DOC 52 **0898/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

28 februari 2008

ICT-VEILIGHEID

VERSLAG

NAMENS DE COMMISSIE VOOR DE INFRASTRUCTUUR, HET VERKEER EN DE OVERHEIDSBEDRIJVEN UITGEBRACHT DOOR DE HEER **Roel DESEYN**

INHOUD

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

28 février 2008

SÉCURITÉ TIC

RAPPORT

FAIT AU NOM DE LA COMMISSION DE L'INFRASTRUCTURE, DES COMMUNICATIONS ET DES ENTREPRISES PUBLIQUES PAR M. **Roel DESEYN**

SOMMAIRE

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

A. — **Vaste leden/Membres titulaires:**		B. — **Plaatsvervangers/Membres suppléants:**
CD&V - N-VA:	Jenne De Potter, Peter Luykx, Roel Deseyn, Jef Van den Bergh	Leen Dierick, Michel Doomst, Liesbeth Van der Auwera, Servais Verherstraeten, N.
MR:	François Bellot, Olivier Chastel, Valérie De Bue	Philippe Collard, Corinne De Permentier, Jean)Jacques Flahaux, Jacqueline Galant
PS:	Linda Musin, Bruno Van Grootenbrulle	Camille Dieu, Karine Lalieux, André Perpète
Open Vld:	Guido De Padt, Ludo Van Campenhout	Herman De Croo, bart Tommelein, Luk Van Biesen
VB:	Jan Mortelmans, Francis Van den Eynde	Luc Sevenhans, Bruno Valkeniers, Linda Vissers
sp.a-spirit:	David Geerts, Bruno Tobback	Hans Bonte, Meryame Kitir
Ecolo-Groen!:	Thérèse Snoy et d'Oppuers	Georges Gilkinet, Stefaan Van Hecke
cdH:	David Lavaux	Josy Arens

cdH	:	*centre démocrate Humaniste*
CD&V–N-VA	:	*Christen-Democratisch en Vlaams/Nieuw-Vlaamse Alliantie*
Ecolo-Groen!	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
FN	:	*Front National*
LDD	:	*Lijst Dedecker*
MR	:	*Mouvement Réformateur*
Open Vld	:	*Open Vlaamse liberalen en democraten*
PS	:	*Parti Socialiste*
sp.a - spirit	:	*Socialistische partij anders - sociaal, progressief, internationaal, regionalistisch, integraal-democratisch, toekomstgericht.*
VB	:	*Vlaams Belang*

Afkortingen bij de nummering van de publicaties :		*Abréviations dans la numérotation des publications :*	
DOC 52 0000/000 :	*Parlementair document van de 52e zittingsperiode + basisnummer en volgnummer*	*DOC 52 0000/000 :*	*Document parlementaire de la 52ème législature, suivi du n° de base et du n° consécutif*
QRVA :	*Schriftelijke Vragen en Antwoorden*	*QRVA :*	*Questions et Réponses écrites*
CRIV :	*Voorlopige versie van het Integraal Verslag (groene kaft)*	*CRIV :*	*Version Provisoire du Compte Rendu intégral (couverture verte)*
CRABV :	*Beknopt Verslag (blauwe kaft)*	*CRABV :*	*Compte Rendu Analytique (couverture bleue)*
CRIV :	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen) (PLEN: witte kaft; COM: zalmkleurige kaft)*	*CRIV :*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes) (PLEN: couverture blanche; COM: couverture saumon)*
PLEN :	*Plenum*	*PLEN :*	*Séance plénière*
COM :	*Commissievergadering*	*COM :*	*Réunion de commission*
MOT :	*moties tot besluit van interpellaties (beigekleurig papier)*	*MOT :*	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen :
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.deKamer.be
e-mail : publicaties@deKamer.be

Publications officielles éditées par la Chambre des représentants

Commandes :
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.laChambre.be
e-mail : publications@laChambre.be

DAMES EN HEREN,

De hoorzittingen in verband met de informatieveiligheid (ICT-veiligheid of *e-security*) hebben plaatsgevonden op 16, 23 en 30 januari 2008. De commissie besliste eenparig, conform artikel 32 van het Reglement van de Kamer, dat van deze hoorzittingen een parlementair document wordt gemaakt.

I. — HOORZITTING VAN 16 JANUARI 2008

1. Uiteenzetting van de heer Luc Beirens, hoofd van de «*Federal Computer Crime Unit*» (de eenheid van de federale – gerechtelijke – politie die zich met de bestrijding van de computercriminaliteit bezighoudt)

De heer Luc Beirens stelt dat zijn dienst tot doel heeft om twee types van veiligheidsrisico's aan te pakken: enerzijds de risico's die met communicatie te maken hebben, anderzijds de risico's die met de infrastructuur verband houden.

Ingevolge de wet van 13 juni 2005 betreffende de elektronische communicatie zijn providers ertoe verplicht om veilige communicatie tot bij de eindgebruiker te waarborgen. Omdat bepaalde types van communicatie een crimineel karakter hebben, is interceptie en retentie van data noodzakelijk; dat vergt een omzetting in Belgisch recht van de betrokken Europese richtlijn (België is ter zake tot dusver in gebreke gebleven).

In de strijd tegen kinderporno, een prioriteit van de FCCU, stelt zich het probleem dat enkel Belgische websites op eenvoudige wijze kunnen worden aangepakt. Voor buitenlandse websites zijn de mogelijkheden beperkter:

– Via Interpol kan een verzoek tot sluiting van een site worden gericht aan het land waar de website wordt aangemaakt;
– Buitenlandse websites met een illegale inhoud kunnen slechts worden geblokkeerd na een uitspraak van de rechterlijke macht in kortgeding. Hoewel een kortgeding in praktijk een snelle procedure is, is ze niet geschikt en te omslachtig om bijvoorbeeld de 800 à 1000 buitenlandse kinderpornowebsites die door de FCCU jaarlijks worden gedetecteerd, snel te kunnen doen afsluiten.

– Sites met kinderporno worden vaak afgeschermd met wachtwoorden. De FCCU zou er zich toegang toe moeten kunnen verschaffen, wat thans niet mogelijk is; de wetgever dient dus de mogelijkheid om zich met toestemming van de onderzoeksrechter toegang te ver-

MESDAMES, MESSIEURS,

Les auditions relatives à la sécurité informatique (sécurité ICT ou *e-security*) ont eu lieu les 16, 23 et 30 janvier 2008. Conformément à l'article 32 du Règlement de la Chambre, la commission a décidé à l'unanimité que ces auditions feraient l'objet d'un document parlementaire.

I. — AUDITION DU 16 JANVIER 2008

1. Exposé de M. Luc Beirens, chef de la «*Federal Computer Crime Unit*» (l'unité de la police – judiciaire – fédérale chargée de la lutte contre la cybercriminalité)

M. Luc Beirens précise que son service a pour objectif de lutter contre deux types de risques en matière de sécurité: d'une part les risques liés aux communications, d'autre part les risques liés à l'infrastructure.

En vertu de la loi du 13 juin 2005 relative aux communications électroniques, les fournisseurs d'accès sont tenus de garantir la sécurité des communications jusqu'à l'utilisateur final. Étant donné que certains types de communications ont un caractère criminel, l'interception et la rétention de données s'imposent, ce qui nécessite une transposition en droit belge de la directive européenne concernée (jusqu'à présent, la Belgique a manqué à ses obligations en la matière).

En ce qui concerne la lutte contre la pornographie enfantine, une priorité de la FCCU, le problème est que l'on ne peut lutter assez facilement que contre les sites internet belges. Pour les sites étrangers, les possibilités sont plus limitées:

– Par le biais d'Interpol, une demande de fermeture d'un site peut être adressée au pays dans lequel le site est conçu;
– Les sites Internet étrangers présentant un contenu illégal ne peuvent être bloqués qu'après une décision du pouvoir judiciaire en référé. Bien que, dans la pratique, le référé soit une procédure rapide, celle-ci est inappropriée et trop compliquée pour pouvoir faire clôturer rapidement, par exemple, les 800 à 1000 sites internet pédopornographiques étrangers, détectés annuellement par la FCCU.
– Les sites de pornographie enfantine sont souvent protégés par des mots de passe. La FCCU devrait pouvoir y accéder, ce qui est impossible actuellement; le législateur doit donc prévoir, pour le monde virtuel, une possibilité similaire à la possibilité d'accéder, avec

schaffen tot een woning, die bestaat in de reële wereld, tot de virtuele wereld uit te breiden.

De volgende problemen dienen eveneens zoveel mogelijk te worden aangepakt:

– Internetfraude is in volle opgang. Omdat het vaak om vele kleine dossiers gaat, zijn maatregelen voor een vlotte aanmelding en de groepering van klachten noodzakelijk;
– Spam maakt 60 tot 90% van het e-mailverkeer uit en is vaak gericht op het plegen van misdrijven;
– Personen worden via computersystemen op diverse manieren verontrust (bijvoorbeeld laster en eerroof op blogs). In geval het misbruik van telefonie (vaste lijnen of gsm) betreft, is de Ombudsdienst voor telecommunicatie hun eerste aanspreekpunt.

De bedreigingen voor computernetwerken zijn uiteenlopend:

1. Vooreerst kan onveiligheid een niet-criminele oorzaak hebben: elektriciteitspannes, overstromingen, brand, aardbevingen,... Ook zorgen een slechte configuratie van en virussen in softwareprogramma's en operationele systemen voor problemen, net als nalatigheid (onvoldoende onderhoud van oudere pc's, het ontbreken van *back-ups*) en het verlies van data en laptops.

2. Defacing impliceert het overnemen van de controle over een website om vervolgens de inhoud ervan te wijzigen. Dit is geen moeilijke opgave, die bovendien wordt gefaciliteerd door het ontbreken van een *up-to-date*versie van webserversoftware en van controle op wijzigingen van de website. De gevolgen ervan blijven in de hypothese van de loutere verspreiding van foutieve informatie beperkt tot schade aan het bedrijfsimago; als de transacties op de website er ook door worden aangetast, kan de schade grotere proporties aannemen.

3. Hackers voeren aanvallen uit op de servers van de staatskas (bijvoorbeeld om de belastinginning in het gedrang te brengen), op mediawebsites en op *e-commerce*sites; zij proberen ook te infiltreren in bankrekeningen en verspreiden persoonlijke informatie en kredietkaartgegevens. De FCCU volgt de mededelingen op hackersites nauwgezet op omdat bepaalde groeperingen hun acties daarop af en toe aankondigen. Zo hebben we recentelijk dreigingen vastgesteld waarbij hackers ermee dreigen aanvallen uit te voeren op de servers van Financiën om bijvoorbeeld de beslastingsinning in het gedrang te brengen, om binnen te dringen in het e-

l'autorisation du juge d'instruction, à une habitation, qui existe dans le monde réel.

Il y a également lieu de remédier, autant que possible, aux problèmes suivants:

– Les fraudes sur l'Internet sont en pleine expansion. Comme il s'agit souvent d'un grand nombre de petits dossiers, des mesures s'imposent afin de permettre un signalement rapide et le regroupement de plaintes;
– Les spams représentent 60 à 90% des courriels et ont souvent une intention frauduleuse;
– Des personnes sont importunées de diverses manières par le biais de systèmes informatiques (par exemple la calomnie et la diffamation sur les blogs). Au cas où un abus de téléphonie (ligne fixe ou gsm) est en jeu, le Service de médiation pour les télécommunications est leur premier interlocuteur.

Les menaces pour les réseaux informatiques sont diverses:

1. En premier lieu, l'insécurité peut être d'origine non criminelle: pannes d'électricité, inondations, incendie, tremblements de terre,… Une mauvaise configuration des programmes de software et des systèmes opérationnels et leur infection par des virus sont également sources de problèmes, de même que la négligence (entretien insuffisant des vieux ordinateurs, absence de *back-ups*), la perte de données et d'ordinateurs portables.

2. Le défaçage implique la prise de contrôle d'un site Internet dans le but de modifier ensuite son contenu. Cette tâche, qui n'est pas difficile, est en outre facilitée par l'absence de version *up-to-date* du software du serveur web et par l'absence de contrôle des modifications du site Internet. Dans l'hypothèse d'une simple diffusion d'informations erronées, les conséquences de ce défaçage se limitent à une atteinte à l'image de marque de l'entreprise. Si les transactions réalisées sur le site Internet sont également affectées, les dégâts peuvent prendre des proportions plus importantes.

3. Les pirates informatiques s'attaquent aux serveurs du Trésor public (par exemple pour mettre en péril la perception de l'impôt), à des sites Internet de médias et à des sites d'*e-commerce*; ils tentent également de s'infiltrer dans des comptes bancaires et diffusent des informations personnelles et des données relatives aux cartes de crédit. La FCCU surveille les informations distillées sur les sites de pirates informatiques parce que certains groupuscules y annoncent parfois leurs actions. C'est ainsi que nous avons récemment appris que des pirates informatiques menaçaient de s'en prendre aux serveurs des Finances pour notamment mettre en péril

bankingverkeer, om persoonlijke gegevens (van onder meer kredietkaart) te verzamelen en te verspreiden. Aansluiting van een computer op het internet is overigens niet altijd nodig om een *hacking*operatie uit te voeren: door medewerking van binnenuit kunnen hackers ook op andere computers hun slag slaan.

4. «*Botnets*» leveren het grootste risico op omdat zij een bedreiging voor de kritische infrastructuur vormen. Botnets zijn grote netwerken van pc's van eindgebruikers die met zogeheten «*Trojan horses*» (kwaadaardige programma's met verborgen functionaliteiten) zijn besmet en vervolgens via intermediaire servers (meestal *chat-servers*) worden bestuurd. Ze worden gebruikt om pc's onklaar te maken of voor de verspreidingen van spam, *spyware* of klikfraude. Er bestaan honderden botnets onder controle van diverse hackers of hackersgroeperingen. Er zijn botnets waargenomen waarbij één hacker online simultaan honderdduizend pc's onder controle had. Al deze pc's te samen kunnen zeer grote datastromen op gang brengen en hierbij een gemeenschappelijk doel aanvallen om het buiten werking te stellen. Het gevaar blijkt uit de praktijk: zo zag Estland er zich in 2007 toe verplicht om alle internetverkeer uit het buitenland tegen te houden om het nationale netwerk in werking te houden.

In deze periode werden aanvallen waargenomen met datastromen tot 40 gigabit per seconde waarmee ook ISP's buitn werking werden gesteld.

5. Trojan horses worden ingezet om in transacties te interfereren, zowel op commerciële websites als op overheidswebsites, wat het vertrouwen in *e-society* en *e-government* kan aantasten.

Wie bedreigt de internetveiligheid?

– Vaak gaat het om «*script kiddies*» (jonge, gevaarlijke hackers) of om ICT-specialisten in een bedrijf, die in veel gevallen zonder controle werken en dus gemakkelijk hun slag kunnen slaan.

– Personen met specialisaties leggen via internet contacten met andere personen om samen een operatie op te zetten of om te geraken aan software die voor hun plannen noodzakelijk is.

– Een grote bedreiging gaat uit van criminele organisaties, die met financiële bedoelingen (gedeelten van) netwerken van legale bedrijven overnemen om van daaruit hun activiteiten te ontplooien; zij werken samen met personen die geld witwassen («*money mules*») en reageren zeer snel op de implementering van nieuwe veiligheidsinstrumenten.

la perception de l'impôt, pour s'infiltrer dans le trafic de l'e-banking, pour collecter et diffuser des informations personnelles (relatives aux cartes de crédit, notamment). La connexion d'un ordinateur à l'Internet n'est d'ailleurs pas toujours nécessaire pour mener une opération de piratage: grâce à des complicités internes, les pirates informatiques peuvent également s'introduire dans d'autres ordinateurs.

4. Les «*botnets*» représentent le principal risque dès lors qu'ils constituent une menace pour l'infrastructure critique. Les botnets sont de grands réseaux d'ordinateurs d'utilisateurs finals qui sont contaminés par des «chevaux de Troie » (programmes malveillants pourvus de fonctionnalités cachées), et qui sont ensuite opérés via des serveurs intermédiaires (le plus souvent des serveurs de chat). Ils sont utilisés pour neutraliser des ordinateurs ou pour diffuser du spamming, du spyware ou des clics frauduleux. Il existe des centaines de botnets, contrôlés par plusieurs «hackers» ou groupes de «hackers». L'on a constaté que certains botnets permettaient à un seul hacker de contrôler simultanément cent mille ordinateurs. Ensemble, tous ces ordinateurs peuvent générer d'énormes flux de données et attaquer une cible commune pour la mettre hors service. La pratique prouve le danger de ce système. C'est ainsi que l'Estonie s'est vue contrainte, en 2007, de bloquer toute la correspondance électronique venant de l'étranger pour éviter la paralysie du réseau national.

