt toegekend.

Naast de FCCU zijn er ook nog 14 RCCU's. Elk gerechtelijk arrondissement heeft een eigen *Computer Crime Unit* die soortgelijke taken vervult, maar voor een ander doelpubliek of voor andere feiten. Zij gaan ook de forensische digitale steun leveren, maar doen dit voor de politiediensten die in hun gerechtelijk arrondissement gevestigd zijn. Zij hebben hun eigen onderzoeken inzake cybercriminaliteit, die lokaal georganiseerd zijn of kleiner van omvang en minder complex zijn.

De cybermisdrijven die worden opgevolgd zijn opgenomen in de wet van 28 november 2000 betreffende de informaticacriminaliteit. Dit zijn de valsheid in informatica (artikel 210*bis* Sw.), het informaticabedrog (artikel 504*quater* Sw.), de hacking (artikel 550*bis* Sw.) en de datasabotage (artikel 550*ter* Sw.). Dit zijn de feiten waarbij de informatica zowel het middel als het doel is in tegenstelling tot de ruimere informaticacriminaliteit waar informatica een middel is om andere misdrijven te plegen.

De spreker verduidelijkt dat de focus ligt op het verzamelen van bewijselementen met het oog op het identificeren en het kunnen vervolgen van daders. Dat is de politionele rol, die een repressief sluitstuk moet vormen om daders te kunnen vatten. Dit is heel belangrijk in de ketenaanpak. Preventie en remediëring zijn zeer

capitale, le volet répressif est également nécessaire pour dissuader les auteurs.

La coopération avec les partenaires est primordiale, principalement parce que les CCU dépendent fortement des services partenaires pour la prévention et la réparation des dommages. Il existe donc une coopération stratégique et opérationnelle avec ces services. Par exemple, la VSSE ou le CERT sont désignés comme experts en matière de dossiers judiciaires avec lesquels la FCCU peut coopérer.

Le cyberplan d'urgence attribue un rôle spécifique à la FCCU. La police fédérale est représentée dans les structures de concertation qui y sont prévues, entre autres par le biais de la FCCU. Avec le CERT, ils contribuent également à l'évaluation permettant de déterminer la catégorie à laquelle l'incident appartient. Il est surtout important qu'ils soient en mesure de fournir une réponse policière rapide et opérationnelle. Il ne suffit pas de faire partie des structures de concertation, la capacité policière doit également pouvoir être déployée sur le terrain. C'est pourquoi la *Quick Reaction Force* a été créée. Il s'agit d'une équipe de collaborateurs spécialisés issus de toutes les CCU et non d'une unité distincte. En cas d'incidents, il est possible d'activer cette équipe et de l'envoyer en intervention sur place afin de recueillir suffisamment de preuves pour permettre une enquête plus approfondie.

En conclusion, l'intervenant reconnaît qu'il est nécessaire d'engager des collaborateurs plus spécialisés et de leur accorder un meilleur statut pour améliorer l'attractivité de ce service pour les candidats. La fonction publique ne sera probablement jamais en mesure de rivaliser avec le secteur privé en termes de rémunération, mais il est également possible de miser sur l'attractivité de l'environnement de travail. De nombreuses personnes choisissent cette voie en raison de la pertinence sociale inhérente à ce type de fonctions. Il ne s'agit donc pas seulement d'augmenter les salaires, mais aussi d'offrir les outils nécessaires aux collaborateurs afin qu'ils puissent agir efficacement et de fournir le cadre adéquat pour effectuer des analyses de qualité.

### B. **Questions et observations des membres**

*M. Michael Freilich (N-VA)* explique qu'il a pris l'initiative d'organiser ces auditions à la suite des récentes cyberattaques menées contre Belnet et le SPF Intérieur. Finalement, on ne saura jamais qui était réellement derrière ces attaques. Cependant, il est important de préciser quels pays sont connus pour leurs cyberstratégies offensives. Quels pays ont-ils quelque chose à gagner ou à perdre de ces récentes attaques? Comment les invités évaluent-ils la déclaration de M. De Vriendt

belangrijk, maar ook een repressief sluitstuk is nodig om daders ook te ontraden.

De samenwerking met de partners is van cruciaal belang voornamelijk omdat zij voor de preventie en remediëring heel sterk leunen op de partnerdiensten. Zo is er strategische en operationele samenwerking met deze diensten. Zo worden bijvoorbeeld de VSSE, of het CERT aangesteld als experten in gerechtelijke dossier en waar het FCCU mee kan samenwerken.

In het cybernoodplan is in een specifieke rol voor het FCCU voorzien. In de overlegstructuren die daarin zijn opgenomen, is de Federale Politie, onder meer via het FCCU, vertegenwoordigd. Zij dragen ook bij tot de evaluatie samen met het CERT om de inschaling van het incident te kunnen bepalen. Belangrijk is zeker dat zij een snelle en operationele politionele respons moeten kunnen leveren. Het volstaat niet om aan de overlegstructuren deel te nemen, er moet ook politiecapaciteit kunnen worden ingezet op het terrein. Daarvoor werd de *Quick Reaction Force* opgericht. Dit is een pool van gespecialiseerde medewerkers over alle CCU's heen en vormt geen aparte eenheid. Uit deze pool kan worden geput, om tijdens incidenten deze mensen te activeren en ter plaatste te sturen met het oog op het verzamelen van voldoende bewijselementen zodat een verder onderzoek mogelijk wordt gemaakt.

De spreker besluit dat er zeker behoefte is aan meer gespecialiseerde medewerkers en een beter statuut om mensen aan te trekken binnen deze dienst. Waarschijnlijk zal het openbaar ambt nooit kunnen concurreren met de private arbeidsmarkt qua verloning, maar er is ook de incentive van een aantrekkelijke werkomgeving. Veel mensen gaan voor dergelijke job omwille van de maatschappelijke relevantie. Het gaat dus niet alleen om meer verloning, maar ook om de nodige tools aan de werknemers te kunnen aanbieden zodat zij efficiënt kunnen handelen en de juiste omkadering bieden om performante analyses te kunnen doen.

### B. **Vragen en opmerkingen van de leden**

*De heer Michael Freilich (N-VA)* geeft aan het initiatief tot de hoorzittingen te hebben genomen, en dat naar aanleiding van de recente cyberaanvallen op Belnet en de FOD Binnenlandse Zaken. Er zal altijd vaagheid blijven bestaan over wie daar uiteindelijk echter achter zat. Wel is het belangrijk dat duidelijk wordt gemaakt welke landen gekend staan om hun offensieve cyberstrategieën. Welke landen hebben bij die recente aanvallen iets te winnen of te verliezen? Hoe beoordelen de genodigden de

par rapport à la Chine? En effet, une audition sur la situation des Ouïghours devait se tenir au Parlement précisément lorsque la cyberattaque DDoS a eu lieu. Dispose-t-on d'éléments suffisants pour démontrer que l'attaque provenait bien de cette zone? Peut-on affirmer avec certitude qu'il s'agissait d'un acteur étatique? Dans tous les cas, une telle attaque de botnets requiert une préparation bien plus approfondie.

Belnet a été la plus grande victime de cette attaque, mais Telenet et Proximus auraient également été touchés, ce qui laisse penser que l'attaque visait davantage les autorités belges. En même temps, il est vrai que les sites web des autorités et de la plupart des établissements de recherche sont connectés au réseau Belnet. Est-il vrai que Telenet et Proximus étaient également visés? Dans l'affirmative, on peut en déduire que l'attaque ne vise pas tellement Belnet, mais plutôt la Belgique.

Un système de vérification est-il utilisé pour repérer les tentatives de "smishing" (*phishing* par SMS)? En effet, l'utilisation de certains mots-clés ou URL devrait permettre de repérer des SMS suspects, qui sont envoyés à des milliers de personnes. Les mesures prises à cet égard sont-elles suffisantes? La responsabilité incombe-t-elle entièrement aux opérateurs? Les autorités peuvent-elles imposer la mise en place d'un tel système de vérification?

Il existe de nombreuses formes de cyberfraude. Le groupe de travail se réunit-il souvent pour discuter de toutes ces questions ou, au contraire, se réunit-il uniquement en cas de crise majeure? L'ampleur de la fraude a provoqué ce que l'on peut désormais qualifier "d'état de crise permanent". Suffisamment d'efforts sont-ils déployés pour lutter contre ce phénomène? Le contrôle politique qui lui est accordé est-il suffisant? Existe-t-il un point de contact au sein du gouvernement auquel il est possible de signaler les problèmes potentiels concernant l'approche adoptée (en termes de vie privée, de RGPD, et cetera)? Est-il compliqué d'adopter une bonne approche en raison de certaines interdictions? En d'autres termes, est-il nécessaire d'élaborer une législation spécifique en la matière? Chaque semaine, le gouvernement devrait plutôt être attentif aux problèmes rencontrés pour ensuite se pencher sur les solutions qu'il convient de mettre en place.

Parmi les problèmes rencontrés, on peut citer l'absence de vérification du nom du bénéficiaire lorsqu'une personne introduit un numéro IBAN. C'est le cas aux Pays-Bas et en Grande-Bretagne. Ces questions pourraient très bien faire l'objet d'une réglementation. Il est donc nécessaire qu'un responsable politique se charge de coordonner et suivre de près tous ces éléments. Que pensent les invités à ce sujet?

uitspraak van de heer De Vriendt in verband met China? Uitgerekend op het moment van de DDoS-cyberaanval zou immers in het Parlement een hoorzitting plaatsvinden over de situatie van de Oeigoeren. Zijn er voldoende elementen die aantonen dat de aanval uit die richting kwam? Kan men met zekerheid zeggen dat het een state actor is geweest? Een dergelijke botnetaanval vergt in ieder geval een uitvoerige voorbereiding.

Belnet was het grootste slachtoffer van de aanval. Telenet en Proximus zouden echter ook door de aanval zijn getroffen. Dat gegeven doet aannemen dat de aanval meer gericht was tegen de Belgische overheid. Tegelijk is het zo dat de websites van de overheid en van de meeste onderzoeksinstellingen bij Belnet zitten. Klopt het dat ook Telenet en Proximus werden geviseerd? Zo ja, dan gaat het niet zozeer om een aanval op Belnet maar op België.

Wordt er een screeningsysteem aangewend om de problematiek van "smishing" (phishing per sms) te detecteren? Het moet immers mogelijk zijn om verdachte sms'en, die aan duizenden personen worden verstuurd, op te sporen op basis van bepaalde trefwoorden of URL's. Wordt daar voldoende aan gedaan? Rust die verantwoordelijkheid volledig bij de operatoren? Kan de overheid een dergelijke screening opleggen?

Er zijn zeer veel vormen van cyberfraude. Komt de Task Force vaak samen om al die zaken te bespreken, of enkel in het geval van een grote crisis? Door de omvang van de fraude kan men inmiddels spreken van een permanente staat van crisis. Wordt die problematiek voldoende aangepakt? Wordt er voldoende politieke sturing aan gegeven? Is er een aanspreekpunt binnen de regering waar mogelijke problemen bij de aanpak (op het vlak van de privacy, de GDPR, enzovoort) kunnen worden gesignaleerd? Bemoeilijken bepaalde verbodsbepalingen een degelijke aanpak? Is er met andere woorden nood aan bepaalde wetgeving? Eigenlijk zou de regering wekelijks oor moeten hebben voor de problemen, om vervolgens na te gaan hoe die moeten worden aangepakt.

Een probleem is dat bij het invoeren van een IBAN-nummer de naam van de begunstigde niet wordt gecheckt. In Nederland en Groot-Brittannië gebeurt dat wel. Dergelijke zaken kunnen perfect wettelijk worden geregeld. Daarbij is er nood aan één politiek verantwoordelijke en coördinator om al die elementen van nabij op te volgen. Hoe zien de genodigden dat?

Est-il possible de travailler avec des "*high risk vendors*" (fournisseurs à haut risque)? Cela est actuellement possible pour la 5G. La boîte à outils européenne prévoit l'obligation, pour les opérateurs, de s'assurer qu'ils reçoivent une autorisation avant de pouvoir traiter avec un fabricant de matériel, par exemple. À l'instar de cette mesure préventive, serait-il judicieux que les autorités dressent une liste de ces "*high risk vendors"* de matériel et de logiciels afin d'interdire la connexion des produits qui figurent sur cette liste aux réseaux des infrastructures critiques? Serait-il possible d'appliquer une telle mesure? Un gestionnaire de réseau peut-il déterminer les personnes qui sont autorisées, ou non, à accéder au réseau et, par exemple, interdire les appareils sur lesquels l'application TikTok est installée? Le ministre de la Justice a évoqué une recommandation visant à interdire les appareils professionnels sur lesquels cette application est installée. Ne faudrait-il pas dépasser le stade de la simple recommandation? M. Freilich n'a trouvé aucune disposition à ce sujet dans la directive SRI2. Quel est l'avis des invités à ce sujet?

Le procureur fédéral a demandé que des sanctions soient imposées aux entreprises qui ne respectent pas les exigences en matière de cybersécurité. Peut-il préciser sa position à ce sujet? Quelles entreprises vise-t-il? Préconise-t-il des sanctions au niveau belge?

Les cyberexperts soulignent la grande qualité des courriels frauduleux, notamment lorsqu'il s'agit d'usurpation d'identité. À cause de cette amélioration méthodologique, il sera bientôt impossible pour un utilisateur individuel de distinguer les vrais messages des messages frauduleux. Quelles solutions existe-t-il pour résoudre ce problème? Peut-on, par exemple, mettre en place un système de filtrage DNS à l'échelle nationale? La mise en place de telles mesures est-elle du ressort des autorités?

Politico indique que l'Union européenne, en collaboration avec ENISA, souhaite mettre en place une *cyber response team* capable d'intervenir rapidement en cas de cyberattaque contre un pays. En effet, ne serait-il pas opportun que les États membres de l'UE unissent leurs forces?

*Mme Eva Platteau (Ecolo-Groen)* souligne d'abord le nombre élevé de signalements reçus par CERT.be. Le cadre de travail actuel permet de gérer ces signalements? L'intelligence artificielle est-elle utilisée pour analyser et traiter ces signalements? Ces applications offrent-elles des possibilités?

Il a également été souligné qu'il est difficile de prévoir le moment précis et la cible d'une future attaque.

Bestaat de mogelijkheid om te werken met "*high risk vendors*"? Vandaag de dag bestaat dat voor 5G. Op basis van de Europese toolbox moeten de operatoren ervoor zorgen dat zij een machtiging ontvangen vooraleer zij in zee mogen gaan met bijvoorbeeld een producent van hardware. Zou het naar analogie daarvan een goed idee zijn dat de overheid een lijst maakt van dergelijke "*high risk vendors*" voor hardware en software, waarbij binnen de kritieke infrastructuren producten van die lijst niet mogen worden geconnecteerd op het netwerk? Zou men zoiets kunnen afdwingen? Mag een netwerkbeheerder bepalen wie al dan niet toegang krijgt tot het netwerk, en bijvoorbeeld toestellen met TikTok weren? De minister van Justitie heeft gesproken over een aanbeveling rond het weren van professionele toestellen waarop die app geïnstalleerd staat. Dient er niet verder te worden gegaan dan een aanbeveling? De heer Freilich vindt hierover niets terug in de NIS 2 richtlijn. Hoe zien de genodigden dat?

De federaal procureur heeft gevraagd om sancties op te leggen aan bedrijven die niet voldoen aan de vereisten van de cyberveiligheid. Kan hij dat standpunt verder verduidelijken? Op welke bedrijven doelt hij? Pleit hij voor sancties op Belgisch niveau?

Cyberexperts wijzen op de hoge kwaliteit van e-mails, onder meer met spoofing. Die evolutie zal ertoe leiden dat een individuele gebruiker binnenkort niet meer de echte van de valse berichten zal kunnen onderscheiden. Wat zijn de oplossingen daarvoor? Kan bijvoorbeeld een DNS-filtersysteem worden uitgerold op landelijk niveau? Kan zoiets een taak zijn voor de overheid?

Politico meldt dat de Europese Unie met ENISA een *cyber response team* wil implementeren dat snelle hulp kan bieden bij een cyberaanval op een land. Is het inderdaad niet aangewezen om binnen de EU de krachten te bundelen?

*Mevrouw Eva Platteau (Ecolo-Groen)* wijst vooreerst op het hoge aantal meldingen die CERT.be ontvangt. Is het beheer van die meldingen momenteel mogelijk binnen het bestaand werkkader? Wordt gebruik gemaakt van artificiële intelligentie om die meldingen te analyseren en te verwerken? Bieden dergelijke toepassingen mogelijkheden?

Voorts werd erop gewezen dat het moeilijk te voorspellen valt wanneer de volgende aanval zal plaatsvinden, en

Quelles applications peuvent-elles néanmoins aider à analyser la situation?

M. De Bruycker a noté que de nombreux utilisateurs ne disposent pas de systèmes de sécurité automatiques. Cependant, le citoyen dispose de peu d'informations sur la fiabilité des logiciels antivirus disponibles sur le marché. Existe-t-il des recommandations que le particulier peut suivre? M. De Bruycker a également souligné la nécessité de mettre en place un correctif de sécurité européen pour ces produits qui proviennent des fournisseurs. À quels fournisseurs pense-t-il en particulier?

Selon le CCB, que faudrait-il mettre en place en matière de législation sur la cybersécurité?

Mme Platteau évoque ensuite l'attaque DDoS. Des preuves indiquent-elles qu'il s'agissait ou non d'un acteur étatique? Traditionnellement, les services de sécurité enquêtent sur des menaces qui apparaissent sur le territoire belge. Or, une cyberattaque est menée à distance. Dans quelle mesure les services de sécurité coopèrent-ils au niveau européen pour enrayer ce phénomène?

Le procureur fédéral a souligné l'importance d'une politique préventive en matière de cybersécurité. Le droit pénal est-il suffisamment adapté pour apporter des réponses aux multiples formes de cybercriminalité?

Le *phishing* semble être le pickpocket 2.0. Plusieurs zones de police locale, où les plaintes sont déposées, ne sont pas encore en mesure de faire face à ce phénomène et mener des enquêtes. Qu'en pense le procureur fédéral? Les formations juridiques mettent-elles suffisamment l'accent sur ce phénomène criminel? En outre, le Procureur fédéral a attiré l'attention, à juste titre, sur la conservation des données afin de permettre le bon déroulement des enquêtes.

L'intervenante demande aux représentants du NCCN si la planification d'urgence dans le contexte de la cyberattaque s'est avérée efficace. Les secteurs critiques se soucient-ils suffisamment de la sauvegarde des données? Quel est le plan B lorsqu'un réseau tombe en panne? Que faut-il entendre concrètement par "réseau 5G robuste"? Est-il encore nécessaire de pouvoir activer un réseau câblé en cas de crise?

Peut-on tirer des leçons du fonctionnement des différents organes de concertation dans le cadre de la gestion de la crise du coronavirus? Une évaluation de ces derniers sera-t-elle effectuée?

op wie die zich zal richten. Welke toepassingen kunnen niettemin helpen bij de analyses hieromtrent?

De heer De Bruycker heeft erop gewezen dat heel wat gebruikers geen automatische veiligheidssystemen hebben. De burger heeft echter weinig zicht op de betrouwbaarheid van de antivirussoftware die op de markt is. Bestaan er aanbevelingen waarvan de particulier gebruik kan maken? De heer De Bruycker heeft tevens gewezen op de nood aan een Europese veiligheidspatch voor dergelijke producten die door de leveranciers worden meegegeven. Welke leveranciers heeft hij concreet voor ogen?

Welke noden ziet het CCB op het vlak van de wetgeving rond cyberveiligheid?

Vervolgens verwijst mevrouw Platteau naar de DDoS-aanval. Zijn er aanwijzingen dat het al dan niet om een state actor ging? Traditioneel werken de veiligheidsdiensten rond dreigingen die zich op Belgisch grondgebied voordoen. Een cyberaanval gebeurt evenwel vanop afstand. In welke mate bestaat er Europese samenwerking tussen de veiligheidsdiensten om op die problematiek te kunnen inspelen?

De federaal procureur heeft het belang van een preventief beleid rond cyberveiligheid benadrukt. Is het strafrecht voldoende aangepast om antwoorden te bieden op de vele vormen van cybercriminaliteit?

Phishing lijkt het nieuwe zakkenrollen te zijn. Een aantal lokale politiezones, waar de klachten worden ingediend, zijn nog niet gewapend om met dat probleem om te gaan en onderzoeksdaden te verrichten. Hoe ziet de federaal procureur dat? Bestaat er in de juridische opleidingen voldoende aandacht voor dit criminaliteitsfenomeen? Voorts heeft de federaal procureur terecht aandacht gevraagd voor dataretentie om onderzoek mogelijk te maken.

Aan de vertegenwoordigers van het NCCN vraagt de spreekster of de noodplanning in het kader van de cyberaanval heeft gewerkt. Bestaat er in de kritische sectoren voldoende aandacht voor het zorgen voor back-ups van data? Wat is het plan B wanneer een netwerk uitvalt? Wat moet concreet worden begrepen onder een robuust 5G-netwerk? Blijft er nood aan een kabelnetwerk om in tijden van crisis te kunnen activeren?

Worden in het kader van het beheer van de coronacrisis lessen getrokken uit de werking van de verschillende overlegorganen? Zal daarvan een evaluatie worden gemaakt?

Le domaine de la cybersécurité nécessite une grande coordination entre de nombreux services. Comment les invités évaluent-ils la coopération actuelle dans ce domaine? Quels sont les points positifs? Que peut-on améliorer? Le flux d'informations est-il suffisant? Des dispositions légales entravent-elles cette coopération? Comment renforcer la coopération européenne en matière de cybersécurité?

*M. Eric Thiébaut (PS)* constate que les cyberattaques récentes sur Belnet et sur le SPF Intérieur font l'objet d'enquêtes avec lesquelles il ne faut pas interférer. Cela étant, il juge que les interventions des orateurs étaient très intéressantes et permettent de mettre en lumière plusieurs points d'attention, certaines critiques et des pistes de réflexion pour l'avenir.

Il retient par ailleurs de l'intervention du représentant de la VSSE que la Défense nationale, elle aussi, travaille sur une quatrième composante. Il lui semblerait intéressant d'entendre le point de vue de la Défense à ce sujet.

En matière de lutte contre la cybercriminalité, les questions liées à la gestion de l'informatique au sein de la police, à la formation des membres du personnel, au recrutement d'experts ou encore aux risques liés à la décentralisation des services d'appui sont essentielles. En outre, si des outils sont mis en place au niveau fédéral, une réflexion est-elle en cours en ce qui concerne la décentralisation de l'expertise? Les zones de police sont en effet demandeuses d'un appui technique spécifique.

Par le passé, des cyberpatrouilles étaient organisées. Est-ce toujours le cas? Si tel n'est pas le cas, ne serait-il pas opportun de les réactiver? Qu'en est-il de la possibilité de faire des signalements en ligne et de la mise sur pied de cybercommissariats?

Concernant le volet judiciaire, M. Thiébaut demande si le procureur fédéral peut donner des chiffres plus précis sur le nombre de dossiers en cours et clôturés.

En matière de coopération internationale, les opérations que ce dernier a évoquées sont-elles structurelles?

Enfin, il ressort de l'exposé du procureur fédéral qu'Internet semble difficile à encadrer. Quel est, de son point de vue, le niveau idéal pour légiférer efficacement? Existe-t-il un forum international où ces questions sont débattues?

*M. Tim Vandenput (Open Vld)* demande au procureur fédéral si les hackers qui ont été arrêtés peuvent se

Het domein van de cyberveiligheid vergt heel wat coördinatie tussen tal van diensten. Hoe evalueren de genodigden de huidige samenwerking op dat vlak? Wat loopt goed en wat kan beter? Is er voldoende informatiedoorstroming? Zijn er wettelijke bepalingen die belemmerend werken? Hoe kan de Europese samenwerking rond cyberveiligheid worden versterkt?

*De heer Eric Thiébaut (PS)* wijst erop dat de recente cyberaanvallen op Belnet en op de FOD Binnenlandse Zaken worden onderzocht en dat inmenging in die onderzoeken uit den boze is. Voorts vond de spreker de betogen van de sprekers erg interessant. Ze hebben meerdere aandachtspunten, bepaalde kritiek en denkpistes voor de toekomst voor het voetlicht gebracht.

De spreker heeft daarnaast uit het betoog van de vertegenwoordiger van de VSSE onthouden dat ook Defensie een vierde component uitwerkt. Derhalve zou de spreker het interessant vinden om het standpunt van Defensie hierover te horen.

Inzake de bestrijding van cybercriminaliteit vormen het IT-beheer binnen de politiediensten, de opleiding van het personeel, de indienstneming van experts of de met de decentralisatie van de ondersteunende diensten gepaard gaande risico's essentiële vraagstukken. De spreker wijst erop dat op federaal niveau tools worden opgezet, maar vraagt of een reflectie aan de gang is over de decentralisatie van de expertise. De politiezones zijn immers vragende partij om specifieke technische ondersteuning.

Vroeger werden cyberpatrouilles ingezet. Is dat nog steeds zo? Zo niet, zou het dan niet gepast zijn om ze opnieuw in te zetten? Hoe zit het met de mogelijkheid om online aangifte te doen en met het opzetten van cybercommissariaten?

Over het gerechtelijk onderdeel vraagt de heer Thiébaut of de federaal procureur nauwkeurigere cijfers kan verstrekken over het aantal lopende en afgesloten dossier.

Zijn de door hem vermelde internationale samenwerkingsverbanden structureel?

Tot slot blijkt uit de uiteenzetting van de federaal procureur dat het moeilijk lijkt om regels op te stellen voor het internet. Wat is volgens hem het ideale beleidsniveau om doeltreffend wetgevend op te treden? Bestaat er een internationaal forum waar dergelijke vraagstukken worden besproken?

*De heer Tim Vandenput (Open Vld)* informeert bij de federaal procureur of gevatte hackers spijtoptant

repentir, étant donné leurs connaissances et leur expertise en la matière. À ce titre, les services de sécurité et de renseignement belges pourraient-ils exploiter les compétences de ces personnes?

Le contre-espionnage a été complètement supprimé au sein du SGRS. Une discussion est actuellement en cours pour déterminer le service qui devrait être chargé des opérations de contre-espionnage. L'intervenant préconise la création d'une cellule qui serait en charge de telles opérations. Est-il possible de la mettre sur pied au sein de la VSSE?

*M. Franky Demon (CD&V)* pose la question suivante à propos de l'attaque contre le SPF Intérieur: l'affaire d'espionnage aurait-elle été révélée si Microsoft n'avait pas annoncé lui-même la fuite?

Peut-on établir une comparaison des moyens humains et financiers consacrés à la cybersécurité dans les pays voisins? Dispose-t-on de chiffres à ce sujet?

Enfin, M. Demon souligne la responsabilité contractuelle de Microsoft concernant les logiciels qu'il fournit aux autorités. Comment les concepteurs de logiciels sont-ils encouragés à commercialiser des logiciels sûrs ayant été soumis à des tests approfondis? Font-ils l'objet de contrôles?

*M. Bert Moyaers (Vooruit)* indique que la cybercriminalité est un phénomène vaste et diversifié. Tant les attaques contre des particuliers que les attaques à grande échelle nécessitent une approche spécifique. Pendant la crise du coronavirus, les chiffres de la criminalité ont diminué, à une exception près: ceux de la cybercriminalité. Les nombreux signalements dépassent les zones de police locale. D'après les calculs de Febelfin, des faits de pishing, dont le montant total de la fraude s'élève à 34 millions d'euros, ont été déclarés en 2020. Comme toutes les victimes ne déclarent pas systématiquement ce genre de faits, ce chiffre est en réalité beaucoup plus élevé.