Au cours de cette période, des attaques ont été réalisées à partir de flux de données pouvant atteindre 40 gigaoctets par seconde et également mis hors service des ISP.

5. Les chevaux de Troie sont utilisés pour interférer dans des transactions, tant sur des sites Internet commerciaux que sur des sites Internet publics, ce qui peut ébranler la confiance dans l'e-society et dans l'e-government.

Qui menace la sécurité de l'Internet?

– Il s'agit souvent de «*script kiddies*» (jeunes pirates informatiques dangereux) ou de spécialistes de la TIC au sein d'une entreprise, qui travaillent souvent en l'absence de tout contrôle et qui peuvent donc opérer facilement.

– Les personnes spécialisées prennent, via Internet, des contacts avec d'autres personnes afin de monter une opération ou de mettre la main sur les logiciels dont ils ont besoin pour exécuter leurs projets.

– Une autre menace importante est constituée par les organisations criminelles, qui, dans un but financier, acquièrent des (parties de) réseaux d'entreprises légales afin d'y déployer leurs activités; elles coopèrent avec des personnes qui blanchissent de l'argent («*money mules*») et réagissent très rapidement à la mise en place de nouveaux instruments de sécurité.

– Terroristen met niet-financiële – politieke of sociale – motieven proberen de economie en de samenleving te destabiliseren door aan te sturen op chaos. Vaak nemen ze ruim de tijd om hun acties voor te bereiden en zijn ze ook goed georganiseerd.

– Sommige staten (Indië, China, Noord-Korea, Rusland,…) ontwikkelen binnen hun defensiecapaciteit «*cybertroops*», systemen om de kritische infrastructuur van overheden en privébedrijven in andere landen aan te vallen.

– Op geheime internetfora verhuren malafide handelaars botnets tegen betaling; zo is de kostprijs voor een grootschalige aanval 1000 dollar per dag.

Zijn we opgewassen tegen de risico's? In het algemeen is België zeer kwetsbaar:

– Sommige diensten (waarvoor men vroeger naar een loket kon gaan) worden enkel nog via het internet aangeboden.

– Er is een grote interconnectie tussen de verschillende netwerken.

– Door de vele operators is het niet altijd duidelijk wie informatie moet verstrekken of op incidenten moet reageren, waardoor een reactie vaak uitblijft.

– Er bestaat geen wettelijke verplichting om de overheid van incidenten op de hoogte te brengen.

Specifieke bedreigingen voor ons land zijn slecht beheerde websites, onbeveiligde computers van eindgebruikers en een onaangepaste internetinfrastructuur.

De spreker somt de belangrijkste zwakke punten van België op:

– Slechts weinig klachten over informaticacriminaliteit worden bij de politie ingediend omdat bedrijven voor imagoschade vrezen.

– Geen enkele instantie in België verzamelt informatie over actuele trends en incidenten of heeft zicht op de volledige kritische ICT-infrastructuur.

– Er bestaan geen procedures om snel te reageren op grootschalige aanvallen met een *botnet*.

Ons land heeft gelukkig ook sterke punten, in de eerste plaats de oprichting van BeNIS (*Belgian Network Information Security*) in 2005.

Op korte termijn moet werk worden gemaakt van betere informatieverstrekking aan webmasters van overheidssites en van een doorgedreven samenwerking binnen het overlegplatform «Bedrijfsbeveiliging».

– Les terroristes mus par des motifs autres que financiers – politiques ou sociaux – tentent de déstabiliser l'économie et la société en semant le chaos. Ils prennent souvent tout leur temps pour préparer leurs actions et ils sont également bien organisés.

– Certains États (Inde, Chine, Corée du Nord, Russie…) développent, dans le cadre de leur capacité de défense, des «*cybertroupes*», des systèmes destinés à attaquer l'infrastructure critique des autorités et des entreprises privées d'autres pays.

– Sur des forums Internet secrets, des commerçants peu scrupuleux louent des botnets contre paiement; ainsi, le coût d'une attaque de grande ampleur est de 1.000 dollars par jour.

Sommes-nous à l'abri de ces risques? Globalement, la Belgique est très vulnérable.

– Certains services (pour lesquels on pouvait précédemment s'adresser à un guichet) ne sont plus disponibles que sur l'Internet.

– Il y a une grande interconnexion entre les différents réseaux.

– En raison du nombre élevé d'opérateurs, on ne sait pas toujours clairement qui doit transmettre l'information ou réagir aux incidents, d'où l'absence fréquente de réaction.

– Il n'y a pas d'obligation légale d'informer les autorités des incidents constatés.

Les menaces spécifiques pour notre pays sont: les sites Internet mal gérés, les ordinateurs non protégés d'utilisateurs finals et l'infrastructure inadaptée de l'Internet.

L'orateur énumère les principaux points faibles de la Belgique:

– Peu de plaintes relatives à la criminalité informatique sont déposées auprès de la police parce que les entreprises craignent que cela ne ternisse leur image.

– Aucune instance ne collecte en Belgique les informations sur les tendances actuelles et les incidents ni n'a une vue d'ensemble sur l'infrastructure TIC critique.

– Il n'existe pas de procédures permettant de réagir rapidement à des attaques d'envergure menées par le biais d'un *botnet*.

Heureusement, notre pays dispose également de points forts, à commencer par la création de BeNIS (*Belgian Network Information Security*) en 2005.

À court terme, il faut œuvrer à améliorer la diffusion de l'information aux webmasters des sites des autorités et à renforcer la coopération au sein de la plate-forme de concertation pour la protection des entreprises. Cela

Daardoor kan informatie beter doorstromen en wordt het opnemen van verantwoordelijkheid binnen de ondernemingen gestimuleerd.

2. Uiteenzetting van de heer Len Lavens, vertegenwoordiger van «*e-securitybloggers*» (een vereniging van gebruikers die zich vragen stellen over de veiligheid van het Belgische internetverkeer)

De spreker neemt als verwoed «*e-securityblogger*» het woord uit persoonlijke naam. Het Belgische internet is veilig maar zou door een aantal praktische ingrepen nog veiliger kunnen worden gemaakt. Het Belgische internet bestaat uit driërlei: de internetaanbieders op commerciële basis zoals Belgacom en Telenet of Belnet ten behoeve van de overheid en allerlei openbare diensten en scholen (ISP's), DNS-servers om naar websites te surfen en 'hosting' websites die soms allerlei diensten aanbieden zonder over een eigen server te beschikken. Alledrie hebben structurele veiligheidsgebreken. De huidige aanvallen op netwerken zijn krachtiger geworden omdat ze veel moeilijker te traceren zijn. De zwakste schakel ligt bij de eindgebruiker. Krachtens de wet van 13 juni 2005 betreffende de elektronische communicatie dienen de internetaanbieders hun klanten gratis antivirus- en antispamprogramma's ter beschikking te stellen. Het BIPT wacht ter zake Europese regelgeving af. Deze zal er misschien nooit komen en dus moet men zelf een initiatief nemen. Nog teveel pc's worden intussen geïnfecteerd, er is geen coördinatie tussen de verschillende internetaanbieders en er zijn geen gemeenschappelijke veiligheidsindicatoren nopens virussen en spam. DNS-servers, netwerkcomputers die de domeinnamen beheren, spelen een cruciale rol in de beveiliging van het internetverkeer. De DNS-infrastructuur en de wijze waarop domeinnamen worden toegekend zou moeten geresponsabiliseerd worden om preventief bepaalde fenomenen te kunnen voorkomen (*phising, typosquatting*). Kritische infrastructuur moet absoluut worden in kaart gebracht en extra beveiligd om een recente aanval zoals die welke het internet in Estland lamlegde het hoofd te bieden. De CERT – het crisisteam dat ingeval van problemen snel en efficiënt moet kunnen optreden – zou een zelfstandige operationele eenheid moeten worden die vierentwintig uur per dag op de bres staat, onder toezicht van het BIPT staat en alle aanvallen beantwoordt ongeacht of ze gevoerd worden tegen het internet of het telefonienetwerk. Dit CERT zou ook «*hosting*»-servers moeten certificeren. De bestaande wetgeving moet worden toegepast, bestaande organisaties moeten nieuwe opdrachten krijgen en intenser samenwerken. Nieuwe regels moeten er vooral komen op het vlak van de meldingsplicht – als gegevens verloren zijn gegaan moet dit gemeld worden. Indien men veiligheidslekken heeft kunnen constateren moet er een systeem van verantwoordelijke onthulling komen zodat men dit kan doen

permettra de mieux diffuser l'information et de stimuler la prise de responsabilités au sein des entreprises.

2. Exposé de M. Len Lavens, représentant de l'association «*e-securitybloggers*» (qui regroupe des utilisateurs qui s'interrogent sur la sécurité du trafic Internet belge)

C'est en qualité d'*e-securityblogger* passionné que l'orateur s'exprime aujourd'hui. Si le réseau Internet est sûr en Belgique, on pourrait néanmoins en accroître encore la sécurité grâce à une série de mesures pratiques. Trois acteurs sont présents sur le réseau Internet belge: les fournisseurs d'accès Internet sur base commerciale comme Belgacom et Telenet ou Belnet pour les pouvoirs publics et toutes sortes de services publics et d'écoles (les ISP) – les serveurs DNS qui permettent de surfer sur les sites web et les sites d'hébergement ('hosting') qui offrent parfois une foule de services sans disposer de son propre serveur. Tous trois présentent des problèmes de sécurité d'ordre structurel. Aujourd'hui, les attaques de réseaux sont plus redoutables parce qu'il est beaucoup plus difficile de les tracer. L'utilisateur final est le maillon le plus fragile. Conformément à la loi du 13 juin 2005 relative aux communications électroniques, les fournisseurs Internet sont tenus de mettre gratuitement des programmes antivirus et antispam à la disposition de leurs clients. L'IBPT attend une réglementation européenne en la matière. Celle-ci ne vera sans doute jamais le jour, de sorte qu'il van falloir prendre une initiative soi-même. En attendant, le nombre de PC infectés est encore trop important et il n'y a aucune coordination entre les différents fournisseurs Internet, ni aucun indicateur de sécurité commun concernant les virus et les spams. Les serveurs DNS, les ordinateurs de réseaux qui gèrent les noms de domaine, jouent un rôle crucial dans la sécurité du trafic Internet. L'infrastructure DNS et la manière dont les noms de domaine sont attribués devraient être gérées de façon responsable afin de s'attaquer préventivement à certains phénomènes (*phising, typosquatting*). Il est absolument indispensable de faire la cartographie de l'infrastructure critique et d'en renforcer la sécurité pour faire face à une attaque du type de celle qui a paralysé récemment le réseau Internet estonien. Le CERT – l'équipe de crise qui doit pouvoir intervenir rapidement et efficacement en cas de problème – devrait devenir une unité opérationnelle autonome sur la brèche 24 heures sur 24 et placée sous la tutelle de l'IBPT, répondant à toutes les attaques, qu'elles soient menées contre l'Internet ou contre le réseau de téléphonie. Ce CERT devrait également certifier les serveurs d'hébergement. Il faut appliquer la législation en vigueur et confier de nouvelles missions aux organisations existantes et intensifier la collaboration entre ces dernières. De nouvelles règles s'imposent, surtout en ce qui concerne l'obligation de

zonder vrees voor vervolging. Tevens dient eenieder die persoonlijke gegevens wil opslaan, gecertifieerd te worden onder het toezicht van de Privacycommissie die meer armslag dient te krijgen. «*E-security*» dient hoger op de agenda te worden geplaatst en ook deel uit te maken van de wetenschappelijke opleidingsprogramma's. Uiteindelijk mag niet uit het oog verloren worden dat informatieveiligheid een economisch pluspunt is om buitenlandse investeringen aan te trekken.

3. Uiteenzetting van de heer Alain Huet, hoofdconsulent informatieveiligheid van FEDICT (federale overheidsdienst die instaat voor «*e-government*»)

Internetbedreigingen doen zich voor bij burgers, kmo's, grote ondernemingen en infrastructuren die van kritiek belang zijn voor het land. Voor burgers en kmo's gaat het vooral om computervirussen, gegevensdiefstal, oplichting (*e-commerce, enz.*) en het ontvangen van ongewenst (spam, enz.) en zelfs ongeoorloofd verkeer (pedopornografie,enz.).

Het niveau van bescherming van de burgers kan worden ingeschat in het licht van een enquête die in 2007 werd uitgevoerd door het BIPT: 74% van de particulieren beschikte over een «*firewall*» (programma bedoeld om bepaalde aanvallen vanuit een netwerk – waaronder het internet – te pareren); 68% bezat een bescherming tegen spionageprogramma's of «*spywares*» (een stiekem geïntroduceerd programma dat gegevens doorstuurt naar het netwerk buiten weten van de gebruiker); 40% van de Wi-Fi-installaties (die het totstandbrengen van een draadloos netwerk mogelijk maakt) zou beveiligd zijn.

De toestand bij de kmo's is zeer wisselvallig volgens een enquête die in 2004 door Belcliv (een Belgische vzw voor informaticaveiligheid) werd uitgevoerd.

De grote ondernemingen en de kritieke infrastructuren van het land zijn blootgesteld aan dezelfde bedreigingen maar zijn wellicht gevoeliger voor '*defacing*' van hun website of voor lamlegging van hun informatiesystemen.

Vandaag zijn de grootste bedreigingen afkomstig van criminele organisaties die over aanzienlijke middelen beschikken en zelfs van vreemde overheden die zich opmaken voor een elektronische oorlog. Als recent geval kan de aanval tegen Estland worden vernoemd benevens gevallen van fraude met bankverrichtingen en aanvallen die werden ontdekt in verschillende landen.

notification – lorsque des données ont été perdues, cela doit être notifié. Lorsqu'on constate des fuites de sécurité il faut mettre sur pied un système de révélation responsable sans crainte de poursuites. En même temps, quiconque souhaite sauvegarder des données à caractère personnel, doit bénéficier d'une certification sous le contrôle de la Commission de la protection de la vie privée dont il faut étendre les pouvoirs. L'*e-security* doit figurer plus haut sur l'agenda et faire également partie des programmes de formation scientifique. En définitive, il ne faut pas oublier que la sécurité de l'information est un plus économique pour attirer des investissements étrangers.

3. Exposé de M. Alain Huet, conseiller en chef sécurité de l'information de FEDICT (le service public fédéral responsable de l'*e-government*)

Les menaces liées à l'Internet concernent les citoyens, les PME, les grandes entreprises et les infrastructures qui revêtent une importance critique pour le pays. En ce qui concerne les citoyens et les PME, il s'agit principalement de virus informatiques, de vol de données, d'escroquerie (commerce électronique, etc.), et de réception de communications non souhaitées (spam, etc.), voire illicites (pédopornographie).

Nous pouvons évaluer le niveau de protection des citoyens à la lumière d'une enquête menée en 2007 par l'IBPT: 74% des particuliers disposaient d'un pare-feu ou *firewall* (un logiciel destiné à parer certaines attaques à partir d'un réseau – Internet notamment); 68% possédaient une protection contre les logiciels espions ou *spywares* (un programme introduit sournoisement et qui transmet des données au réseau à l'insu de l'utilisateur); 40% des installations Wi-FI (qui permettent la mise sur pied d'un réseau sans fil) seraient sécurisées.

La situation des PME est très variable selon une enquête menée en 2004 par Clusib (une ASBL belge active en matière de sécurité informatique).

Les grandes entreprises et les infrastructures critiques du pays sont exposées aux mêmes menaces, mais sont sans doute plus sensibles quant aux '*defacing*' de leur site web et à la paralysie de leurs systèmes informatiques.

Aujourd'hui, les plus grosses menaces proviennent d'organisations criminelles qui disposent de moyens colossaux, voire d'autorités étrangères qui se préparent à la guerre électronique. L'attaque menée contre l'Estonie en est un exemple récent ainsi que les cas de fraudes relative à des opérations bancaires, et des attaques détectées dans plusieurs pays.

Het door de federale ministerraad van 30 september 2005 in het leven geroepen Overlegplatform voor informatieveiligheid (en waar onder meer de FCCU, FEDICT, het BIPT, de Privacycommissie, het Crisiscentrum, de Kruispuntbank van de Sociale Zekerheid en diverse ministeriële diensten deel van uitmaken) heeft in 2007 een witboek samengesteld met als titel «Voor een nationaal beleid van de informatieveiligheid». Dit witboek verbindt vandaag alleen de deskundigen die eraan hebben meegewerkt. Het is nog niet op het niveau van het beleid behandeld. Van de negen themata die in het witboek aan bod komen, zijn er twee die het parlement meer zullen interesseren, met name de maatschappijvoorlichting en het crisisbeheer enerzijds en de computercriminaliteit anderzijds.

Ondanks bepaalde initiatieven in de openbare of privésfeer, bestaat er geen gestructureerd beleid van sensibilisering inzake informatieveiligheid. Hetzelfde geldt voor de bescherming van de kritieke informatiestructuren en, als logisch gevolg hiervan, het beheer van crisissen ingeval van aanvallen op deze structuren. De meeste landen hebben hiervoor een «*Computer Security Information Response Team*» *(CSIRT)* in het leven geroepen. Dit team is belast met de permanente evaluatie van de bedreigingen met een grote maatschappelijke impact.

Het witboek stelt daarom voor een inventaris te maken van alle kritieke informatiestructuren teneinde de eigenaars van deze infrastructuren ertoe te bewegen gepaste veiligheidsmaatregelen te nemen.

De justitie is ook niet altijd voldoende gewapend om de computercriminaliteit aan te pakken. Het witboek stelt daarom voor gespecialiseerde referentiemagistraten aan te stellen. Ook wetgevend kan nog worden opgetreden om bepaalde vergrijpen (bijvoorbeeld diefstal van identiteit en data) strafbaar te stellen.

4. Uiteenzetting van de heer Jean-Marc Vekeman, ombudsman voor de telecommunicatie

De Ombudsdienst voor telecommunicatie heeft als wettelijke opdracht:

– alle beroepsklachten van de eindgebruikers te onderzoeken die verband houden met de activiteiten van telecommunicatie-ondernemingen, waarvoor de Ombudsdienst bevoegd is;
– te bemiddelen om een minnelijke schikking te vergemakkelijken voor geschillen tussen de telecommunicatieondernemingen en de eindgebruikers;
– een aanbeveling te richten tot de telecommunicatieonderneming indien geen minnelijke schikking kan

La Plate-forme de concertation de Sécurité de l'information créée par le Conseil des ministres fédéral du 30 septembre 2005 (à laquelle étaient notamment associés la FCCU, FEDICT, l'IBPT, la Commission de la protection de la vie privée, le Centre de crise, la Banque-carrefour de la Sécurité sociale et différents services ministériels) a rédigé un livre blanc en 2007 intitulé «Pour une politique nationale de la sécurité de l'information». Aujourd'hui, ce livre blanc engage uniquement les experts qui y ont collaboré. Il n'a pas encore atteint le niveau politique. Sur les neuf thèmes qui sont abordés dans le livre blanc, il en est deux qui intéresseront particulièrement le parlement, à savoir l'information de la société et la gestion de crise, d'une part, et la criminalité informatique, d'autre part.

Hormis certaines initiatives issues de la sphère publique ou privée, une politique structurée de sensibilisation à la sécurité de l'information fait toujours défaut. Il en est de même pour la protection des infrastructures critiques d'information et son corollaire, la gestion de crises en cas d'attaques contre ces infrastructures. La plupart des États ont créé à cet effet une *Computer Security Information Response Team* (CSIRT). Cette équipe est chargée de l'évaluation permanente des menaces ayant un impact sociétal important.

Le livre blanc propose dès lors de dresser l'inventaire de toutes les infrastructures critiques d'information afin d'inciter leurs propriétaires à prendre les mesures appropriées en matière de sécurité.

La justice n'est pas non plus toujours suffisamment armée pour faire face à la criminalité informatique. Le livre blanc propose dès lors de désigner des magistrats de référence spécialisés. Sur le plan législatif également, des initiatives peuvent encore être prises en vue d'incriminer certains délits (usurpation d'identité et vol de données par exemple).

4. Exposé de M. Jean-Marc Vekeman, médiateur pour les télécommunications

La mission légale du médiateur pour les télécommunications est la suivante:

– examiner toutes les plaintes en deuxième instance des utilisateurs finals liées aux activités des opérateurs de télécommunications relevant de la compétence du service de médiation;
– s'entremettre pour faciliter un compromis à l'amiable des différends entre les opérateurs de télécommunications et les utilisateurs finals;
– adresser une recommandation à l'opérateur de télécommunications au cas où un compromis à l'amiable

worden bereikt; een afschrift van de aanbeveling wordt aan de klager toegezonden; in dit geval beschikt het telecombedrijf over een termijn van twintig werkdagen om haar beslissing te motiveren indien ze de gegeven aanbeveling niet volgt. Na het verstrijken van deze termijn verstuurt de Ombudsdienst een herinnering aan het betrokken bedrijf. Deze beschikt over een nieuwe termijn van twintig werkdagen om haar beslissing alsnog te motiveren indien zij de aanbeveling niet volgt. In dergelijke gevallen wordt de met redenen omklede beslissing naar de klager en naar de Ombudsdienst opgestuurd;

– van elke eindgebruiker die beweert het slachtoffer te zijn van kwaadwillig gebruik van een elektronischecommunicatiedienst het verzoek om inlichtingen te krijgen over de identiteit en het adres van de betreffende oproepers te onderzoeken. De Ombudsdienst willigt het verzoek in indien de feiten lijken vast te staan én het verzoek betrekking heeft op precieze data en uren.

In de uitoefening van voormelde opdrachten waakt de Ombudsdienst voor telecommunicatie over het respect voor het privéleven. Hij is bijzonder waakzaam bij de behandeling van klachten inzake kwaadwillige oproepen en ingeval gebruikers een lijst van inkomende gesprekken vragen.

Betreffende informaticacriminaliteit beperkt de Ombudsdienst, gezien zijn bevoegdheden, zich enkel tot een specifiek type van spam. Met betrekking tot andere vormen van informaticacriminaliteit, zoals *SPIM*, *phishing*, kinderpornografie, virussen en diefstal van gevoelige informatie uit databanken, ontduiking van btwverplichtingen door illegale sites, kan de Ombudsdienst waarschijnlijk geen relevante ervaring voorleggen.

Aan deze zogenaamde «*teasing-SMS*» werd in het laatst verschenen jaarverslag 2006 een tekstonderdeel gewijd.

Hieronder geven we een weergave van dit tekstonderdeel uit het Jaarverslag 2006 van de Ombudsdienst voor Telecommunicatie, hoofdstuk 8: «betalende SMSdiensten, een update»:

«Een actueel probleem waarmee diverse klagers in 2006 werden geconfronteerd is het probleem van de «*teasing-sms*». De Ombudsdienst heeft uit diverse identieke getuigenissen van klagers kunnen afleiden dat zij werden aangespoord op verschillende manieren: door een sms-bericht waarin de dienstaanbieder doet alsof hij een persoon is uit zijn vriendenkring; door een sms-bericht met een nieuwe vraag in het kader van een spel; of door een sms-bericht met het voorstel voor een andere nieuwe *ringtone*, waarmee tegelijkertijd een

ne peut être trouvé; une copie de la recommandation est adressée au plaignant; l'opérateur concerné dispose dans ce cas d'un délai de vingt jours ouvrables pour motiver sa décision au cas où il ne suivrait pas la recommandation. Après l'expiration de ce délai, le service de médiation envoie un rappel à l'entreprise concernée. Celle-ci dispose d'un délai de vingt jours ouvrables pour tout de même motiver sa décision au cas où elle ne suivrait pas la recommandation. La décision motivée est alors envoyée au plaignant et au service de médiation;

– examiner la demande de toute personne se prétendant victime d'une utilisation malveillante d'un service de communications électroniques visant à obtenir communication de l'identité et de l'adresse des auteurs de ces appels. Le service de médiation accède à la demande si les faits semblent établis et si la demande se rapporte à des dates et heures précises.

Dans l'exercice des missions précitées, le Service de médiation pour les télécommunications veille au respect de la vie privée. Il est particulièrement vigilant lors du traitement des plaintes en matière d'appels malveillants et lorsque des utilisateurs demandent une liste d'appels entrants.

En ce qui concerne la criminalité informatique, le Service de médiation se limite uniquement, eu égard à ses compétences, à un type spécifique de spam. En ce qui concerne d'autres formes de criminalité informatique, comme les *SPIM*, le *phishing*, la pornographie enfantine, les virus, le vol d'informations sensibles dans des banques de données, la fraude aux obligations en matière de TVA par des sites illégaux, le Service de médiation ne peut probablement pas se prévaloir d'une expérience pertinente.

Dans le dernier rapport annuel paru (celui de 2006), un passage a été consacré à cette pratique dite du «*teasing-sms*».

Nous reproduisons ci-dessous ce passage du chapitre 8 «Services sms payants: le point sur la question» du rapport annuel 2006 du Service de médiation pour les télécommunications:

«Un problème actuel auquel plusieurs plaignants ont été confrontés en 2006 est celui des sms incitatifs («*teasing-sms*»). À partir d'un certain nombre de témoignages identiques, le service de médiation a pu identifier les méthodes utilisées par les fournisseurs: il s'agit soit d'un message sms dans lequel, se faisant passer pour une personne de son entourage, le fournisseur de services éveille la curiosité du destinataire, soit d'un message sms formulant une nouvelle demande dans le cadre d'un jeu, soit encore d'un message sms proposant

nieuw abonnement zou worden afgesloten. Met andere woorden: een gsm-gebruiker die zich ooit inschreef voor een bepaalde dienst (abonnement, spel of *chat*), wordt later vaak via – meestal gratis, maar vaak ook betalende – sms-berichten aangespoord om terug deel te nemen aan een nieuwe wedstrijd, om zich opnieuw voor een abonnement in te schrijven of om terug een *chat*, quiz of andere dienst te starten. Dit komt dan niet noodzakelijk van hetzelfde korte nummer waarvan men destijds een bepaalde dienst ontving. Dergelijke sms-berichten kan men vergelijken met «spam». Aangezien er tegen «spam» ook reeds maatregelen genomen worden, dient er ook op vlak van sms-spam-berichten of teasing-sms-berichten opgetreden te worden. Een algemeen verbod op *teasing-sms*-berichten bestaat er nog niet. Tot dusver voorzien de GOF-richtlijnen wel reeds in een verbod op ongevraagde stimulering bij diensten voor minderjarigen (aansporing tot herinschrijving voor dezelfde dienst of inschrijving voor een andere dienst), alsook een verbod op de ongevraagde activering of stimulering van speldeelname via sms of mms. Dit is volgens de mening van de Ombudsdienst ontoereikend. Een verbod op dergelijke *teasing*-berichten zou moeten uitgebreid worden naar ALLE sms-diensten, zelfs al zijn deze *teasing*-sms gratis. Deze sms-berichten zijn niet alleen ergerlijk om te ontvangen, ze zijn voor sommige gebruikers te aanlokkelijk om niet te reageren (vooral bij *chat*-berichten en quizzen), waardoor zij (soms ook onwetend over de prijs) verdere kosten genereren. Voor de controle op de naleving van de reeds bestaande verboden van teasing-sms voor minderjarigen en bij speldeelname, is het voor de Ombudsdienst noodzakelijk het bestaan van deze *teasing*-sms-berichten te kunnen vaststellen. Dit is echter een probleem. Deze «*teasing*»-berichten worden door de dienstenaanbieders niet steeds vermeld in de zogeheten «*traffic*-lijsten» die de operatoren en de Ombudsdienst opvragen om een onderzoek te kunnen voeren. De dienstaanbieders laten op die manier uitschijnen dat de gsm-gebruiker zelf de deelname aan een wedstrijd startte en dus zelf verantwoordelijk blijft. De operatoren zijn, door gebrek aan bewijs van deze *teasing*-sms-berichten, niet geneigd te aanvaarden dat er een aansporing is geweest door de dienstaanbieder en crediteren bijgevolg niet de onterecht verzonden en ontvangen sms-berichten die volgden. De Ombudsdienst hoopt dat hiervoor weldra maatregelen genomen worden, zowel op het niveau van een verbod voor dienstenaanbieders om nog langer teasing/spam-sms-berichten te versturen, als op het niveau van de weergave ervan op «*traffic-listings*», zodat de naleving van de maatregelen gecontroleerd kan worden, in eerste instantie door de gsm-operator, in tweede instantie door de Ombudsdienst en in de toekomst ook door de Ethische Commissie ingeval van betwisting. De Ombudsdienst roept de gsm-operatoren alvast op om

une autre sonnerie et entraînant la souscription d'un nouvel abonnement. Autrement dit, l'utilisateur du GSM qui a, un jour, souscrit à un service donné (abonnement, jeu ou chat) se voit à nouveau sollicité ultérieurement via des messages sms – souvent gratuits mais parfois payants – pour participer à un nouveau concours, pour souscrire à un nouvel abonnement ou pour initier un nouveau chat, quiz ou autre service. Ces messages ne proviennent pas nécessairement du même numéro abrégé à partir duquel l'utilisateur a reçu jadis un service donné. De tels messages sms sont comparables aux fameux spams. Étant donné que des mesures ont déjà été prises contre les spams, il convient également d'agir contre le spamming ou le teasing par sms. Il n'existe pas encore d'interdiction générale frappant les messages sms incitatifs. Jusqu'à présent, les directives GOF ne prévoient une interdiction d'incitation non sollicitée que pour les services destinés aux mineurs d'âge (incitation à se réinscrire au même service ou à s'inscrire à un autre service), ainsi qu'une interdiction d'activation ou d'incitation non sollicitée à participer à un jeu par sms ou mms. De l'avis du service de médiation, cela ne suffit pas. L'interdiction de tels messages incitatifs devrait être étendue à tous les services sms, même si ces sms incitatifs sont gratuits. Non seulement, il est désagréable de recevoir de tels messages sms mais en plus, ils sont pour certains utilisateurs trop tentants pour ne pas y réagir (surtout en cas de messages *chat* et de quiz), de sorte que ces derniers engendrent des frais supplémentaires, parfois même sans connaissance du prix. Pour pouvoir contrôler le respect des interdictions déjà en vigueur frappant les sms incitatifs pour les mineurs d'âge et en cas de participation à un jeu, il est nécessaire de pouvoir constater l'existence de ces messages sms incitatifs. Ceci pose toutefois problème. Ces messages incitatifs ne sont pas toujours mentionnés par les fournisseurs de services dans les listings de trafic que réclament les opérateurs et le service de médiation pour pouvoir mener leur enquête. Les fournisseurs de services laissent ainsi sous-entendre que c'est l'utilisateur qui a initié la participation à un concours donné et qu'il en reste donc personnellement responsable. Faute de preuve de l'existence de ces messages sms incitatifs, les opérateurs ne sont pas enclins à accepter le fait qu'il y a eu incitation de la part du fournisseur de services et ne créditent donc pas les messages sms, indûment envoyés et reçus, qui ont suivi. Le service de médiation espère que, d'ici peu, des mesures seront prises en la matière. Celles-ci devraient viser, d'une part, à interdire aux fournisseurs de services d'envoyer encore des messages sms incitatifs/spams et, d'autre part, à les faire figurer sur les listings de trafic. Cette mesure permettrait le contrôle du respect des directives, d'abord par l'opérateur et, ensuite, par le service de médiation et, à l'avenir, aussi par la Commission d'éthique en cas

de dienstenaanbieders aan te sporen deze informatie vrijwillig mee op de «*traffic-listings*» te vermelden.»

5. Vragen en opmerkingen van de leden

A. Vragen aan de heer Luc Beirens

De heer Roel Deseyn (CD&V – N-VA) vraagt over hoeveel personeelsleden de FCCU dient te beschikken opdat de dienst goed zou kunnen functioneren. Acht de heer Beirens langdurige dataretentie noodzakelijk voor het voeren van een integraal veiligheidsbeleid? Hoe lang kunnen gegevens het best worden bewaard? Dreigt de bescherming van het privéleven daardoor niet in het gedrang te komen? Is een massaal verlies van vertrouwelijke gegevens, zoals in het Verenigd Koninkrijk gebeurd is, ook mogelijk in België of bestaan er efficiënte protocollen die dat kunnen verhinderen? Is er nood aan een evaluatiecentrum voor veiligheidsaccreditatie, dat de opdracht zou krijgen om een veiligheidslabel toe te kennen aan betrouwbare hard- en software? De verkrijging van dergelijk label zou een vereiste voor deelname aan overheidsopdrachten kunnen worden en zou het vertrouwen van consumenten in belangrijke mate kunnen bevorderen.

De heer Jan Mortelmans (VB) vraagt hoeveel de huidige personeelscapaciteit van de FCCU bedraagt. Hij is van oordeel dat de FCCU momenteel over te weinig medewerkers beschikt. Wordt dit tekort veroorzaakt door een te beperkt kader of door moeilijkheden bij het vinden van geschikte medewerkers? Beschikt de dienst over geschikte technische middelen om informaticacriminaliteit te bestrijden? Doet de FCCU voor vertaalwerk een beroep op vrijwilligers? Wordt de achtergrond van losse medewerkers in voorkomend geval nagetrokken? Werd de samenwerking met Europol versterkt, zoals de minister van Binnenlandse Zaken in het vooruitzicht heeft gesteld?