En 2020, quelque 670 000 liens frauduleux ont été bloqués via Safeonweb. Outre cette mesure, que fait le CCB pour contrer ces liens? Les identifie-t-il? Se contenter de les bloquer reviendrait à mettre un emplâtre sur une jambe de bois. L'information est-elle transmise au parquet? Une collaboration avec pointdecontact.belgique.be est-elle mise en place? En raison des nombreux points de contact, on ne peut évidemment pas se rendre compte de l'ampleur du phénomène. Ne serait-il pas opportun de créer des synergies?

kunnen zijn, gelet op hun kennis en expertise in de materie. Kunnen deze personen in die hoedanigheid worden ingeschakeld in de Belgische veiligheids- en inlichtingendiensten?

Bij ADIV werd de counterintelligence volledig afgebouwd. Momenteel is de discussie aan de gang waar de counterintelligence moet worden ondergebracht. De spreker pleit voor een cel die daarmee wordt belast. Is het een optie om die binnen de VSSE te organiseren?

*De heer Franky Demon (CD&V)* vraagt in verband met de aanval op de FOD Binnenlandse Zaken of de spionage aan het licht zou zijn gekomen indien Microsoft niet zelf het lek kenbaar had gemaakt.

Kan een vergelijking worden gemaakt met de buurlanden op het vlak van het aantal mensen en middelen die worden gezet voor cyberveiligheid? Bestaan daar cijfers over?

Tot slot wijst de heer Demon op de contractuele aansprakelijkheid van Microsoft ten aanzien van de software die het aan de overheid levert. Op welke wijze worden softwareontwikkelaars aangezet om veilige en uitvoerig geteste software op de markt te brengen? Wordt daar controle op uitgeoefend?

*De heer Bert Moyaers (Vooruit)* geeft aan dat cybercriminaliteit een uitgebreid en divers gegeven is. Zowel de aanvallen op de individuele burgers als de grootschalige hackings vragen om een eigen aanpak. Tijdens de coronacrisis gingen de criminaliteitscijfers naar omlaag, met één grote uitzondering: de cybercriminaliteit. De vele meldingen daarover groeien boven de hoofden van de lokale politiezones uit. Febelfin heeft berekend dat in 2020 voor 34 miljoen euro aan aangiften werd gedaan over phishing. Aangezien niet iedereen aangifte doet, ligt dat cijfer in werkelijkheid nog heel wat hoger.

In 2020 werden er via Safeonweb zo'n 670 000 frauduleuze links geblokkeerd. Wat doet het CCB nog naast het blokkeren van de links? Worden die URL's ook geïdentificeerd? Indien het enkel bij blokkeren blijft, lijkt het wel dweilen met de kraan open. Wordt de informatie overgezonden aan het parket? Wordt er samengewerkt met Meldpunt.belgie.be? Door de vele meldpunten ziet men immers door de bomen het bos niet meer. Is het niet aangewezen om voor een synergie te zorgen?

La question de la cybersécurité est également traitée au sein de différents cabinets ministériels. Dans ce contexte, l'exécutif travaille-t-il efficacement? M. Moyaers estime déjà qu'un changement structurel est souhaitable. En effet, travailler sans aucune cohésion facilite la tâche à l'adversaire. Est-il possible d'attribuer l'entière responsabilité de cette matière à un seul et unique cabinet? M. De Bruycker a mis en évidence un manque de sensibilité à la sécurité informatique. Estime-t-il que l'attaque DDoS a permis d'initier les changements d'attitude nécessaires? Le gouvernement fédéral a ensuite annoncé un investissement supplémentaire conséquent. À quoi ce budget devrait-il être alloué en priorité? Ces crédits supplémentaires seront-ils suffisants? Dans quels domaines les investissements sont-ils insuffisants, voire inexistants?

Le procureur fédéral estime que les moyens disponibles sont insuffisants pour atteindre les objectifs ambitieux du CCB. Aux Pays-Bas, le budget consacré à la cybersécurité est six fois plus élevé. Comment M. De Bruycker pense-t-il pouvoir hisser la Belgique au rang des pays les moins vulnérables avec les moyens disponibles?

Les FCCU et RCCU sont également confrontées à un manque de personnel, de moyens et d'expertise. Est-il vrai que le cadre du personnel de la FCCU, qui compte 44 ETP, n'est toujours pas au complet? Quel est l'état d'avancement de la question? Quelle est la situation au sein des RCCU?

La rémunération est-elle le seul élément qui pousse les experts en TIC à choisir le secteur privé? Augmenter les barèmes salariaux permettra-t-il de répondre aux attentes de ces personnes?

L'enquête sur la cyberattaque contre le SPF Intérieur est en cours. En outre, la ministre des Affaires étrangères a annoncé la procédure d'attribution diplomatique. En raison de leurs ramifications internationales, les enquêtes judiciaires sur les affaires de cybercriminalité donnent souvent peu de résultats. Il convient de préciser que l'attribution diplomatique est également une question sensible. Les deux éléments peuvent-ils se renforcer mutuellement ou se compléter? Si des hackers sont désignés coupables via la procédure d'attribution diplomatique, la justice peut-elle exploiter ce dispositif, ou une telle procédure doit-elle d'abord faire l'objet de négociations au niveau européen?

De aandacht voor cyberveiligheid is ook verdeeld over verschillende ministeriële kabinetten. Is de uitvoerende macht in het licht daarvan efficiënt aan het werken? De heer Moyaers is alvast van oordeel dat een structurele verandering aangewezen is. Een verdeelde slagorde maakt het de tegenstander immers makkelijker. Hoe kunnen de verschillende verantwoordelijkheden in één hand worden gebracht? De heer De Bruycker heeft gewezen op een te lage "*security awareness*". Heeft hij het gevoel dat de DDoS-aanval voor de noodzakelijke kentering heeft gezorgd? De federale regering heeft nadien een forse bijkomende investering aangekondigd. Waar moet dat budget prioritair voor worden aangewend? Zullen die bijkomende kredieten volstaan? Op welke vlakken wordt niet of onvoldoende geïnvesteerd?

De federaal procureur acht de beschikbare middelen te beperkt om de hoge ambities van het CCB te kunnen waarmaken. Het budget in Nederland voor cyberveiligheid ligt 6 maal hoger. Hoe denkt de heer De Bruycker met de beschikbare middelen toch tot de wereldtop te kunnen behoren?

Ook de FCCU's en de RCCU's kampen met een tekort aan mensen, middelen en expertise. Klopt het dat het personeelskader van de FCCU van 44 VTE tot op vandaag niet volledig ingevuld is? Wat is de stand van zaken? Wat is de situatie binnen de RCCU's?

Heeft de keuze van IT-mensen voor de privésector enkel te maken met de verloning? Zullen hogere loonbarema's voor deze mensen een oplossing bieden?

Het onderzoek naar de cyberaanval op de FOD Binnenlandse Zaken loopt. Daarnaast heeft de minister van Buitenlandse Zaken de maatregel van de diplomatieke attributie aangekondigd. Door de internationale vertakkingen leveren gerechtelijke onderzoeken naar cybercriminaliteit vaak niet veel op. Tegelijk is ook de diplomatieke attributie een gevoelig punt. Kunnen beide elementen elkaar versterken of aanvullen? Indien hackers via de diplomatieke attributie gevat worden, kan justitie daar dan iets mee aanvangen, of moet zoiets eerst aan een Europese onderhandelingstafel worden behandeld?

C. **Réponses**

1. ***Réponses de M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité Belgique (CCB)***

*M. Miguel De Bruycker* indique qu'élaborer une politique et mettre les moyens à disposition représentent un exercice permanent pour le CCB. En tant que service public, le CCB est bien entendu tenu de respecter les règles en matière de recrutement et de marchés publics. Cela signifie qu'il n'est pas toujours possible de répondre rapidement à certains besoins.

Rien n'indique pour l'instant que l'attaque DDoS provient de Chine. Les 129 serveurs dans le monde n'ont pas été infiltrés. Les serveurs n'ont pas été piratés, mais ont été spécifiquement sélectionnés par le propriétaire du botnet. L'attaque était bien plus importante que celle contre *Smartschool*. Cependant, il n'est pas nécessaire d'être un service public pour pouvoir lancer une attaque DDoS contre Belnet. Le constat est différent pour l'attaque contre le SPF Intérieur, car la technologie utilisée et la méthode de travail sont typiques d'un service de renseignement.

Le CCB respecte les compétences des autres services responsables de l'attribution. D'une part, il y a l'attribution dans le contexte de l'enquête pénale. Les éléments disponibles sont transmis à tous les partenaires (justice, services de renseignement). D'autre part, il existe désormais également l'attribution qui entraîne des conséquences sur le plan politique ou diplomatique.

L'intervenant confirme l'importance de la vérification par SMS. Il soutient pleinement l'initiative de la ministre De Sutter en la matière. Elle élabore actuellement un projet avec de nombreux partenaires visant à appliquer un certain nombre de filtres aux SMS. Une adaptation du cadre légal a été initiée à la demande de l'IBPT. Entretemps, l'Autorité de protection des données a rendu un avis négatif, car elle estime que le principe de proportionnalité n'est pas respecté. Cependant, si le filtrage est automatique, l'intervenant ne voit aucune différence avec les filtres *antispam* installés sur les boîtes mail par les fournisseurs. Actuellement, ce système permet de filtrer 90 % des courriels, transférant les indésirables en dehors de la boîte mail. Il est judicieux d'appliquer également ce système aux messages reçus par SMS. L'intelligence artificielle peut jouer un rôle à cet égard en détectant rapidement et automatiquement certains modèles types.

Le plus grand mérite du CCB est de parvenir à réunir régulièrement tous les partenaires impliqués dans la cybersécurité au sein de la *Task Force*. Le CCB gère

C. **Antwoorden**

1. ***Antwoorden van de heer Miguel De Bruycker, directeur van het "Center for Cybersecurity Belgium" (CCB)***

*De heer Miguel De Bruycker* geeft aan dat het uittekenen van een beleid en het beschikken over middelen voor het CCB een voortdurende oefening is. Als overheidsdienst is het CCB uiteraard gebonden door de regels inzake rekrutering en overheidsopdrachten. Het zorgt ervoor dat niet steeds snel kan worden ingespeeld op bepaalde noden.

Er is tot nu toe geen enkele aanwijzing dat de DDoS-aanval uit China komt. Er zijn geen 129 servers in de wereld geïnfiltreerd. De servers werden niet gehackt, maar werden zeer goed geselecteerd door botneteigenaar. De aanval was veel groter dan die op *Smartschool*. Om de DDoS-aanval tegen Belnet op touw te kunnen zetten, hoeft men evenwel geen overheidsdienst te zijn. Anders is het bij de aanval op de FOD Binnenlandse Zaken. De daarbij gebruikte technologie en manier van werken zijn kenmerkend voor een inlichtingendienst.

Het CCB respecteert de bevoegdheden van de andere diensten die instaan voor attributie. Er is enerzijds attributie in het domein van het strafonderzoek. De beschikbare elementen worden overgezonden aan alle partners (justitie, de inlichtingendiensten). Anderzijds is er thans ook een attributie met politieke of diplomatieke gevolgen.

De spreker onderschrijft het belang van de sms-screening. Hij steunt volledig het initiatief van minister De Sutter ter zake. Zij voert momenteel een project uit met tal van partners om een aantal filters op sms'en toe te passen. Op initiatief van het BIPT wordt gewerkt aan een aanpassing van het wettelijk kader. Er is inmiddels weliswaar een negatief advies van de Gegevensbeschermingsautoriteit, die het proportionaliteitsbeginsel niet gerespecteerd acht. Als de filtering automatisch gebeurt, ziet de spreker evenwel geen verschil met de antispamfilters op de mailboxen bij de providers. Momenteel wordt 90 % van alle mails op die manier weggefilterd uit de mailboxen. Het is een goed idee om dat ook op sms-berichten toe te passen. Artificiële intelligentie kan daarbij een rol spelen door snel en geautomatiseerd bepaalde patronen te herkennen.

De grootste verdienste van het CCB is dat alle bij de cyberveiligheid betrokken partners regelmatig samenkomen in de *Task Force*. Het CCB beheert een

une dizaine de plateformes de collaboration (services de renseignement et de sécurité, autorités sectorielles, une cellule de réflexion, des groupes de travail internationaux, et cetera). Outre l'élaboration du cyberplan d'urgence, le travail de coordination est la deuxième grande mission du CCB.

L'approche fragmentée de la cybersécurité est également liée à la nature même du phénomène. La cybersécurité touche effectivement à de nombreuses questions sociales: élections, pédophilie, terrorisme, espionnage, criminalité organisée, fraude financière, et cetera. La cybersécurité doit donc être introduite étape par étape à tous les niveaux. Elle fait désormais partie de la société. Cela confirme l'absolue nécessité de la coordination et du contrôle central. L'intervenant ne pense cependant pas que tout doit être centralisé à un seul endroit. Il n'est pas opportun de créer un grand et tout-puissant CCB. La meilleure façon d'obtenir des résultats rapides et efficaces est d'assurer une bonne coopération avec tous les partenaires.

M. De Bruycker laisse la VSSE répondre à la question sur les "*high risk vendors*", car la définition de cette notion n'est pas d'ordre technique, mais géopolitique.

La question relative à des applications comme TikTok a été posée à juste titre. Les sites web et les applications les plus utilisés ne sont pas européens. Les plus populaires sont d'origine américaine, mais des acteurs d'autres continents occuperont également une place importante à l'avenir. Cela signifie que les entreprises européennes stockent toutes leurs informations, y compris les recherches, sur un cloud qui n'est pas européen, ni même probablement américain. C'est une question sur laquelle il convient de se pencher.

Le CCB est en mesure de traiter les nombreux signalements, car il peut compter sur 3 partenaires commerciaux. Aucun pays européen n'est évidemment en mesure d'analyser tous les messages envoyés par les citoyens. En Belgique, les citoyens peuvent signaler eux-mêmes les messages suspects, une méthode unique en Europe. Un système est actuellement en phase de test et permettrait à DNS, qui a été mis en place avec les fournisseurs d'accès à internet, de rediriger des sites vers des pages d'avertissement. Aucun autre pays ne dispose actuellement d'un tel système.

M. De Bruycker estime également que la dimension européenne revêt une grande importance, mais craint que l'Union européenne ne soit actuellement pas capable d'agir rapidement et fermement. À l'heure actuelle, il n'existe aucune politique européenne contraignante en

tiental samenwerkingsplatformen (inlichtingen- en veiligheidsdiensten, sectorale overheden, een denktank, internationale werkgroepen, enzovoort). Coördinatie is, na de uitwerking van het cybernoodplan, de tweede hoofdopdracht van het CCB.

De versnipperde aanpak van cyberveiligheid heeft ook te maken met de aard van het fenomeen zelf. Cyberveiligheid raakt immers aan tal van maatschappelijke thema's: verkiezingen, pedofilie, terrorisme, spionage, georganiseerde misdaad, financiële fraude, enzovoort. Cyberveiligheid moet dan ook stap voor stap worden ingevoerd op alle niveaus. Het maakt inmiddels deel uit van de maatschappij. Dat maakt de coördinatie en de centrale aansturing absoluut noodzakelijk. De spreker meent wel niet dat alles gecentraliseerd moet worden op één plaats. Het is niet aangewezen om één groot en almachtig CCB te creëren. Een goede samenwerking met alle partners rond dezelfde tafel zal de snelste en beste resultaten opleveren.

De heer De Bruycker laat de reactie over de "*high risk vendors*" over aan de VSSE, aangezien de definitie van het begrip niet technisch is maar geopolitiek.

Terecht werd de vraag gesteld naar toepassingen zoals TikTok. De meest gebruikte websites en toepassingen zijn niet-Europees. De belangrijkste zijn Amerikaans, en in de toekomst zullen er ook belangrijke spelers zijn van andere continenten. Dat betekent dat de Europese bedrijven al hun informatie, ook over hun research, opslaan in een cloud die niet Europees en misschien ook niet langer Amerikaans is. Daar moet over worden nagedacht.

Het CCB is in staat om de vele meldingen te verwerken omdat het beroep doet op 3 commerciële partners. Terecht kan geen enkel Europees land zomaar alle berichten van alle burgers scannen. Het feit dat in België de burgers wel zelf verdachte berichten kunnen melden, is uniek in Europa. Momenteel is een systeem in testfase waarbij waarschuwingspagina's worden gegeven op basis van Secure DNS dat samen met internetserviceproviders is opgezet. Geen enkel ander land doet momenteel zoiets.

De heer De Bruycker onderschrijft het belang van een Europese dimensie, maar vreest dat de Europese Unie momenteel niet in staat is om snel en krachtdadig op te treden. Momenteel wordt geen strikt Europees beleid gevoerd. Initiatieven die in België worden genomen

la matière. Les initiatives prises en Belgique (Safeonweb, le *Belgium Anti-Phishing Shield*) sont des questions très sensibles au niveau européen.

Le citoyen n'est probablement plus capable de distinguer les messages frauduleux des messages réels. Ce constat montre la nécessité d'une identité numérique (comme Itsme), qui pourrait être associée aux boîtes mail. Cela permettrait de connaître avec certitude l'identité de l'expéditeur des emails envoyés. Une telle mesure est réalisable d'un point de vue technologique. Cependant, eu égard aux dispositions en matière de vie privée, l'Europe est-elle prête à autoriser un tel système? Depuis 2018, les services de sécurité et de renseignement, notamment, n'ont plus accès à une base de données WHOIS pour des raisons liées au RGPD.

Si l'intelligence artificielle peut certainement être un outil, il convient toutefois de noter que les organisations criminelles l'utilisent actuellement davantage que les services publics. Elle doit être exploitée, mais les possibilités qu'elle offre ne sont pas illimitées.

Quelle législation convient-il de remanier? L'intervenant évoque la loi télécom et la loi sur la conservation des données.

En conclusion, M. De Bruycker estime que la Belgique prend un certain nombre d'initiatives uniques en Europe. Comment peut-on s'améliorer davantage? Il est essentiel d'accorder suffisamment de moyens à la police et à la justice. Le travail du CCB concerne principalement le volet préventif (campagnes de sensibilisation, protection préalable au crime). Le travail postérieur au crime (recherche des auteurs, identification des structures utilisées, lutte contre l'organisation en question, et cetera) peut encore être amélioré. Il est avant tout nécessaire d'instaurer un cadre au sein des services publics qui permette d'attirer les experts dont nous avons besoin.

2. ***Réponses de M. Peter Lanssens, représentant de la Sûreté de l'État (VSSE)***

*M. Peter Lanssens* indique que la VSSE ne dispose pas non plus d'éléments attestant clairement de l'implication d'un acteur étatique. Cela prouve que l'attribution reste un processus difficile.

En ce qui concerne la question sur la coopération entre les services de sécurité européens, l'intervenant précise que, comme pour les autres menaces, il existe également une coopération renforcée entre les services de renseignement européens dans le domaine de la cybersécurité. Concrètement, cela signifie que les données relatives aux cyberattaques sont partagées

(Safeonweb, het *Belgium Anti-Phishing Shield*) liggen op Europees niveau zeer gevoelig.

De burger is allicht nu al niet meer in staat om de goede en de slechte berichten van elkaar te onderscheiden. Dat gegeven wijst op de nood tot het hebben van een digitale identiteit (bijvoorbeeld Itsme), die zou kunnen worden gekoppeld aan de mailboxen. Aldus kan zekerheid worden geboden dat een bepaalde e-mail door een bepaalde persoon werd verstuurd. Technologisch is zoiets haalbaar. Is Europa in het licht van de privacy evenwel bereid om een dergelijk systeem te aanvaarden? Sinds 2018 hebben veiligheids- en inlichtingendiensten bijvoorbeeld geen toegang meer tot een WHOIS-databank om redenen van GDPR.

Artificiële intelligentie kan zeker een hulmiddel zijn, al past de opmerkingen dat de criminele organisaties er thans meer gebruik van maken dan de overheidsdiensten. Het moet worden ingezet, maar is niet onbeperkt in zijn mogelijkheden.

Aan welke wetgeving moet worden gesleuteld? De spreker wijst op de telecomwet en de dataretentiewet.

De heer De Bruycker besluit dat België een aantal initiatieven neemt die uniek zijn in Europa. Wat kan nog beter? Het is van essentieel belang dat voldoende middelen worden gegeven aan politie en justitie. Het CCB werkt voornamelijk op preventief vlak (campagnes rond *awareness*, de bescherming alvorens het misdrijf plaatsvindt). Het werk nadat het misdrijf is gepleegd (het zoeken van de daders, het identificeren van de gebruikte structuren, de aanpak van die infrastructuur, enzovoort) kan nog beter. Daarbij is vooral nood aan een kader binnen de overheidsdiensten dat in staat is om de nodige experten aan te trekken.

2. ***Antwoorden van de heer Peter Lanssens, vertegenwoordiger van de Veiligheid van de Staat (VSSE)***

*De heer Peter Lanssens* stelt dat de VSSE evenmin beschikt over elementen die ondubbelzinnig wijzen op de betrokkenheid van een state actor. Het bewijst dat attributie steeds een moeilijk proces is.

In verband met de vraag naar samenwerking tussen de Europese veiligheidsdiensten, antwoordt de spreker dat er, net zoals rond andere dreigingen, ook een intensieve samenwerking bestaat tussen de Europese inlichtingendiensten op het vlak van cyber. Dat betekent concreet dat gegevens over cyberaanvallen met andere landen worden gedeeld. Die informatie deelt de VSSE op

avec d'autres pays. À son tour, la VSSE partage ces informations avec les partenaires nationaux, le CCB en priorité. Sur la base de ces informations, des contrôles de sécurité peuvent alors être effectués en Belgique. Un certain nombre de partenaires internationaux surveillent également les *Command and Control Servers*. La VSSE est informée si des transferts suspects vers des adresses IP belges sont détectés. La VSSE informe à son tour les partenaires nationaux, notamment le CCB en premier lieu. En outre, la coopération européenne en matière de cybersécurité ne cesse de se développer.

Plusieurs projets sont actuellement en cours pour renforcer la coopération entre la VSSE et le SGRS dans le but de permettre aux deux services d'utiliser plus efficacement les moyens dont ils disposent. Ces projets font partie du Plan stratégique national du renseignement (PSNR) qui a été présenté au Conseil national de sécurité. L'un des premiers projets est la création d'une plateforme CT (contre-terrorisme) qui permet de rassembler les capacités en matière de lutte contre le terrorisme. Ce projet est considéré comme un succès. C'est aussi la raison pour laquelle il a été décidé de mettre en place une coopération dans d'autres domaines. Récemment, une coopération plus étroite entre les deux services de renseignement belges en matière de contre-espionnage a été initiée. Il ne s'agit pas de rassembler "physiquement" les collaborateurs – comme pour la plateforme CT –, mais plutôt d'établir une répartition claire des tâches afin d'assurer le partage de toutes les informations utiles (remplacer le principe du "besoin de savoir" par le "besoin de partager") et de pouvoir partager les informations obtenues grâce à la coopération. En marge de ces discussions, on s'interroge également sur l'approche à adopter pour la cybermenace. Depuis lors, les premières mesures ont été mises en place pour améliorer la coopération.

3. ***Réponses de M. Frédéric Van Leeuw, procureur fédéral***

*M. Frédéric Van Leeuw* explique que les directives SRI et SRI2 sont un énorme pas en avant. Tout comme pour la sécurité alimentaire, il est nécessaire de mettre en place un cadre réglementaire approprié visant à assurer la sécurité des systèmes informatiques.

Les services de sécurité ont déjà mené d'innombrables missions officielles dans des pays à risque où la sécurité en matière de communication n'est pas garantie, ce qui engendre des conséquences très sérieuses. Dans certains pays, les téléphones sont systématiquement piratés. Pour l'instant, il n'existe pas vraiment de culture de la sécurité en Belgique dans ce domaine, mais d'autres pays zijn beurt met de nationale partners. In de eerste plaats is dat het CCB. Op basis van die informatie kunnen dan in België veiligheidschecks worden uitgevoerd. Een aantal internationale partners houden ook *Command and Control Servers* in het oog. Wanneer daar verdacht verkeer naar Belgische IP-adressen wordt opgemerkt, wordt de VSSE daarover ingelicht. Het VSSE licht op zijn beurt de nationale partners in, met in de eerste plaats het CCB. De Europese samenwerking rond cyber is bovendien voortdurend in ontwikkeling.

Momenteel lopen meerdere projecten om de samenwerking tussen de VSSE en ADIV te versterken met de doelstelling dat de beide diensten hun beschikbare middelen efficiënter kunnen inzetten. Die projecten maken deel uit van het Nationaal Strategisch Inlichtingenplan (NSIP) dat werd voorgesteld aan de Nationale Veiligheidsraad. Eén van de eerste projecten is de oprichting van een platform CT (contraterrorisme) waar de contraterrorismecapaciteit wordt samengebracht. Dat project wordt als een succes beschouwd. Dat is ook de reden waarom werd beslist om ook op andere domeinen een samenwerking op poten te zetten. Recent werd dan ook gewerkt aan nauwere samenwerking tussen de twee Belgische inlichtingendiensten rond *counterintelligence*. Het is niet de bedoeling om de mensen fysiek samen te zetten – zoals bij het CT-platform – maar wel om zeer duidelijke afspraken te maken rond wie wat doet, om ervoor te zorgen dat alle nuttige informatie gedeeld wordt (het *need to share* principe in plaats van het *need to know principe*), en om elkaar deelgenoot te kunnen maken van informatie die wordt verkregen via de samenwerkingsverbanden. In de marge van die gesprekken wordt ook bekeken hoe de cyberdreiging daarin aan bod kan komen. Inmiddels werden de eerste stappen gezet om de samenwerking te verbeteren.

3. ***Antwoorden van de heer Frédéric Van Leeuw, federaal procureur***

*De heer Frédéric Van Leeuw* licht toe dat de wetgeving van NIS en NIS2 een enorme vooruitgang betekent. Net zoals voor voedselveiligheid is er nood aan een goed regelgevend kader rond cyberveiligheid ten aanzien van informaticasystemen.

Het aantal officiële zendingen van veiligheidsdiensten naar risicolanden waarbij geen enkele veiligheidsgarantie bestaat inzake de communicatie zijn ontelbaar. De consequenties daarvan zijn enorm. Er zijn landen waar systematisch de telefoons worden gehackt. Op dit ogenblik bestaat op dat gebied in België echt geen veiligheidscultuur. Andere landen zijn daar wel alert

y sont attentifs. Il conviendrait d'accorder une attention beaucoup plus grande à la formation sur les aspects sécuritaires en lien avec l'utilisation des technologies.

Concernant le *hacking*, le procureur fédéral explique qu'en Belgique, accéder à un système qui n'est pas le sien constitue déjà un acte punissable. En Allemagne, on parle de *hacking* dès qu'une personne force l'accès à un système sécurisé. Cette disposition met davantage l'accent sur l'importance de la protection des réseaux ainsi que du comportement des citoyens et de l'usage qu'ils font d'internet.

Le Parquet fédéral peine parfois à obtenir des informations. Il arrive qu'un pays refuse de partager les informations demandées au prétexte que leur communication est contraire à ses propres intérêts. Il arrive aussi qu'un pays prétende que l'information est classifiée. Si ces informations peuvent servir de base à une procédure d'attribution, elles ne permettent cependant pas d'aboutir à un procès.

Le procureur fédéral souligne les éléments suivants concernant les questions sur les chiffres: le parquet fédéral joue un rôle central dans la lutte contre les images à caractère pédopornographique qui circulent sur internet, dans la mesure où il reçoit toutes les adresses IP identifiées et qui ont un lien avec la Belgique. En 2019, il y avait 450 dossiers, contre 2 638 dossiers en 2020. Cette augmentation démontre l'ampleur du phénomène. Si le parquet fédéral ne peut avoir recours à la conservation des données, il est dès lors impossible de retrouver ces dossiers. En outre, ce type de dossiers exige beaucoup d'efforts de la part de la police et de la justice.

En ce qui concerne les forums internationaux, l'intervenant souligne les travaux du Conseil de l'Europe sur la révision de la Convention de Budapest (Convention sur la cybercriminalité). Cette convention contient des instruments importants et utiles dans le cadre de la cybersécurité. En outre, Europol a également investi massivement dans la lutte contre la cybercriminalité.