De heer Francis Van den Eynde (VB) wijst op het feit dat een spanning kan ontstaan tussen de strijd tegen kinderporno enerzijds en de waarborging van de vrijheid van meningsuiting op het internet anderzijds. Hoe kunnen de beide legitieme doelstellingen worden verzoend? Hoe pakt de FCCU de pogingen tot oplichting aan die vanuit West-Afrika per e-mail worden ondernomen? Gaat het effectief om Afrikaanse netwerken? Voert de FCCU ter zake een preventief beleid? Raadt de dienst personen die dergelijke e-mails ontvangen aan om er steeds melding van te maken bij de politie? Handelen de banken in België voldoende voorzichtig om fraude bij internetbankieren te verhinderen? Pleit de FCCU voor

de contestation. Le service de médiation invite d'ores et déjà les opérateurs à inciter les fournisseurs de services à mentionner cette information dans les listings de trafic de leur propre initiative.»

5. Questions et observations des membres

A. Questions à M. Luc Beirens

M. Roel Deseyn (CD&V – N-VA) demande de quel effectif de personnel FCCU doit disposer pour que le service fonctionne convenablement. M. Beirens estime-t-il qu'une longue rétention des données est nécessaire pour mener une politique de sécurité intégrale? Combien de temps est-il préférable de conserver les données? Ne risque-t-on pas de porter atteinte à la protection de la vie privée? Une perte massive de données confidentielles, comme cela s'est produit au Royaume-Uni, est-elle également possible en Belgique, ou existe-t-il des protocoles efficaces susceptibles de l'empêcher? A-t-on besoin d'un centre d'évaluation pour les accréditations de sécurité, qui se verrait confier la mission d'attribuer un label de sécurité aux hardwares et softwares fiables? L'obtention d'un tel label pourrait devenir une condition pour pouvoir participer à des marchés publics et pourrait augmenter considérablement la confiance des consommateurs.

M. Jan Mortelmans (VB) demande quelle est la capacité en personnel actuelle de la FCCU. Il estime que la FCCU dispose actuellement d'un nombre trop peu élevé de collaborateurs. Ce déficit en personnel est-il dû à un cadre trop limité ou à la difficulté de trouver des collaborateurs appropriés? Le service dispose-t-il de moyens techniques appropriés pour lutter contre la criminalité informatique? La FCCU fait-elle appel à des bénévoles pour les traductions? Les antécédents des collaborateurs occasionnels sont-ils contrôlés, le cas échéant? La collaboration avec Europol a-t-elle été renforcée, comme le ministre de l'Intérieur l'a promis?

M. Francis Van den Eynde (VB) souligne qu'il peut y avoir une tension entre la lutte contre la pédopornographie, d'une part, et la garantie de la liberté d'expression sur internet, d'autre part. Comment peut-on concilier ces deux objectifs légitimes? Comment la FCCU s'attaque-t-elle aux tentatives d'escroquerie envoyées par e-mail depuis l'Afrique de l'Ouest? S'agit-il effectivement de réseaux africains? La FCCU mène-t-elle une politique de prévention en la matière? Le service recommande-t-il aux personnes qui reçoivent ce genre d'e-mails de toujours le signaler à la police? Les banques en Belgique font-elles preuve de suffisamment de prudence pour empêcher la fraude liée à l'internet banking? La FCCU

de toekenning van de mogelijkheid aan de politie om undercoveroperaties op het internet uit te voeren?

De heer Ludo Van Campenhout (Open Vld) informeert naar de veiligheid van internetbankieren. Vinden fraudegevallen hun oorsprong in het kraken van wachtwoorden? Is de elektronische identiteitskaart een instrument dat de veiligheid van elektronisch bankieren kan verbeteren?

De heer Guido De Padt (Open Vld) vraagt of er ook fraude gebeurt met telefonie, in het bijzonder gsm's.

De heer Philippe Henry (Ecolo-Groen!) vraagt welke instanties het meest preventief werk leveren op het vlak van informaticaveiligheid. Hoe verloopt het overleg met internationale instellingen over de problematiek?

De heer François Bellot (MR) stelt vast dat de voorliggende problematiek, die bij uitstek een grensoverschrijdend karakter heeft, voornamelijk wordt aangepakt met nationale reactiemechanismen. Vereist het uittekenen van een efficiënte technische en gerechtelijke aanpak van criminele fenomenen op het internet een stroomlijning van de initiatieven van landen op EU-niveau? Is het problematisch dat de instrumenten voor een strafrechtelijke beteugeling zeer beperkt zijn? Hoe groot zijn de economische gevolgen van informaticacriminaliteit? Industriële spionage is een belangrijk probleem, zowel op wereldvlak als op lokaal niveau. Zo werden de afdeling Luchtvaart van de universiteit van Luik en Electrabel nog niet zo lang geleden het slachtoffer van spionage.

B. Vragen aan de heer Alain Huet

De heer Roel Deseyn (CD&V – N-VA), rapporteur, wenst te vernemen of FEDICT gewonnen is voor het opzetten van een vorm van een «forum» welke de samenwerking met de officiële instanties kan verbeteren en waar de club van «*security researchers*» zijn veiligheidsopmerkingen, testen en bedenkingen kan bespreken zonder risico op vervolging. Hij constateert voorts dat de verschillende federale overheidsdiensten van bijvoorbeeld Buitenlandse Zaken en Defensie ieder afzonderlijk beschikken over eigen beveiligingssystemen.

De spreker stelt zich daarbij de volgende vragen:

Zijn de kritische informatie in het bijzonder en de systemen in het algemeen voldoende beveiligd? Beschikken deze FOD's over voldoende expertise?

plaide-t-elle pour que l'on donne à la police la possibilité de mener des opérations d'infiltration sur internet?

M. Ludo Van Campenhout (Open Vld) s'enquiert de la sécurité des opérations bancaires en ligne. Les cas de fraude sont-ils imputables au déchiffrage de mots de passe? La carte d'identité électronique est-elle un instrument susceptible d'améliorer la sécurité des opérations bancaires électroniques?

M. Guido De Padt (Open Vld) demande si la fraude touche également la téléphonie, et en particulier les gsm.

M. Philippe Henry (Ecolo-Groen!) demande quelles instances jouent le rôle le plus préventif en matière de sécurité informatique. Comment se déroule la concertation avec les institutions internationales à propos de cette problématique?

M. François Bellot (MR) constate que l'on s'attaque surtout à la problématique à l'examen, transfrontalière par excellence, par le biais de mécanismes de réaction nationaux. La définition d'une lutte technique et judiciaire efficace contre la cybercriminalité requiert-elle une rationalisation des initiatives nationales au niveau européen? Est-il problématique que les instruments de répression pénale soient extrêmement limités? Quelle est l'ampleur des conséquences économiques de la criminalité informatique? L'espionnage industriel est un problème important, tant à l'échelle mondiale qu'au niveau local. C'est ainsi que le département Aéronautique de l'université de Liège et Electrabel ont été victimes d'espionnage il n'y a pas si longtemps.

B. Questions à M. Alain Huet

M. Roel Deseyn (CD&V – N-VA), rapporteur, demande si FEDICT est favorable à la création d'une sorte de «forum» qui permette d'améliorer la coopération avec les instances officielles et dans le cadre duquel le club des «*security researchers*» puisse discuter de ses observations relatives à la sécurité, de ses tests et de ses critiques sans risque de poursuites. Il constate également que chacun des différents services publics fédéraux, comme les Affaires étrangères et la Défense par exemple, dispose de ses propres systèmes de protection.

L'intervenant se pose dès lors les questions suivantes:

Les systèmes, en général, et les informations critiques, en particulier, sont-ils suffisamment sécurisés? Ces SPF disposent-ils d'une expertise suffisante?

Kan een zekere coördinatie van deze beveiligingssystemen leiden tot een hoge efficiëntie en kwaliteit van beveiliging? Er is ooit sprake geweest tot het uitvaardigen van een koninklijk besluit welke Fedict de bevoegdheid zou geven voor de veiligheid van alle federale overheidsdiensten. Wat is de stand van dit dossier?

Deze verschillende FOD's beschikken over hun eigen *back-up*systemen. Zijn deze systemen nog operationeel en *up-to-date*? Wordt de betrouwbaarheid en werking hiervan regelmatig getest? Zijn deze *back-up*systemen afdoende versleuteld?

Het Belgisch paspoort zou een RFID-chip bevatten (een draadloze chip die leesbaar is vanop afstand en waar ook persoonsgegevens op staan). Naar verluidt zou dit zonder de medewerking van FEDICT zijn doorgevoerd. Klopt dit? Is deze chip voldoende beveiligd? Kunnen globale veiligheidsnormen en controles voor het geheel van de federale infrastructuur de beveiliging van dergelijke applicaties ten goede komen?

Zijn de verschillende crisiscentra in België zelf voldoende beveiligd zodat zij bij een aanval van bijvoorbeeld een megavirus of zelfs een stroompanne steeds in staat zijn te reageren of is de beveiliging van hun eigen responsesystemen dringend aan verbetering toe?

Er zou een (extern) rapport bestaan over de veiligheid van de elektronische identiteitskaart. Kan dit rapport worden ingekeken? Is het niet nodig om dit rapport te actualiseren?

6. Antwoorden van de genodigde sprekers

A. Antwoorden van de heer Luc Beirens

1. De capaciteit van het FCCU

Samen met de 22 regionale eenheden bedraagt het personeelsbestand van de FCCU 156 eenheden. In 2006 werd een capaciteitsstudie verricht. Niet-dringende aanvragen worden in een aantal grote arronidssementen pas na een jaar behandeld. Nochtans ondergaat het aantal handelingen die moeten worden gesteld een exponentiële groei. Tussen 2007 en 2011 zouden er 160 eenheden moeten bijkomen. Geschikte kandidaten worden via universiteiten en hogescholen aangetrokken. Het werk van de FCCU gebeurt niet met vrijwilligers maar met personeel dat gemachtigd is om op te treden in gerechtelijke onderzoeken. Er is wel samenwerking met BeNIS (de Belgische overheidsinstantie die zich bezighoudt met ICT-veiligheid).

Une certaine coordination de ces systèmes de protection peut-elle être le gage d'une efficacité élevée et d'une grande qualité en matière de protection? Il a déjà été question de prendre un arrêté royal qui habiliterait Fedict à sécuriser tous les services publics fédéraux. Où en est le dossier?

Ces différents SPF disposent de leurs propres systèmes de *back-up*. Ces systèmes sont-ils toujours opérationnels et à jour? Leur fiabilité et leur fonctionnement sont-ils régulièrement contrôlés? Ces systèmes de *back-up* sont-ils suffisamment cryptés?

Le passeport belge contiendrait une puce RFID (une puce sans fil, lisible à distance et contenant également des données personnelles). Cela aurait été mis en place sans la collaboration de FEDICT. Est-ce exact? Cette puce est-elle suffisamment protégée? Des normes de sécurité et des contrôles globaux pour l'ensemble de l'infrastructure fédérale peuvent-ils être bénéfiques pour la sécurisation de telles applications?

Les différents centres de crise en Belgique sont-ils eux-mêmes suffisamment sécurisés de sorte à pouvoir réagir, par exemple, en cas d'attaque par un mégavirus ou même en cas de panne de courant, ou la sécurisation de leurs propres systèmes de réaction doit-elle être améliorée d'urgence?

Il existerait un rapport (externe) sur la sécurité de la carte d'identité électronique. Ce rapport peut-il être consulté? N'est-il pas nécessaire d'actualiser ce rapport?

6. Réponses des orateurs

A. Réponses de M. Luc Beirens

1. La capacité de FCCU

Compte tenu des vingt-deux unités régionales, l'effectif du personnel de la FCCU compte 156 unités. Une étude de capacité a été réalisée en 2006. Les cas non urgents ne sont examinés qu'après une année. Le nombre d'actes à accomplir connaît cependant une croissance exponentielle. Cent soixante unités supplémentaires devraient être prévues entre 2007 et 2011. Les candidats appropriés sont recrutés par le biais des universités et des écoles supérieures. La FCCU ne travaille pas avec des bénévoles, mais avec du personnel habilité à intervenir dans des enquêtes judiciaires. Il y a en revanche une collaboration avec BeNIS (l'organe public belge chargé de la sécurité ICT).

2. De middelen van het FCCU

Op basis van de capaciteitsstudie van 2006 zou voor elke CCU-lid jaarlijks een bedrag van 4.500 € aan individueel materiaal moeten worden aangekocht en 30.000 € aan collectief materiaal voor een grote CCU. Deze bedragen werden tot op heden helemaal niet gehaald. Het gemiddeld jaarlijks beschikbaar bedrag voor investeringen lag van 2001 tot en met 2005 op 187.000 € voor alle CCU's te samen. Het budget bedroeg in 2007 783.000 € wat voor het eerst in jaren een echt werkbaar investeringsbudget was. De investeringsinspanning moet worden aangehouden om het materiaal elke drie jaar te kunnen vervangen of de software jaarlijks te kunnen upgraden.

3. De bewaartijd van verkeersgegevens

De Europese dataretentie-richtlijn uit 2006 legt de bewaarperiode vast van de verkeersgegevens van telefoon- en e-mail-verkeer. Deze termijn moet liggen tussen de zes maanden en twee jaar. Elk land moet de richtlijn uitwerken in nationale wetgeving.

In het verleden is de Belgische bewaartermijn van 12 maanden voor telefonieverkeer een werkbare periode gebleken. Het is echter maar zeer de vraag of de bewaarperiode van 12 maand nog voldoende lang is om bijvoorbeeld terrorisme te bestrijden. Aan terroristische aanslagen gaan vaak heel lange voorbereidingen vooraf. Bovendien lijkt deze periode voor de internetverkeersgegevens onvoldoende omdat deze gegevens vaak moeten bekomen worden via internationaal rechtshulpverzoek. Een identificatie van een internetgebruiker vereist bovendien een procedure in verschillende stappen met vorderingen naar de verschillende tussenkomende partijen (internetdienstenleverancier, internettoegangsleverancier en de telecomoperator ADSL of kabel).

De Europese richtlijn is nog niet omgezet in Belgisch recht. Ondertussen bevinden de operatoren zich in een grijze zone. Want wat niet wettelijk verplicht of toegestaan is om bij te houden als verkeersgegeven moet verplicht anoniem gemaakt worden of worden gewist.

4. De grensoverschrijdende samenwerking

Naar gelang van het soort criminaliteit, wordt nauw samengewerkt met Interpol of met Europol. Sommige gerechtelijke procedures dateren nog uit de 19° eeuw. Ze houden niet echt rekening met de snelheid van de internetcriminelen. Zo moet men rekening houden met websites zeer snel verdwijnen en soms enkele uren of dagen later opduiken in een ander land.

Zelfs als men naar huidige normen van de rechtsprocedure snel werkt met internationale rechtshulpverzoeken en die binnen één à twee weken overmaakt, dan nog

2. Les moyens de la FCCU

Sur la base de l'étude de capacité de 2006, chaque année, il faudrait acheter, pour chaque membre CCU, du matériel individuel pour un montant de 4 500 euros et, pour une grande CCU, du matériel collectif à concurrence de 30 000 euros. Jusqu'à présent, ces montants n'ont pas été atteints. Le montant annuel moyen disponible pour les investissements s'est chiffré, de 2001 à 2005, à 187 000 euros pour l'ensemble des CCU. En 2007, le budget s'élevait à 783 000 euros, ce qui constitue, pour la première fois depuis des années, un véritable budget d'investissement opérationnel. L'effort d'investissement doit être maintenu pour pouvoir remplacer le matériel tous les trois ans ou pour pouvoir mettre le logiciel à niveau tous les ans.

3. La durée de conservation des données

La directive européenne de 2006 relative à la rétention des données fixe la période de conservation des correspondances téléphoniques et électroniques. Ce délai doit être compris entre six mois et deux ans. Chaque pays doit transposer la directive dans sa législation nationale.

Autrefois, le délai belge de conservation de 12 mois pour les correspondances téléphoniques s'était avéré acceptable. L'on peut néanmoins se demander si cette durée de 12 mois est encore suffisamment longue pour, par exemple, lutter contre le terrorisme. Les attentats terroristes sont souvent précédés par de très longs préparatifs. En outre, pour les échanges de données par internet, cette période semble insuffisante, dans la mesure où l'obtention de ces données requiert souvent une entraide judiciaire internationale. L'identification d'un internaute nécessite par ailleurs une procédure en plusieurs étapes, comprenant des demandes aux différents intermédiaires (fournisseur de services internet, fournisseur d'accès internet et opérateur du réseau de télécommunications ADSL ou câble).

La directive européenne n'a pas encore été transposée en droit belge. Dans l'intervalle, les opérateurs se trouvent dans une zone grise. Car les données de trafic que la loi n'oblige ni n'autorise à conserver doivent obligatoirement être rendues anonymes ou être effacées.

4. La coopération transfrontalière

En fonction du type de criminalité, il y a une coopération étroite avec Interpol ou avec Europol. Certaines procédures judiciaires datent encore du dix-neuvième siècle. Elles ne tiennent pas vraiment compte de la rapidité des criminels opérant sur Internet. Il faut ainsi prendre en compte le fait que les sites Internet disparaissent très vite pour, parfois, refaire surface quelques heures ou quelques jours plus tard dans un autre pays.

Même si, selon les normes de la procédure judiciaire, on fait rapidement une demande d'entraide internationale et qu'on la transmet dans un délai de une à deux

riskeren we verlies van bewijsmateriaal. Als voorbeeld kan de spreker hier een dossier aanhalen waar de procedure bij een buitenlands rechtshulpverzoek één week nam vooraleer een afstapping kon worden gedaan bij de verdachte. Hierdoor ging de helft van het mogelijke bewijsmateriaal verloren gezien die server slechts twee weken logginggegevens bijhield.

Gezien het grensoverschrijdende karakter van de ICT-criminaliteit, is de internationale samenwerking, zowel Europees als mondiaal, absoluut noodzakelijk. Ook wordt thans meer aandacht gegeven aan de internationale samenwerking van de magistratuur via Eurojust.

Men moet komen tot een goede internationale beeldvormen en daarom samenwerken. De Verenigde Staten hebben bijvoorbeeld een beter beeld van de internetfraude dan in Europa.

5. Undercoveroperaties

www.eCops.be is het uniek loket om bedriegelijke praktijken op het internet te melden. Soms wordt via eCops een forum met bijvoorbeeld kinderporno aangemeld waarbij de toegangscodes voor het verdachte forum eveneens worden overgemaakt. De vraag dringt zich hier op of de politiediensten met overgemaakte toegangscodes dit forum mogen nachecken zonder dat dit nazicht als hacking zou worden beschouwd. Op dit gebied zou een wetgevend initiatief welkom zijn om het arsenaal van de gerechtelijke overheden uit te breiden met de mogelijkheid om met een bevel binnen te dringen in beveiligde computersystemen. Dit is de cybervariant van de bevoegdheid van de onderzoeksrechter die een slotenmaker opdracht geeft om een deur te openen om een huiszoeking te kunnen uitvoeren.

6. Economische fraude

Bedrijfsgeheimen worden vaak door medewerkers van het bedrijf zelf misbruikt of onthuld.

B. Antwoorden van de heer Alain Huet

Veiligheidscertificering

Voor wettelijk als geclassificeerde bestempelde informatie zou een veiligheidscertificering de regel moeten zijn. Een studie hierover heeft op 6 februari 2007 het groen licht gekregen van het Ministerieel Comité voor Inlichtingen en Veiligheid.

semaines, on court encore le risque de perdre des éléments de preuve. À titre d'exemple l'intervenant cite le cas d'un dossier où la procédure de demande d'entraide étrangère a pris une semaine avant de permettre une descente chez le suspect. La moitié des éléments de preuve avait ainsi disparu dès lors que ce serveur ne conservait que pendant deux semaines les informations relatives aux loggings.

Compte tenu du caractère transfrontalier de la criminalité TIC, une coopération internationale, tant européenne que mondiale, s'avère indispensable. À l'heure actuelle, on attache également un intérêt accru à la coopération internationale de la magistrature via Eurojust.

Il faut se forger une bonne idée de ce qui se passe au niveau international et pour cela il faut coopérer. Les États-Unis ont par exemple une meilleure idée de la fraude sur Internet qu'en Europe.

5. Opérations d'infiltration

www.eCops.be est le guichet unique pour signaler des pratiques frauduleuses sur Internet. On est parfois avisé, via eCops, de l'existence d'un forum contenant de la pédopornographie, ainsi que des codes d'accès au forum suspecté. La question se pose de savoir si les services de police peuvent, grâce aux codes d'accès transmis, vérifier le contenu de ce forum sans que ce contrôle soit considéré comme du piratage informatique. Dans ce domaine, une initiative législative serait la bienvenue pour élargir l'arsenal des autorités judiciaires à la possibilité de pénétrer, avec un mandat, dans des systèmes informatiques sécurisés. C'est la cyber-variante de la compétence du juge d'instruction qui charge un serrurier d'ouvrir une porte afin de pouvoir exécuter une perquisition.

6. Fraude économique

Les secrets d'entreprises sont souvent utilisés abusivement ou dévoilés par des collaborateurs de l'entreprise elle-même.

B. Réponses de M. Alain Huet

Certification en matière de sécurité

Pour les informations légalement qualifiées de classifiées, une certification en matière de sécurité devrait être la règle. Une étude en ce sens a reçu le 6 février 2007 un accord de principe du Comité ministériel de Reseignements et de la Sécurité

II. — HOORZITTING VAN 23 JANUARI 2008

1. Uiteenzetting van de heer Willem De Beuckelaere, voorzitter, en de heer Dieter Verhaeghe, juridisch adviseur van de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna «Privacycommissie» genoemd)

De heer Willem De Beuckelaere verwijst naar artikel 16 van de wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens («privacywet»), dat de basis vormt van de geldende regelgeving met betrekking tot de verhouding tussen privacy en informatieveiligheid. De privacycommissie focust in de context van dit debat over informatieveiligheid vooral op het probleem «spam».

De heer Dieter Verhaeghe onderzoekt eerst de toepasselijkheid van de privacywet op het fenomeen spam, analyseert vervolgens de problemen voor de effectieve toepassing van de wet op spam en besluit met mogelijke oplossingen voor het probleem. De privacywet is slechts van toepassing wanneer er een verwerking van persoonsgegevens gebeurt, zowel in een private als in een professionele context. Dit is het geval bij spam en phishing: een bepaald e-mailadres figureert immers in een verzendingslijst. De Privacycommissie legt zich vooral toe op het fenomeen «*direct marketing*» (*mailing*, verkoop van adressen, telemarketing), waartegen burgers zich, met toepassing van artikel 12 van de privacywet, kunnen verzetten.

Andere wetten hebben een belangrijke aanvullende rol:

– het Strafwetboek;

– de wet van 11 maart 2003 betreffende sommige juridische aspecten van de diensten uit de informatiemaatschappij (art. 14, § 1: principe van «*opt-in*» voor reclame per e-mail);
– de wet van 14 juli 1991 betreffende de handelspraktijken en de voorlichting en bescherming van de consument (artikel 29);
– het principe van «*opt-in*» voor reclame per fax of geautomatiseerde oproepsystemen.

Door toepassingsproblemen is de privacywet niet steeds het meest geschikte instrument om het probleem van spam effectief aan te pakken:

II. — AUDITION DU 23 JANVIER 2008

1. Exposé de M. Willem De Beuckelaere, président, et de M. Dieter Verhaeghe, conseiller juridique de la Commission de protection de la vie privée (appelée ci-après «Commission vie privée»)

M. Willem De Beuckelaere se réfère à l'article 16 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel («loi sur la protection de la vie privée»), qui se trouve à la base de la réglementation en vigueur en ce qui concerne la relation entre la vie privée et la sécurité de l'information. Dans le contexte du présent débat sur la sécurité de l'information, la Commission vie privée se focalise essentiellement sur le problème des spams.

M. Dieter Verhaeghe examine tout d'abord l'applicabilité de la loi sur la protection de la vie privée au phénomène des spams, analyse ensuite les problèmes de l'application effective de la loi aux spams et conclut en proposant des solutions possibles au problème. La loi sur la protection de la vie privée ne s'applique qu'en cas de traitement de données à caractère personnel, tant dans un contexte privé que dans un contexte professionnel. C'est le cas pour les spams et le phishing, puisqu'une adresse électronique donnée figure sur une liste d'envoi. La Commission vie privée s'intéresse surtout au phénomène du «*marketing direct*» (*mailing*, vente d'adresses, télémarketing), auquel les citoyens peuvent s'opposer en application de l'article 12 de la loi sur la protection de la vie privée.

D'autres lois jouent un rôle complémentaire important:

– le Code pénal;

– la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information (art. 14, § 1er: principe de l'«*opt-in*» pour la publicité par courrier électronique);
– la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur (article 29);
– le principe de l'«*opt-in*» pour la publicité par fax ou par systèmes automatisés d'appel.

Eu égard à des problèmes d'application, la loi sur la protection de la vie privée n'est pas toujours l'instrument le plus adéquat pour s'attaquer réellement au problème des spams:

– De verzender van spam en zijn lokalisatie moeten bekend zijn om een beroep te kunnen doen op de privacywet, wat bij spam normaliter niet het geval is;

– In de privacywet wordt niet expliciet melding gemaakt van de problemen in een ICT-context (spam, *phishing*, Nigeriaanse *scams*, valse loterijen, identiteitsfraude,…);
– De privacycommissie beschikt niet over een eigen manuele en technische analysecapaciteit in verhouding tot het actuele volume van het fenomeen;

– Het instrumentarium van de privacywet is niet geschikt voor het aanpakken van misdrijven met criminele intenties (oplichting, misbruik van vertrouwen, identiteitsfraude); die problemen behoren tot de opdrachten van de *Federal Computer Crime Unit*.

Een efficiënte aanpak impliceert snelle technische analyses, de ontwikkeling van een coherente visie en samenwerking op verschillende niveaus (zowel nationaal als internationaal). De bewustmaking van particuliere burgers volstaat niet: vooral de privésector (banken, IT-sector) moet worden geresponsabiliseerd.

Sommige oplossingen functioneren reeds:

– Op www. spamsquad.be, een nationale publiek-private samenwerking, wordt de burger ertoe gestimuleerd om zelf verantwoordelijkheid op te nemen;
– Op www.ecops.be werken de FCCU en de FOD Economie samen bij de nationale afhandeling van klachten uit de publieke sector;
– Op internationaal niveau werken CNSA (*Contact Network for Spam Authorities*) en LAP (*London Action Plan*, een Angelsaksisch initiatief) samen aan een beveiliging van de openbare sector;
– In de private sector wordt werk gemaakt van de filtering via zwarte lijsten van IP-adressen en ISP's.

Andere oplossingen zijn in voorbereiding:

– Een nationale en Europese spambox staan in de steigers;
– Via «*privacy enhancing technologies*» (PET) kunnen klachten automatisch worden aangegeven en verwerkt, zowel op nationaal als op Europees niveau.

De spreker besluit met een aantal reglementaire oplossingen voor de geschetste problemen:

– De verantwoordelijkheid van de privésector kan worden vergroot door een effectieve klachtenbehandeling. Thans zijn de telecommunicatieoperatoren niet aansprakelijk voor de inhoud van de boodschappen die

– L'expéditeur de spam et sa localisation doivent être connus pour pouvoir invoquer la loi sur la protection de la vie privée, ce qui n'est normalement pas le cas lorsqu'il s'agit de spam;
– La loi sur la protection de la vie privée ne fait pas explicitement mention de problèmes situés dans le contexte de la TIC (spam, *phishing*, *scams* nigérians, fausses loteries, fraude à l'identité,…);
– La commission de la protection de la vie privée ne dispose pas d'une capacité d'analyse manuelle et technique propre en rapport avec le volume actuel du phénomène;
– Les instruments prévus par la loi sur la protection de la vie privée ne sont pas adaptés à la lutte contre les infractions de nature criminelle (escroquerie, abus de confiance, fraude à l'identité); ces problèmes relèvent des missions de la *Federal Computer Crime Unit*.

Une approche efficace implique des analyses techniques rapides, le développement d'une vision cohérente et la collaboration à différents niveaux (tant national qu'international). Il ne suffit pas de sensibiliser les citoyens: il convient surtout de responsabiliser le secteur privé (banques, secteur IT).

Certaines solutions fonctionnent déjà:

– Sur www.spamsquad.be, une collaboration publique-privée nationale incite le citoyen à prendre lui-même ses responsabilités;
– Sur www.ecops.be, la FCCU et le SPF Économie collaborent au traitement national des plaintes émanant du secteur public;
– Au niveau international, le CNSA (*Contact Network for Spam Authorities*) et le LAP (*London Action Plan*, une initiative anglosaxonne) collaborent à la sécurisation du secteur public;
– Dans le secteur privé, on s'occupe du filtrage par le biais de listes noires d'adresses IP et d'ISP.

D'autres solutions sont en préparation:

– Une spambox nationale et européenne sont en chantier;
– Les plaintes peuvent être automatiquement déposées et traitées, tant au niveau national qu'au niveau européen, par le biais de «*Privacy Enhancing Technologies*» (PET).

L'orateur conclut en présentant un certain nombre de solutions réglementaires pour les problèmes évoqués:

– La responsabilité du secteur privée peut être étendue par un traitement effectif des plaintes. Pour l'heure, les opérateurs de télécommunications ne sont pas responsables du contenu des messages diffusés par le

via hun netwerk worden verspreid (al is er wel reeds een corrigerende marktwerking die van de zwarte lijsten uitgaat) en zwijgen zij soms als veiligheidsproblemen ontstaan uit vrees voor imagoschade;

– De rechtspositie van slachtoffers van identiteitsdiefstal is vandaag onzeker. Zij riskeren niet geloofd te worden door hun dienstenleverancier en zelfs geplaatst worden op de lijst van wanbetalers bij de Nationale Bank. Los van de mogelijkheid om identiteitsdiefstal als zelfstandig misdrijf te erkennen, dient de status van slachtoffer van identiteitsdiefstal duidelijker te worden geregeld;

– Banken moeten ertoe worden verplicht gevallen van identiteitsfraude bekend te maken: de bevolking heeft immers recht op technisch correcte informatie als er een *phishing*schandaal is;

– Er moet een betere wettelijke basis worden gecreëerd voor de bestaande samenwerking tussen publieke en private sector, met respect voor kwesties zoals beroepsgeheim en confidentialiteitsverplichtingen van overheidsdiensten.

2. Uiteenzetting van de heer Rudi Vansnick, voorzitter ISOC *Belgium* («*Internet Society*»)

ISOC *Belgium* bestaat sedert 1998. De vereniging stelt zich tot doel internet tot een stabiel, toegankelijk en veilig medium voor iedereen te maken. Als zodanig is de Belgische afdeling slechts een van de 100 die wereldwijd verspreid zijn over meer dan 180 landen. Om dit doel te bereiken moet het internet zowel inhoudelijk (standaarden, protocols,…) als maatschappelijk (digitale kloof, classificering inhoud,…) voortdurend aan de behoeften van de gebruikers worden aangepast. ISOC Belgium gaat daarvoor samenwerkingsverbanden aan op internationaal vlak en biedt haar expertise aan voor alle aspecten die te maken hebben met de informatiemaatschappij en de digitale kloof die allerminst kleiner wordt.

Vanuit de vaststelling dat de Ombudsdienst voor telecommunicatie niet kan inspelen op de specificiteit van het internet, heeft ISOC Belgium in 2005 een ombudsdienst voor het internet opgestart, dat zowat 400 klachten heeft behandeld. De vereniging hecht ook veel belang aan bescherming van de privacy in familieverband, zowel wat classificering van de inhoud van sites als wat de rechten van het kind betreft. Kinderen beseffen niet altijd dat hun blogs door iedereen – hun ouders incluis – kunnen gelezen worden, wat soms tot nodeloze spanningen kan leiden. Anderzijds moeten ze ook beschermd worden tegen ongewenste informatie.

biais de leur réseau (même si un correctif du marché émane déjà des listes noires) et il leur arrive de se taire lorsque des problèmes de sécurité surgissent par crainte de voir leur image ternie;

– Actuellement, la position juridique de victimes d'un vol d'identité est incertaine. Elles risquent de ne pas être crues par leur fournisseur de services et même d'être inscrites sur la liste des mauvais payeurs auprès de la Banque nationale. Indépendamment de la possibilité de reconnaître le vol d'identité en tant qu'infraction autonome, il convient de régler plus précisément le statut de la victime d'un vol d'identité;

– Les banques doivent être contraintes de signaler les cas de fraude à l'identité: la population est en effet en droit d'obtenir une information technique correcte lorsque se produit un scandale de *phishing*;

– Il faut créer une base légale plus appropriée pour la collaboration existante entre le public et le privé, dans le respect de questions telles que le secret professionnel et les obligations de confidentialité des services publics.

2. Exposé de M. Rudi Vansnick, président d'ISOC Belgium («*Internet Society*»)

ISOC Belgium existe depuis 1998. L'association se fixe pour objectif de faire d'Internet un moyen de communication stable, accessible et sûr pour tous. En tant que telle, la division belge ne représente que l'une des 100 divisions présentes à l'échelle mondiale, qui se répartissent entre plus de 180 pays. Pour atteindre cet objectif, l'Internet doit être adapté en permanence aux besoins des utilisateurs, tant en termes de contenu (normes, protocoles,…) que d'un point de vue social (fracture numérique, classification du contenu,…). Dans cette optique, ISOC Belgium établit des accords de coopération à l'échelle internationale et propose son expertise pour tous les aspects liés à la société de l'information et à la fracture numérique – qui ne diminue pas le moins du monde.