Il est envisagé de travailler avec les repentis dans le domaine de la cybersécurité. Par "repenti", nous entendons toute personne qui fait des déclarations substantielles, sincères et complètes sur des infractions commises. Cependant, il ne leur est pas demandé de jouer un rôle actif dans les affaires. Les déclarations ou le *hacking* de son propre système ou de celui d'autrui pourraient être envisagés dans ce contexte. Or, demander à un hacker de mettre ses compétences au profit des autorités n'est pas en accord avec l'actuel régime des repentis. Cela pourrait éventuellement s'organiser dans le cadre de la législation relative à l'infiltration civile. Il

voor. Er zou veel meer aandacht moeten zijn voor opleidingen rond de veiligheidsaspecten rond het gebruik van technologieën.

Wat de hacking betreft, licht de federaal procureur toe dat in België iemand strafbaar is van zodra hij toegang krijgt tot een systeem dat niet het zijne is. In Duitsland gaat het om hacking van zodra iemand de toegang forceert tot een systeem dat beveiligd is. In de laatste optie wordt meer de nadruk gevestigd op het belang van de bescherming van de netwerken en van het gedrag van de burger op het internet.

Het Federaal Parket ondervindt soms moeilijkheden bij het verkrijgen van informatie. Soms deelt een land de gevraagde informatie omdat het stelt dat de mededeling in strijd is met de belangen van die Staat. Soms stelt een land dat het om geclassificeerde informatie gaat. Dergelijke informatie kan de basis vormen van een attributieprocedure, maar kan niet leiden tot een openbaar proces.

Op de vraag naar cijfers wijst de federaal procureur op het volgende. Het federaal parket speelt in verband met de aanpak van beelden van kinderporno op het internet een centrale rol, in die zin dat het alle geïdentificeerde IP-adressen ontvangt die verband houden met België. In 2019 waren er 450 dossiers, en in 2020 ging het om 2 638 dossiers. Die stijging onderlijnt de omvang van de problematiek. Indien de federaal parket geen beroep kan doen op dataretentie, kunnen die dossiers niet worden getraceerd. Bovendien vergen dat soort dossiers heel wat inspanningen van politie en justitie.

Wat de internationale fora betreft, wijst de spreker op de werkzaamheden van de Raad van Europa rond de herziening van de conventie van Boedapest (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken). Dat verdrag bevat belangrijke en nuttige instrumenten in het kader van de cyberveiligheid. Daarnaast heeft ook Europol sterk geïnvesteerd in de aanpak van cybercriminaliteit.

Er wordt nagedacht of met spijtoptanten kan worden gewerkt in het domein van de cyberveiligheid. Een spijtoptant is iemand die substantiële, oprechte en volledige verklaringen aflegt over een gebeurtenis. Er wordt evenwel van een spijtoptant niet gevraagd om iets op actieve wijze te doen. Verklaringen of eigen hacking of die van anderen zouden wel in dat kader kunnen passen. Vragen om aan hacking te doen ten dienste van de overheid past niet binnen de huidige spijtoptantenregeling. Eventueel zou dat wel kunnen gebeuren in het kader van de wetgeving rond de burgerinfiltratie. Dat is evenwel een recente wetgeving met zeer strikte voorwaarden.

s'agit toutefois d'une législation récente assortie de conditions très strictes. Des réflexions sont actuellement menées afin de déterminer si une personne possédant des connaissances spécifiques (par exemple, en matière d'intelligence artificielle) répond aux conditions pour être considérée comme repenti. Un tel système existe déjà dans certains autres pays.

La cybercriminalité fait de très nombreuses victimes. Cependant, la politique en matière de poursuites pénales exige de faire des choix et de fixer des priorités. Un nouveau plan national de sécurité pour la police est en cours d'élaboration. Au cours de ces discussions, la question des plaintes relatives à la cybercriminalité sera abordée. Si l'on détermine que les enquêtes sont du ressort de la police locale, on court le risque de créer des inégalités: en effet, certaines zones de police disposent des moyens nécessaires pour mener ce type d'enquête, mais ce n'est pas le cas pour d'autres. Ce débat s'inscrit dans le cadre plus large de la question suivante: quel niveau est-il le plus approprié pour mener chaque type d'enquêtes? Il existe également différents niveaux de criminalité informatique. En outre, ce type de crime revêt souvent une dimension internationale, ce qui nécessite donc une approche internationale.

4. ***Réponses de M. Piet Pieters en Mme Leen Depuydt, représentants du Centre de Crise National (NCCN)***

*M. Piet Pieters* estime que des mesures supplémentaires sont effectivement nécessaires en ce qui concerne les opérateurs de services essentiels et d'infrastructures critiques. Il est vrai que nous sommes sur la bonne voie à ce sujet. Dans ce contexte, il est primordial de faire la distinction entre une analyse de la menace et une analyse de risque. Une analyse de la menace examine la menace telle qu'elle nous parvient depuis un acteur en particulier qui démontre une certaine capacité et une certaine intention (par exemple, une idéologie spécifique). Dans ce cas, l'accent est mis sur la probabilité. Une analyse de risque, en revanche, s'intéresse principalement à l'impact. M. De Bruycker a affirmé que lors d'une cyberattaque, l'auteur choisit sa cible, sa technique et la puissance de l'attaque. M. Van Leeuw a ajouté que de petits investissements peuvent prévenir des dommages importants. C'est le cœur du problème: il s'agit de la culture de la sécurité. Il faut finalement accepter que le type de risque auquel on est confronté ne soit pas toujours clair et qu'il ne puisse être prédit avec précision. Cela signifie qu'il convient de travailler sur la dimension défensive compte tenu du fait que l'on ignore l'origine du futur ennemi. Afin de renforcer la culture de la sécurité, les autorités et les secteurs vitaux devront donc effectivement s'armer davantage en se dotant de protections et de pare-feux supplémentaires, même

Momenteel wordt wel onderzocht of iemand die beschikt over specifieke kennis (bijvoorbeeld over artificiële intelligentie) in aanmerking kan komen als spijtoptant. In enkele andere landen bestaat zoiets al.

Cybercriminaliteit zorgt voor heel veel slachtoffers. In het strafvervolgingsbeleid moeten evenwel keuzes worden gemaakt en prioriteiten worden gesteld. Momenteel wordt gewerkt aan een nieuw nationaal veiligheidsplan voor de politie. Bij die besprekingen komt de problematiek van de klachten over cybercriminaliteit aan bod. Indien het onderzoek daarover aan het lokaal politieniveau wordt overgelaten, dreigt men ongelijkheid te creëren: sommige politiezones hebben de middelen voor dat soort onderzoek, andere niet. Dit debat kadert binnen de ruimere vraag op welk niveau welke onderzoeken het best worden gevoerd. Er zijn ook verschillende niveaus van informaticacriminaliteit. Bovendien is er vaak een internationaal aspect aan dat soort criminaliteit, die dus een internationale aanpak vergt.

4. ***Antwoorden van de heer Piet Pieters en mevrouw Leen Depuydt, vertegenwoordigers van het Nationaal Crisiscentrum (NCCN)***

*De heer Piet Pieters* is van oordeel dat er inderdaad meer maatregelen nodig zijn ten aan zien van aanbieders van essentiële diensten en van kritieke infrastructuren. Wel is het zo dat we op dat vlak op de goede weg zitten. Belangrijk in deze context is het onderscheid tussen een dreigingsanalyse en een risicoanalyse. Bij een dreigingsanalyse wordt gekeken naar de dreiging zoals ze op ons afkomt vanuit een bepaalde actor die een bepaalde capaciteit en intentie (bijvoorbeeld een bepaalde ideologie) heeft. In dit geval ligt de nadruk op de probabiliteit. Bij een risicoanalyse wordt dan weer vooral gekeken naar de impact. De heer De Bruycker heeft gesteld dat bij een cyberaanval de aanvaller zijn target, techniek en kracht kiest. De heer Van Leeuw vulde dat aan met de stelling dat kleine investeringen grote schade kunnen vermijden. Dat is de kern van de zaak: het gaat om de veiligheidscultuur. Op een bepaald ogenblik moet men aanvaarden dat het type risico waar men voor staat niet eenduidig is en dat het niet precies te voorspellen valt. Dat betekent dat men moet werken aan de kant van de verdediging in de wetenschap dat men niet weet vanwaar de vijand zal komen. De verhoging van de veiligheidscultuur betekent dus inderdaad dat de overheid en de vitale sectoren zich extra zullen moeten wapenen door bijkomende walls en firewalls aan te leggen, ook al is het reële dreigingsniveau niet

si le niveau de menace réel est inconnu. La sécurité générale devra donc être renforcée. La directive SRI et la directive CER l'encouragent indéniablement.

En outre, il s'agit d'une solution à plusieurs niveaux. Cela signifie qu'une combinaison de mesures est toujours nécessaire. Dans le même temps, les risques sont également de natures diverses. C'est comme une maison avec un excellent système d'alarme, mais dont la clé de la porte est cachée sous le paillasson et la fenêtre a été laissée ouverte. La sécurité doit être organisée selon les principes de sûreté et de sécurité. C'est exactement l'objectif des deux directives susmentionnées. L'attention est également attirée sur les plans d'urgence internes: il faut se préparer à une situation dans laquelle les choses tournent mal. Dans cette préparation, il faut supposer que l'approche ne sera pas entièrement couronnée de succès. Les risques non intentionnels doivent également être pris en compte, au même titre que les risques intentionnels. Par exemple, des accidents se produiront tout simplement en raison de la forte interconnectivité de la 5G (défaillance technologique). Des sauvegardes peuvent bien sûr être prévues, mais même de telles mesures de prévention peuvent s'avérer insuffisantes dans la pratique, à l'instar de l'incident Proximus de janvier, où le backup utilisait le même réseau que le système principal.

*Mme Leen Depuydt* explique que l'on a déjà connu quatre phases fédérales de planification d'urgence au printemps 2021 (pour les télécommunications, le terrorisme, le cyber et le COVID-19). Le déclenchement des phases fédérales a montré que les structures de gestion de crise fonctionnent efficacement.

Des leçons ont-elles déjà été tirées de la phase fédérale déclenchée à la suite de la cyberattaque contre le SPF Intérieur? L'incident est trop récent pour pouvoir l'affirmer, mais une évaluation est bien évidemment prévue. On peut déjà en conclure que la coopération entre les services concernés s'est bien déroulée. La discrétion dont a fait preuve chaque organisme impliqué a permis de mener l'opération en toute sécurité. La communication n'a eu lieu qu'après avoir transféré les données en lieu sûr.

Pour accroître la résilience de la Belgique face aux incidents de télécommunications, il convient de recenser les vulnérabilités de chaque type de service de télécommunications et de déterminer quelles mesures préventives peuvent être prises pour réduire ces vulnérabilités.

Si les systèmes de communication alternatifs ne sont pas disponibles pendant la gestion de la crise, le NCCN dispose d'une série de systèmes de secours, notamment le système radio ASTRID et le réseau REGETEL. Ce

gekend. De algemene beveiliging zal dus moeten worden verhoogd. De NIS-richtlijn en de CER-richtlijn moedigen dat in elk geval aan.

Bovendien is de oplossing *multi layer*. Dat betekent dat steeds een combinatie van maatregelen vereist is. Tegelijk zijn ook de risico's divers. Het is zoals een huis met een uitstekend alarmsysteem, maar waar de huissleutel onder de mat ligt en het raam openstaat. De beveiliging moet worden georganiseerd vanuit de zorg voor *safety* en security. Dat is precies wat de twee genoemde richtlijnen doen. Er wordt ook aandacht gevraagd voor de interne noodplanning: er is voorbereiding nodig op een situatie waarin het fout loopt. Bij die voorbereiding moet men ervan uitgaan dat de aanpak niet volledig zal lukken. Er moet dus evengoed rekening worden gehouden met niet-intentionele risico's als met intentionele risico's. De grote interconnectiviteit van 5G zal er bijvoorbeeld ook voor zorgen dat er gewoonweg ongelukken gebeuren (technologisch falen). Uiteraard kan in back-ups worden voorzien, maar ook dat blijkt in de praktijk niet altijd voldoende te zijn, zoals bleek uit het incident bij Proximus in januari, waarbij het backupsysteem gebruik maakte van hetzelfde netwerk als het hoofdsysteem.

*Mevrouw Leen Depuydt* legt uit dat het voorjaar van 2021 al vier keer een federale fase van de noodplanning heeft gekend (voor telecom, voor terrorisme, voor cyber en voor COVID-19). De federale fases hebben aangetoond dat de structuren van het crisisbeheer performant werken.

Werden reeds lessen getrokken uit de federale fase rond de cyberaanval op de FOD Binnenlandse Zaken? Daarvoor is het incident te recent. De evaluatie staat uiteraard wel op de planning. De samenwerking tussen de betrokken diensten is alvast vlot verlopen. De discretie van elke betrokken organisatie liet toe dat de operatie op een veilige manier kon worden uitgevoerd. Er werd pas gecommuniceerd nadat de gegevens naar een veilige omgeving werden overgebracht.

Om de weerbaarheid van België bij telecomincidenten te verhogen zou voor elke soort telecomdienst in kaart moeten worden gebracht wat de kwetsbaarheden zijn en welke preventieve maatregel kunnen worden genomen om die kwetsbaarheid te verkleinen.

Wanneer de alternatieve communicatiekanalen tijdens het crisisbeheer niet beschikbaar zouden zijn, beschikt het NCCN over een reeks back-upkanalen, waaronder de ASTRID-radio's en het Regitel-netwerk. Het laatste is

dernier est un réseau physique qui dispose de serveurs autonomes dans le centre de Bruxelles. Grâce à ce réseau, les partenaires avec lesquels le NCCN échange le plus et les autorités politiques restent joignables en permanence.

Concernant la gestion de la crise en contexte de crise COVID-19, l'intervenant se réfère à la position du NCCN qui a été mise en avant lors de la commission spéciale compétente. Lors de la crise du coronavirus, les structures de crise existantes n'ont pas été utilisées comme indiqué dans le plan général d'urgence nationale. Selon le NCCN, cela s'explique par le fait que ces structures ne sont pas suffisamment connues. L'un des enseignements que l'on peut en tirer est qu'il est nécessaire d'informer davantage les groupes cibles. En outre, il faut accorder au NCCN un budget suffisant pour faire face aux dépenses nécessaires au fonctionnement opérationnel et, en particulier, à la gestion des crises au niveau national. Concrètement, il s'agit de budgets consacrés à la planification d'urgence, à l'organisation d'exercices et à l'élaboration de méthodes utiles à la gestion des crises. Le budget doit également être rapidement disponible pendant la gestion de la crise en tant que telle.

5. ***Réponses de M. Michaël De Laet, représentant de la Federal Computer Crime Unit (FCCU) de la police fédérale***

*M. Michaël De Laet* explique qu'Europol propose un certain nombre de plateformes de concertation et d'outils (par exemple, des systèmes d'analyse des logiciels malveillants). Une concertation est également prévue avec les pays voisins afin de favoriser le partage des connaissances et de l'expertise dans certains domaines. En outre, il est vrai que l'enquête sera menée en grande partie en Belgique. En effet, de nombreuses recherches doivent être effectuées dans le pays où les systèmes ont été forcés.

En outre, la coopération et l'échange d'informations fonctionnent sur une base de réciprocité. Entretenir de bonnes relations avec des pays tiers permet un échange d'informations qui aboutit ensuite à des enquêtes en Belgique. Il est donc également nécessaire de disposer de capacités permettant de mener des enquêtes sur la base d'informations obtenues par le biais de la concertation internationale.

Une attaque DDoS n'est pas une forme typique de *hacking*. Lors d'une telle attaque, il n'y a pas d'intrusion, ce qui rend l'attribution de l'attaque encore plus difficile d'un point de vue technique.

een fysiek netwerk dat beschikt over autonome servers in het centrum van Brussel. Het laat toe dat de meest courante partners van het NCCN en de politieke overheden ononderbroken bereikbaar zijn.

Voor het crisisbeheer in het kader van de COVID-19-crisis verwijst de spreekster naar het standpunt van het NCCN dat naar voren werd gebracht in de bevoegde bijzondere commissie. Tijdens de coronacrisis werden de bestaande crisisstructuren niet gebruikt zoals dat bepaald is in het algemeen nationaal noodplan. Dat ligt volgens het NCCN aan het feit dat die structuren niet voldoende gekend zijn. Eén van de lessen bestaat erin dat meer lessen moeten worden gegeven aan de doelgroepen. Daarnaast moet binnen het NCCN in voldoende budget worden voorzien voor noodzakelijke uitgaven voor de operationele werking, en in het bijzonder voor het beheer van crisissen op nationaal niveau. Concreet gaat het om budgetten in de noodplanning voor het organiseren van oefeningen en voor het uitwerken van systemen die kunnen helpen binnen het crisisbeheer. Ook tijdens het crisisbeheer zelf moet snel budget beschikbaar zijn.

5. ***Antwoorden van de heer Michaël De Laet, vertegenwoordiger van de Federal Computer Crime Unit (FCCU) van de Federale Politie***

*De heer Michaël De Laet* legt uit dat Europol een aantal overlegplatformen en tools (bijvoorbeeld malware analysesystemen) aanbiedt. Daarnaast is er ook overleg met de buurlanden, zodat kennis en expertise op bepaalde domeinen kan worden gedeeld. Tegelijk is het zo dat een groot deel van het onderzoek in België zal worden gevoerd. Er dient immers heel wat onderzoek te worden gevoerd in het land waar de infiltratie plaatsvindt.

De samenwerking en de informatie-uitwisseling werkt bovendien in beide richtingen. Een goede verstandhouding met andere landen heeft tot gevolg dat inlichtingen worden gegeven die aanleiding geven tot onderzoeken in België. Er is dus ook een behoefte aan capaciteit om onderzoek te voeren op basis van buitenlandse informatie.

Een DDoS-aanval is geen typische vorm van hacking. Bij een dergelijke aanval is er geen intrusie, wat de attributie van de aanval vanuit technisch oogpunt nog moeilijker maakt.

Il est vrai que certaines zones de police locale sont submergées par les plaintes pour cybercriminalité. La cybercriminalité fait désormais partie de la formation de base de tous les inspecteurs de police. Le phénomène est donc pris au sérieux, même s'il est encore possible de s'améliorer. Actuellement, un guide de signalement est également mis en place comme outil pratique pour les agents de première ligne (et donc principalement pour la police locale).

En outre, un groupe de travail rédige actuellement une circulaire sur le *phishing*. Cette circulaire n'apportera pas toutes les réponses organisationnelles, mais elle prouve déjà que la question fait l'objet d'une grande attention.

La FCCU ne joue pas un rôle central dans les cyberpatrouilles. Ce travail est principalement effectué par la section i2-IRU de la Direction de la lutte contre la criminalité grave et organisée (DGJ/DJSOC). Elle est chargée de mener des enquêtes *open source* et d'effectuer des cyberpatrouilles en second lieu. Une telle mission engendre également des problèmes de capacité.

Il ne s'agit pas tant d'un manque de connaissances techniques de la part de la police, car les membres du personnel sont tous formés pour les aspects techniques. La formation académique ne suffit généralement pas pour être immédiatement opérationnel. Même les personnes qui ont suivi une formation spéciale en cybersécurité ont malgré tout besoin de suive une formation continue. Par ailleurs, il ne faut pas surestimer les capacités techniques des auteurs. Les criminels peuvent même acheter des outils pour mener des attaques très élaborées. Ce ne sont donc pas nécessairement des experts en TIC.

Même sans le signalement de Microsoft, la cyberattaque aurait fini par être découverte. Le "*dwell time*" (la durée pendant laquelle le cybercriminel reste sur le réseau) est de 90 jours en moyenne. Certaines actions – comme les *ransomware* – sont découvertes assez rapidement, tandis que d'autres peuvent passer entre les mailles du filet pendant plus longtemps.

Un sondage a été mené auprès des pays voisins sur leurs investissements en matière de cybersécurité, mais cet exercice n'a pas permis d'obtenir beaucoup d'informations utiles. Dans tous les cas, il est difficile fournir des données chiffrées à ce sujet. Par exemple, le salaire du personnel de la FCCU est-il également considéré comme un investissement dans la lutte contre la cybercriminalité?

Il est vrai que l'application Safeonweb du CCB revient, en quelque sorte à mettre un emplâtre sur une jambe de bois. Cependant, cela n'enlève rien à l'ampleur de

Het klopt dat sommige lokale politiezones overspoeld worden met klachten over cybercriminaliteit. Informaticacriminaliteit zit thans in de basismodule van alle politie-inspecteurs. Er is dus zeker aandacht voor de problematiek, al is er welllicht nog ruimte voor verbetering. Momenteel wordt ook een aangiftegids al praktische werktool uitgerold ten behoeve van de eerstelijns politiemedewerkers (en dus in hoofdzaak voor de lokale politie).

Voorts is een werkgroep bezig met een omzendbrief over phishing op punt te stellen. Die omzendbrief zal niet alle organisatorische antwoorden ter zake aanreiken, maar het toont alvast aan dat de problematiek heel wat aandacht krijgt.

De FCCU doet niet zozeer aan cyberpartrouillering. Dergelijk werk wordt vooral uitgevoerd door de sectie i2-IRU van de Directie van de bestrijding van de zware en georganiseerde criminaliteit (DGJ/DJSOC). Die is belast met *open source* onderzoeken, en voert in tweede instantie cyberpatrouilles uit. Ook een dergelijke taak gaat gepaard met capaciteitsproblemen.

Het gaat bij de politie niet zozeer om een gebrek aan technische kennis. De personeelsleden worden sowieso op technisch vlak bijgeschoold. De academische opleiding volstaat doorgaans niet om meteen operationeel te zijn in de materie. Ook de personen die opleidingen hebben genoten die toegespitst waren op cyberveiligheid hebben een blijvende nood aan bijscholing. Tegelijk mogen ook de technische capaciteiten van de daders niet worden overschat. Criminelen kunnen zelfs tools aankopen om geavanceerde aanvallen te kunnen uitvoeren. Het zijn dus niet per definitie IT-experten.

Ook zonder de melding van Microsoft de cyberaanval uiteindelijk ontdekt geworden zijn. De gemiddelde "*dwell time*" (de termijn binnen dewelke de cybercrimineel in het netwerk vertoeft) 90 dagen bedraagt. Sommige feiten – zoals bij ransomware – worden vrij snel ontdekt, terwijl andere activiteiten langer onder de radar kunnen blijven.

Er is een bevraging geweest van de buurlanden naar hun investeringen in cyberveiligheid, maar die oefening heeft weinig bruikbare informatie opgeleverd. Het is hoe dan ook een moeilijke opdracht om dat te becijferen. Is bijvoorbeeld ook het loon van de personeelsleden van de FCCU een investering in de strijd tegen cybercriminaliteit?

Het is juist dat het CCB met de toepassing Safeonweb in zekere zin dweilt met de kraan open. Dat doet echter niets af van het feit dat dit belangrijk werk is. Het spreekt

la tâche que cette application représente. Il va sans dire que tous les signalements ne peuvent pas donner lieu à une enquête approfondie. C'est précisément en cela que la cybercriminalité se différencie des autres formes de criminalité. Un cambrioleur ordinaire ne peut réaliser qu'un nombre limité de cambriolages. Un cybercriminel peut, quant à lui, escroquer des milliers de personnes à la fois, d'où l'importance capitale d'une politique préventive. Certes, il est recommandé de renforcer la capacité de la FCCU, mais il ne sera pour autant jamais possible d'enquêter de manière approfondie sur tous les signalements.

Le tableau organique de la FCCU prévoit 44 ETP. Il y a actuellement 30 collaborateurs. Il s'agit d'une tendance positive, car l'année dernière, la section s'est considérablement développée. Il convient de noter en parallèle que le recrutement de personnel est structurellement trop faible pour remplir ce cadre. Les RCCU font face au même problème. La rigidité des structures et des statuts entrave tout simplement la mise en place d'une politique de recrutement flexible. Il ne s'agit donc pas seulement de rémunération, mais aussi d'organisation. Le tableau organique de la FCCU, par exemple, comprend principalement des postes d'inspecteur principal spécialisé. Par conséquent, leur sélection – et parfois leur rejet – se fait en fonction des capacités requises pour un fonctionnaire de police dirigeant. En conséquence, des candidats qui ont les capacités techniques nécessaires sont régulièrement laissés de côté.

voor zich dat niet alle meldingen aanleiding kunnen geven tot een doorgedreven onderzoek. Het is net de schaalgrootte die de cybercriminaliteit anders maakt dan andere criminaliteitsvormen. Een gewone inbreker kan maar een beperkt aantal inbraken uitvoeren. Een cybercrimineel kan tegelijk duizenden mensen oplichten. Dat maakt een preventief beleid ontzettend belangrijk. Een capaciteitsuitbreiding van de FCCU valt aan te bevelen, maar sowieso zullen nooit alle melding uitvoerig kunnen worden onderzocht.

De organieke tabel van de FCCU voorziet in 44 VTE. Momenteel zijn er 30 medewerkers. Dat is een positieve trend, want het voorbije jaar is de sectie sterk uitgebreid. Tegelijk dient te worden opgemerkt dat er structureel te weinig personeelsinstroom is om dat kader op te vullen. De RCCU's kampen met hetzelfde probleem. De strakke structuren en statuten staan nu eenmaal een flexibel rekruteringsbeleid in de weg. Het gaat dan niet enkel om verloning, maar ook om organisatie. De organieke tabel van de FCCU bestaat bijvoorbeeld hoofdzakelijk uit gespecialiseerde hoofdinspecteurs. Zij worden dus ook gescreend – en soms afgewezen – op de capaciteiten van een leidinggevend politieambtenaar. Hierdoor vallen geregeld kandidaten uit de boot die op technisch vlak wel degelijk over de nodige capaciteiten beschikken.

## III. — **AUDITION DU 29 JUIN 2021**

### A. **Exposés introductifs**

#### 1. ***Exposés introductifs de M. Fernando Ruiz, Head of Operations, et de M. Philipp Amann, Head of Expertise and stakeholder management, représentants du Centre européen de lutte contre la cybercriminalité d'Europol***

*M. Fernando Ruiz* explique la façon dont le Centre européen de lutte contre la cybercriminalité d'Europol (EC3) apporte son soutien aux États membres dans leur lutte contre la cybercriminalité. L'EC3 a été fondé en 2013 par les États membres afin d'apporter une réponse coordonnée aux cybermenaces. Ce centre a pour mission la lutte contre les cyberattaques, la lutte contre la fraude en ligne ainsi que la lutte contre l'exploitation sexuelle en ligne des enfants. Trois unités ont été créées afin de soutenir les services médicolégaux des États membres: l'unité relative aux opérations, l'unité relative à la stratégie et l'unité relative au soutien à la police judiciaire.

## III. — **HOORZITTING VAN 29 JUNI 2021**

### A. **Inleidende uiteenzettingen**

#### 1. ***Inleidende uiteenzettingen van de heer Fernando Ruiz, Head of Operations, en de heer Philipp Amann, Head of Expertise and stakeholder management, vertegenwoordigers van het European Cybercrime Centre van Europol***

*De heer Fernando Ruiz* geeft nader toelichting bij de manier waarop het *European Cybercrime Centre* van Europol (EC3) ondersteuning geeft aan de lidstaten in hun strijd tegen cybercriminaliteit. Het EC3 werd in 2013 opgericht als reactie van de lidstaten om een gecoördineerd antwoord te geven op cyberbedreigingen. Het moet verschillende opdrachten vervullen: het bestrijden van cyberaanvallen, het online fraude bestrijden en de strijd tegen het seksueel uitbuiten van kinderen online. Om ondersteuning te bieden aan de politionele overheden van de lidstaten, werden drie eenheden opgericht: de eenheid operaties, de eenheid voor strategie en de eenheid voor forensische ondersteuning.

L'orateur attire l'attention sur le rapport annuel IOCTA (*Internet Organized Crime Treath Assessment*) de son organisation, lequel décrit les menaces majeures identifiées cette année sur l'Internet. La dernière version (d'octobre 2020) fait référence à différentes attaques, telles que des attaques DDoS, des logiciels malveillants, des rançongiciels (l'une des menaces principales, notamment pour les entreprises), mais également le vol des identifiants de connexion, la fraude en ligne et l'utilisation criminelle du *darkweb*. Le rapport étudie également l'utilisation de la cryptomonnaie par les criminels. Ce dernier indique en outre que les organisations criminelles profitent de la crise du COVID-19. Les criminels adaptent continuellement leur mode opératoire. C'est ainsi que, pendant la pandémie, ceux-ci ont davantage eu recours à des techniques telles que le phishing et autres afin de mener à bien leurs missions. La criminalité est synonyme d'évolution. Le rapport ne fait état d'aucune nouvelle menace, mais souligne que les criminels adaptent leur mode opératoire et en renforce l'efficacité.

M. Ruiz précise qu'en tant qu'agence, Europol n'a aucune compétence politique. Europol ne mène aucune enquête. Son unique rôle consiste à apporter un soutien aux États membres dans leur lutte contre la cybercriminalité au moyen d'un certain nombre de produits et de services, tels qu'un échange d'informations sécurisé entre Europol et les États membres, et entre les États membres. L'agence dispose également de capacités analytiques. Elle échange non seulement des informations, mais analyse également les informations reçues, ce qui permet d'identifier les lacunes et d'aider les États membres à développer des stratégies communes et adéquates.

L'EC3 fournit également un soutien médicolégal et analytique, notamment pour l'analyse des logiciels malveillants. En outre, il permet aussi d'analyser de grandes quantités de données (big data).

La confiance constitue l'une des valeurs fondamentales de la coopération policière. Cette dernière est essentielle afin de garantir une coopération fructueuse entre les partenaires. En vue de l'accroitre, il convient de connaitre les partenaires et de coopérer régulièrement. Pour ce faire, la J-CAT (force d'action anticybercriminalité européenne) a vu le jour en 2014 et rassemble plusieurs pays. Un *Cyber Liaison Officer* est désigné par pays et travaille quotidiennement avec ses homologues dans un seul et même espace. Ces acteurs représentent non seulement leur pays, mais forment également une équipe en matière de coopération. Ils partagent toutes les informations des enquêtes sur lesquelles ils travaillent avec l'ensemble des participants. Cette coopération est

De spreker vestigt de aandacht op het jaarlijks IOCTA-rapport (*Internet Organized Crime Treath Assessment*) van zijn organisatie, waarin een omschrijving wordt gegeven van de belangrijkste bedreigingen op het internet die dat jaar werden geïdentificeerd. In de laatste versie (van oktober 2020) wordt verwezen naar verschillende aanvallen zoals DDoS-aanvallen, malware, ransomware (één van de belangrijkste bedreigingen, voornamelijk voor bedrijven), maar ook het stelen van onlineinloggegevens, online fraude en het crimineel gebruik van het darkweb. Het rapport gaat ook dieper in op het gebruik van cryptomunten door criminelen. Verder wordt vastgesteld dat criminele organisaties gebruik maken van de COVID-19-crisis. Criminelen passen voortdurend hun *modus operandi* aan. Zo werd gedurende de pandemie meer gebruik gemaakt van technieken als phishing en dergelijke om succesvoller te zijn. Criminaliteit is een evolutie. Er worden geen nieuwe bedreigingen vastgesteld, maar in plaats daarvan passen criminele hun *modus operandi* aan en maken die meer effectief.

De heer Ruiz benadrukt dat Europol als agentschap geen beleidsbevoegdheden heeft. Zij voeren zelf geen onderzoeken uit. Hun enige rol bestaat erin om ondersteuning te bieden aan de lidstaten in hun strijd tegen cybercriminaliteit. Dit gebeurt aan de hand van een aantal producten en diensten. Eén daarvan is een beveiligde informatie-uitwisseling tussen Europol en de lidstaten en tussen de lidstaten onderling. Zij beschikken ook over analytische mogelijkheden. Er gebeurt niet enkel informatie-uitwisseling, maar de dienst analyseert ook de ontvangen informatie. Op die manier kunnen hiaten geïdentificeerd worden, en kunnen de lidstaten geholpen worden om de gepaste en gezamenlijke strategieën te ontwikkelen.

Het EC3 biedt ook forensisch en analytische ondersteuning, bijvoorbeeld voor malware analyse. Daarnaast bieden ze ook mogelijkheden aan om grote hoeveelheden data-analyses (big data) te doen.

Eén van de kernwaarden bij politionele samenwerking is vertrouwen. Dat is heel belangrijk om een succesvolle samenwerking tussen de partners te garanderen. Om dat vertrouwen te verhogen, is het nodig om de partners te kennen en regelmatig samen te werken. Hiervoor werd sinds 2014 de J-CAT (*Joint Cybercrime Action Taskforce*) opgericht met een aantal landen. Vanuit die landen wordt een *Cyber Liaison Officer* afgevaardigd, die op dagelijkse basis in één en dezelfde ruimte samenwerken. Deze mensen vertegenwoordigen niet enkel hun land maar werken ook samen als een team. Zij delen alle informatie over de onderzoeken waaraan zij werken met iedereen die eraan deelneemt. Deze samenwerking is heel buitengewoon. Door de J-CAT

exceptionnelle. La J-CAT a permis de coordonner toutes les grandes opérations en matière de cybercriminalité des dernières années.

Le démantèlement du *botnet* EMOTET constitue un exemple d'une opération de coopération au sein de la J-CAT. Ce réseau fut probablement identifié comme l'une des premières menaces par la communauté en ligne. Le *botnet* a été utilisé pour infecter plusieurs systèmes de toutes sortes de logiciels malveillants. Sous la direction des services allemands, EMOTET a pu être complètement détruit. Les administrateurs ont été arrêtés et l'infrastructure technique entièrement démantelée. Par ailleurs, le logiciel malveillant EMOTET a été remplacé par d'autres logiciels, lesquels ont permis de nettoyer tous les systèmes des victimes.

M. Ruiz aborde ensuite l'*EU Law Enforcement Emergency Response Protocol*. Il y a quelques années, il est apparu que, en cas de crise majeure, il importait de mieux coordonner les opérations. C'est pourquoi le protocole a été élaboré et constitue désormais l'un des mécanismes de réaction à une cybercrise. Son objectif consiste à apporter rapidement un soutien aux services policiers en cas de cyberattaque. Des ressources supplémentaires sont alors octroyées, notamment en matière d'analyse, de communication et de coordination.

*M. Philipp Amann* insiste à son tour sur l'importance de la diversité des partenaires du réseau, ce qui faisait partie du plan initial au lancement de l'EC3. De cette façon, les groupes de travail se composent de diverses unités de police provenant de différents États membres. Trois groupes consultatifs existent actuellement: le premier pour le secteur financier, le deuxième pour la sécurité internet et le troisième pour les fournisseurs de télécommunications. Parallèlement, il existe un réseau d'universitaires et des réseaux techniques pour la prévention ou l'enquête médicolégale. Une opération telle qu'EMOTET nécessite un tel réseau. La coopération avec différents partenaires doit être possible.

L'orateur poursuit ensuite sur la problématique des passeurs d'argent; l'un des systèmes que les criminels mettent en place pour en aider d'autres à blanchir de l'argent. Il s'agit d'annonces qui incitent les citoyens à gagner rapidement de l'argent depuis leur domicile en donnant simplement accès à leur compte bancaire. Ceux-ci ignorent ce dans quoi ils s'engagent. L'EC3 a mis sur pied un réseau avec des établissements financiers en vue de pallier ce problème, lequel s'est révélé très important pendant la pandémie. Plus de 1 000 établissements de 26 pays se sont réunis pour s'y atteler. Tout a commencé par un programme test en 2016 avec

konden alle grote operaties inzake cybercriminaliteit van de afgelopen jaren gecoördineerd worden.

Een voorbeeld van een operatie die door de samenwerking binnen J-CAT kon worden gerealiseerd, is het ten val brengen van het botnet EMOTET. Dit netwerk werd waarschijnlijk als één van de eerste bedreigingen geïdentificeerd door de internetgemeenschap. Het botnet werd gebruikt om verschillende systemen met allerlei vormen van malware te infecteren. Onder leiding van de Duitse diensten kon men EMOTET volledig vernietigen. De administrators werden gearresteerd en de technische infrastructuur werd volledig ontmanteld. Bovendien werd de EMOTET-malware vervangen door andere software waardoor alle systemen van de slachtoffers gezuiverd konden worden.

De heer Ruiz gaat vervolgens dieper in op het *EU Law Enforcement Emergency Response Protocol*. Enige jaren geleden al is gebleken dat, in geval van een grote crisis, er nood is aan een betere coördinatie van de operaties. Om die reden werd het protocol ontwikkeld. Het maakt nu deel uit van de mechanismen om te reageren op een cybercrisis. Het doel ervan bestaat erin om de politionele diensten snel ondersteuning te kunnen bieden in geval van een cyberaanval. Op dat moment worden bijkomende middelen toegekend onder meer voor analyse, communicatie en coördinatie.

*De heer Philipp Amann* benadrukt op zijn beurt het belang van het netwerk van verschillende partners. Daarin was bovendien reeds voorzien in het origineel opzet bij de start van het EC3. Zo zijn er de taskforces met de leiders van de verschillende politie-eenheden uit de verschillende EU-lidstaten. Er zijn momenteel drie adviesgroepen: voor de financiële sector, voor de internet security-sector en voor de communicatieproviders. Daarnaast is er een netwerk van academici en technische netwerken voor preventie of forensisch onderzoek. De aanpak van een operatie zoals EMOTET heeft behoefte aan een dergelijk netwerk. Men dient immers met verschillende partners te kunnen samenwerken.

De spreker gaat vervolgens verder in op de problematiek van de geldezels. Dit is één van de systemen die criminelen opzetten om andere criminelen te helpen bij het witwassen van geld. Dat zijn de typische advertenties waarbij mensen gelokt worden om snel geld te verdienen van thuis uit door eenvoudigweg toegang te verlenen tot hun bankrekeningen. Die mensen weten niet waar ze in verzeild raken. Het EC3 heeft een netwerk opgezet met financiële instellingen om dit probleem aan te pakken. De problematiek was zeer groot tijdens de pandemie. Er werden meer dan 1 000 instellingen uit 26 landen verzameld om eraan mee te werken. Het

huit pays pour évoluer, en 2019, à 31 pays participants. Le nombre d'institutions financières participantes a également augmenté durant cette période. Toutefois, les opérations ne sont pas le seul élément important. Les actions portent également sur la prévention et la sensibilisation. Pour ce faire, ce réseau organise des campagnes de prévention et des programmes de sensibilisation paneuropéens.

L'initiative "*No More Ransom*" constitue un autre exemple relatif à cette problématique et est probablement l'un des partenariats mis en place entre des partenaires publics et privés le plus réussi. Cette initiative a été lancée il y a environ cinq ans. Il s'agissait initialement d'un projet entre deux partenaires industriels et la police néerlandaise en vue d'offrir une plateforme aux victimes de rançongiciels et de mettre des instruments à leur disposition pour décrypter gratuitement leurs données et leur fournir des conseils en matière de prévention et de sensibilisation. Désormais, cette plateforme existe en 37 langues différentes, compte plus de 150 partenaires et plus de 120 instruments téléchargeables gratuitement afin de décrypter quelque 120 ransom files. À la quatrième année du programme, une estimation assez prudente a indiqué que cette initiative a permis de sauver plus de 630 millions d'euros des mains de criminels.

Enfin, M. Amann aborde la directive NIS 2. L'EC3 est un partenaire unique pour les services de police pouvant fournir des capacités et des renseignements singuliers à ces derniers. La directive NIS 2 constitue un excellent moyen de doter les services de police de davantage de possibilités afin de lutter contre les cyberattaques.

### 2. ***Exposé introductif de M. Bart Preneel, professeur à la KU Leuven, groupe de recherche "Computer Security and Industrial Cryptography" (COSIC)***

*M. Bart Preneel* déclare que l'évolution technologique fait que de plus en plus d'objets sont contrôlés électroniquement et connectés à l'Internet. Cette évolution ne peut être arrêtée. D'autre part, pour des raisons de coûts et de capacité, nous stockons de plus en plus de données sur le cloud. Il s'agit de clouds privés. Il convient de se rendre compte que le cloud ne nous appartient pas. Dès que l'on y stocke des données, l'on en perd le contrôle au profit d'un tiers. Si le réseau ou le cloud cessent de fonctionner, toutes les données sont perdues. Ce système contribue clairement à la résilience de la société et est une tendance qui ne peut être inversée.

C'est pourquoi les menaces changent également. Alors que dans les années 70 et 80, l'on pensait encore aux pirates amateurs, dans les années 90, des intérêts

begon met een testprogramma in 2016 met 8 landen en groeide in 2019 uit tot 31 deelnemende landen. Ook het aantal deelnemende financiële instellingen is in die periode toegenomen. Maar het zijn niet enkel de operaties die belangrijk zijn. De werkzaamheden hebben ook betrekking op preventie en awareness. Hiervoor voeren ze paneuropese awareness programma's en preventiecampagnes.

Een ander voorbeeld rond deze problematiek en waarschijnlijk één van de succesvolste partnerschappen die werden opgezet tussen publieke en private partners, is het "*No More Ransom*"-initiatief. Dit werd zo'n vijf jaar geleden opgestart. Initieel was dit een initiatief tussen twee industriële partners en de Nederlandse politie om een platform aan te bieden voor slachtoffers van ransomware en hen instrumenten ter beschikking te stellen om gratis hun data te decrypteren en preventie en awareness advies aan te bieden. Dit is ondertussen gegroeid tot een platform in 37 verschillende talen, met meer dan 150 partners, waar meer dan 120 instrumenten gratis kunnen gedownload worden om meer dan 120 ransom files te decrypteren. Toen het programma 4 jaar bestond werd een vrij conservatieve schatting gemaakt die aangaf dat hierdoor meer dan 630 miljoen euro verhinderd werd om in de handen van criminelen te vallen.

Tot slot gaat de heer Amann dieper in op de NIS 2-richtlijn. Het EC3 is een unieke partner voor de politionele diensten die unieke mogelijkheden en inlichtingen kan aanbieden voor deze diensten. De NIS 2-richtlijn is een uitstekende kans om politionele diensten meer mogelijkheden te bieden in de aanpak van cyberaanvallen.

### 2. ***Inleidende uiteenzetting van de heer Bart Preneel, professor aan de KU Leuven, research group "Computer Security and Industrial Cryptography" (COSIC)***

*De heer Bart Preneel* geeft aan dat de technologische evolutie ervoor zorgt dat steeds meer gebruiksvoorwerpen elektronisch gestuurd zijn en met het internet verbonden zijn. Dit is een evolutie die niet te stoppen is. Aan de andere kant slaan we omwille van kosten en capaciteit steeds meer gegevens op in de cloud. Dat zijn private clouds. Men moet goed beseffen dat de cloud de computer van iemand anders is. Op het moment dat men gegevens opslaat in de cloud, verliest men de controle erover aan iemand anders. Als het netwerk of de cloud uitvalt heeft men geen data meer. Dit heeft duidelijk implicaties op de robuustheid van de maatschappij, maar is een trend die niet te keren valt.

Daardoor veranderen ook de bedreigingen. Waar men in de jaren 70 en 80 nog dacht aan amateurhackers, komen in de jaren 90 meer financiële belangen kijken,

financiers plus importants sont entrés en jeu, grâce auxquels la criminalité organisée pouvait gagner plus d'argent. Il importe de savoir que cette criminalité est organisée de manière très professionnelle. Ce sont des groupes spécifiques qui se chargent de tâches précises de cybercrime, telles que l'exploitation de botnets, les passeurs d'argent, l'élaboration d'exploits (la découverte des failles des systèmes), etc. Cette criminalité s'articule également à l'échelle internationale.

Depuis peu, l'on constate aussi une augmentation du "hacktivisme", soit le recours au piratage à des fins politiques. À l'origine, cette pratique était le fait de groupes individuels, mais de plus en plus d'États-nations y auront également recours, notamment pour manipuler les débats politiques dans d'autres pays.

Enfin, l'on constate que les États-nations vont se lancer dans le domaine de la cybersécurité et il n'est pas uniquement question d'acteurs formels. Cette tâche incombe bien entendu à la police et aux services de renseignement, mais aussi à un nombre croissant de groupes informels qui agissent indépendamment du gouvernement, mais sont dirigés et tolérés par ce dernier, en utilisant des techniques floues sur l'Internet. En ligne, l'attribution est toujours difficile, mais l'on disposera d'un certain nombre d'attaques provenant de ces organisations informelles pour se défendre. Dès qu'il y a une fuite, l'on peut nier toute implication.

M. Preneel insiste sur le fait que la situation est devenue très complexe et étendue. L'on parle également de milliards d'euros d'investissement dans les attaques, ce qui a une incidence sur les consommateurs, qui en deviennent les victimes. Par ailleurs, il existe également de nombreux produits dangereux. Des articles sur des piratages paraissent au quotidien, et cela ne va qu'augmenter. Plus nous serons dépendants de l'information, plus ce problème prendra de l'ampleur en cas de non-fonctionnement.

L'orateur fournit ensuite un certain nombre d'exemples d'appareils technologiques qui fonctionnent par communication sans fil, tels que les pacemakers. Ces derniers ne sont absolument pas sécurisés et peuvent être facilement piratés. Pourtant, encore peu d'efforts semblent être fournis pour accroître leur sécurité. Le gouvernement doit agir à cet égard.

Une évolution similaire touche également les infrastructures critiques. Nous dépendons toujours plus de la technologie, notamment en matière de services de première nécessité, mais aussi concernant les informations du gouvernement. M. Preneel fournit plusieurs

waarmee de georganiseerde misdaad meer geld kon verdienen. Belangrijk om weten is dat deze zeer professioneel georganiseerd zijn. Het gaat om specifieke groepen die zich bezighouden met specifieke takken van online misdaad zoals het runnen van botnets, geldezels, het schrijven van exploits (het vinden van zwakheden in systemen) en dergelijke. Dit is ook heel internationaal georganiseerd.

Recent zien we ook het toenemend "hacktivisme". Dit is het voor politieke doeleinden gebruik maken van hacken. Dat gebeurde in eerste instantie door individuele groepen, maar ook meer een meer natiestaten zullen hiervan gebruik maken, bijvoorbeeld voor het manipuleren van politieke debatten in andere landen.

Ten slotte kan men vaststellen dat de natiestaten zich zullen begeven op het pad van de cyberveiligheid. Het gaat niet alleen om formele actoren. Natuurlijk is dat een taak voor politie en inlichtingendiensten, maar ook een toenemend aantal losse groeperingen die onafhankelijk van de overheid, maar wel aangestuurd en getolereerd door de overheid, aan de hand van schimmige technieken op het internet gaan ageren. Online is attributie altijd al moeilijk, maar men zal als bijkomende verdedigingslaag een aantal aanvallen vanuit die losse organisaties laten vertrekken. Van zodra iets uitlekt, kan men dan natuurlijk alle betrokkenheid ontkennen.

De heer Preneel benadrukt dat het landschap dus heel complex is geworden en heel omvattend. Het gaat ook om miljarden euro die worden geïnvesteerd in aanvallen. Dit heeft ook een impact op de consumenten. Zij worden daar het slachtoffer van. Er zijn ook heel wat onveilige producten. We lezen ook dagelijks over hacks en dit zal alleen maar toenemen. Hoe meer we afhankelijk worden van informatie, hoe groter dit probleem ook zal worden als die dingen niet werken.

De spreker geeft vervolgens een aantal voorbeelden van technologische toepassingen die met draadloze communicatie worden bestuurd, zoals pacemakers. Die zijn helemaal niet zo veilig en kunnen gemakkelijk gehackt worden en daar is nog steeds weinig verbetering zichtbaar om die veiliger te maken. Het is duidelijk dat de overheid op dat vlak moet ingrijpen.

Een gelijkaardige evolutie is ook vast te stellen bij de kritische infrastructuur. We worden steeds meer afhankelijk van technologie ook voor nutsvoorzieningen, maar ook voor informatie van de overheid. De heer Preneel geeft een aantal voorbeelden van internationale incidenten

exemples d'incidents internationaux au cours desquels l'approvisionnement en énergie, entre autres, fut paralysé par des cyberattaques.

Il convient de se rendre compte que ces attaques peuvent provenir d'appareils privés. Le *botnet* Mirai en est la preuve. Il s'agit notamment de webcams et autres appareils utilisés à domicile. Ceux-ci sont piratés et utilisés dans un *botnet* en vue d'attaquer d'autres réseaux. Le *botnet* Mirai a été utilisé en vue de couper quelque temps l'Internet de la côte est des États-Unis. L'attaque de SolarWinds, révélée à l'automne 2020, constitue un exemple plus récent.

Il y a une vingtaine d'années, le *Common Vulnerabilities and Exposures* (CVE) a commencé à enregistrer des données numériques à ce sujet, et ces incidents sont également classés en fonction de leur incidence. À l'heure actuelle, deux nouvelles faiblesses sont trouvées toutes les heures, soit entre 18 000 et 19 000 failles par an. Une faiblesse sur sept est sévère, c'est-à-dire qu'elle permet de prendre le contrôle d'un système à distance. Une solution n'est parfois jamais trouvée, mais cette situation ne dure généralement pas plus de 60 jours. Il existe souvent des moyens d'exploiter cette faiblesse un petit mois avant qu'elle ne devienne publique.

Des systèmes extrêmement complexes interagissent avec d'autres réseaux tout aussi complexes. L'être humain a créé un outil qu'il ne peut maitriser entièrement et qui comporte encore de nombreuses failles. La responsabilité de cela est floue, surtout au sujet des appareils informatiques. Si une webcam s'avère piratable, personne n'est responsable. L'on manque également clairement d'expertise.

Il s'agit plutôt d'une question économique, car des codes antipiratages peuvent être élaborés, mais sont très onéreux. La question reste donc de savoir si nous sommes prêts à ouvrir le portefeuille pour accroître la sécurité, ce qui n'est apparemment pas le cas. De plus, ceux qui lancent un produit sur le marché en voient rarement les inconvénients. Par conséquent, ils ne voient pas l'intérêt d'investir davantage dans la sécurité.

La fraude en matière de cartes de crédit illustre cette tendance. Toutes les x années, l'on reçoit une nouvelle carte de crédit, souvent parce que les systèmes ont été piratés et qu'un tiers a retiré de l'argent à l'aide de cette carte. La banque envoie une nouvelle carte et continue comme si de rien n'était. La fraude en matière de cartes de crédit s'élève à des dizaines de milliards d'euros. Cependant, cette technologie n'a été que très

waarbij onder meer energievoorzieningen werden lamgelegd door cyberaanvallen.

Het is belangrijk te beseffen dat die aanvallen kunnen uitgaan van particuliere toestellen. Het Mirai botnet is zo'n voorbeeld. Het betreft onder meer webcams en andere toestellen die thuis worden gebruikt. Die worden gehackt en gebruikt in een botnet als hulpmiddel om andere netwerken te gaan aanvallen. Het Mirai botnet is gebruikt geweest om het internet een tijdlang plat te leggen in de Oostkust van de Verenigde Staten. Meer recent is er ook de Solarwinds-aanval, die aan het licht is gekomen in de herfst van 2020.

Zo'n twintig jaar geleden is men begonnen met het registreren van cijfergegevens hierover door het *Common Vulnerabilities and Exposures* (CVE) en waarbij deze incidenten ook worden geclassificeerd op grond van hun impact. Op dit moment worden elk uur twee nieuwe zwakheden gevonden. Zo worden 18 à 19 000 zwakheden per jaar gevonden. Eén op zeven daarvan is ernstig, wat dus toelaat om op afstand een systeem over te nemen. Een oplossing komt soms nooit, maar gemiddeld duurt het 60 dagen. Vaak is het zo dat er manieren zijn om die zwakheid uit te buiten een kleine maand voor die publiek wordt.

Het gaat om heel complexe systemen die in zeer complexe netwerken met elkaar interageren. We hebben als mensen iets gecreëerd dat we niet volledig kunnen beheersen en dat vol fouten blijft zitten. De verantwoordelijkheid ervoor is onduidelijk, voornamelijk voor informaticatoestellen. Als een webcam hackbaar blijkt te zijn, dan is er niemand aansprakelijk. Er is ook duidelijk een gebrek aan expertise.

Het gaat echter om een economische vraag, want niet hackbare codes kunnen wel gemaakt worden, maar kosten duizendmaal meer. De vraag blijft dus of we zoveel meer willen betalen voor meer veiligheid. Blijkbaar is dat niet zo. Het is ook zo dat diegene die het product op de markt brengt er meestal niet het nadeel van heeft. Hij heeft er dus geen belang bij om meer te investeren in die veiligheid.

Voorbeelden hiervan zijn de fraude met creditcards. Om de zoveel jaar krijgt men een nieuwe creditcard, vaak omdat systemen werden gehackt en iemand anders bedragen afhaalt met die kaart. Men krijgt dan een nieuwe kaart, en alles gaat gewoon verder. Dit gaat om een zeer groot volume van tientallen miljarden euro aan creditcardfraude. Nochtans is die technologie heel weinig aangepast en doet men daar dus eigenlijk weinig aan.

peu adaptée. Par conséquent, la situation ne bouge pas beaucoup. Les sociétés de cartes de crédit récupèrent ces pertes auprès des commerçants.

C'est ainsi que nait le phénomène du "*market of lemons*". Un "*lemon*" est une voiture d'occasion aux États-Unis comportant de nombreux défauts cachés que l'on constate après l'achat. Les Américains savent qu'un vendeur de voitures d'occasion peut acheter de telles voitures et dépenseront, par conséquent, très peu d'argent pour ce type de véhicules. Il en va de même pour la sécurité en ligne. L'utilisateur ne peut pas savoir si une webcam est mieux qu'une autre. Il faut parfois des mois pour identifier les systèmes sûrs et ceux qui ne le sont pas. De plus, le consommateur va également acheter le produit le moins cher et le producteur ne va pas investir davantage dans la sécurité de ce dernier. L'on peut donc parler de défaillance du marché.

Dans 20 ans, nous regarderons la sécurité internet d'aujourd'hui avec beaucoup d'incompréhension. L'orateur se demande également comment l'on peut autant dépendre des technologies informatiques sans toutefois suivre des règles de sécurité minimales.

Une réglementation est nécessaire. Le secteur ne l'entend pas de cette oreille, car, compte tenu de la complexité, il ne considère pas appropriée une réglementation relative à la responsabilité. L'année dernière, l'Union européenne a rédigé le Règlement sur la cybersécurité, lequel n'a pas remporté un franc succès. La certification constitue la solution principale: contrôler ce qui existe plutôt que dire ce qu'il convient de faire. C'est également volontaire. C'est de cette façon que les critères communs ont été adoptés. Ces derniers datent du début des années 90. Ce système est lent, chronophage et n'est pas très efficace. C'est la première solution que propose l'Europe. Les États membres, qui disposent d'une infrastructure considérable de laboratoires et de fournisseurs et collaborateurs gouvernementaux, lesquels travaillent sur des critères communs et estiment que c'est l'unique solution, exercent une très forte pression.

M. Preneel estime qu'il ne s'agit pas d'une bonne solution. Il vaudrait mieux commencer par exercer une pression sur les fournisseurs afin de fournir davantage de solutions en matière de sécurité et de meilleures directives sur la façon de renforcer la sécurité. Ce n'est qu'ensuite que l'on pourrait vérifier si ces exigences sont respectées au moyen de la certification.

En outre, des différences existent entre les États membres. Il est beaucoup plus intéressant de chercher à obtenir la certification par le biais d'un grand État membre que par celui d'un plus petit.

Dat verlies verhalen de kredietkaartmaatschappijen op de handelaars.