Partant du constat que le Service de médiation pour les télécommunications ne peut faire face à la spécificité de l'Internet, ISOC Belgium a lancé en 2005 un service de médiation pour l'Internet, qui a traité quelque 400 plaintes. L'association attache également beaucoup d'importance à la protection de la vie privée des familles, tant en ce qui concerne la classification du contenu des sites que les droits de l'enfant. Les enfants ne sont pas toujours conscients du fait que leurs blogs sont accessibles à tous – y compris leurs parents – ce qui peut parfois engendrer des tensions inutiles. D'autre part, ils doivent également être protégés contre les informations non souhaitées.

De veiligheid op het internet neemt vele vormen aan: er is de spam, de voor kinderen schadelijke inhoud van websites, de diefstal en het misbruik van persoonlijke gegevens, frauduleuze handelingen die via diverse veilingplatformen verricht worden, waarvan de initiatiefnemers buiten schot blijven en waarbij misbruik gemaakt wordt van labels die men heeft aangekocht, en ten slotte het online-gokken dat in principe verboden is maar intussen steeds meer slachtoffers maakt. Er wordt niet opgetreden tegen spam, zelfs wanneer deze vanop Belgische bodem wordt verstuurd. Ook andere dan kinderpornosites kunnen enorme schade toebrengen aan zwakkere internetgebruikers. Veel studenten verdienen een cent bij door op hostingsites door te linken, maar deze praktijk kan misbruikt worden door hackers en internetterroristen.

Er zou sowieso een scherpere externe controle moeten worden uitgeoefend bij en op de toekenning van domeinnamen «.be», want de laksheid wat dit betreft zet de deur wagenwijd open voor misbruiken.

Al bij al hoeft het niet te verbazen dat de Belgische sites bij de top-10 van de meest onveilige ter wereld hoort, in gezelschap van de Russische en de Chinese sites.

De ISP's en hostingbedrijven opereren soms zonder zelfs maar officieel geregistreerd zijn als bedrijf of zelfstandige.

De drempel voor de internetgebruiker om misbruik aan te klagen is te hoog. In die context heeft de «internet ombudsdienst» reeds vierhonderd dossiers behandeld, waarbij het vaakst werd doorverwezen naar officiële instanties maar waarbij ook veel van gezond werstand getuigende en rationele oplossingen werden aangereikt.

ISOC Belgium was graag lid geworden van het «Internet Observatorium», maar heeft op dit verzoek nooit antwoord gekregen. Het heeft de Kansspelcommissie ertoe aangezet meer aandacht te hebben voor online gokken. De vereniging wenst ook een rol te spelen in het raam van «e-government» en wenst vertegenwoordigd te zijn in de nieuwe structuur van het BIPT.

Tot slot dringt ISOC Belgium aan op nauwere samenwerking tussen alle diensten die het internet bewaken. Waar nodig, moet repressief worden opgetreden, zoals in Nederland. Projecten als «Internet voor Iedereen» hebben hun doel voorbijgeschoten omdat men niet nauwgezet genoeg tewerk is gegaan.

La sécurité de l'Internet se présente sous de nombreuses formes: il y a le spam, le contenu de sites Internet préjudiciable pour les enfants, le vol et l'abus de données à caractère personnel, les opérations frauduleuses réalisées via diverses plates-formes de vente aux enchères, dont les initiateurs restent hors d'atteinte et dans le cadre desquelles l'on abuse de labels que l'on a achetés, et enfin, les paris en ligne qui sont en principe interdits, mais qui font désormais de plus en plus de victimes. L'on ne prend aucune mesure contre le spam même lorsque celui-ci est envoyé depuis la Belgique. Il n'y a pas que les sites à caractère pédopornographique qui peuvent être extrêmement préjudiciables pour les internautes plus vulnérables. De nombreux étudiants se font un peu d'argent de poche en renvoyant vers des sites d'hébergement, mais cette pratique peut être utilisée à mauvais escient par des hackers et des cyberterroristes.

Il conviendrait dans tous les cas d'exercer un contrôle extérieur plus rigoureux en ce qui concerne l'octroi des noms de domaine «.be», car le laxisme en la matière ouvre la porte à tous les abus.

Somme toute, il ne faut pas s'étonner du fait que les sites belges figurent parmi les dix les moins sûrs au monde, en compagnie des sites russes et chinois.

Il arrive que les ISP et les hébergeurs opèrent sans même être enregistrés officiellement en tant qu'entreprise ou qu'indépendant.

Le seuil à franchir pour un utilisateur d'internet qui souhaite déposer plainte pour abus est trop important. Dans ce contexte, le «service de médiation internet» a déjà traité quatre cents dossiers, dans le cadre desquels il a en général renvoyé à des instances officielles, mais également proposé de nombreuses solutions rationnelles et de bon sens.

ISOC Belgium aurait aimé devenir membre de l'«Observatoire internet», mais sa candidature est restée lettre morte. Elle a incité la Commission des jeux de hasard à s'intéresser davantage aux paris en ligne. L'association entend également jouer un rôle dans le cadre de l'«e-government» et souhaite être représentée au sein de la nouvelle structure de l'IBPT.

Enfin, ISOC Belgium insiste sur la nécessité de resserrer la collaboration entre tous les services qui surveillent internet. Au besoin, il faut intervenir de manière répressive, comme aux Pays-Bas. Des projets tels que «Internet pour tous» ont manqué leur cible, parce que leur mise en œuvre a manqué de rigueur.

3. Uiteenzetting van professor Bart Preneel, cryptoloog aan de Katholieke Universiteit Leuven (KUL)

De heer Bart Preneel is gewoon hoogleraar aan de K.U. Leuven. Hij staat aan het hoofd van de onderzoeksgroep COSIC, die op 30 jaar ervaring kan bogen en waarin 55 wetenschappers actief zijn. Verder is hij ook voorzitter van L-SEC (*Leaders in e-Security*).

De volgende evoluties doen zich voor op het vlak van internetveiligheid:

– Beveiliging wordt minder snel ontwikkeld dan de evolutie van de bedreigingen, zodat de omvang van de risico's systematisch toeneemt.
– De informatie over problemen en de zichtbaarheid van aanvallen via het internet zijn beperkt, onder meer omdat bedrijven er vaak naar streven om de problemen waarmee zij kampen geheim te houden.

– De klemtoon ligt niet meer op hacking voor het plezier, maar op professionele criminaliteit met financiële motieven.
– Er is een toename van industriële spionage door de beschikbaarheid van online-informatie over ondernemingen.
– Bedreigingen krijgen een wereldomvattende schaal (tot zelfs een door staten georganiseerde cyberoorlog).

Inzake informatica doet zich op alle vlakken een exponentiële groei en evolutie voor, die door niemand volledig kan worden gevat. Dit komt in de volgende variabelen tot uiting:

– Een individuele computer bevat 100 miljoen transistoren.
– Een beheerssysteem (Windows, Linux) functioneert met 20 tot 200 miljoen lijnen code.

– Een applicatie omvat 1 tot 20 miljoen lijnen code.

– 500 miljoen computers zijn op het internet aangesloten.
– Er zijn 2 miljard gebruikers van mobiele telefonie.

Als één schakel in een informaticaproces een kleine fout bevat, kan de goede werking van de hele keten in het gedrang komen.

De computertechnologie en de industrie zijn per definitie internationaal, terwijl de interstatelijke coördinatie van het veiligheidsbeleid niet optimaal functioneert. Dat blijkt onder meer uit de werking van ENISA (*European*

3. Exposé du professeur Bart Preneel, cryptologue à la *Katholieke Universiteit Leuven* (KUL)

M. Bart Preneel est professeur ordinaire à la K.U. Leuven. Il dirige le groupe de recherche COSIC, riche d'une expérience de 30 ans et au sein duquel 55 scientifiques sont actifs. Il est également président de L-SEC (*Leaders in e-Security*).

Les évolutions suivantes ont été notées dans le domaine de la sécurité sur internet:

– La sécurisation évolue moins vite que les menaces, de sorte que l'ampleur des risques augmente systématiquement.
– L'information relative aux problèmes rencontrés et la visibilité des attaques par le biais d'Internet sont limitées, notamment parce que les entreprises s'efforcent souvent de garder le secret sur les problèmes auxquels elles sont confrontées.
– L'accent est mis non plus sur le piratage pour le plaisir, mais sur la criminalité professionnelle pour des motifs financiers.
– On observe une augmentation de l'espionnage industriel du fait de la disponibilité d'informations en ligne sur les entreprises.
– Les menaces prennent une dimension mondiale (jusqu'à même une cyberguerre organisée par des États)

En matière d'informatique, on observe, dans tous les domaines, une croissance et une évolution exponentielle que personne ne peut maîtriser entièrement. Les chiffres suivants en témoignent:

– Un ordinateur personnel contient 100 millions de transistors.
– Un système d'exploitation (Windows, Linux) fonctionne au moyen de 20 à 200 millions de lignes de code.
– Une application comporte de 1 à 20 millions de lignes de code.
– 500 millions d'ordinateurs sont connectés à Internet.
– La téléphonie mobile compte 2 milliards d'utilisateurs.

Si un seul maillon d'un processus informatique contient une petite erreur, c'est le bon fonctionnement de l'ensemble de la chaîne qui peut être compromis.

Les technologies informatiques et l'industrie sont par définition internationales, alors que la coordination entre États de la politique de sécurité ne fonctionne pas de manière optimale. C'est ce qui ressort notamment du

Network Information Security Agency), dat een taak van te beperkte omvang heeft en onvoldoende informatie aanlevert. De EU-lidstaten die op het vlak van ICT-veiligheid het meest ervaring hebben (Duitsland, het Verenigd Koninkrijk, Frankrijk en Nederland) achten het niet in hun belang om naar volledige synergie te streven. Ook landen buiten de EU leggen de nadruk op hun nationaal belang. Zo probeert China om alle onderdelen van de informaticaketen zelf te ontwikkelen om afhankelijkheid van de VS en de EU te vermijden.

De dieperliggende oorzaak van de onveiligheid van ICT-systemen is van economische aard: in de ICT-wereld is marktaandeel belangrijker dan beveiliging. Succes op informaticavlak vergt een quasi-universele adoptie, waardoor producenten prioritair inzetten op een snelle verovering van de markt en minder aan veiligheid werken. bovendien wordt vastgesteld dat de gebruiker niet bereid is om voor privacy te betalen en veilige en onveilige producten niet van elkaar kan onderscheiden. Ook wanneer een ICT-systeem zich op de markt gevestigd heeft, blijft de aandacht voor veiligheid te beperkt omdat de entiteit die voor de investeringen zou moeten betalen in veel gevallen niet het (belangrijkste) slachtoffer van een gebrek aan beveiliging is. Zo worden computers die deel worden van een botnet er meestal niet zelf door getroffen.

Het spamprobleem kan maar op twee manieren worden opgelost: door een betere authentificatie en door de verhoging van de prijs voor de verzending van een e-mail, wat een optimale en gecoördineerde samenwerking op internationaal niveau vergt. De menselijke factor blijft de zwakke schakel: doordat consumenten nauwelijks weten hoe het internet werkt en de voorkeur geven aan gebruiksvriendelijke systemen, die vaak minder veilig zijn, moedigen zij investeringen in veiligheid niet aan.

De gevolgen en de reactiemechanismen zijn verschillend voor industrie, individu en overheid:

– Bedrijven worden het slachtoffer van het verlies van persoonsgegevens, bedrijfsspionage, chantage, onbeschikbaarheid van hun website, reputatieschade en gemiste kansen. Grote ondernemingen hebben al ervaring met het beheer van risico's, kleinere ondernemingen zijn kwetsbaarder.

– Burgers leveren op hun privacy in doordat zij in een ongelijke strijd met technologie en het zakenleven verwikkeld zijn: persoonlijke gegevens worden steeds meer beschikbaar, de kost voor het opslaan en verwerken van gegevens daalt, door gedragsanalyse van consumenten

fonctionnement de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), dont la mission est trop limitée et qui livre trop peu d' informations. Les États membres de l'Union européenne qui ont le plus d'expérience dans le domaine de la sécurité TIC (l'Allemagne, le Royaume-Uni, la France et les Pays-Bas) estiment qu'il n'est pas de leur intérêt de tendre vers une synergie totale. Des pays hors Union européenne mettent également l'accent sur leur intérêt national. C'est ainsi que la Chine tente de développer elle-même toutes les composantes de la chaîne informatique, afin d'éviter d'être dépendante des États-Unis et de l'Union européenne.

La cause profonde de l'insécurité des systèmes TIC est de nature économique: dans le monde TIC, la part de marché est plus importante que la sécurité. Le succès dans le domaine informatique nécessite une adoption quasi universelle du produit, ce qui fait que les producteurs misent prioritairement sur une conquête rapide du marché et moins sur la sécurité. On constate en outre que l'utilisateur n'est pas prêt à payer pour la protection de la vie privée et n'est pas en mesure de distinguer les produits sûrs des produits non sûrs. Même lorsqu'un système TIC s'est établi sur le marché, le souci de la sécurité reste trop limité, dès lors que l'entité qui devrait faire les investissements n'est pas, dans de nombreux cas, la (principale) victime d'un manque de sécurisation. C'est ainsi que les ordinateurs qui font partie d'un botnet ne sont généralement pas touchés eux-mêmes.

Le problème des spams ne peut être résolu que de deux manières: en améliorant l'authentification et en augmentant le prix de l'envoi d'un courriel, ce qui nécessite une collaboration et une coordination optimales au niveau international. Le facteur humain reste le maillon faible: étant donné que les consommateurs n'ont pratiquement aucune idée du mode de fonctionnement d'Internet et accordent leur préférence aux systèmes conviviaux, qui sont souvent moins sûrs, ils n'encouragent pas les investissements dans la sécurité.

Les conséquences et les mécanismes de réaction sont différents pour l'industrie, les individus et les pouvoirs publics:

– Les entreprises sont victimes de la perte de données à caractère personnel, d'espionnage industriel, de chantage, de l'indisponibilité de leur site Internet, d'atteinte à leur réputation et d'opportunités manquées. Les grandes entreprises ont déjà acquis une certaine expérience de la gestion des risques, les petites entreprises sont plus vulnérables.

– Les citoyens voient la protection de la vie privée se réduire, du fait qu'ils sont engagés dans un combat inégal avec la technologie et le milieu des affaires: les données à caractère personnel sont de plus en plus disponibles; le coût du stockage et du traitement des données diminue;

kan een gericht marketingbeleid worden gevoerd en kan aan prijsdiscriminatie worden gedaan. Consumenten zijn ook kwetsbaar voor fraude en hebben een gefundeerd gevoel van onveiligheid.

– De overheid heeft de opdracht om de privacy en het vermogen van de burger te beschermen en de overheidssystemen (onder meer *e-government*diensten) en de kritische infrastructuur te beveiligen. Ook moet zij adequate regulering voor de complexe ICT-omgeving creëren.

ICT-onveiligheid dient te worden aangepakt door in te werken op processen, mensen en technologie. Elke benadering start met preventie, wordt gevolgd door detectie en moet ten slotte aanleiding geven tot respons.

Op het vlak van opleiding moet langs drie sporen worden gewerkt:

– ICT-veiligheid moet een onderwerp in het algemeen onderwijs worden.
– Elk personeelslid in de ICT-sector moet 60 tot 120 uur vorming in informatiebeveiliging krijgen.

– Een ICT-beveiligingscoördinator dient een opleiding van 240 tot 280 uur te volgen.

Het onderzoek in België staat op zeer hoog niveau, maar wordt niet optimaal geabsorbeerd door industrie en overheid.

De aanpak van ICT-onveiligheid in België behoeft verbetering:

– Om optimaal gebruik te maken van beschikbare expertise in overheid, universiteiten en industrie, moet de coördinatie worden versterkt. Dit kan resulteren in *baseline*documenten voor cryptografische algoritmen, netwerkbeveiliging, beveiliging van gegevensbanken, biometrie en organisatorische maatregelen. ook inzake opleiding is stroomlijning nodig.

– De versnippering dient te worden teruggeschroefd, al zou volledige machtsconcentratie ook geen goede zaak zijn.

– Nieuwe structuren mogen niet met elkaar in concurrentie gaan voor de schaarse mensen en middelen, wat onder meer de aanwijzing vereist van een «*chief risk officer*» van de overheid, die door het parlement kan worden gecontroleerd.
– De opstelling van een nationaal ICT-beveiligingsplan, dat ook de kritische infrastructuur omvat, is nodig.

l'analyse du comportement des consommateurs permet aux entreprises de mener une politique de marketing ciblée et de faire de la discrimination par les prix. Les consommateurs sont également exposés à la fraude et ont un sentiment d'insécurité fondé.
– Les autorités ont pour mission de protéger la vie privée et le patrimoine du citoyen ainsi que de sécuriser les systèmes des services publics (notamment l'*e-government*) et l'infrastructure critique. Elles doivent également créer la régulation adéquate pour le complexe environnement des TIC.