Zo krijg je ook het fenomeen van "*market of lemons*". Een "*lemon*" is een tweedhandswagen in de Verenigde Staten die heel veel verborgen mankementen heeft die pas na de aankoop zichtbaar worden. Mensen weten dus dat de kans bestaat dat een tweedhandswagenverkoper een dergelijke wagen kan verkopen en zullen dus ook heel weinig geld uitgeven aan zo'n wagen. Hetzelfde treffen we aan bij internetbeveiliging. De gebruiker kan niet zien of een webcam beter is of niet. Het kost vaak maanden werk om na te gaan welk systeem veilig is en welk niet. De consument zal dan ook de goedkoopste kopen en de producent zal niet investeren in meer veiligheid. Er is dus duidelijk sprake van marktfalen.

Over 20 jaar zullen we terugkijken op de huidige internetbeveiliging met heel wat onbegrip. De spreker vraagt zich dan ook of hoe het kan dat we heel afhankelijk zijn van IT, maar qua veiligheid toch niet een aantal minimale regels volgen.

Er is duidelijk nood aan regelgeving. De industrie hoort dat niet graag. Gezien de complexiteit zien zij een aansprakelijkheidsregelgeving niet zitten. Vorig jaar heeft de Europese Unie de *Cybersecurity Act* geproduceerd, maar dit is eigenlijk een vrij zwak antwoord. Het antwoord ligt vooral in certificatie. Dat is checken wat er aanwezig is en niet zeggen wat er moet gebeuren. Het is ook vrijwillig. Zo heeft men in de eerste plaats de common criteria aangenomen. Die dateren van begin de jaren 90. Dit systeem is traag, duur en niet erg effectief. Dit is de eerste oplossing die Europa nu voorstelt. Er is namelijk een heel grote druk van de lidstaten, die een enorm grote infrastructuur hebben van labo's en overheidsleveranciers en -medewerkers, die aan common criteria werken en dit als enige oplossing zien.

De heer Preneel meent dat dit een verkeerde oplossing is. Men zou eerst de leveranciers onder druk moeten zetten om in meer beveiligingsoplossingen te voorzien. Betere richtlijnen geven over hoe dingen beter te beveiligen. Pas daarna zou men via certificatie kunnen testen of daaraan voldaan is.

Er is ook een verschil tussen de lidstaten. Het is veel interessanter om via een grote lidstaat om certificering te vragen dan via een kleinere.

Le rôle de la police et de la justice intervient également. Ces acteurs doivent garantir la sécurité du citoyen. Les juges d'instruction peuvent autoriser des perquisitions à domicile ou des écoutes téléphoniques. Ils préfèrent garder cette possibilité et estiment que la technologie ne devrait pas changer cela. À l'inverse, un certain nombre d'experts et d'ONG estiment que les systèmes actuels ne sont déjà plus très sûrs. Le fait d'autoriser la police à pénétrer dans toutes sortes de failles renforce davantage cette insécurité. Les autorités demandent donc une sorte de solution magique qu'elles seules peuvent utiliser.

Par ailleurs, un très grand risque de surveillance massive existe, ce qui permet aux pays de récolter de très nombreuses informations. Il s'agit bien entendu d'un tout autre débat, mais il importe surtout de souligner que ces problèmes sont interdépendants. L'on ne peut pas demander un accès pour la police ou la justice, et penser que cela n'aura pas d'incidences sur la cybersécurité des citoyens, des entreprises et des autorités.

L'orateur fait ensuite référence à la déclaration d'Edward Snowden: "*Collect it all, know it all, exploit it all.*" Les services de renseignement étaient limités par les budgets et le nombre de collaborateurs à leur disposition. La technologie a fait disparaitre cette barrière. La technologie permet de collecter toutes les informations de tout le monde à partir de moins de ressources, mais cette dernière est également sujette aux piratages. Sur l'Internet, la différence entre l'écoute clandestine et l'intrusion n'est qu'un tout petit pas. Des services de renseignement sont passés en très peu de temps de l'écoute clandestine à l'intrusion dans des systèmes, ce qui a de nombreuses incidences en matière de risques et sur l'État de droit.

Un petit pays comme la Belgique ne dispose peut-être pas des ressources nécessaires pour développer un service tel que celui de la NSA. Cependant, tout un écosystème commercial s'est développé autour de cette dernière. Des entreprises, comme Hackingteam, proposent des services de piratage aux services de police ou de renseignement. La fuite des données de Hackingteam a révélé que leur liste de clients comprenait un certain nombre de régimes non démocratiques. L'orateur constate donc que l'Union européenne tolère, voire soutient, des services de piratage qui, d'une part, aident les forces de police, mais, d'autre part, causent des dommages à l'échelle mondiale. L'on ne peut donc pas agir de la sorte sans causer de dommages collatéraux. De telles pratiques reviendront comme un boomerang dans le visage des autorités.

Normalement, les chercheurs étudient les faiblesses des systèmes et les notifient. Ces équipes de piratage

Daarnaast is er ook de rol van politie en justitie. Die moeten instaan voor de veiligheid van de burger. Onderzoeksrechters kunnen zo huiszoekingen of telefoontaps toestaan. Zij willen dit liefst ook zo behouden en vinden dat de technologie dit niet mag veranderen. Daartegenover staan een aantal experts en ngo's die aangeven dat de systemen nu reeds heel onveilig zijn. Het toelaten van allerlei achterpoortjes voor politiediensten om binnen te dringen, maakt dit nog onveiliger. Wat de overheid hier dus vraagt, is een soort magische sleutel die alleen zij mogen gebruiken.

Bovendien is er ook een heel groot gevaar voor "*mass surveilance*". Op die manier kunnen landen heel veel gegevens gaan verzamelen. Dit is natuurlijk een heel ander debat, maar het is vooral belangrijk te benadrukken dat die problemen aan elkaar gelinkt zijn. Je kan niet toegang vragen voor politie of justitie en denken dat dit geen implicaties zou hebben op de cyberveiligheid van de burgers, de bedrijven en de overheden.

De spreker verwijst vervolgens naar de stelling van Edward Snowden: "*Collect it all, know it all, exploit it all.*" De inlichtingendiensten waren steeds beperkt door budgetten en door het aantal mensen die zij hadden. Door de technologie is die beperking weg gevallen. Door technologie kan men met minder middelen alles verzamelen van iedereen. Maar op die manier kan men ook hacken. Digitaal is het verschil tussen afluisteren en inbreken slechts een heel kleine stap. Inlichtingendiensten zijn op zeer korte tijd verschoven van iemand afluisteren naar inbreken in systemen. Dit heeft heel wat implicaties zowel op de risico's als op de rechtsstaat.

Een klein land als België heeft mogelijks niet de middelen om zo'n dienst als de NSA uit te bouwen. Er is hierrond echter een heel commercieel ecosysteem ontstaan. Zo zijn er bedrijven, bijvoorbeeld Hackingteam, die diensten als hacken aanbieden aan politiediensten of inlichtingdiensten. Uit de gelekte gegevens van Hackingteam is gebleken dat zij onder meer een aantal niet-democratische regimes in hun klantenlijst hadden. De spreker stelt dus vast dat de Europese Unie hackingdiensten tolereren of zelfs ondersteunen die enerzijds politiediensten helpen maar anderzijds globaal schade aanrichten. Je kan zoiets dus niet doen zonder collaterale schade. Dergelijke praktijken zullen als een boemerang in het gezicht van die overheden terugkomen.

Normaal is het zo dat onderzoekers op zoek gaan naar zwakheden in systemen die ze dan vervolgens melden.

ou entreprises cherchent donc des faiblesses dans les systèmes de fabricants, mais gardent ces informations pour elles, les vendent voire les utilisent. M. Preneel fournit l'exemple du gouvernement qui trouve une faille dans le système de Microsoft, n'informe pas l'entreprise et le pirate en s'y introduisant. Il perd ensuite ce piratage, duquel peuvent découler des effets indésirables.

L'orateur recommande donc au gouvernement de renforcer les moyens en matière de cybersécurité. Certes, le CCB a été créé, mais le budget de ce service, en comparaison avec des services similaires de nos pays voisins, est beaucoup plus maigre.

Il convient également d'envisager la fusion de la sécurité civile, des services de police et de renseignement, et de l'armée. L'orateur explique qu'au niveau européen, de plus en plus de recherches en matière de cybersécurité sont effectuées par l'armée. Le monde universitaire est en quelque sorte mis à l'écart.

En outre, il convient également d'investir dans des formations. Le Parlement doit aussi investir davantage dans les services gouvernementaux. Le gouvernement travaille de plus en plus de manière numérique et par conséquent, participe aux outils de piratage et s'introduit dans des systèmes. Plus le pouvoir du gouvernement augmente, plus il convient de renforcer et adapter le contrôle.

Il souligne également que de nombreux appareils sont produits en Asie et que les logiciels sont principalement développés aux États-Unis. Nous sommes donc "cybercolonisés", ce qui affecte considérablement notre autonomie et notre souveraineté. Cette situation nous rend extrêmement vulnérables. Il convient de préciser que, lorsque l'on stocke toutes nos données sur le cloud, ce dernier n'est pas européen non plus. Toutefois, il est possible de stocker des données localement.

Enfin, M. Preneel prône également l'utilisation de systèmes libres, lesquels présentent de nombreux avantages, tels que le fait de ne plus dépendre des autres. L'on peut façonner nos propres solutions ou faire appel à plusieurs fournisseurs. La problématique des failles disparait également. L'Europe devrait donc investir encore plus dans le développement d'une technologie européenne qui reflète les valeurs européennes, loin de l'idéologie selon laquelle les données constituent le nouveau pétrole susceptible de nous rendre encore plus puissants. Nous avons besoin de systèmes plus décentralisés et plus robustes, qui ne planteront pas si

Die hackingteams of bedrijven gaan dus ook op zoek naar zwakheden in systemen van producenten, maar gaan die voor zich houden, verkopen of zelf gebruiken. De heer Preneel geeft het voorbeeld van de overheid die een zwakheid in het systeem van Microsoft vindt, dit niet meldt aan Microsoft, maar via een hack gaan inbreken in het systeem. Vervolgens verliezen ze die hack waardoor de nevenschade kan ontstaan.

De spreker beveelt dus aan dat de overheid de capaciteit in cybersecurity moet versterken. Er is wel het CCB opgericht, maar het budget van die dienst is in vergelijking met gelijkaardige diensten in onze buurlanden vele malen kleiner.

Er moet ook goed worden nagedacht over de versmelting tussen enerzijds de civiele veiligheid, de politie- en inlichtingendiensten en de militaire diensten. Op Europees niveau stelt spreker vast dat steeds meer onderzoek in cyberveiligheid militair wordt gestuurd. De academische wereld wordt voor een stuk buiten spel gezet.

Verder moet er ook meer worden geïnvesteerd in opleidingen. Het Parlement moet ook meer investeren op overheidsdiensten. De overheid werkt steeds meer digitaal. De overheid werkt dus ook mee aan hackingtools en breekt in in systemen. Naarmate de macht van de overheid groter wordt moet tegelijk de controle daarop versterkt worden en veranderen.

Hij wijst er vervolgens op dat heel wat toestellen in Azië worden geproduceerd en de software veelal in de Verenigde Staten wordt ontwikkeld. Op die manier worden wij "gecyberkoloniseerd", wat een enorme impact heeft op onze autonomie en soevereiniteit. Hierdoor worden we heel kwetsbaar. Door onze gegevens allemaal in de cloud te stoppen, moet duidelijk zijn dat die cloud ook niet Europees is. Het is ook mogelijk om gegevens lokaal te houden.

Tot slot pleit de heer Preneel ook voor open systemen. Dit geeft heel wat voordelen. Zo is men niet meer afhankelijk van anderen. Men kan zelf oplossingen bedenken. Je kan ook bij meerdere leveranciers gaan. Er is dan ook niet meer de problematiek van de achterdeurtjes. Europa zou dus nog meer moeten investeren op het ontwikkelen van Europese technologie die de Europese waarden weerspiegelt, weg van de ideologie dat data de nieuwe olie is waardoor men nog machtiger kan worden. Er moeten meer decentrale en robuuste systemen zijn, die niet omvallen als er ergens op één centraal punt veel gegevens samen komen of een hack gebeurt. Tot slot

de nombreuses données sont rassemblées en un point central ou si un piratage a lieu. Enfin, une transparence accrue sur les décisions qui influencent les systèmes est également de mise.

L'orateur reconnait que cela n'est pas une mince affaire. Dans tous les cas, le secteur européen et le monde universitaire doivent être soutenus dans l'élaboration de tels systèmes. L'on doit également compter sur l'innovation, c'est-à-dire investir dans la recherche et le développement, tout en veillant à ce que cela ne soit pas effectué par l'armée. L'innovation doit principalement se concentrer sur des applications civiles.

La numérisation offre, selon l'orateur, d'importantes possibilités, mais aussi d'importants risques. Le gouvernement devra s'adapter et investir en matière de vie privée, et doit veiller à ce que les entreprises se protègent mieux. Une coordination accrue est également nécessaire en matière d'innovation. Il convient également d'investir davantage dans la formation par le biais des marchés publics, c'est-à-dire les achats effectués par le gouvernement. Le gouvernement doit soigneusement réfléchir à la réglementation et à la surveillance, à la façon dont surveiller dans un monde complexe. Cela devra être fait très différemment que dans un monde non numérique.

### 3. ***Exposé introductif de M. Dirk Haex, codirecteur de Belnet***

*M. Dirk Haex* explique la mission spécifique de Belnet. Il fait référence à la loi du 7 mai 1999 portant création, au sein des Services fédéraux des affaires scientifiques, techniques et culturelles, d'un service de l'État à gestion séparée dénommé "Réseau télématique belge de la recherche, BELNET". Le réseau a été établi comme un service autonome avec une autonomie comptable. Concernant les activités du réseau, l'orateur renvoie à l'article 3 de la loi susmentionnée.

Le groupe "*Research and Education*" a pour principale mission de proposer des services innovants et de qualité spécifiquement conçus pour la recherche et l'enseignement supérieur. Ce groupe réunit non seulement toutes les universités belges, les hautes écoles, les centres de recherche, mais aussi les établissements scientifiques fédéraux, les hôpitaux universitaires, etc.

À l'origine, le réseau de recherche national se concentrait principalement sur la connectivité, mais la transformation numérique a de plus en plus conduit les utilisateurs de Belnet à proposer d'autres services. C'est ainsi que parallèlement à la connectivité, des missions supplémentaires ont vu le jour, telles que le pilier "*Identity, Mobility and Federation*". Le service Eduroam que

moet er ook meer transparantie zijn over beslissingen die de systemen beïnvloeden.

De spreker geeft aan dat het niet eenvoudig is om dit te bereiken. In elk geval moet de Europese industrie en de academische wereld ondersteund worden om dergelijke systemen uit te bouwen. Men moet ook rekenen op innovatie. Dit betekent investeren in R&D, maar daarbij moet men erop letten dat dit niet door de militaire wereld gebeurt. Innovatie moet in de eerste plaats op civiele toepassingen gericht zijn.

Digitalisering biedt volgens de spreker enorme mogelijkheden maar ook enorme risico's. De overheid zal zich moeten aanpassen en moeten investeren in privacy. De overheid moet ervoor zorgen dat bedrijven zich beter beveiligen. Er moet ook meer gecoördineerd worden aan de hand van innovatie. Meer investeringen in opleiding is nodig ook door procurement, de aankopen die de overheid doet. De overheid moet goed nadenken over regulering en toezicht. De manier waarop men toezicht kan houden in dergelijke complexe wereld. Dit zal heel anders moeten dan in een wereld die nog gebaseerd was op pen en papier.

### 3. ***Inleidende uiteenzetting van de heer Dirk Haex, codirecteur van Belnet***

*De heer Dirk Haex* gaat dieper in op de specifieke missie van Belnet. Hij verwijst hiervoor naar de wet van 7 mei 1999 houdende oprichting, binnen de Federale diensten voor wetenschappelijke, technische en culturele aangelegenheden, van een Staatsdienst genoemd "Belgisch telematica-onderzoeksnetwerk, BELNET". De dienst werd opgericht als autonome dienst met boekhoudkundige autonomie. Voor de opdrachten van de dienst verwijst de spreker naar het artikel 3 van deze wet.

Wat de doelgroep "*Research and Education*" betreft, bestaat de kerntaak erin om innovatieve en kwaliteitsvolle dienstverlening aan te bieden specifiek op maat van het onderzoek en het hoger onderwijs. Binnen deze doelgroep bevinden zich alle Belgische universiteiten, de hogescholen, de onderzoekscentra, maar ook de federale wetenschappelijke instellingen, de academische ziekenhuizen, en dergelijke meer.

Bij aanvang van Belnet lag de focus voor het nationaal onderzoeksnetwerk voornamelijk op de connectiviteit. Door de digitale transformatie keken de gebruikers van Belnet steeds meer naar andere vormen van dienstverlening. Naast de connectiviteit zijn er dus een aantal bijkomende opdrachten toegevoegd. Zo is het de pijler "*Identity, Mobility and Federation*". Een voorbeeld

tous les étudiants de l'enseignement supérieur utilisent pour se déplacer d'un campus à l'autre tant au niveau national qu'international en se connectant à l'aide de leurs identifiants constitue un exemple.

Il existe aussi le pilier "*Trust and Security*", qui s'est fortement développé ces dernières années et sur lequel le réseau compte miser davantage dans les années à venir.

Par ailleurs, l'on constate que les universités optent de plus en plus pour l'utilisation du cloud. Il importe donc d'établir un bon équilibre et de jouir d'une bonne approche en matière de risques. Les questions suivantes sont à se poser: pourquoi utiliser le cloud et pourquoi ne pas travailler avec nos propres systèmes? Faut-il travailler en local ou à mi-chemin entre le cloud et le local?

Le pilier "*Community Support*" propose des services sur mesure aux utilisateurs. Il importe également pour ce groupe-cible que Belnet soit enclin à la cocréation. Ce dernier a des besoins spécifiques que le réseau écoute en leur fournissant des services.

M. Haex montre le réseau auquel les utilisateurs peuvent se connecter. L'accent est mis sur la redondance et la fiabilité. Il importe que ces services soient disponibles 24h/24 et 7j/7 pour le secteur de l'enseignement, surtout durant la crise de COVID-19. Outre ces utilisateurs, les services fédéraux peuvent également se connecter. Le schéma montre aussi les points de connexion des core data centers ainsi que ceux d'un certain nombre de pays voisins. Pour ce faire, en Europe, l'intégration avec le réseau de recherche paneuropéen est très importante.

Les clients se connectent au réseau au moyen du bouton d'accès. Belnet conseille aux clients de prévoir des redondances, c'est-à-dire se connecter avec différents circuits de différents opérateurs à plusieurs nœuds. Le client est bien entendu personnellement responsable de sa gestion des risques et des budgets. Toutes les institutions ne disposent pas du budget nécessaire pour intégrer toutes les redondances ni de l'expertise pour le faire.

Il est ensuite question des connexions entre le réseau Belnet et le monde extérieur. L'orateur déclare à cet égard que le réseau est connecté à différents points d'échange internet, tels que des points d'échange internet belges, mais aussi de pays tiers, à l'Internet global ainsi qu'au réseau Géant.

Tous les pays possèdent leur réseau de recherche et sont interconnectés par l'intermédiaire du réseau Géant,

hiervan is het Eduroam-service dat alle studenten van het Hoger Onderwijs gebruiken om zich te verplaatsen naar campussen zowel nationaal al internationaal, en waardoor ze met hun username en password overal kunnen inloggen.

Er is ook de pijler "*Trust and Security*" die in de afgelopen jaren sterk is gegroeid en waar zij de komende jaren nog verder op willen inzetten.

Daarnaast zien we dat universiteiten ook steeds meer de stap zetten naar het gebruik van de cloud. Daar is een goede evenwichtsoefening en een goede risk approach belangrijk. De volgende vragen moeten hier gesteld worden: waarom de cloud te gebruiken, en waarom niet met eigen systemen werken? Moet er lokaal gewerkt worden of met iets tussenin?

De "*Community Support*"-pijler is dienstverlening op maat van de gebruikers. Tot slot is het voor deze doelgroep belangrijk dat Belnet beschikbaar is om in cocreatie te gaan. Dit is een doelgroep met specifieke noden waar zij naar luisteren en waarvoor zij diensten opleveren.

De heer Haex toont een voorstelling van het netwerk waar de gebruikers op kunnen aansluiten. Belangrijk hierbij is de inzet op redundantie en betrouwbaarheid. Voornamelijk met de COVID-19-crisis is het voor het onderwijs belangrijk dat die diensten 24/7 beschikbaar zijn. Naast deze gebruikers zijn de mogelijkheden voor de aansluiting van federale diensten en zien we op het schema ook de aansluitpunten voor core data centers. Daarnaast zijn ook nog de verbindingspunten met een aantal buurlanden. Heel belangrijk hierbij is de integratie in Europa met het paneuropese onderzoeksnetwerk.

Via de access-laag sluiten de klanten aan op het netwerk. Belnet beveelt de klanten aan om in redundantie te voorzien, dit betekent aan te sluiten met verschillende circuits van verschillende operatoren naar verschillende knooppunten. Het is natuurlijk de klant zelf die instaat voor zijn risicobeheer en zijn budgetten. Niet elke instelling beschikt over budgetten om alle redundanties in te bouwen, noch over de expertise om dit te doen.

Vervolgens zijn er de verbindingen tussen het Belnet-netwerk en de externe wereld. Hierbij moet aangegeven worden dat zij verbonden zijn met verschillende internet-exchangers, enerzijds naar het Belgisch internetknooppunt, maar ook naar andere landen, naar het globale internet, en ten slotte ook naar het Géant-netwerk.

Elk land heeft zijn onderzoeksnetwerk. Alle landen zijn met elkaar verbonden via het Géant-netwerk. Dit

le réseau de recherche paneuropéen. De cette façon, le réseau compte 50 millions d'utilisateurs finaux répartis dans 10 000 organisations. L'époque où il s'agissait d'une simple infrastructure en ligne est révolue. Aujourd'hui, les membres du réseau Géant se penchent sur l'innovation, l'échange et la coopération en matière d'informations. Le travail relatif au cloud est un exemple. Des contrats-cadres ont été élaborés à l'échelon européen avec les grands acteurs de ce monde (Amazon, Microsoft, etc.) afin d'offrir les meilleures conditions aux utilisateurs finaux.

M. Haex aborde ensuite les services fournis à l'administration fédérale. Belnet apporte une expertise spécifique sur des questions précises auxquelles l'administration fédérale est confrontée. Le réseau reçoit une dotation pour cela. C'est ainsi que l'administration fédérale connait le G-cloud depuis plusieurs années. Il s'agit d'un partenariat visant des gains d'efficacité au sein de l'administration fédérale.

En 2022, cela fera 20 ans que Belnet fournit des services à l'administration fédérale au moyen des services FedMAN et WAN. Ces derniers constituent la base sur laquelle reposent tous les services électroniques de cette administration. Belnet se charge de simplifier le transport des données vers ces applications. L'orateur insiste sur le fait que Belnet n'exploite pas personnellement les systèmes. En effet, ce sont les différents services gouvernementaux ou services de la sécurité sociale qui les exploitent.

Belnet dispose de SLA strictes avec les conseils d'administration qui gèrent le G-cloud. Des rapports sont rédigés tous les mois, lesquels font état des programmes d'amélioration du service et des modifications apportées au service en fonction des besoins de leurs clients.

À la suite de l'attaque DDoS (limitée) en 2015, un service Mitigation a été lancé en collaboration avec le CCB. Il s'agit d'une plateforme capable de bloquer les attaques volumétriques DDoS. Cette dernière est active depuis 2016 et des attaques DDoS sont mitigées tous les jours. Il s'agit d'une architecture entièrement redondante au sein de leurs centres de données, pour laquelle ils fournissent également un suivi et des rapports en temps réel. Ces plateformes évoluent également parallèlement aux techniques utilisées pour les cyberattaques.

Le renouvellement de l'infrastructure a commencé en début d'année, car les sources indiquent que l'on évolue vers des attaques plus violentes, d'une part, et car les clients demandent des fonctionnalités supplémentaires, d'autre part.

Cependant, la réalité a dépassé ce calendrier avec l'incident DDoS du 4 mai 2021, une attaque volumétrique

is dus het paneuropese onderzoeksnetwerk. Op die manier komen zij tot 50 miljoen eindgebruikers verspreid over 10 000 organisaties. De tijd dat dit een pure e-infrastructuur was, ligt reeds lang achter ons. Vandaag wordt binnen Géant gewerkt aan innovatie, uitwisseling en samenwerking rond informatie. Zo'n voorbeeld is het werken met cloud, waarvoor op het Europese niveau kadercontracten gemaakt zijn met de hyperscalers van deze wereld (Amazon, Microsoft enzovoort) om de beste voorwaarden te kunnen bieden aan de eindgebruikers.

De heer Haex gaat verder in op de dienstverlening aan de federale overheid. Belnet biedt bepaalde expertises aan op bepaalde vragen waar de federale overheid mee kampt. Zij ontvangen hiervoor een dotatie. Zo kent de federale overheid sinds enkele jaren het G-cloud-verhaal. Dit is een samenwerkingsverband waarbij gestreefd wordt naar efficiëntiewinsten binnen de federale overheid.

Belnet levert volgend jaar 20 jaar dienstverlening aan de federale overheid onder de vorm van de FedMAN en WAN-dienstverlening. Dit is de bouwsteen waar alle e-services van de federale overheid op draait. Belnet zorgt ervoor dat het transport van de data naar die applicaties wordt gefaciliteerd. De spreker benadrukt dat Belnet de systemen zelf niet exploiteert. Het zijn de verschillende overheidsdiensten of de diensten van de sociale zekerheid die de applicaties exploiteren.

Belnet heeft strenge SLA's met de bestuursorganen die de G-cloud beheren. Daarover wordt maandelijks gerapporteerd, waarbij zij service-improvement programma's en wijzigingen aan de dienstverlening in functie van de noden van hun klanten gaan toelichten.

Naar aanleiding van (beperkte) DDoS-aanvallen in 2015 werd in samenwerking met het CCB een mitigatiedienstverlening opgestart. Dat is een platform dat toelaat volumetrische DDoS-aanvallen te blokkeren. Dat platform is sinds 2016 actief en dagelijks worden DDoS-aanvallen gemitigeerd. Dit is een volledig redundante architectuur binnen hun datacenters waarbij zij ook in real time monitoring en rapportering voorzien. Deze platformen evolueren uiteraard ook mee met de technieken die gebruikt worden bij cyberaanvallen.

Begin 2021 is gestart met het vernieuwen van de infrastructuur omdat enerzijds de bronnen aantonen dat er een evolutie bezig is naar sterkere aanvallen, en anderzijds omdat door klanten naar extra functionaliteiten werd gevraagd.

De realiteit heeft die timing echter ingehaald door het DDoS-incident van 4 mei 2021. Toen was er een

extrêmement lourde du système. Le réseau Belnet a été saturé en cinq vagues. Il a rapidement été décidé de parler de cette attaque, notamment dans la presse. Plusieurs clients de Belnet ont partiellement ou intégralement perdu leur connexion. Certains clients n'ont pas été touchés ou n'ont pas signalé le problème.

Cette attaque avait été préparée. En effet, des points et clients spécifiques du réseau Belnet furent la cible de l'attaque. L'on ignore encore qui se cache derrière celle-ci. L'enquête est toujours en cours. L'on sait toutefois que l'attaque a été exécutée depuis 29 pays.

À 12h10, le plan de gestion *Major Incident & Crisis* a été mis en œuvre. Ce plan consiste à réunir plusieurs collaborateurs au sein de Belnet afin de permettre aux experts techniques de réaliser leur travail. En intervenant manuellement, les experts et les auteurs de l'attaque ont joué au chat et à la souris. Les partenaires suivants ont été impliqués dans ce plan de gestion: le CISO, le DPO, les experts réseau et sécurité, les départements opérationnels, le service de communication (externe et interne, dont le SPF Intérieur et BE-Alert), le service de gestion et le service à la clientèle. Le CCB et la CERT ont également été impliqués, tout comme le cabinet Politique scientifique, l'IBPT et la FCCU. Une plainte formelle a également été déposée le lendemain.

M. Haex explique que des travaux étaient menés dans le cadre de diverses séances de travail concernant des options de prévention très rapides. L'on craignait qu'une telle attaque pût à nouveau se produire dans les jours suivants. Les experts internes, les partenaires nationaux et internationaux, et les fournisseurs se sont préparés à mettre en œuvre une protection volumétrique supplémentaire. Apporter des changements à des infrastructures complexes comporte des risques. Là aussi, il a fallu peser le risque de prendre ou non des mesures de protection supplémentaires. Il a finalement été décidé d'ajouter une protection volumétrique supplémentaire, en faisant dévier le grand volume de données entrantes vers un "centre de nettoyage" externe. Cette expression doit être prise au pied de la lettre, car le trafic sale des données est nettoyé et seul le trafic propre est transmis au réseau.

Depuis le 5 mai 2021, de nombreuses maintenances ont été effectuées. Une plainte formelle a tout d'abord été déposée. La communication avec les clients a été très transparente. Le 7 mai 2021, une première version du rapport de l'incident est parue. Des réunions ont été organisées avec différents clients. La commission de gestion et tous les responsables IT de l'administration

extreem zware volumetrische aanval op het systeem. Het Belnet-netwerk is verzadigd geweest in vijf golven. Er is voor geopteerd om vrij snel hierover te communiceren, onder meer via de pers. Verschillende klanten van Belnet hebben gedeeltelijk of volledig verlies van connectiviteit ervaren. Er waren ook klanten die geen impact ervaren hebben, of dit niet gerapporteerd hebben.

Het was duidelijk dat dit een voorbereide aanval was. Specifieke punten van het Belnet-netwerk waren het doelwit van de aanval, en ook enkele specifieke Belnet-klanten. Wie achter de aanval zit is nog niet geweten. Het onderzoek is nog lopende. Wel is geweten dat de aanval vanuit 29 landen werd uitgevoerd.

Om 12u10 werd beslist om het *Major Incident & Crisis* managementplan in werking te laten treden. Dat bestaat erin om verschillende mensen binnen Belnet samen te brengen en te focussen om de technische experten hun werk te laten doen. Door manuele interventies werd een kat-en-muis-spel gespeeld met de aanvallers. Bij dit managementplan zijn volgende stakeholders betrokken: de CISO, de DPO, de Netwerk- en security experten, de Operationele departementen, communicatie (extern en intern, onder meer de FOD Binnenlandse Zaken en BE-Alert), het Service Management en de klantenafdeling. Ook het CCB en het CERT werden betrokken, net als het kabinet Wetenschapsbeleid, het BIPT en de FCCU. De dag nadien werd ook een formele klacht ingediend.

De heer Haex geeft verder aan dat er werd gewerkt aan de hand van diverse werksessies rond heel snelle preventiemogelijkheden. Het gevoel was er immers dat dit binnen de volgende dagen zich opnieuw kon voordoen. Samen met de eigen experten en nationale en internationale partners, en de leveranciers werd een voorbereiding gemaakt om een extra volumetrische bescherming te implementeren. Indien men aan complexe infrastructuren wijzigingen aanbrengt, houdt dit een risico in. Ook daar moesten afwegingen gemaakt worden het risico te lopen door al dan niet extra beschermingsmaatregelen te nemen. Er werd dan ook gekozen om een extra volumetrische bescherming toe te voegen. Dit gebeurt door het installeren van een afleiding van het grote volume aan data dat binnenkomt naar een externe "wasstraat". Dit moet letterlijk genomen worden omdat de vuile trafiek aan data wordt gewassen en enkel de propere trafiek wordt doorgelaten naar het netwerk.

Sinds 5 mei 2021 is ook heel wat nazorg gebeurd. In de eerste plaats werd een formele klacht ingediend. Naar de klanten toe is er heel transparant gecommuniceerd. Op 7 mei 2021 was er een eerste versie van het incidentrapport. Met verschillende klanten werden meetings georganiseerd. De beheerscommissie en alle IT-managers van de federale overheid werden

fédérale ont été informés. Lors de tels incidents, il importe grandement de procéder à une analyse post mortem et d'élaborer un *Service Improvement Plan* sur la base des informations recueillies auprès des clients et des experts. Cela permet en effet de tirer les leçons de cet incident en matière de communication, de technique et de gestion des risques.

L'orateur insiste également sur l'importance de la prévention. Belnet s'est réuni avec différents acteurs, dont le CCB dans le cadre de la stratégie de cybersécurité, laquelle a été approuvée par le gouvernement, et le cabinet politique scientifique afin de souligner leur besoin de ressources supplémentaires en la matière. Des explications ont été fournies au comité d'audit de l'administration fédérale et à l'IBPT.

Belnet a également été interrogé par d'autres opérateurs européens et belges, car il ne s'agit pas d'un cas isolé. Par conséquent, il importe de coopérer et de partager les expériences afin de résoudre le problème.

Enfin, l'orateur précise qu'un programme composé de trois projets a été lancé pour mettre en œuvre le *Service Improvement Plan*. La prévention reste bien entendu au centre des préoccupations, mais il s'agit d'un difficile exercice d'équilibre entre l'utilisation des ressources publiques et la prise de risque. La sécurité de l'information reste une priorité au sein de Belnet, tout comme la coopération nationale et internationale.

### 4. ***Exposé introductif de M. Geert Baudewijns, CEO de Secutec***

*M. Geert Baudewijns* précise que Secutec engage 58 collaborateurs travaillant pour l'entreprise dans le monde entier depuis la Belgique, le Canada, l'Irlande et les Pays-Bas. À l'heure actuelle, l'entreprise compte quelque 350 clients répartis dans 32 pays. Secutec est une société de sécurité active dans des domaines sur lesquels les autres entreprises ne se concentrent pas. L'orateur insiste sur l'importance des connaissances en matière de sécurité, non seulement en ce qui concerne le pouvoir humain, mais en particulier concernant les flux de renseignements nécessaires. En Belgique, les ressources sont extrêmement limitées en comparaison avec les ressources disponibles aux États-Unis ou en Chine. Ces dernières années, Secutec s'est fortement spécialisée dans ce domaine. C'est pourquoi, à la fin de l'année dernière, elle a remporté un important marché public du gouvernement belge, grâce auquel elle aidera à sélectionner les sources d'information intéressantes en vue de suivre des éléments spécifiques de manière précoce ou assez rapidement pour comprendre ce qui s'est passé.

geïnformeerd. Bij dergelijke incidenten is het uiteraard ook heel belangrijk om een post mortem analyse te doen en op basis van de input van de klanten en experten een *Service Improvement Plan* op te stellen. Dit moet ervoor zorgen dat op het vlak van communicatie, techniek en risk management, uit dit incident lessen worden getrokken.

De spreker benadrukt eveneens het belang van preventie. Hiervoor werd samen gezeten met verschillende actoren. Onder meer het CCB in het kader van de cybersecuritystrategie die door de regering werd goedgekeurd. Ook met het kabinet Wetenschapsbeleid om aan te geven dat zij op dit vlak nood hebben aan extra middelen. Er werd toelichting gegeven aan het auditcomité van de federale overheid en aan het BIPT.

Belnet is hierover ook bevraagd geweest door andere Europese operatoren maar ook door Belgische. Dit is immers geen alleenstaand feit. Het is dus belangrijk dat er wordt samengewerkt en dat ervaring worden gedeeld om hieraan het hoofd te bieden.

Tot slot wijst de spreker erop dat een programma werd opgestart dat uit drie projecten bestaat om het *Service Improvement Plan* op te starten. Preventie blijft natuurlijk de focus, maar dit is een moeilijke evenwichtsoefening tussen de inzet van publieke middelen en de risicobereidheid. Informatieveiligheid blijft een prioriteit bij Belnet. Ook de samenwerking op nationaal en internationaal vlak blijft in deze cruciaal.

### 4. ***Inleidende uiteenzetting van de heer Geert Baudewijns, CEO van Secutec***

*De heer Geert Baudewijns* verduidelijkt dat Secutec 58 mensen tewerkstelt die over de hele wereld voor hen werken vanuit België, Canada, Ierland en Nederland. Vandaag hebben zij een 350-tal klanten verdeeld over 32 landen. Zij zijn een security firma die werken op domeinen waar anderen niet op werken. De spreker benadrukt dat het belangrijk is bij security om kennis te hebben, niet enkel de human power maar in het bijzonder de nodige intel feeds. In België zijn de middelen zeer beperkt. Als je dit vergelijkt met de bronnen die men in de Verenigde Staten of in China of Rusland heeft, dan stelt dit bij ons niet zoveel voor. Dit is voor Secutec een specialisatie waar zij afgelopen jaren heel sterk in bezig zijn geweest. Om die reden hebben zij eind vorig jaar een grote overheidsopdracht gewonnen bij de Belgische overheid, waarin zij mee gaan selecteren welke informatiebronnen interessant zijn om bepaalde elementen vroegtijdig of redelijk snel op te volgen en te bekijken wat er gebeurd is.

Une attaque DDoS utilise des milliers d'ordinateurs en vue d'établir une connexion simultanée à un site internet ou une adresse IP, ce qui n'est pas un problème en soi. Cela devient en revanche problématique lorsque de nombreuses personnes se connectent et que des informations volumineuses entrent, car le site internet sous-jacent ne peut pas supporter cela. C'est ce qui s'est passé les 4 et 5 mai 2021. Le 4 mai 2021, il s'agissait d'une attaque DDoS par amplification. En d'autres termes, le *botnet* utilisé lors de l'attaque multiplie par 64 l'ensemble initial d'informations, ce qui provoque un trafic colossal vers un site internet.

De telles techniques sont monnaie courante de nos jours, également pour les attaques par rançongiciel. Il s'agit de la cybercriminalité 2.0. Il est beaucoup plus facile de mettre en œuvre une attaque DDoS et de créer une forme de rançongiciel. En ce qui concerne les clients de Secutec, une enquête est menée environ deux à trois fois par semaine à cet égard.

Secutec s'occupe de cette enquête, car elle a accès à certains renseignements que les autorités et les services de renseignement utilisent, ce qui lui confère une vue d'ensemble d'environ 70 % de l'entièreté du trafic internet mondial. La société n'a pas accès aux données en tant que telles, mais aux détails de connexion. Il s'agit des fichiers journaux, lesquels renseignent l'origine, la cible, le type de protocole et le portail utilisés. C'est tout de même unique. Secutec est probablement la seule à avoir accès à ces informations en Belgique, ce qui permet de bénéficier d'une vue d'ensemble rapide et complète de la situation.

C'est ainsi qu'il a été possible de déterminer que l'attaque a été menée de 29 pays et que 257 000 adresses IP ont été utilisées dans une source d'environ 8 millions de règles. Belnet n'a pas été la seule cible. En effet, d'autres partenaires de Secutec ont également fait les frais de cette attaque. L'orateur déclare que l'attaque provenait de 17 serveurs *botnet*. Seuls les criminels utilisent de tels serveurs. Il s'agit de serveurs très faciles à induire en erreur ou à contrôler. Il convient de noter que les serveurs qui ont été utilisés dans le cadre de cette attaque n'étaient pas connus comme serveurs, ce qui souligne la complexité de cette dernière. Cette attaque n'a pas été mise sur pied en quelques jours. Les auteurs maitrisaient très bien les fonctionnalités de sorte que l'on n'a pas pu les découvrir rapidement. Un trafic de 150 gigabytes par minute a été observé sur certains serveurs utilisés, ce qui constitue une quantité considérable de données.

Si l'on transpose l'attaque sur une ligne du temps, l'on constate deux pics, mais l'on observe également qu'entre 20h et minuit, Brutélé (qui fait partie de VOO)

Een DDoS-aanval maakt gebruik van duizenden computers om op hetzelfde moment een connectie te maken naar een website of een IP-adres. Op zich is daarmee niets verkeerd, het probleem is als men dit met zoveel op hetzelfde moment doet en met dergelijke grote data, dat de achterliggende website dit niet aankan. Dat is ook wat op 4 en 5 mei 2021 is gebeurd. Op 4 mei 2021 had men een *amplified DDoS-attack*. "*Amplified*" betekent dat het botnet dat bij de aanval gebruikt wordt, het initiële pakket informatie 64 maal zal vergroten. Dit brengt dus een enorme trafiek teweeg naar één website.

Dergelijke techniek wordt vandaag heel veel gebruikt. Ook voor ransomware aanvallen. Het is de nieuwe manier van cybercrime. Het is veel eenvoudiger om een DDoS-aanval op te zetten en op die manier een vorm van ransomware te creëren. Wat de klanten van Secutec betreft, moet gemiddeld 2 tot 3 keer per week hiernaar een onderzoek worden uitgevoerd.

Dit komt bij Secutec terecht omdat zij inzage hebben in bepaalde intel die gebruikt wordt door de overheden en inlichtingendiensten waardoor zij een overzicht hebben van ongeveer 70 % van alle internettrafiek die er wereldwijd is. Zij hebben geen inzage in de data zelf, maar wel in de connectiviteitsdetails. Dit zijn de logfiles: van waar kwam het, naar waar ging het, welk protocol is gebruikt en op welke poort is dit gebruikt. Dit is toch wel uniek. Voor België zijn zij waarschijnlijk de enige die toegang hebben tot deze informatie waardoor men vrij snel een volledig overzicht kan hebben van wat er gebeurd is.

Op die manier kon worden vastgesteld dat de aanval vanuit 29 landen werd gevoerd en werden 257 000 IP-adressen gebruikt in een bron van ongeveer 8 miljoen regels. Niet enkel Belnet had een aanval, maar ook andere partners van Secutec hadden een aanval. De spreker geeft aan dat de aanval kwam vanuit 17 botnetservers. Een botnetserver wordt enkel door criminelen gebruikt. Het is een server die zeer eenvoudig te misleiden is, of waar men controle over heeft. Belangrijk aan te geven is, dat de botnetservers die hier gebruikt werden, niet gekend waren als botnetserver. Dit wijst op de complexiteit van deze aanval. Dit is geen aanval die op enkele dagen is opgezet. Men wist zeer goed de elementen te gebruiken zodanig dat deze niet snel konden ontdekt worden. Vanuit sommige servers die gebruikt werden zagen zij een trafiek van meer dan 150 gigabyte per minuut. Dat is een enorme hoeveelheid data.

Wanneer we dit op een tijdlijn zetten, zien we inderdaad twee pieken, maar daarop zien we ook dat 's avonds tussen 20u00 en 0u00 Brutélé (onderdeel van

a connu un pic beaucoup plus important, devant traiter davantage de données que Belnet. L'attaque s'est atténuée après minuit, mais une seconde a eu lieu le lendemain, visant cette fois le réseau de Proximus et de Telenet. Selon M. Baudewijns, l'attaque de Belnet a eu plus d'incidence que l'attaque des autres réseaux, car Belnet était la première cible. Dès que la première cible est attaquée, la mise à jour de l'attaque est connue des autres et est transmise. Par conséquent, la protection des autres contre les attaques DDoS est meilleure que celle du premier attaqué.

L'orateur présente ensuite un aperçu des pays d'où provenaient les attaques. Environ 70 % provenaient du réseau nord-américain. Ce n'est pas parce que l'on voit 70 % du trafic venir des États-Unis que l'attaque y trouve son origine. L'on ne peut pas le savoir. L'enquête judiciaire devra éclaircir davantage cette inconnue. Il importe de connaitre cette information, car un opérateur met facilement fin à une attaque provenant de Corée, d'Inde ou du Bangladesh en fermant l'accès aux pays. En revanche, c'est une autre paire de manches si 90 % proviennent des États-Unis et du Royaume-Uni. Dans ce cas, il faudrait fermer tout l'Internet, car ces derniers sont les partenaires les plus importants avec lesquels communiquer. Ce point a donc aussi été très bien réfléchi.

M. Baudewijns se penche ensuite sur les adresses IP utilisées lors de l'attaque. Il convient de noter qu'il s'agit principalement d'adresses IP de Proximus. L'orateur n'est pas certain qu'il s'agissait d'une attaque contre Belnet. Le réseau a peut-être eu le malheur d'être attaqué en premier. Environ 85 % de l'attaque provenait d'une vingtaine d'adresses.

B. **Questions et observations des membres**

*M. Michael Freilich (N-VA)* aborde les opérations d'Europol à l'égard des passeurs d'argent (*money mules*). Europol a-t-elle également coopéré avec les banques belges à cet égard? Quelles étapes concrètes peuvent-elles être prises à l'encontre des passeurs d'argent? L'intervenant a introduit une proposition de résolution (DOC 55 2043/001) à ce sujet. En effet, les banques belges signalent être empêchées de partager des données en raison des règles relatives à la confidentialité et du RGPD. Les Pays-Bas et le Royaume-Uni ont recours à une vérification de l'identité IBAN afin de lutter contre les passeurs d'argent. Que pense Europol de cette mesure? L'Union européenne souhaite, par le biais de l'ENISA, créer une *cyber response team*. Europol fera-t-elle partie de cette équipe? Europol participe-t-elle aux enquêtes relatives à la récente attaque DDoS contre Belnet et à la cyberattaque du SPF Intérieur? De

VOO) een veel hogere piek kreeg waarbij zij veel meer data te verwerken kregen dan Belnet. Na middernacht is die aanval naar beneden gegaan, maar de volgende dag was er weer een aanval, toen op het netwerk van Proximus en Telenet. De aanval op Belnet heeft volgens de heer Baudewijns een grotere impact gehad als de aanval op de andere netwerken, omdat Belnet de eerste was. Van zodra de eerste aangevallen is, merk je dat de update van de aanval gekend is bij anderen en wordt doorgegeven. De DDoS-beveiliging bij de anderen is dus reeds beter dan deze van de eerste aanval.

De spreker geeft vervolgens een overzicht van de landen van waaruit de aanvallen kwamen. Ongeveer een 70 % kwam uit het Noord-Amerikaanse netwerk. Het is niet omdat we 70 % van de trafiek uit de Verenigde Staten zien komen dat de aanval van daaruit kwam. We kunnen dit niet weten; hiervoor zal het gerechtelijk onderzoek meer duidelijkheid moeten brengen. Dit is wel belangrijk, want indien een aanval komt uit Korea, of India of Bangladesch, dan is dit voor een operator eenvoudig te stoppen. Je kan dit dan op basis van de landen gaan dichtschroeven. Als om en bij de 90 % uit de Verenigde Staten en het Verenigd Koninkrijk komt, kan je dit niet doen. Dan zou je het volledige internet stilleggen omdat dit de belangrijkste partners zijn om mee te communiceren. Dus ook daar is heel goed over nagedacht.

Verder gaat de heer Baudewijns in op de IP-adressen die werden gebruikt bij de aanval. Belangrijk hierbij te vermelden is, dat dit voornamelijk IP-adressen van Proximus zijn. Het is volgens de spreker niet duidelijk of het een aanval op Belnet was. Mogelijks hebben ze de pech gehad dat zij als eerste waren. Ongeveer 85 % van de aanval kwam van een 20-tal adressen.

B. **Vragen en opmerkingen van de leden**

*De heer Michael Freilich (N-VA)* gaat in op de werkzaamheden van Europol rond de aanpak van de geldezels (*money mules*). Heeft Europol in dat verband ook met de Belgische banken samengewerkt? Welke concrete stappen kunnen tegen de geldezels worden ondernomen? De spreker heeft over de problematiek een voorstel van resolutie ingediend (DOC 55 2043/001). De Belgische banken geven immers aan dat zij verhinderd worden om gegevens te delen vanwege de regels inzake privacy en GDPR. In Nederland en in het Verenigd Koninkrijk maakt men in de strijd tegen de geldezels gebruik van een IBAN *name check*. Wat vindt Europol van die maatregel? De Europese Unie wil met ENISA werk maken van een *cyber response team*. Wordt Europol daarbij betrokken? Werkt Europol mee aan de onderzoeken rond de recente DDoS-aanval tegen Belnet en de cyberaanval op de FOD Binnenlandse Zaken? Dergelijke politionele

telles enquêtes policières et judiciaires ne peuvent pas seulement être menées par la Belgique.

M. Preneel a souligné que peu de choses avaient changé ces dernières années concernant la sécurité en matière de paiement par carte de crédit. Il existe toutefois des méthodes permettant de faire un lien avec la personne qui effectue le paiement (comme un SMS de vérification ou une application bancaire qui demande une confirmation des paiements). De telles méthodes ont-elles du sens ou les pirates informatiques peuvent-ils les éviter?

Avec l'IDO (l'Internet des objets), de nombreux appareils sont connectés à l'Internet. Contrairement aux smartphones ou aux ordinateurs portables, ces derniers ne font jamais l'objet de mises à jour de sécurité ni de corrections. Que pense M. Preneel de la proposition de retirer du marché européen les appareils qui n'autorisent pas ces mises à jour (par radio transmission, par exemple, comme le fait Tesla)? Un tel règlement est-il réaliste ou fera-t-il trop augmenter le coût de ces appareils?

Belnet s'attèle à une protection volumétrique supplémentaire. Existe-t-il une évaluation des coûts? Les ressources disponibles suffisent-elles pour payer cette protection ou faut-il des moyens supplémentaires? Le coût de la cyberattaque proprement dite a-t-il été quantifié? Est-il possible de calculer le coût d'un tel évènement?

L'enquête sur l'attaque DDoS est en cours. Il est particulièrement difficile d'effectuer une attribution dans de tels cas. Bien que les auteurs aient déjà pu être identifiés, ils peuvent toujours tenter de minimiser leur rôle. Une telle enquête est-elle donc utile?

Belnet dispose-t-il d'un CISO (responsable central de la sécurité informatique)? Belnet effectue-t-il la gestion de la sécurité en interne ou fait-il également appel à des partenaires externes? Le SPF Intérieur pourrait par exemple coopérer avec des partenaires externes en matière de gestion de la sécurité de l'information.

Existe-t-il au sein du gouvernement une personne de contact précise et facilement joignable en matière de cybersécurité? Lors de l'attaque DDoS, par exemple, la presse ignorait au début à qui s'adresser: au ministre de la Politique scientifique (ministre de tutelle de Belnet), au ministre de l'Intérieur (responsable de la sécurité), au premier ministre (responsable de la cybersécurité) ou au ministre de la Justice. À quel responsable politique Belnet peut-il s'adresser en cas de tels incidents?

en gerechtelijke onderzoeken kunnen immers allicht niet alleen door België worden gevoerd.

Professor Preneel liet optekenen dat er inzake de betaling met kredietkaarten op het vlak van beveiliging tijdens de voorbije decennia weinig is veranderd. Er bestaan evenwel toepassingen die een link maken met de persoon die de betaling uitvoert (bijvoorbeeld via een sms-verificatie of een bank-app die om een bevestiging van de betalingen vraagt). Hebben dergelijke toepassingen zin of kunnen hackers die omzeilen?

Met IoT (*Internet of Things*) zijn heel wat toestellen geconnecteerd met het internet. In tegenstelling tot smartphones of pc's krijgen die evenwel nooit veiligheidsupdates of computer patches. Wat vindt professor Preneel van het voorstel om toestellen die upgrades (bijvoorbeeld via radiotransmissie), zoals Tesla dat doet) niet toelaten van de Europese markt te weren? Is dergelijke regelgeving realistisch, of zal die de kosten van de toestellen te fel opdrijven?

Belnet maakt werk van een extra volumetrische bescherming. Bestaat daar een kostenraming van? Wordt die bekostigd met beschikbare middelen of zijn daar bijkomende kredieten voor nodig? Werden ook de kosten van de eigenlijke cyberaanval becijferd? Valt iets dergelijks überhaupt te berekenen?

Het onderzoek naar de DDoS-aanval loopt. Het is bijzonder moeilijk om in dergelijke gevallen naar een attributie te gaan. Indien de daders al kunnen worden gevonden, kunnen zij steeds hun rol trachten te relativeren. Is een dergelijk onderzoek bijgevolg wel zinvol?

Beschikt Belnet over een CISO (*Chief Information Security Officer*)? Gebeurt het veiligheidsbeheer bij Belnet intern, of worden daarrond ook samengewerkt met externe partners? De FOD Binnenlandse Zaken zou bijvoorbeeld wel met externe partners werken voor het beheer van de informatieveiligheid.

Bestaat er binnen de overheid een duidelijk en makkelijk toegankelijk aanspreekpunt voor cyberveiligheid? Bij de DDoS-aanval wist bijvoorbeeld de pers in het begin niet wie zij daarover diende aan te spreken: de minister van Wetenschapsbeleid (de toezichthoudende minister van Belnet), de minister van Binnenlandse Zaken (bevoegd voor veiligheid), de eerste minister (bevoegd voor cyberveiligheid) of de minister van Justitie. Bij welke politiek verantwoordelijke kan Belnet terecht kan in dergelijke gevallen?

M. Haex a avancé que tous les clients de Belnet n'avaient pas été victimes de l'attaque. Comment l'explique-t-il?

Le CEO de Secutec a déclaré que sa société était l'une des rares à avoir accès au trafic des données. Le gouvernement dispose-t-il de ces dernières? M. Freilich conclut, sur la base de la présentation de M. Baudewijns, que l'attaque DDoS ne visait pas Belnet, mais plutôt le système belge: VOO, Proximus, Telenet et Belnet. Y avait-il encore d'autres acteurs? Était-ce une attaque géographique ou une attaque contre un certain nombre de fournisseurs spécifiques?

Les réponses à ces questions font une grande différence en ce qui concerne l'attribution. Que dit le type d'attaque sur l'auteur potentiel? Est-il possible de mieux s'armer contre de telles attaques? Les grands fournisseurs disposent-ils automatiquement d'une protection volumétrique?

*M. Eric Thiébaut (PS)* indique tout d'abord que compte tenu de l'instruction en cours, il convient d'être prudent lorsqu'on évoque la cyberattaque du 4 mai dernier.

Il est d'avis que la cybersécurité doit garantir la sécurité des citoyens de la même manière que la police traditionnelle. Pour créer ces conditions de sécurité, la coopération internationale est essentielle. Lors des auditions du 22 juin 2021, on a en effet entendu que de nombreux faits n'étaient pas déclarés ou que s'ils l'étaient, l'opportunité de poursuivre posait question vu les moyens importants qui devaient être mis en œuvre pour ce faire et le montant souvent limité des dommages. Les représentants d'Europol pensent-ils qu'il serait possible de remédier à ce problème en regroupant, à leur niveau, l'ensemble des victimes?

L'intervenant souligne ensuite que l'exposé du professeur Preneel contient des éléments inquiétants. Concernant la sécurité des objets connectés, quel est, selon lui, le niveau le plus pertinent pour fixer un cadre législatif obligeant les fabricants à prévoir dès la chaine de production les dispositifs de protection requis? D'un point de vue juridique, comment garantir la protection des consommateurs et imposer le respect de ces normes de production? Comment pourra-t-on poursuivre ceux qui les contourneraient? Qu'en est-il de la responsabilité juridique des constructeurs en cas de piratage? Cette responsabilité a-t-elle déjà été engagée devant les cours et tribunaux? Qu'en est-il de la coopération

De heer Haex heeft erop gewezen dat niet alle klanten van Belnet slachtoffer waren van de aanval. Hoe verklaart hij dat?

De CEO van Secutec heeft gestel dat zijn onderneming als één van de weinigen toegang heeft tot de gegevenstrafiek. Beschikt de overheid over die gegevens? De heer Freilich besluit op basis van de uiteenzetting van de heer Baudewijns dat de DDoS-aanval geen aanval was tegen Belnet. Het was veeleer een aanval op het Belgische systeem: VOO, Proximus, Telenet en Belnet. Zaten er nog andere spelers bij? Was het een geografische aanval of was hij gericht tegen een aantal specifieke providers?

Naar attributie maken de antwoorden op deze vragen een groot verschil. Wat zegt het soort aanval over de mogelijke dader? Is het mogelijk om zich beter te wapenen tegen dergelijke aanvallen? Beschikken grote providers automatisch over een volumetrische bescherming?

*De heer Eric Thiébaut (PS)* geeft allereerst aan dat men, gezien het lopende onderzoek, voorzichtig moet zijn wanneer men het over de cyberaanval van 4 mei jongstleden heeft.