Il faut combattre l'insécurité des TIC en agissant sur les processus, les gens et la technologie. Toute approche débute par la prévention, continue par la détection et doit enfin donner lieu à une réaction.

Il convient de mener une triple action au niveau de la formation:

– La sécurité des TIC doit être abordée dans l'enseignement général.
– Tout membre du personnel occupé dans le secteur des TIC doit recevoir 60 à 120 heures de formation à la sécurisation de l'information.
– Le coordinateur de la sécurisation des TIC doit suivre une formation de 240 à 280 heures.

La recherche en Belgique est d'un très haut niveau, mais elle n'est pas utilisée de manière optimale par l'industrie et les autorités.

Il faut améliorer la lutte contre l'insécurité dans le domaine des TIC en Belgique:

– Il convient de renforcer la coordination en vue d'exploiter au maximum l'expertise disponible dans le secteur public, les universités et l'industrie, ce qui peut déboucher sur l'établissement de documents de base pour des algorithmes cryptographiques, la sécurisation des réseaux, la sécurisation des banques de données, la biométrie et des mesures organisationnelles. Une rationalisation est également nécessaire en matière de formation.
– Il faut diminuer la dispersion, même si une concentration totale des pouvoirs ne serait pas non plus une bonne chose.

– Les nouvelles structures ne peuvent se faire concurrence pour attirer les rares moyens et personnels disponibles, ce qui requiert notamment la désignation d'un «*chief risk officer*» des autorités, sur lequel le parlement peut exercer un contrôle.
– Il est nécessaire d'établir un plan national de sécurisation des TIC qui englobe également l'infrastructure critique.

– Er moet een samenwerkingsverband worden opgezet voor de evaluatie en certificatie van producten, procedures en expertises voor overheid en industrie.

– Er dient werk te worden gemaakt van certificatie, meer bepaald de toetsing van ICT-systemen in overheid en industrie aan sectorspecifieke criteria voor veiligheid en privacy.

– Voor alle veiligheidsfenomenen is er nood aan procedures voor respons op korte termijn.

– De internationale vertegenwoordiging en samenwerking moet worden verstevigd.

– Open standaarden verdienen ondersteuning omdat ze de veiligheid bevorderen.

– De aansprakelijkheid van softwareproducenten moet geleidelijk worden verhoogd op een manier die de innovatie en het initiatief niet fnuikt.

– Inzake bescherming van het privéleven dient de opslag van data te worden beperkt.

De spreker besluit met een analyse van de verhouding tussen de bescherming van het privéleven, beveiliging en de respectieve belangen van overheid, industrie en burgers.

Elke nieuwe technologie maakt het eenvoudiger en goedkoper om de privacy van mensen aan te tasten. Vaak worden veiligheid en privacy voorgesteld als communicerende vaten: een toename van de veiligheid zou afbreuk doen aan privacy en omgekeerd. Deze voorstellingswijze is foutief: de massale opslag van gegevens over personen leidt zelf tot een vermindering van de veiligheid, met name als de gegevens in verkeerde handen terechtkomen, geen enkel databestand is immers volledig veilig.

De spreker kant zich daarom tegen de ontwerprichtlijn met betrekking tot dataretentie, op grond waarvan gegevens zes maanden tot twee jaar zouden moeten worden bewaard: de risico's die dergelijke maatregel zou veroorzaken, zouden groter zijn dan de vooruitgang in de strijd tegen criminaliteit en terrorisme die er mogelijk uit zou voortvloeien. De huidige wetgeving is niet effectief: het strekt tot aanbeveling dat adequate beveiliging wordt opgelegd en geverifieerd (certifiëring), dat een meldingsplicht met betrekking tot het verlies van persoonsgegevens wordt ingevoerd en dat privacybevorderende technologieën worden ontwikkeld en gebruikt.

4. Vragen en opmerkingen van de leden

A. Vragen aan de heer Dieter Verhaeghe

De heer Guido De Padt (Open Vld) vraagt welke wetgevende initiatieven kunnen worden genomen om de geschetste problemen beter te kunnen aanpakken.

– Il faut établir un accord de collaboration pour l'évaluation et la certification des produits, procédures et expertises pour les autorités et l'industrie.

– Il faut mettre en oeuvre la certification, plus particulièrement vérifier que les systèmes TIC dans les secteurs public et de l'industrie remplissent les critères de sécurité et de vie privée qui leur sont spécifiques.

– On a besoin de procédures permettant de réagir à court terme pour tous les phénomènes de sécurité.

– Il convient de renforcer la représentation et la coopération internationales.

– Il faut soutenir les standards ouverts parce qu'ils favorisent la sécurité.

– Il faut progressivement accroître la responsabilité des producteurs de logiciels d'une manière qui ne freine pas l'innovation et l'initiative.

– En ce qui concerne la protection de la vie privée, il convient de limiter le stockage de données.

L'orateur conclut par une analyse de la relation entre la protection de la vie privée, la sécurisation et les intérêts respectifs du secteur public, de l'industrie et des citoyens.

Chaque nouvelle technologie rend plus simples et moins onéreuses les atteintes à la vie privée des gens. On présente souvent la sécurité et la vie privée comme des vases communicants: un renforcement de la sécurité porterait atteinte à la vie privée et inversement. Cette vision est erronée: le stockage massif de données relatives aux personnes entraîne même une diminution de la sécurité, notamment lorsque les données aboutissent dans de mauvaises mains. Aucune base de données n'est en effet complètement sûre.

L'orateur s'élève dès lors contre le projet de directive sur la rétention des données, en vertu duquel les données devraient être conservées de six mois à deux ans: les risques que ferait courir pareille mesure seraient plus grands que les progrès qui pourraient en découler dans la lutte contre la criminalité et le terrorisme. La législation actuelle n'est pas efficace: il se recommande d'imposer et de vérifier (certification) une sécurisation adéquate, d'instaurer une obligation de notification en cas de perte de données personnelles et de développer et d'utiliser des technologies favorisant la protection de la vie privée.

4. Questions et observations des membres

A. Questions à M. Dieter Verhaeghe

M. Guido De Padt (Open Vld) demande quelles initiatives législatives peuvent être prises afin de s'attaquer plus efficacement aux problèmes décrits.

De heer Philippe Henry (Ecolo-Groen!) vraagt welke wetgevende of technische maatregelen ter zake in andere landen worden genomen. Is de privacywetgeving niet dermate dwingend dat ze uiteindelijk niet heel erg gerespecteerd wordt? Moet niet naar een nieuw evenwicht worden gezocht tussen de regelgeving en de werkelijkheid?

De heer Jef Van den Bergh (CD&V – N-VA) wenst te vernemen of de Privacycommissie over voldoende personeel beschikt om de nieuwste tendezen inzake schending van de privacy aan te kunnen. Als bedrijven persoonlijke gegevens verliezen, bestaat dan geen aangifteverplichting ten aanzien van de personen waarvan de gevens zijn verlorengegaan? Hoe is deze problematiek in België geregeld? Wat zijn de gevolgen als het verlies niet wordt gemeld?

De heer François Bellot (MR), voorzitter, kaart verschillende problemen aan. De eerste soort heeft te maken met gegevens aangaande de burgers die door de overheid of door de federale overheidsdiensten worden bewaard. Welke reglementaire en technische instrumenten staan de Privacycommissie ter beschikking om de ongewenste en ongeoorloofde verspreiding van deze gegevens tegen te gaan? De tweede soort heeft te maken met de licenties van internetfirma's als Google en Adobe: met één klik verklaart men zich akkoord de gegevens die men meedeelt te gebruiken in het raam van commerciële marketing en profilering. Zijn dergelijke clausules wel toelaatbaar? Kunnen de betrokkenen hun akkoord op een of andere manier intrekken? De derde soort heeft te maken met een veroordeling, in Nederland, van een bedrijf dat persoonlijke gegevens doorstuurde naar zo'n 13.000 bedrijven om profilering van de internetgebruiker toe te laten. Ten vierde blijkt dat de in Boston gevestigde firma Blackberry om het even welk toestel kan intercepteren. Dit zou zelfs gebeurd zijn in diplomatieke aangelegenheden. Wat kan hiertegen worden gedaan? Ten slotte is de voorzitter ter ore gekomen dat alle aanbiedingen op e-Bay worden geanalyseerd om criminaliteit tegen te gaan. Verdient het geen aanbeveling eenieder die een website zoals e-Bay exploiteert, een charter te laten ondertekenen teneinde de gebruiker tegen malafide praktijken te beschermen? Gebeurt dit best op Europees of op mondiaal vlak?

B. Vragen aan de heer Rudi Vansnick

De heer François Bellot (MR), voorzitter, vraagt of men een concentratie van de computercriminaliteit in bepaalde landen constateert.

M. Philippe Henry (Ecolo-Groen!) demande quelles mesures législatives ou techniques sont prises en la matière dans d'autres pays. La législation sur la vie privée n'est-elle pas à ce point contraignante qu'elle n'est, en fin de compte, pas très respectée? Ne faudrait-il pas chercher un nouvel équilibre entre la réglementation et la réalité?

M. Jef Van den Bergh (CD&V – N-VA) souhaiterait savoir si la commission de la protection de la vie privée dispose de suffisamment de personnel pour faire face aux nouvelles tendances en matière de violation de la sphère privée. Si les entreprises perdent des données personnelles, n'y a-t-il pas d'obligation de déclaration vis-à-vis des personnes dont les données ont été perdues? Comment cette problématique est-elle réglée en Belgique? Quelles sont les conséquences lorsque la perte n'est pas signalée?

M. François Bellot (MR), président, aborde différents problèmes. Le premier type de problèmes a trait aux données relatives aux citoyens qui sont conservées par les autorités ou par les services publics fédéraux. Quels sont les instruments réglementaires et techniques à la disposition de la Commission de la protection de la vie privée pour lutter contre la divulgation indésirée et illicite de ces données? Le deuxième type de problèmes concerne les licences des firmes liées à l'internet comme Google et Adobe: par un seul clic, on déclare marquer son accord pour que les données que l'on communique soient utilisées dans un cadre de marketing et de profilage commercial. De telles clauses sont-elles admissibles? Les intéressés peuvent-ils retirer leur accord d'une manière ou d'une autre? Le troisième type de problèmes a trait à une condamnation, aux Pays-Bas, d'une entreprise qui avait transmis des données personnelles à près de 13.000 entreprises pour permettre de profiler les utilisateurs de l'internet. Quatrièmement, il s'avère que la firme Blackberry établie à Boston peut intercepter n'importe quel appareil. Cela aurait même eu lieu dans le cadre d'affaires diplomatiques. Que peut-on faire pour lutter contre cela? Enfin, le président a appris que toutes les offres sur e-Bay sont analysées afin de lutter contre la criminalité. Ne serait-il pas recommandé de faire signer une charte par toute personne qui exploite un site comme e-Bay, afin de protéger le consommateur contre les pratiques malhonnêtes? Ne serait-il pas préférable que cela se fasse au niveau mondial ou européen?

B. Questions à M. Rudi Vansnick

M. François Bellot (MR), président, demande si l'on observe une concentration de la cybercriminalité dans certains pays.

De heer Guido De Padt (Open Vld) wenst te vernemen of de kans op diefstal via banken zeer reëel is.

De heer Jan Mortelmans (VB) vraagt welke kwaliteitsnormen aan een bepaald label verbonden zijn. Hoe kan tegen gokken via het internet worden opgetreden?

C. Vragen aan de heer Bart Preneel

De heer Guido De Padt (Open Vld) brengt in herinnering dat op de telecommunicatieoperatoren ingevolge de wet van 13 juni 2005 betreffende de elektronische communicatie de verplichting rust om data op hun netwerk gedurende zes maanden te bewaren. Wordt deze verplichting het best weer opgeheven?

5. Antwoorden van de genodigde sprekers

A. Antwoorden van de heer Dieter Verhaeghe

a.1 Buitenlandse voorbeelden

Een aantal zaken, zoals vertrouwelijkheid en veiligheidscertificering, wordt het best op nationaal vlak geregeld. Wanneer evenwel het vrij verkeer van goederen en diensten in het geding is, is men praktisch op Europese regelgeving aangewezen. In de Angelsaksische wereld gaat ook aandacht naar slachtofferhulp.

a.2 Actieterrein

De Privacycommissie treedt op tegen directe marketing. Hiervoor heeft het een aantal reglementaie bepalingen en technische hulpmiddelen ter beschikking. Tegen criminele activiteiten kan de Privacycommissie minder beginnen, vermits de FCCU hiervoor instaat.

a.3 Personeel

Er wordt online veel informatie uitgewisseld via het CNSA («*Contact Network of Spam enforcement Authorities*»). Anti-spamautoriteiten in dertien Europese landen werken samen in de strijd tegen spam. De autoriteiten wisselen informatie en ingediende klachten uit over spammers om zo over landsgrenzen heen te kunnen optreden. De CNSA faciliteert het delen van informatie en van best practices op het gebied van anti-spamwetten tussen nationale autoriteiten van de lidstaten van de Europese Unie en de Europese Economische Ruimte. Dit stelt de Privacycommissie in staat de nieuwste tendenzen op de voet te volgen.

a.4 Verlies data

Er bestaan geen exacte statistieken over identiteitsdiefstal. Op basis van de klachten die de Commissie jaarlijks ontvangt met betrekking tot registraties op het gebied van consumentenkrediet bestaat het ver-

M. Guido De Padt (Open Vld) demande si le risque de vol par le biais des banques est bien réel.

M. Jan Mortelmans (Vlaams Belang) s'enquiert des normes de qualité auxquelles un label donné est lié. Que faire contre les paris en ligne?

C. Questions à M. Bart Preneel

M. Guido De Padt (Open Vld) rappelle qu'en vertu de la loi du 13 juin 2005 relative aux communications électroniques, les opérateurs de télécommunications sont tenus de conserver les données sur leur réseau durant six mois. Serait-il préférable de lever de nouveau cette obligation?

5. Réponses des orateurs invités

A. Réponses de M. Dieter Verhaeghe

a.1 Exemples à l'étranger

Il vaut mieux régler un certain nombre de questions, comme la confidentialité et la certification en matière de sécurité, au niveau national. Néanmoins, lorsque la libre circulation des marchandises et des services est en jeu, concrètement, on en est réduit à appliquer la réglementation européenne. Dans le monde anglo-saxon, l'aide aux victimes est également prise en compte.

a.2 Terrain d'action

La Commission de la vie privée sévit contre le marketing direct. Elle dispose pour ce faire d'un certain nombre de dispositions réglementaires et de moyens techniques. Elle peut prendre moins d'initiatives contre les activités criminelles, étant donné que celles-ci sont du ressort de la FCCU.

a.3 Personnel

Beaucoup d'informations sont échangées en ligne via le CNSA («*Contact Network of Spam enforcement Authorities*»). Les autorités «anti-spam» coopèrent dans treize pays européens dans le cadre de la lutte contre le spam. Les autorités échangent des informations et les plaintes déposées relatives aux spammers pour pouvoir agir de façon transfrontalière. Le CNSA facilite le partage des informations et des exemples à suivre en matière de législation anti-spam entre les autorités nationales des États membres de l'Union européenne et l'Espace économique européen. Cela permet à la Commission de la vie privée de suivre de près les dernières tendances.

a.4 Perte de données

Il n'existe pas de statistiques précises relatives au vol d'identité. Sur la base des plaintes que la Commission reçoit chaque année, en ce qui concerne les enregistrements en matière de crédit à la consommation, l'on

moeden dat er sprake is van een tiental gevallen van identiteitsdiefstal per jaar. Meer onderrzoek lijkt echter aangewezen. Zo zou kunnen worden nagegaan of bij de registratie in de Centrale door kredieten aan particulieren bij de Nationale Bank kan worden rekening gehouden met het feit dat de registratie wordt betwist wegens identiteitsdiefstal.

a.5 Licentievoorwaarden

Op dit ogenblik worden de licentievoorwaarden van bekende internetfirma's niet geanalyseerd. Dit fenomeen is grensoverschrijdend. Er zijn reeds pogingen geweest om dit Europees te regelen, maar daar is het ook bij gebleven.

a.6 Diefstal data

De diefstal van gegevens is een groot probleem. Privébedrijven doen er evenwel om redenen van imago zeer geheimzinnig over zodat weinig gevallen in de openbaarheid worden gebracht.

a.7 Misbruik Blackberry

Het Europees Parlement heeft haar bezorgdheid over de mogelijkheid van spionage reeds geuit in de zaak «Swift». Dit probleem moet politiek worden besproken. Technisch gesproken kan men zijn toevlucht nemen tot alternatieven om spionage via de Blackberry te vermijden. In het dossier «Swift» (behandeld door de Privacycommissie in 2006, het ging over de mededeling van financiële gegevens aan de VS-autoriteiten door de n België gevestige firma Swift) zijn elementen van dit misbruik aan het licht gekomen.