Volgens hem moet de cyberveiligheid de veiligheid van de burgers op dezelfde manier garanderen als de traditionele politie. Om die veiligheidsomstandigheden te creëren, is internationale samenwerking van cruciaal belang. Tijdens de hoorzittingen van 22 juni 2021 werd immers aangegeven dat van veel voorvallen geen aangifte werd gedaan of dat, zo dit wel gebeurde, bij de wenselijkheid van vervolging vraagtekens werden geplaatst omdat daarvoor aanzienlijke middelen moesten worden ingezet en vaak slechts voor een beperkt bedrag schade was geleden. Zou het volgens de vertegenwoordigers van Europol mogelijk zijn dat knelpunt te verhelpen door alle slachtoffers op hun niveau te groeperen?

Vervolgens beklemtoont de spreker dat de uiteenzetting van professor Preneel verontrustende elementen bevat. Wat is, in verband met de veiligheid van de via het internet of things verbonden voorwerpen, volgens hem het relevantste echelon om een wetgevingskader op te zetten dat de fabrikanten ertoe verplicht om vanaf de productieketen voor de vereiste beschermingsvoorzieningen te zorgen? Hoe kunnen uit juridisch oogpunt de bescherming van de consument worden gewaarborgd en de naleving van die productienormen worden opgelegd? Hoe zullen degenen die ze zouden omzeilen, kunnen worden vervolgd? Quid met de juridische aansprakelijkheid van de fabrikanten in geval van hacking? Is die

entre pouvoirs publics et universités dans le domaine de la cybersécurité?

*M. Dries Van Langenhove (VB)* indique que la problématique de la cybercriminalité gagnera encore en importance dans les prochaines années. Trop peu d'attention y est accordée par la société, les médias et la politique. En ce qui concerne la politique, le Parlement peut prêter mainforte. Des initiatives législatives efficaces doivent découler des informations reçues afin de renforcer la cybersécurité nationale.

M. Preneel a avancé qu'il existe une distorsion du marché en matière de certification, notamment dans les petits États membres. Quelles mesures peut-on prendre à l'encontre de cela au niveau fédéral?

L'intervenant s'inquiète également de la cybercolonisation, c'est-à-dire de la dépendance technologique des États-Unis et de la Chine. M. Preneel voit-il des améliorations à court terme à cet égard? L'Union européenne prend-elle entre-temps les mesures nécessaires? Peut-on entreprendre quoi que ce soit à court et long terme à l'échelon belge en vue de réduire cette dépendance?

*M. Philippe Pivin (MR)* dit apprécier les tentatives de vulgarisation faites par les intervenants pour permettre aux non-initiés de mieux comprendre la problématique des cyberattaques. L'explosion des cas est un phénomène inquiétant. Les représentants d'Europol ont évoqué l'existence d'un protocole d'urgence en cas de crise ou d'attaque de grande envergure. Peuvent-ils préciser combien de fois ce plan a été activé et si son efficacité et sa pertinence ont été évaluées? Quel est leur sentiment en ce qui concerne la coopération intraeuropéenne? Celle-ci fonctionne-t-elle de manière optimale? Qu'en est-il du degré de coopération avec des pays tiers comme les États-Unis? L'intervenant évoque à ce sujet le rapport annuel sur les crimes sur Internet publié par le FBI, dont il ressort que la Belgique figure à la dixième place dans le classement des pays (hors USA) dans lesquels on a recensé le plus de victimes de cyberattaques. Qu'en est-il de l'échange d'information et de bonnes pratiques avec les États-Unis?

M. Baudewijns a, au cours de son exposé, montré un graphique détaillant l'origine de l'attaque. À partir de ces informations, est-il techniquement possible d'identifier précisément les auteurs? Les services sont-ils outillés pour épingler les coupables?

Il semble par ailleurs que le réseau *botnet* soit utilisé de manière légale, mais aussi à des fins criminelles.

aansprakelijkheid al ter sprake gekomen voor de hoven en rechtbanken? Hoe staat het met de samenwerking tussen overheden en universiteiten op het gebied van cyberveiligheid?

*De heer Dries Van Langenhove (VB)* geeft aan dat de problematiek van de cybercriminaliteit de komende jaren de komende jaren nog aan belang zal winnen. Er wordt nog te weinig aandacht aan besteed in de samenleving, de media en de politiek. Aan dat laatste kan in het Parlement worden verholpen. Uit de ontvangen informatie moeten effectieve wetgevende initiatieven voortvloeien die de cyberveiligheid van het land bevorderen.

Professor Preneel heeft gesteld dat er marktverstoring is bij de certificering, en dat vooral in kleine EU-landen. Welke maatregelen kunnen daartegen of federaal niveau worden ondernomen?

De spreker maakt zich ook zorgen over de cyberkolonisering, zijnde de technologische afhankelijkheid van de Verenigde Staten en China. Ziet de professor op korte termijn beterschap op dat vlak? Zet de Europese Unie inmiddels de nodige stappen? Kan op het Belgisch niveau op korte en lange termijn iets worden ondernomen om die afhankelijkheid te doen afnemen?

*De heer Philippe Pivin (MR)* uit waardering voor de vulgarisatiepogingen van de gastsprekers om niet-ingewijden beter inzicht te verschaffen in het vraagstuk van de cyberaanvallen. De gigantische toename van het aantal gevallen is verontrustend. De Europol-vertegenwoordigers hebben aangegeven dat er een noodprotocol bestaat in geval van een crisis of van een grootschalige aanslag. Kunnen zij preciseren hoe vaak dat plan in werking is gesteld, alsook of de doeltreffendheid en de relevantie ervan zijn geëvalueerd? Wat vinden zij van de intra-Europese samenwerking? Werkt die optimaal? In welke mate wordt samengewerkt met derde landen, zoals de Verenigde Staten? De spreker verwijst in dat verband naar het door het FBI gepubliceerde jaarverslag over de internetcriminaliteit, waaruit blijkt dat België op de tiende plaats staat in de lijst van landen (met uitzondering van de VS) waar de meeste slachtoffers van cyberaanvallen zijn geregistreerd. Hoe staat het met de uitwisseling van informatie en best practices met de Verenigde Staten?

Tijdens zijn uiteenzetting heeft de heer Baudewijns een grafiek getoond waarop de oorsprong van de aanvallen met alle bijzonderheden stond weergegeven. Is het technisch mogelijk om aan de hand van die informatie de daders nauwkeurig te identificeren? Zijn de diensten toegerust om de schuldigen te vatten?

Voorts lijkt het erop dat het botnet niet alleen legaal maar ook voor criminele doeleinden wordt gebruikt.

Peut-on parvenir à faire la part des choses et à tracer les criminels qui en font usage?

En conclusion, M. Pivin constate que de grands efforts ne doivent pas seulement être réalisés en matière d'investissements, mais aussi en vue du recrutement de profils qualifiés.

*M. Bert Moyaers (Vooruit)* souligne que la cybersécurité constitue l'un des piliers d'activité d'Europol. Outre les cyberattaques majeures, de nombreuses victimes individuelles sont escroquées par le biais du phishing. Les passeurs d'argent incarnent de petits acteurs en matière de blanchiment d'argent. Est-il également possible de s'attaquer aux gros bonnets qui se cachent derrière ceux-ci?

Les représentants d'Europol ont abordé l'existence de la force d'action anticybercriminalité européenne. Pourquoi la Belgique n'y participe-t-elle pas? Est-il encore possible de rejoindre cette force d'action? Un certain nombre de pays ont également été impliqués dans les opérations relatives à EMOTET. Cette initiative peut-elle être plus approfondie?

La pandémie de COVID-19 traverse les frontières, la cybercriminalité encore plus. Quel rôle l'Union européenne peut-elle jouer à cet égard?

Concernant les propos de M. Preneel, l'intervenant se demande si l'approche en matière de cybercriminalité n'est pas fragmentée entre le secteur privé et le gouvernement, d'une part, et au sein du gouvernement, d'autre part. Le gouvernement ne peut-il pas acquérir plus d'expertise en réunissant les forces au sein d'un département? Les experts peuvent-ils encore être suffisamment motivés pour un emploi dans le secteur public? Comment le gouvernement peut-il attirer les talents nécessaires?

M. Haex a apporté des précisions au sujet de l'attaque DDoS. Le Conseil national de sécurité a entre-temps décidé d'investir considérablement dans la cybersécurité. Une série de crédits avait déjà été affectée. Sait-on ce à quoi ces crédits supplémentaires serviront? Les ressources supplémentaires suffisent-elles? Y a-t-il d'autres points en ligne de mire?

M. Baudewijns s'est penché sur l'achat de flux de renseignements par les institutions de cybersécurité. Dans le cadre d'un marché public, le CCB achète ces informations à Secutec. Quelle suite le CCB donne-t-il à ces informations recueillies? Que fait-on avec ce type de données? Le CCB met-il à son tour ces informations à la disposition des services de renseignement?

Kunnen die twee van elkaar worden onderscheiden en kunnen de criminelen die er gebruik van maken, worden getraceerd?

Tot besluit stelt de heer Pivin vast dat niet alleen inzake investeringen grote inspanningen moeten worden geleverd, maar ook wat de indienstneming van gekwalificeerde profielen betreft.

*De heer Bert Moyaers (Vooruit)* wijst erop dat internetveiligheid één van de activiteitenpijlers is van Europol. Naast de grote cyberaanvallen zijn er de vele individuele slachtoffers die via phishing worden opgelicht. De geldezels zijn binnen die geldtrafiek in feite de kleine garnalen. Bestaan er ook mogelijkheden om de achterliggende grootverdieners aan te pakken?

De vertegenwoordigers van Europol hebben gewezen op het bestaan van de Joint Cybercrime Taskforce. Waarom participeert België er niet aan? Bestaat er een mogelijkheid om daar alsnog in te stappen? Ook bij de werkzaamheden rond EMOTET zijn een aantal landen betrokken. Kan dit initiatief verder worden toegelicht?

COVID-19 stopt niet aan de landsgrenzen, cybercriminaliteit evenmin. Welke rol kan de EU in deze materie bijgevolg spelen?

Ten aanzien van professor Preneel stelt de spreker de vraag of de aanpak van de cybercriminaliteit niet te versnipperd is tussen de privésector en de overheden enerzijds, en binnen de overheid anderzijds? Kan de overheid niet meer expertise uitbouwen door de krachten te bundelen binnen één departement? Kunnen deskundigen nog voldoende worden gemotiveerd voor een overheidsfunctie? Hoe kan de overheid de nodige expertise aantrekken?

De heer Haex heeft toelichting verschaft over de DDoS-aanval. De Nationale Veiligheidsraad heeft inmiddels beslist tot een forse investering in cyberveiligheid. Een aantal kredieten werden reeds geoormerkt. Bestaat er al duidelijkheid waarvoor die bijkomende kredieten zullen worden gebruikt? Zijn die bijkomende middelen voldoende? Zijn er nog zaken die over het hoofd worden gezien?

De heer Baudewijns heeft gewezen op de aankoop van intel feeds door cyberveiligheidsinstanties. Het CCB koopt in het kader van een overheidsopdracht die informatie aan bij Secutec. Welk gevolg geeft het CCB aan die ingewonnen informatie? Wat doet men met dat soort gegevens? Stelt het CCB op zijn beurt die informatie ter beschikking van inlichtingendiensten?

C. **Réponses**

1. ***Réponses de M. Fernando Ruiz, Head of Operations, et de M. Philipp Amann, Head of Expertise and stakeholder management, représentants du Centre européen de lutte contre la cybercriminalité d'Europol***

*M. Fernando Ruiz* explique qu'une opération à l'encontre des passeurs d'argent est organisée chaque année à l'échelon européen. Cette dernière a eu lieu pour la première fois en 2016. Pour ce faire, l'on s'est appuyé sur un modèle utilisé par la police néerlandaise. La police belge participe à ces actions depuis 2017.

Chaque pays gère l'échange d'informations à l'échelon national. Par conséquent, les autorités belges partagent les informations avec les institutions financières belges. Si les autorités belges reçoivent des informations, elles les transmettent à Europol en vue d'exécuter une analyse globale. L'objectif des actions va au-delà de l'identification des passeurs d'argent. Dans certains cas, ces derniers ignorent avoir été utilisés à cette fin. Le but consiste à identifier les cerveaux aux commandes de ces opérations criminelles qui coordonnent le réseau des passeurs d'argent.

La Police fédérale belge a contacté Europol au sujet de l'attaque DDoS. L'enquête est toujours en cours. Comme d'habitude, la coopération entre les autorités belges et Europol se déroule très bien.

L'*EU Law Enforcement Emergency Response Protocol* (LE ERP) a été approuvé en 2018 par le Conseil européen. Depuis, ce dernier n'a été activé qu'une seule fois (partiellement), et ce en 2020 dans le cadre de la crise de COVID-19. Il ne s'agissait pas d'une cyberattaque nette. Cependant, le protocole a été partiellement utilisé, car un certain nombre d'organisations criminelles ont profité de la crise de COVID-19 pour déployer des cyberactivités. Une partie du protocole a été activée afin de contrôler l'évolution de la situation.

Europol possède des accords de coopération avec une dizaine d'agences gouvernementales policières américaines, lesquels permettent d'échanger des données à caractère personnel et des données opérationnelles avec ces dernières. Europol coopère étroitement avec le FBI et le *United States Secret Service* dans le domaine de la cybercriminalité. Ces deux organisations sont membres de la force d'action anticybercriminalité européenne (J-CAT), laquelle coordonne toutes les opérations d'envergure. La Belgique ne fait pour l'instant pas partie de cette force d'action. Elle a déjà exprimé son intérêt à participer, mais aucune demande officielle

C. **Antwoorden**

1. ***Antwoorden van de heer Fernando Ruiz, Head of Operations en de heer Philipp Amann, Head of Expertise and stakeholder management, vertegenwoordigers van het European Cybercrime Centre van Europol***

*De heer Fernando Ruiz* legt uit dat er op Europees niveau elk jaar een operatie plaatsvindt gericht tegen de geldezels. Die operatie vond voor het eerst plaats in 2016. Er werd daarbij een model overgenomen dat door de Nederlandse politie werd gebruikt. De Belgische politie participeert sedert 2017 aan deze acties.

Elk land beheert de informatie-uitwisseling op het nationaal niveau. De Belgische overheid deelt de informatie dus met de Belgische financiële instellingen. Indien de Belgische overheid informatie ontvangt, deelt zij die met Europol met het oog op het uitvoeren van een globale analyse. De doelstelling van de acties gaat verder dan het identificeren van de geldezels. In sommige gevallen weten deze immers zelf niet dat zij als geldezel worden gebruikt. Het is echt de bedoeling om de echte breinen achter de criminele operaties te identificeren. Zij coördineren het netwerk van geldezels.

De Belgische Federale Politie heeft Europol gecontacteerd in verband met de DDoS-aanval. Het onderzoek zelf is nog lopend. Zoals steeds, verloopt de samenwerking tussen de Belgische overheid en Europol zeer goed.

Het *EU Law Enforcement Emergency Response Protocol* (LE ERP) werd in 2018 onderschreven door de Europese Raad. Sedertdien werd het protocol slechts eenmaal – gedeeltelijk – geactiveerd, en dat in 2020 in het kader van de coronaviruscrisis. Het ging weliswaar niet om een zuivere cyberaanval. Wel werd het protocol ten dele aangewend omdat een aantal criminele organisaties de COVID-19-crisis aanwendden voor de uitrol van cyberactiviteiten. Er werd een tussenstap van het protocol geactiveerd om goed te kunnen monitoren of de situatie zou escaleren.

Europol heeft samenwerkingsovereenkomsten met een tiental Amerikaanse politionele overheidsagentschappen. Dat houdt in dat met deze agentschappen persoonsgegevens en operationele data kunnen worden uitgewisseld. In het domein van de cybercriminaliteit wordt nauw samengewerkt met de FBI en met de *United States Secret Service*. Deze twee organisaties zijn lid van de *Joint Cybercrime Action Taskforce* (J-CAT) waarin alle grote operaties worden gecoördineerd. België maakt vooralsnog geen deel uit van de J-CAT. België heeft wel reeds interesse getoond in een deelname, maar het is nog niet gekomen tot een officieel verzoek. Lidmaatschap

n'a été introduite. L'adhésion à la J-CAT s'accompagne de certaines obligations, telles que le détachement à temps plein d'un officier de liaison en matière de cybercriminalité.

EMOTET constitue l'un des *botnets* les plus dangereux. Un *botnet* est un réseau d'ordinateurs infectés étant sous le contrôle d'une organisation criminelle. Celui-ci peut notamment être utilisé pour crypter les ordinateurs de nombreuses victimes contre une rançon ou pour obtenir des données bancaires. L'opération contre EMOTET a démontré qu'une bonne coopération internationale peut efficacement démanteler les cybermenaces.

*M. Philipp Amann* aborde la question relative à la coopération entre Europol et l'ENISA. L'ENISA fait partie du *Program Board* de l'EC3. Ces deux entités se consultent deux fois par an à haut niveau. En 2018, les deux organisations ont conclu un mémorandum d'accord devant garantir une meilleure coopération entre l'EC3 et l'ENISA, la CERT-UE et l'agence européenne de la défense (EAD). Cet accord n'est pas juridiquement contraignant et a bénéficié de nombreux retours positifs de l'Union. Les quatre agences coopèrent sur la base d'une feuille de route et d'un plan d'action. Toutes sortes d'initiatives sont élaborées: des programmes de formation, l'échange de personnel, etc.

Enfin, l'orateur se penche sur la proposition de la Commission européenne concernant la plateforme de la *Joint Cyber Unit* contre les cyberattaques. Un premier atelier se tiendra en juillet 2021 à cet égard, auquel Europol est invité à participer. L'ENISA constitue un partenaire extrêmement important pour Europol. Leur coopération revêt différentes formes.

Se pose ensuite la question importante de savoir ce que l'on peut faire pour la cybersécurité des citoyens. Comment rendre le citoyen européen plus résistant face aux cybermenaces? L'on peut déjà en faire beaucoup en matière de prévention et de sensibilisation. C'est pourquoi des campagnes de prévention sont déployées à l'égard de groupes-cibles spécifiques (les jeunes, par exemple). Les actions d'Europol seront toujours couplées à une campagne de prévention. L'opération relative aux passeurs d'argent sera notamment couplée à une coopération avec les banques ainsi qu'à des campagnes d'information sur les risques. En outre, Europol coopère également avec le secteur concerné ainsi qu'avec un certain nombre de groupes consultatifs, conformément à plusieurs principes fondamentaux, tels que l'approche "*security by design*" et "*privacy by design*". En coopération avec le secteur, des outils sont développés, tels qu'un

van de J-CAT zorgt voor bepaalde verplichtingen, zoals het afvaardigen van een voltijds verbindingsofficier voor cybercriminaliteit.

EMOTET is een van de gevaarlijkste botnets. Een botnet is een netwerk van geïnfecteerde computers die onder de controle staat van een criminele organisatie. Aan de hand daarvan kunnen bijvoorbeeld computers van heel veel slachtoffers worden geëncrypteerd voor losgeld of worden gebruikt voor het verkrijgen van bankgegevens. De operatie tegen EMOTET heeft aangetoond dat een goede internationale samenwerking effectief kan zijn bij het ontmantelen van cyberdreigingen.

*De heer Philipp Amann* gaat in op de vraag rond de samenwerking tussen Europol en ENISA. Deze laatste maakt deel uit van het EC3 *Program Board*. Europol en ENISA plegen minstens tweemaal per jaar overleg op hoog niveau. In 2018 hebben beide organisaties een MoU (*Memorandum of Understanding*) gesloten. Die moet zorgen voor een betere samenwerking tussen EC3 en ENISA, CERT-Eu en het *European Defense Agency* (EDA). Deze overeenkomst is juridisch niet bindend. Zij krijgt wel veel positieve feedback vanuit de EU. De 4 agentschappen werken samen aan de hand van een roadmap en een werkprogramma. Er worden samen allerlei initiatieven ontwikkeld: trainingsprogramma's, de uitwisseling van personeel, enzovoort.

De spreker wijst in dit verband tot slot op het voorstel van de Europese Commissie voor het platform van de *Joint Cyber Unit* tegen cyberaanvallen. In juli 2021 vindt daarover een eerste workshop plaats. Europol heeft een uitnodiging ontvangen om daar aan deel te nemen. ENISA is voor Europol een zeer belangrijke partner. De samenwerking tussen beide neemt verschillende vormen aan.

Daarnaast is er de belangrijke vraag wat kan worden gedaan aan de cyberveiligheid van de individuele burger. Hoe kan de Europese burger weerbaarder worden gemaakt tegen cyberdreigingen? Er kan alvast heel wat worden gedaan op het vlak van preventie en het creëren van "*awareness*". Zo worden preventiecampagnes uitgerold ten aanzien van specifieke doelgroepen (bijvoorbeeld jongeren). De acties van Europol gaan steeds gepaard met een preventiecampagne. De actie rond de geldezels gaat bijvoorbeeld gepaard met een samenwerking met de banken en een informatiecampagnes die de risico's belicht. Daarnaast wordt ook samengewerkt met de betrokken industrie en met een aantal raadgevende groepen. Er wordt gewerkt aan de hand van een aantal basisprincipes, zoals dat van "*security by design*" en "*privacy by design*". Samen met de industrie worden tools ontwikkeld, zoals een certificeringsprogramma

programme de certification pour les appareils de l'IDO, où l'on se concentre sur les mises à jour de sécurité.

Comment prendre des mesures perturbatrices contre les criminels? À cet égard également, la prévention et la sensibilisation constituent les maitres-mots, permettant notamment d'éviter que des citoyens soient utilisés comme passeurs d'argent à leur insu. Une coopération de qualité avec les autres forces de police et le secteur constitue un autre instrument de taille. Cette dernière peut empêcher les criminels d'utiliser certains services pour leur modèle d'entreprise. Le démantèlement d'EMOTET en est un exemple.

2. ***Réponses de M. Bart Preneel, professeur à la KU Leuven, groupe de recherche "Computer Security and Industrial Cryptography" (COSIC)***

*M. Bart Preneel* confirme que les outils de vérification présentent certainement des avantages supplémentaires lors des paiements électroniques. Ces outils ne sont pourtant pas généralisés. L'ensemble de l'écosystème des paiements demeure non sécurisé, car aucune obligation n'impose de fixer des normes minimales, même en cas de montants importants. De nos jours, des paiements de centaines d'euros peuvent encore être effectués sans qu'un SMS de vérification soit envoyé ou qu'un code complémentaire soit demandé. Tout comme la sécurité physique, la cybersécurité doit également constituer une préoccupation collective. Si certains des acteurs clés ne participent pas pour des raisons économiques, tout le monde en pâtit.

En ce moment, aucun règlement n'existe concernant les appareils connectés à l'IDO. Il existe pourtant des normes en matière d'isolation ou de prise d'un appareil, par exemple. De telles normes ont un coût et émanent de préférence de l'Europe. L'État de Californie aux États-Unis a, par exemple, promulgué une loi relative à l'IDO. Il serait peut-être judicieux d'entamer de plus petites étapes en la matière sous la forme d'un certain nombre de lignes directrices de base.

En outre, il est également question de vigilance lorsqu'un appareil nécessite des mises à jour de sécurité. Si un appareil est réglable à distance, il se peut que le système soit piraté à son tour et adapté à distance. Un test a notamment été effectué avec des clés Tesla. Ces dernières ont été piratées et une copie pouvait être créée à partir d'une mise à jour. En conclusion, une mise à jour peut constituer un outil de sécurité supplémentaire, mais aussi une nouvelle faiblesse. La mise à jour à distance d'un appareil signifie donc que l'on perd le contrôle de ce dernier. Il est donc utile de faire vérifier par une autorité nationale ou européenne si une mise

voor IoT-toestellen, waarin aandacht wordt besteed aan veiligheidsupdates.

Hoe kan disruptief worden opgetreden tegen cybercriminelen? Ook op dat vlak zijn preventie en "*awareness*" sleutelwoorden. Er kan bijvoorbeeld voorkomen worden dat personen geheel onwetend worden gebruikt als geldezel. Een ander belangrijk instrument is de goede samenwerking met andere politieorganisaties en met de industrie. Die samenwerking kan ervoor zorgen dat criminelen geen gebruik kunnen maken van bepaalde diensten voor hun businessmodel. Het uitschakelen van EMOTET is daar een voorbeeld van.

2. ***Antwoorden van de heer Bart Preneel, professor aan de KU Leuven, research group "Computer Security and Industrial Cryptography" (COSIC)***

*De heer Bart Preneel* bevestigt dat er zeker bijkomende voordelen verbonden zijn aan verificatietools bij het uitvoeren van elektronische betalingen. Die toepassingen zijn evenwel niet veralgemeend. Het gehele ecosysteem van de betalingen blijft onveilig omdat er geen verplichting bestaat om overal die minimumnormen op te leggen, zelfs niet als het om grote bedragen gaat. Vandaag de dag kunnen nog steeds betalingen worden gedaan van honderden euro zonder dat een sms-verificatie of bijkomende code wordt gevraagd. Net zoals de fysieke veiligheid dient ook de cyberveiligheid een gemeenschappelijke bezorgdheid te zijn. Indien een aantal belangrijke spelers daar uit economische overwegingen niet aan meewerkt, lijdt eenieder daaronder.

Op dit ogenblik is er geen enkele regulering van IoT-toestellen. Wel zijn er normen waaraan bijvoorbeeld de isolatie of de stekker van een toestel moeten voldoen. Aan dergelijke normen is een kostprijs verbonden. Een dergelijke normering gebeurt best op Europees niveau. De Amerikaanse staat Californië heeft bijvoorbeeld een IoT-wet uitgevaardigd. Het is misschien aangewezen om op dit vlak te starten met kleinere stappen in de vorm van een aantal basisrichtlijnen.

Daarnaast is ook waakzaamheid geboden wanneer een toestel veiligheidsupdates vereist. Indien een toestel vanop afstand aanpasbaar is, kan ook dat systeem op zijn beurt worden gehackt en aangepast vanop afstand. Zo was er de testcase waarin Tesla-sleutels werden gehackt en via een update een kopie van de sleutels konden worden gemaakt. Een update kan dus een bijkomend veiligheidselement zijn, maar op zijn beurt ook een nieuwe zwakheid zijn. Het laten updaten van een toestel vanop afstand betekent dus het verlies van de controle over het toestel. Het is een mogelijkheid om een nationale of een Europese instantie te laten nagaan

à jour spécifique représente ou non une amélioration en termes de sécurité.

La Belgique et l'Europe disposent d'expertise dans le domaine de la sécurité des appareils connectés à l'IDO, mais il est une nouvelle fois question de personnel et de moyens. Dans tous les cas, il est recommandé de responsabiliser les fabricants. Actuellement, un producteur de webcams n'est pas responsable de la sécurité en ligne de ses appareils. Le secteur s'oppose également fermement à l'introduction éventuelle de cette responsabilité. Il va de soi qu'une telle mesure ferait grimper le prix des appareils concernés. L'orateur n'a pas connaissance d'affaires judiciaires à ce sujet. Il s'agit d'ailleurs en grande partie d'appareils à un prix relativement bas. Le sujet est plus sensible dans le secteur automobile. Certaines marques, par exemple, n'offrent plus les mises à jour nécessaires au-delà d'une certaine période.

Le monde universitaire et le secteur coopèrent considérablement. L'orateur a fondé le L-SEC (*Leuven Security Excellence Consortium*) en 2004. Il est également l'un des fondateurs de la *Cyber Security Coalition* créée en 2016 et réunissant le gouvernement, le monde universitaire et le secteur. Une coopération *ad hoc* est également mise en place avec le CCB concernant des sujets précis. Par le passé, l'équipe de M. Preneel a déjà contribué au développement de la carte d'identité électronique, au vote électronique et à l'application *Coronalert*. Aux Pays-Bas, la coopération s'effectue de manière plus structurelle par le biais du *Cyber Security Raad* (CSR). En Belgique, les compétences sont bien entendu réparties entre les niveaux politiques: le fédéral est en grande partie chargé de la sécurité, alors que les régions sont responsables de la recherche et de l'enseignement. De plus, le financement des projets n'est pas très flexible. Pourtant, une politique de financement moins stricte est nécessaire pour les projets relatifs à la cybersécurité. D'un autre côté, la Belgique possède une riche expertise dans ce domaine. La KU Leuven regroupe à elle seule 220 collaborateurs qui travaillent sur des aspects techniques et non techniques en matière de cybersécurité.

La distorsion du marché en matière de certification constitue en effet une préoccupation. Les grands pays possèdent d'importants laboratoires de certification. La Belgique peut se joindre à eux par le biais d'accords de coopération. Il serait également préférable que les petits pays coopèrent davantage, unissent leurs forces, élaborent des solutions et demandent le soutien de l'Europe à cet égard. Une certification abordable doit également être automatisée. Des recherches supplémentaires doivent encore être effectuées à cet égard. La certification est encore un processus manuel trop lent assorti de beaucoup de paperasse.

Er is in België en Europa zeker expertise aanwezig op het vlak van de beveiliging van IoT-toestellen, maar ook wat dat betreft, is het een kwestie van mensen en middelen. Het verdient in ieder geval aanbeveling om de producenten te responsabiliseren. Een producent van een webcam draagt momenteel geen enkele verantwoordelijkheid voor de online veiligheid ervan. De industrie lobbyt ook sterk tegen de eventuele invoering ervan. Het spreekt voor zich dat een dergelijke maatregel de prijs van de betrokken toestellen de hoogte zou instuwen. De spreker heeft geen weet van rechtszaken hierover. Het gaat immers veelal om toestellen met een relatief lage kostprijs. In de autosector liggen de zaken wat gevoeliger. Er zijn merken waar bijvoorbeeld noodzakelijke updates na een bepaalde termijn niet langer gratis zijn.

Er wordt al heel wat samengewerkt tussen de academische wereld en de industrie. De spreker heeft in 2004 L-SEC (*Leuven Security Excellence Consortium*) opgericht. Hij is tevens één van de stichters van de *Cyber Security Coalition* in 2016, die de overheid, de academische wereld en de industrie samenbrengt. Daarnaast is er over bepaalde onderwerpen ad-hocsamenwerking met het CCB. Het team van de heer Preneel heeft in het verleden reeds zijn medewerking verleend aan de ontwikkeling van de eID, van het elektronisch stemmen of de app *Coronalert*. In Nederland verloopt de samenwerking wel op een meer structurele wijze in de *Cyber Security Raad* (CSR). In België zijn natuurlijk de bevoegdheden verspreid over de beleidsniveaus: het federaal niveau is grotendeels bevoegd voor veiligheid, terwijl het deelstatelijk niveau bevoegd is voor onderzoek en onderwijs. Bovendien valt de financiering van projecten niet echt flexibel te noemen. Een soepeler financieringsbeleid is nochtans nodig voor projecten rond cyberveiligheid. Daar staat tegenover dat er in België wel degelijk heel wat expertise in dat domein bestaat. Alleen al aan de KU Leuven werken 220 personen rond technische en niet-technische aspecten van cyberveiligheid.

De marktverstoring bij de certificering is inderdaad een bezorgdheid. De grote landen beschikken over grote laboratoria die aan certificering doen. Wat België kan doen, is daar aansluiting bij zoeken in de vorm van samenwerkingsovereenkomsten. Het zou ook beter zijn indien de kleinere landen meer samenwerken, de krachten bundelen, oplossingen uitwerken en daar Europese steun voor vragen. Een betaalbare certificatie moet bovendien automatiseerbaar zijn. Daarvoor is nog bijkomend onderzoek nodig. Certificering is nog te zeer een traag en manueel proces met veel papierwerk.

La cybercolonisation s'est développée au fil des décennies et ne peut être résolue par quelques interventions miracles à court terme. Il est déjà question d'une sensibilisation de la dépendance actuelle de l'Union à la Commission européenne. Il convient de veiller à ce que les solutions proposées respectent les intérêts nationaux individuels. À court terme, toutefois, le financement de la recherche sur les logiciels libres et le matériel pourrait être envisagé. À cet égard, il convient d'investir à l'échelon européen. Par le passé, la ville de Munich a mis sa propre version de Linux (LiMax) à l'essai. Une alternative libre à Zoom existe également, à savoir *BigBlueButton*. La Belgique et l'Europe devraient délibérément opter pour de telles solutions libres et les exploiter, les gérer et les renforcer davantage. Ce réflexe n'est que trop rare. Un tel travail nécessite un effort, mais est faisable.

La Belgique est riche d'expertise, également au sein du gouvernement. Toutefois, un manque de personnel persiste. C'est pourquoi il convient d'investir dans des formations. Les pays voisins proposent déjà des formations spécialisées en cybersécurité (bachelier et master en cybersécurité). En Flandre, un master complémentaire ne peut être créé que si un autre est supprimé. C'est compréhensible, mais cela empêche les universités de proposer une offre de formations flexible.

Les compétences en matière de cybersécurité sont en effet réparties au sein du gouvernement. Le CCB est délibérément restreint, et les SPF disposent d'une grande autonomie concernant leur politique informatique. D'un point de vue technique, cette situation n'est pas optimale. Le CCB est trop petit (sous-critique) pour disposer de suffisamment d'expertise. Il s'agit d'ailleurs d'un domaine politique très vaste. Une coordination et une centralisation accrues sont nécessaires. D'autre part, des projets informatiques de grande envergure peuvent également tourner au vinaigre. La prudence est donc toujours de mise lorsqu'il s'agit d'informatique à échelle. Cependant, la question de l'informatique à échelle doit être posée et étudiée. La fragmentation doit toujours être une préoccupation.

Enfin, il convient de chercher des manières créatives d'attirer l'expertise au sein du gouvernement. Les détenteurs d'un diplôme en cybersécurité peuvent obtenir une offre intéressante dans le secteur privé. Le gouvernement doit adopter une attitude réaliste et pragmatique, et réfléchir aux constructions qui peuvent être mises en place pour attirer certains profils.

De cyberkolonisering is doorheen de decennia gegroeid en valt niet op te lossen met enkele mirakelingrepen op korte termijn. Bij de Europese Commissie is er alvast sprake van een bewustwording van de huidige afhankelijkheid van de EU. Men dient erover te waken dat de voorgestelde oplossingen de individuele nationale belangen overstijgen. Op korte termijn kan men wel werk maken van een financiering van onderzoek naar open software en hardware. Daar moet op Europese schaal in worden geïnvesteerd. In het verleden heeft de stad München een eigen versie van Linux (LiMax) uitgeprobeerd. Er bestaan ook een open alternatief voor Zoom, namelijk *BigBlueButton*. België en Europa zouden bewust moeten kiezen voor dergelijke open oplossingen en die uitbaten, beheren en verder verbeteren. Die reflex is er veel te weinig. Zoiets vraagt een inspanning, maar is zeker haalbaar.

Er is heel wat expertise aanwezig in België, ook bij de overheid. Niettemin blijft er een tekort aan mensen, en moet er dus meer worden geïnvesteerd in opleidingen. In de buurlanden bestaan al gespecialiseerde opleidingen in cyberveiligheid (een bachelor en master in *Cyber Security*). In Vlaanderen mag maar een bijkomende master worden gecreëerd indien een andere wordt afgeschaft. Daar is begrip voor, maar het maakt het de universiteiten wel moeilijk om een flexibel opleidingsaanbod in te richten.

Het klopt dat de bevoegdheid voor cyberveiligheid binnen de overheid versnipperd is. Het CCB wordt bewust klein gehouden, en de FOD's beschikken over veel autonomie bij hun IT-beleid. Dat is vanuit technisch oogpunt geen optimale situatie. Het CCB is eigenlijk te klein (sub-kritisch) om echt over voldoende expertise te beschikken. Het gaat immers over een erg breed beleidsdomein. Er moet meer worden gecoördineerd en gecentraliseerd. Daar staat tegenover dat ook grootschalige IT-projecten kunnen foutlopen. Voorzichtigheid over de schaalgrootte is dus steeds geboden. Dat neemt niet weg dat de vraag naar de schaalgrootte moet worden gesteld en onderzocht. De versnippering moet steeds een bezorgdheid zijn.

Tot slot dienen creatieve manieren te worden gezocht om expertise aan te trekken binnen de overheid. Mensen met een diploma in cyberveiligheid kunnen in de privésector een mooi aanbod krijgen. De overheid moet een realistische en pragmatische houding aannemen, en nagaan welke constructies opgezet kunnen worden om bepaalde profielen aan te trekken.

3. ***Réponses de M. Dirk Haex, codirecteur de Belnet***

*M. Dirk Haex* répond d'abord à la question concernant le coût de la remise à zéro des supports d'information supplémentaire à la suite de l'attaque DDoS. L'un des fournisseurs de Belnet est venu à la rescousse pendant la nuit, ce qui a permis de suivre les règles prescrites et de laisser jouer le marché. Diverses entreprises spécialisées ont contacté Belnet, ce qui a permis d'entamer des négociations. L'inspecteur des Finances a approuvé le budget le 23 mai 2021, lequel s'élève à plusieurs centaines de milliers d'euros par an. En tout état de cause, le renouvellement de la protection contre les DDoS avait déjà commencé au début de l'année 2021.

Ce coût n'est pas repris dans le budget de Belnet et sera couvert par des ressources provenant de la provision interdépartementale. Le SPF BOSA a donné son accord le 10 juin 2021. Il est évident que les besoins budgétaires de Belnet en matière de sécurité sont d'un tel ordre de grandeur qu'il convient d'agir structurellement.

Il est extrêmement difficile de quantifier le coût de l'incidence de l'attaque DDoS. Ce calcul n'a pas encore été effectué à l'heure actuelle. Des mesures de prévention supplémentaires et l'information des clients constituent les priorités. S'il peut être démontré qu'un tiers n'a pas fourni les services spécifiques stipulés dans le contrat, la quantification de ces services fera partie des actions par défaut. Le tiers est alors déclaré en défaut. La situation actuelle est différente, car l'auteur n'est pas connu.

La recherche d'attribution a-t-elle un sens? L'orateur est d'avis que tout un chacun a un rôle à jouer. Il croit en l'enquête menée par la FCCU, mais les chances de retrouver les auteurs sont faibles. Toutefois, certains cas ont été couronnés de succès. Il ne faut donc pas perdre espoir.

Depuis plusieurs années, Belnet dispose d'un CISO qui travaille à plein temps sur la sécurité de l'information et dirige un programme ambitieux à ce sujet. L'objectif est que Belnet soit entièrement certifié ISO 27001 d'ici à 2024. Le programme se divise en cinq objectifs stratégiques, dont les objectifs "*risk based decision making*" et "*security by design*". En outre, Belnet dispose également d'un DPO et de plusieurs experts en sécurité. Belnet travaille en parallèle avec des partenaires privés dans le cadre de certaines missions, notamment dans le domaine de la sécurité (comme pour l'*Operation Center* accessible 24h/24 et 7j/7). Belnet a désespérément besoin de cet échange et de cette coopération avec le secteur privé car,

3. ***Antwoorden van de heer Dirk Haex, codirecteur van Belnet***

*De heer Dirk Haex* gaat vooreerst in op de vraag naar de kostprijs van de extra scrubbing ingevolge de DDoS-aanval. Eén van de leveranciers van Belnet is de nacht zelf te hulp geschoten. Dat heeft toegelaten de voorgeschreven regels te volgen en de markt te laten spelen. Verschillende gespecialiseerde bedrijven hebben Belnet gecontacteerd. Dat heeft toegelaten om in onderhandeling te gaan. De inspecteur van Financiën heeft op 23 mei 2021 zijn goedkeuring gegeven op het budget. Dat situeert zich op enkele honderdduizenden euro per jaar. Begin 2021 was hoe dan ook reeds gestart met de vernieuwing van de DDoS-bescherming.

Deze kosten waren niet opgenomen in het budget van Belnet. Hij zal worden gedekt met middelen uit de interdepartementale provisie. De FOD BOSA heeft daar op 10 juni 2021 zijn akkoord voor gegeven. Het is duidelijk dat de budgettaire noden op het vlak van beveiliging voor Belnet van die orde zijn dat er iets structureels moet worden ondernomen.

Het is zeer moeilijk om de kostprijs van de impact van de DDoS-aanval te becijferen. Die oefening is op dit ogenblik nog niet gemaakt. De prioritaire aandacht is uitgegaan naar de extra preventieve maatregelen en het informeren van de klanten. Indien kan worden aangetoond dat een derde partij gefaald heeft bij het verlenen van de contractueel vastgelegde specifieke diensten, maakt de becijfering daarvan deel uit van de standaardacties. De derde partij wordt dan in gebreke gesteld. Deze situatie is anders want de dader is niet gekend.

Heeft het onderzoek naar de attributie zin? De spreker is persoonlijk van mening dat eenieder zijn rol te spelen heeft. Hij heeft vertrouwen in het onderzoek dat door de FCCU wordt gevoerd. De kans is inderdaad klein dat de daders gevonden zullen worden. Er zijn evenwel gevallen waarin wel succes werd geboekt. Men mag dus bij voorbaat de hoop niet opgeven.

Belnet heeft sedert enkele jaren een eigen CISO aan boord die zich voltijd bezighoudt met informatieveiligheid en de leiding heeft over een ambitieus programma rond informatieveiligheid. Het is de bedoeling om Belnet tegen 2024 volledig ISO 27001 gecertificeerd te maken. Het programma spitst zich toe op vijftal strategische doelstellingen, waaronder "*risk based decision making*" en "*security by design*". Daarnaast beschikt Belnet over een DPO en een aantal eigen veiligheidsexperten. Tegelijk werkt Belnet voor een aantal zaken samen met private partners, ook op het vlak van security (bijvoorbeeld voor het 24/7 *Operation Center*). Belnet heeft die uitwisseling en samenwerking met de privésector hard nodig omdat

compte tenu des procédures de recrutement actuelles, il n'est pas facile d'obtenir ces experts en interne. C'est un point épineux qu'il convient de résoudre. Toutefois, la demande d'une solution structurelle fait partie du contrat d'administration en cours de finalisation.

L'orateur souligne à cet égard la coopération au sein de l'administration fédérale concernant le G-Cloud. Il est en effet question de fragmentation, mais également de coopérations et de centralisations éventuelles. Les contrats-cadres permettent de recourir à l'expertise du secteur privé. Par conséquent, chacun n'utilise pas son propre contrat-cadre, ce qui facilite la mise en œuvre de ce type de service.

Belnet dispose-t-il d'une personne de contact en matière de cybersécurité? L'orateur souligne que la responsabilité finale incombe de toute façon à Belnet, le secrétaire d'État à la politique scientifique étant le responsable politique. En outre, le CCB est bien entendu compétent pour le volet stratégique et politique. Belnet et le CCB se consultent régulièrement. Ces derniers font également partie du laboratoire d'idées concernant les PIC. Dans tous les cas, la clarification des compétences en matière de cybersécurité peut être considérée comme un domaine à améliorer.

L'orateur déclare ce qui suit concernant le fait que tous les clients de Belnet n'ont pas été victimes de l'attaque DDoS: Belnet gère également le réseau BNIX, une plateforme sur laquelle les opérateurs télécoms belges, d'une part, et les fournisseurs de contenu, d'autre part, échangent leurs données. Il s'est avéré que la majeure partie de l'attaque est arrivée par "transit", et non par les échanges internet. Ceci, ainsi que les interventions techniques sur les réseaux ont permis de sauvegarder le trafic de données vers les principaux acteurs utilisés par les clients de Belnet. La raison pour laquelle tous les clients n'ont pas ressenti l'attaque est donc de nature technique.

Selon les informations de l'orateur, les ressources supplémentaires pour la cybersécurité n'ont pas encore été affectées. Belnet n'a pas encore reçu la confirmation que des ressources supplémentaires seraient fournies. Toutefois, il a été clairement indiqué au secrétaire d'État compétent que des ressources supplémentaires sont nécessaires pour faire face aux menaces croissantes. Chez Belnet, les analyses de risques forment la base de la communication avec les partenaires, dont le responsable politique. Bien entendu, un équilibre réaliste est toujours recherché pour couvrir les risques.

het, gelet op de geldende rekruteringsprocedures, inderdaad geen sinecure is om die experten zelf in huis te halen. Dat is een pijnpunt dat moet worden aangepakt. De vraag naar een structurele oplossing maakt evenwel deel uit van de bestuursovereenkomst die momenteel wordt gefinaliseerd.

De spreker wijst in dat verband op de samenwerkingsverbanden binnen de federale overheid rond de G-Cloud. Er is inderdaad sprake van versnippering, maar tegelijk wordt toch gekeken naar mogelijke samenwerkingen en centraliseringen. Aan de hand kadercontracten kan gebruik worden gemaakt van de expertise binnen de privésector. Het is dus niet zo dat eenieder een eigen soort overeenkomst hanteert. Het zorgt voor een vlottere aanwending van dat soort dienstverlening.

Heeft Belnet een aanspreekpunt voor cyberveiligheid? De spreker benadrukt dat de eindverantwoordelijkheid sowieso bij Belnet ligt, met de staatssecretaris voor Wetenschapsbeleid als politiek verantwoordelijke. Daarnaast is er uiteraard de bevoegdheid van het CCB voor het strategisch en beleidsmatig luik. Belnet en het CCB plegen regelmatig overleg. Beide maken ook deel uit van de denktank rond de ISP's. In ieder geval kan het verduidelijken van de bevoegdheden rond cyberveiligheid als een verbeterpunt worden aangemerkt.

In verband met de stelling dat niet alle Belnet-klanten slachtoffer waren van de DDoS-aanval, wijst de spreker op het volgende. Belnet beheert ook het BNIX-netwerk. Dat is een platform waarop enerzijds de Belgische telecomoperatoren en anderzijds de contentproviders hun dataverkeer uitwisselen. Er werd vastgesteld dat het gros van de aanval via "transit" is binnengekomen, en dus niet via de internet exchanges. Dat heeft er, samen met de technische interventies op de netwerken, toe geleid dat het dataverkeer naar de belangrijkste spelers waar de Belnet-klanten gebruik van maken, gevrijwaard kon worden. De reden waarom niet alle klanten de impact van de cyberaanval hebben gevoeld, is dus technisch van aard.

Volgens de informatie van de spreker werden de bijkomende middelen voor cyberveiligheid nog niet geoormerkt. Belnet heeft nog geen bevestiging ontvangen dat bijkomende middelen zullen worden uitgetrokken. Wel werd aan de bevoegde staatssecretaris duidelijk gemaakt dat bijkomende middelen nodig zijn om de toenemende dreigingen het hoofd te bieden. Bij Belnet vormen de risicoanalyses de basis voor de communicatie naar de stakeholders, waaronder de politieke verantwoordelijke. Uiteraard wordt steeds gestreefd naar een realistisch evenwicht om de risico's af te dekken.

4. ***Réponses de M. Geert Baudewijns, CEO de Secutec***

*M. Geert Baudewijns* explique que l'accord avec le gouvernement stipule le partage d'une quantité de flux de renseignements. Les flux à partir desquels les informations sur la cyberattaque ont été extraites ne sont pas inclus. Il s'agit de renseignements très spécifiques.

L'orateur a été interrogé par la police dans le cadre de l'enquête sur la cyberattaque. Ce dernier a précisé que si ces informations avaient été achetées, elles n'auraient pas pu être utilisées pour des raisons juridiques. Or, les informations étaient utilisables, car elles avaient été données.

La cyberattaque visait-elle la Belgique? Un test a été effectué, car Secutec possède également des bureaux aux Pays-Bas. Il s'est avéré qu'aucune attaque similaire n'avait été commise contre les Pays-Bas à cette période. Ce constat est important, car 80 % de ce qui se passe en Belgique s'observe également aux Pays-Bas. Les cybercriminels utilisent les mêmes éléments pour attaquer des pays précis. Sur la base des informations et de l'estimation de Secutec, seule la Belgique était concernée.

L'orateur explique également qu'un lien existe entre les attaques DDoS et les rançongiciels. Il arrive qu'après une telle attaque, un e-mail soit envoyé pour demander une rançon, accompagné de la menace de nouvelles attaques. M. Baudewijns a également été appelé à jouer le rôle de négociateur en raison de sa fonction. Il veille donc à négocier de manière rationnelle avec les cybercriminels. Cela évite d'exploiter les émotions des victimes touchées. Il s'agit souvent de montants allant de 10 000 à 60 000 euros par transaction. Dernièrement, une somme de 22 000 euros a été versée après une attaque par rançongiciel. Une enquête sur les adresses Bitcoin utilisées a révélé que 3,5 millions d'euros de bitcoins avaient été retirés de ce compte. Cela illustre clairement la fréquence à laquelle un tel incident se produit à l'échelle mondiale et souligne l'ampleur du problème.

Il convient de contacter les autorités du pays à partir duquel un contact est établi dès que l'on constate qu'un *botnet* est utilisé depuis l'extérieur. Les autorités en question doivent saisir les serveurs concernés. L'étape suivante consiste à déterminer où se trouvent les PC qui se sont connectés au *botnet*. En ce qui concerne l'attaque DDoS contre la Belgique, il s'agit de 17 serveurs et de 29 pays. L'enquête est difficile et lente, et les cybercriminels sont rarement attrapés, ce qui ne cesse de renforcer la problématique. Il est également

4. ***Antwoorden van de heer Geert Baudewijns, CEO van Secutec***

*De heer Geert Baudewijns* legt uit dat de overeenkomst met de overheid het meedelen van een hoeveelheid intel feeds bepaalt. De feeds waaruit de informatie over de cyberaanval werden gehaald, zitten daar niet in. Dat gaat om zeer specifieke intelligence.

De spreker werd in het kader van het onderzoek naar de cyberaanval verhoord door de politie. Die laatste liet verstaan dat indien die informatie zou worden aangekocht, ze om juridische redenen niet zou kunnen worden gebruikt. De informatie was wel bruikbaar omdat ze gewoonweg werd gegeven.

Was de cyberaanval tegen België gericht? Aangezien Secutec ook over kantoren in Nederland beschikt, werd daar een test uitgevoerd. Daaruit bleek dat er tijdens die periode geen gelijkaardige aanval tegen Nederland was uitgevoerd. Die vaststelling is belangrijk, want 80 % van wat in België gebeurt, valt ook te zien in Nederland. Cybercriminelen maken voor een aanval in bepaalde landen gebruik van dezelfde elementen. Op basis van de informatie en inschatting van Secutec ging het dus enkel om België.

Voorts legt de spreker uit dat er wel degelijk een verband bestaat tussen DDoS-aanvallen en ransomware. Er zijn gevallen waarbij na een dergelijke aanval een mail wordt verstuurd met de vraag naar losgeld, gekoppeld aan de dreiging met nieuwe aanvallen. De heer Baudewijns wordt vanuit zijn functie ook gevraagd om te fungeren als onderhandelaar. Dat houdt in dat hij er mee voor zorgt dat er op een rationele manier wordt onderhandeld met cybercriminelen. Aldus wordt vermeden dat gebruik wordt gemaakt van de emoties van de getroffen slachtoffers. Vaak gaat het om bedragen van 10 000 euro tot 60 000 euro per transactie. In een recent geval werd een bedrag van 22 000 betaald na een aanval met ransomware. Uit een onderzoek naar de gebruikte bitcoinadressen bleek dat er voor 3,5 miljoen euro aan bitcoins werd afgehaald van die rekening. Dat schetst duidelijk hoe vaak zoiets gebeurt op wereldniveau, en dat benadrukt de omvang van de problematiek.

Van zodra wordt vastgesteld dat een botnet van buitenaf wordt gebruikt, moet contact worden opgenomen met de autoriteiten van het land van waaruit het contact wordt gemaakt. Die overheid moet de betrokken servers in beslag nemen. Vervolgens wordt onderzocht waar de pc's die zich met de botnet hebben geconnecteerd, zich bevinden. Wat de DDoS-aanval op België betreft, gaat het om 17 botnetservers en 29 landen. Het is moeilijk en traag onderzoek, en zelden worden de cybercriminelen gevat. Dat maakt dat de problematiek groter en groter

extrêmement important que les entreprises victimes d'une attaque contactent les autorités. Cela ne se passe malheureusement pas souvent, car elles ne croient pas en l'enquête.

En ce qui concerne le recrutement de personnel, l'orateur signale qu'une entreprise privée n'est pas tenue par les statuts ni les barèmes. Toutefois, il n'est pas facile pour une entreprise de dénicher des collaborateurs passionnés. Dans le même temps, les ressources que le gouvernement consacre à l'obtention de renseignements garantissent que les connaissances des autres pays et organisations sont transmises à la CERT ou au CCB. C'est une constatation importante, car un pays ne doit pas personnellement effectuer toutes les analyses. Il s'agit de disposer des flux d'informations. Ce sont souvent des justificatifs d'identité fermés (mots de passe, noms d'utilisateur) et des indicateurs de compromis (IOC). Le fait de disposer rapidement de ces données est beaucoup plus important pour un pays que le fait de posséder une armée d'analystes. C'est en réalité une meilleure manière d'investir.

En Belgique, il existe également l'adresse de secours *Safeonweb*, qui est unique en son genre. Aux Pays-Bas, seuls les e-mails de phishing flous peuvent être publiés. En Belgique, l'on peut faire beaucoup plus. Secutec reçoit aussi au quotidien les milliers de signalements de messages suspects pour analyse, et les envoie ensuite à 35 partenaires dans le monde entier qui utilisent à leur tour ces informations en vue d'améliorer leur technologie. Dans d'autres pays, la législation en matière de vie privée ne permet pas ces démarches. Le produit SecureDNS permet d'interrompre de nombreuses connexions à la suite des nombreux signalements des citoyens belges. De cette manière, des flux importants pour le monde entier sont créés en Belgique.

*Le rapporteur,* *Le président,*

Michael FREILICH Ortwin DEPOORTERE

wordt. Het is dan ook ontzettend belangrijk dat de ondernemingen die het slachtoffer worden contact opnemen met de overheid. Dat gebeurt jammer genoeg niet vaak omdat zij niet veel heil verwachten van het onderzoek.

Wat het aantrekken van personeel betreft, geeft de spreker toe dat een privéonderneming inderdaad niet gebonden is aan statuten en loonbarema's. Niettemin is het ook voor een onderneming niet evident om gepassioneerde medewerkers te vinden. Tegelijk is het zo dat de middelen die de overheid besteedt aan het verkrijgen van intel feeds ervoor dat de kennis vanuit andere landen en organisaties toch terugvloeit naar het CERT of het CCB. Dat is een belangrijke vaststelling. Een land hoeft heus niet zelf alle analyses uit te voeren. Het komt erop aan om over de intel feeds te kunnen beschikken. Vaak gaat het om gestolen credentials (paswoorden, gebruikersnamen) en Indicators of compromise (IOC's). Het snel kunnen beschikken over die data is voor een land veel belangrijker dan de beschikking te hebben over een leger analisten. Het is dus in feite een slimmere manier van investeren.

In België bestaat ook het meldadres *Safeonweb*. Die toepassing is vrij uniek. In Nederland mogen op basis van een meldpunt enkel geblurde phishing-mails worden gepubliceerd. In België kan veel verder worden gegaan. Ook Secutec ontvangt dagelijks de duizenden meldingen van verdachte berichten voor analyse, en stuurt die op zijn beurt door naar 35 partners wereldwijd die de informatie op hun beurt gebruiken voor de verbetering van hun technologie. In andere landen laat de privacywetgeving die stappen niet toe. Het product SecureDNS zorgt ervoor dat heel wat connecties worden tegengehouden als gevolg van de vele meldingen van de Belgische burgers. Op die manier worden in België feeds gemaakt die voor de hele wereld belangrijk zijn.

*De rapporteur,* *De voorzitter,*

Michael FREILICH Ortwin DEPOORTERE



Imprimerie centrale – Centrale drukkerij