B. Antwoorden van de heer Rudi Vansnick

b.1 Toekenning dommeinnaam

Er is te weinig controle op en bij de toekenning van een domeinnaam. De identiteit wordt niet gecheckt. In Frankrijk moet men een fysiek adres bezitten. In Nederland en België – voor respectievelijk een domeinnaam gevolgd door .nl of .be – is zelfs deze voorwaarde niet vereist. In België gaat men er prat op tot voor kort een miljoen domeinnamen te hebben geregistreerd, aantal dat intussen met een vierde is verminderd. De huidige wetgeving kan niets verbieden ter zake. De domeinnaam «.eu» is weliswaar strenger, maar wordt met een soortgelijke procedure toegekend.

b.2 Betrouwbaarheid labels

Labels werden in het leven geroepen om vertrouwen te schenken. Jammer genoeg garanderen ze niets. Een label kan verkregen worden door lid te worden van de organisatie die het label verstrekt. Er is geen regelgeving ter zake. Sommige bekende labels – zoals Visa – ontberen zelfs snelle controle, zodat malafide operaties toch doorgang kunnen vinden zonder dat de consument enig

suppose qu'il est question d'une dizaine de cas de vol d'identité par an. Toutefois, il semble nécessaire d'approfondir l'examen. Cela permettrait de vérifier si, lors de l'enregistrement auprès de la Centrale des crédits aux particuliers de la Banque nationale, il est possible de tenir compte de la contestation de l'enregistrement pour cause de vol de données.

a.5 Conditions de licence

Pour l'instant, les conditions de licence d'entreprises Internet connues ne sont pas analysées. Ce phénomène est transfrontalier. Bien que l'on ait essayé de régler cette matière au niveau européen, les choses en sont restées là.

a.6 Vol de données

Le vol de données constitue un gros problème. Pour préserver leur image de marque, les entreprises privées sont extrêmement discrètes à ce sujet, de sorte que peu de cas sont rendus publics.

a.7 Abus Blackberry

Dans le cadre de l'affaire «Swift», le Parlement européen a déjà exprimé son inquiétude quant à un éventuel espionnage. Ce problème doit être abordé au niveau politique. D'un point de vue technique, on peut recourir à des alternatives pour éviter tout espionnage via le Blackberry. Dans le dossier Swift (examiné par la Commission de la protection de la vie privée en 2006, et qui portait sur la communication de données financières aux autorités américaines par la société Swift établie en Belgique), des éléments de cet abus sont apparus.

B. Réponses de M. Rudi Vansnick

b.1 Attribution de noms de domaine

Un contrôle insuffisant est exercé sur et lors de l'attribution d'un nom de domaine. L'identité n'est pas vérifiée. En France, il faut posséder une adresse physique. Aux Pays-Bas et en Belgique, cette condition n'est même pas requise pour obtenir un nom de domaine suivie respectivement de .nl ou de .be. En Belgique, on se targuait, jusqu'il y a peu, d'avoir enregistré un million de noms de domaine, mais ce nombre a été réduit d'un quart entre temps. La législation actuelle ne peut rien interdire en la matière. Le nom de domaine «eu» est certes plus strict, mais est attribué par une procédure analogue.

b.2 Fiabilité des labels

Les labels ont été créés pour inspirer confiance. Hélas, ils ne garantissent rien. On peut obtenir un label en s'affiliant à l'organisation qui délivre celui-ci. Il n'y a aucune réglementation en la matière. Certains labels connus, comme Visa, ne sont même pas soumis à un contrôle rapide, de sorte que des opérations malhonnêtes peuvent avoir lieu sans le moindre recours pour le

verhaal heeft. Het internetbankieren verloopt in België relatief veilig.

b.3 Gokken op het internet

Gokken is verboden zonder licentie. Er werd ter zake in België geen enkele licentie aangevraagd. Dit hoeft ook niet te verwonderen vermits de bezitter van de betrokken site vaak in het buitenland is gevestigd.

C. Antwoorden van professor Bart Preneel

In essentie is de vraag van de heer Guido De Padt een politieke vraag, waar geen eenduidig en objectief antwoord op bestaat. Persoonlijk is hij geen voorstander van zulke verplichting wegens de ermee verbonden risico's en omdat ze niet noodzakelijk is om de strijd tegen terrorisme aan te gaan. Indien de overheid niettemin voor verplichte dataretentie opteert, moet ze de operatoren er tegelijkertijd toe dwingen om die gegevens op afdoende wijze te beveiligen. Dit vloeit al voort uit regelgeving, maar de naleving ervan wordt niet of onvoldoende afgedwongen. Ook zijn dan maatregelen nodig om ervoor te zorgen dat databestanden niet op oneigenlijke wijze worden gebruikt door de instanties die ze kunnen raadplegen.

III. — **HOORZITTING VAN 30 JANUARI 2008**

1. Uiteenzetting van de heer Rudi Smit, vertegenwoordiger van de Raad van het BIPT (Belgisch Instituut voor Postdiensten en Telecommunicatie)

De heer Rudi Smit stipt aan dat de opdrachten van het BIPT inzake netwerkbeveiliging worden bepaald in de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector en in de wet van 13 juni 2005 betreffende de elektronische communicatie:

– bijdragen tot de bescherming van gegevens die tot de persoonlijke levenssfeer behoren;
– toezien op de integriteit en veiligheid van publieke netwerken;
– coördineren van veiligheidsinitiatieven;
– uitwerken van maatregelen die in geval van crisis moeten worden genomen;
– bepalen van criteria waaraan materiaal dat voor elektronische communicatie wordt gebruikt, moet voldoen;
– vaststellen van normen voor dienstkwaliteit en veiligheid van netwerken en diensten;
– toezien op de naleving van de nog vigerende bepalingen van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

consommateur. Les opérations bancaires effectuées sur Internet sont relativement sûres en Belgique.

b.3 Parier sur Internet

Il est interdit de parier sans licence. Aucune licence n'a été demandée à cet effet en Belgique. Cela ne doit pas étonner étant donné que le propriétaire du site concerné est souvent établi à l'étranger.

C. Réponses du professeur Bart Preneel

La question de M. Guido De Padt est essentiellement politique et n'a pas de réponse claire et objective. Personnellement, l'orateur n'est pas favorable à une telle obligation en raison des risques qu'elle implique et parce qu'elle n'est pas indispensable pour lutter contre le terrorisme. Si les autorités optent néanmoins pour la rétention obligatoire de données, elles doivent dans le même temps contraindre les opérateurs à sécuriser suffisamment celles-ci. C'est déjà ce que prévoit la réglementation, mais le contrôle de son respect fait défaut ou est insuffisant. De même, il faut alors prendre des mesures pour éviter que les fichiers de données soient utilisés de manière inappropriée par les instances qui peuvent les consulter.

III. — **AUDITION DU 30 JANVIER 2008**

1. Exposé de M. Rudi Smit, représentant du Conseil de l'IBPT (Institut belge des Services postaux et des Télécommunications)

M. Rudi Smit souligne que les missions de l'IBPT en matière de sécurisation de réseau sont définies dans la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges et dans la loi du 13 juin 2005 relative aux communications électroniques:

– contribuer à assurer la protection des données à caractère personnel et de la vie privée;
– veiller à l'intégrité et la sécurité des réseaux publics;
– coordonner les initiatives relatives à la sécurité;
– élaborer les mesures à prendre en cas de crise;

– fixer les critères auxquels doit répondre le matériel utilisé pour les communications électroniques;

– fixer des normes en matière de qualité du service et de sécurité des réseaux et des services;
– veiller au respect des dispositions encore en vigueur de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;

– samenwerken met de Gemengde Commissie Telecommunicatie.

Beveiliging dient op verschillende niveaus te worden uitgewerkt:

– op het vlak van de fysieke infrastructuur;
– in organisatorisch en procedureel opzicht;
– inzake de continuïteit van de werking (zowel in normale omstandigheden als in geval van crisis);
– met betrekking tot de bescherming van de eindgebruiker;
– op het domein van de behoeften die van openbare orde zijn (wettelijke onderschepping, het verhinderen van illegale activiteiten).

De evolutie van het landschap van elektronische communicatie in België is zeer groot geweest: na een monopoliesituatie (met de vroegere RTT als enige operator) verscheen in 1996 een tweede operator op de markt, waarna de sector van de elektronische communicatie in 1998 werd geliberaliseerd. Die vrijmaking heeft aanleiding gegeven tot een exponentiële toename van actoren, technologieën, diensten en interacties.

De spreker haalt een Belgisch initiatief ter bevordering van ICT-veiligheid uit het verleden aan: het Belgisch Agentschap Informatieveiligheid voerde in de periode 2002-2003 voor het College Inlichting en Veiligheid een haalbaarheidsstudie uit. Bij de voorstelling van het eindverslag van het Agentschap op 24 maart 2003 werd op vraag van het BIPT voorgesteld om over te gaan tot de oprichting van een gouvernementele *Computer Security Incident Response Team* (CSIRT). Concrete maatregelen volgden er echter niet, enerzijds als gevolg van de moeilijke budgettaire situatie, anderzijds omdat het plan bestond om het ondertussen opgerichte Europees Agentschap voor Informatieveiligheid (ENISA) de opdrachten van de bevoegde nationale instanties te laten overnemen. Dat plan lukte in de praktijk echter niet door een te beperkte omkadering: ENISA beschikt slechts over twintig experten, zodat de uitwerking van een effectief veiligheidsbeleid op EU-niveau vooralsnog geen haalbare kaart is.

Een ander initiatief van het BIPT werd wel geïmplementeerd: sinds 2000 is in zijn schoot een *e-Security*team met meldpunt actief, dat 24 uur per dag en 7 dagen per week bereikbaar is voor waarschuwingen met betrekking tot schadelijke virussen. Dat team heeft goed werk geleverd, maar zijn werking is thans voorbijgestreefd door de technische evolutie: grootschalige aanvallen, zoals met het «*I love you*»-virus, komen niet meer voor, terwijl professionele, complexe en doelgerichte aanvallen met een voornamelijk crimineel motief in de plaats zijn gekomen. Door het ontbreken van knowhow,

– collaborer avec la Commission mixte des télécommunications;.

La sécurisation doit être menée sur plusieurs fronts:

– au niveau de l'infrastructure physique;
– dans une optique organisationnelle et procédurale;
– en matière de continuité du fonctionnement (tant dans conditions normales qu'en cas de crise);
– en ce qui concerne la protection de l'utilisateur final;
– dans le domaine des besoins qui relèvent de l'ordre public (interception légale, prévention d'activités illégales).

Le paysage des communications électroniques a connu une évolution sensible en Belgique: après une situation de monopole (l'ancienne RTT étant alors le seul opérateur), un deuxième opérateur est apparu sur le marché en 1996, le secteur des communications électroniques ayant été libéralisé en 1998. Cette libéralisation a conduit à une croissance exponentielle du nombre d'acteurs, de technologies, de services et d'interactions.

L'orateur évoque une initiative belge passée visant à promouvoir la sécurité TIC: au cours des années 2002-2003, l'Agence belge pour la sécurité de l'information a réalisé une étude de faisabilité pour le Collège du renseignement et de la sécurité. Lors de la présentation du rapport final de l'Agence, le 24 mars 2003, il a été proposé, à la demande de l'IBPT, de créer une *Computer Security Incident Response Team* (CSIRT) gouvernementale. Cela n'a toutefois pas été suivi de mesures concrètes, d'une part en raison des difficultés budgétaires et, d'autre part, parce qu'il était prévu de confier les missions des instances nationales compétentes à l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), instituée dans l'intervalle. Dans la pratique, ce plan n'a toutefois pas abouti en raison d'un manque d'encadrement: l'ENISA ne dispose que de vingt experts, de sorte que, pour l'instant, il n'est pas possible de développer une politique de sécurité effective au niveau européen.

Une autre initiative de l'IBPT a en revanche été mise en œuvre: depuis 2000, il existe en son sein un groupe *e-security* avec un point de contact accessible 24 heures sur 24 et 7 jours sur 7 pour les alertes concernant des virus nuisibles. Ce groupe a bien travaillé, mais son fonctionnement est à présent dépassé en raison de l'évolution technique: les attaques à grande échelle, du type du virus «*I love you*», ne se produisent plus et ont cédé la place à des attaques professionnelles, complexes et ciblées à des fins essentiellement criminelles. Du fait du manque de savoir-faire, de formation et de serveurs

opleiding en beveiligde servers en communicatiekanalen werd het BIPT als waarnemer geweigerd in de *European Governmental* CERT (*Computer Emergency Response Team*) *Group*, een EU-netwerk van overheidsinstanties die aan ICT-veiligheid werken.

In de nabije toekomst zal de EU nieuwe verplichtingen aan de lidstaten opleggen:

– De kritieke infrastructuur behoeft meer bescherming. In België is er eerst nood aan de definiëring van de infrastructuur voor elektronische communicatie die als kritiek moet worden beschouwd. Vervolgens dienen plannen te worden opgesteld door de FOD Economie of het BIPT (welke instantie hiervoor bevoegd wordt, is nog niet beslist). Voor het crisiscentrum van de regering is telecommunicatie tot dusver geen prioriteit.

– Bij de elektronische uitwisseling van informatie tussen de EU en de lidstaten zullen garanties moeten bestaan op het vlak van de beveiliging van de informatie (InfoSec-verordening).

Het regelgevingskader voor elektronische communicatie zal tegen eind 2009 of begin 2010 worden herzien, voornamelijk op drie vlakken:

– Er komt een herziening van de richtlijn met betrekking tot de veiligheid van netwerken en diensten, op grond waarvan veiligheidsincidenten door operatoren verplicht moeten worden gerapporteerd en de lidstaten ter zake een belangrijke controleopdracht krijgen.

– De verhouding tussen privacy en elektronische communicatie krijgt andere contouren: voortaan zal de behandeling van gegevens veilig moeten verlopen en zal de uitvoering van en de controle op de betrokken regelgeving strikter moeten gebeuren.

– Inzake universeledienstverlening komt «beschikbaarheid van diensten» in de plaats van «integriteit van het netwerk».

ENISA werkt momenteel aan het opstarten van een Europees Informatie- en Alarmeringssysteem (EISAS), dat eind 2008 operationeel zou moeten zijn. België heeft nood aan een nationaal contactpunt met voldoende knowhow en technische capaciteit dat aan dat systeem zijn medewerking kan verlenen.

De *European Governmental CERT Group* omvat thans zeven EU-landen (België is daar niet bij) en twee staten van de Europese Vrijhandelssassociatie, maar zou idealiter tot alle EU-lidstaten moeten worden uitgebreid.

De spreker evalueert de huidige capaciteit van het BIPT inzake netwerkbeveiliging: voor controle van de netwerken, informatievergaring en netwerkbeveiliging beschikt de instelling over een zeer beperkt personeels-

sécurisés et de canaux de communication, l'IBPT a été refusé en tant qu'observateur au sein du *European Governmental CERT* (*Computer Emergency Response Team*) *Group*, un réseau européen d'instances publiques travaillant sur la sécurité TIC.

L'Union européenne imposera prochainement de nouvelles obligations aux États membres:

– L'infrastructure critique doit être mieux protégée. En Belgique, il convient d'abord de définir l'infrastructure de communication électronique devant être considérée comme critique. Ensuite, le SFP Économie ou l'IBPT (il n'a pas encore été décidé quelle sera l'instance compétente en la matière) devra élaborer des plans. Jusqu'à présent, les télécommunications ne constituent pas une priorité pour le centre de crise gouvernemental.

– Lors de l'échange électronique d'informations entre l'UE et les États membres, des garanties devront être fournies en matière de protection des informations (règlement InfoSec).

Le cadre réglementaire relatif aux communications électroniques sera revu d'ici fin 2009, voire début 2010, dans trois domaines principalement:

– La directive relative à la sécurité des réseaux et des services fera l'objet d'une révision en vertu de laquelle les opérateurs devront faire rapport sur les incidents en matière de sécurité et les États membres seront investis d'une mission de contrôle importante à cet égard.

– Le lien entre la vie privée et les communications électroniques sera conçu différemment: désormais, le traitement des données devra être sécurisé et il conviendra d'être plus rigoureux lors de la mise en oeuvre de la réglementation en la matière ainsi que du contrôle de son respect.

– En matière de service universel, «la disponibilité des services» remplace «l'intégrité du réseau».

ENISA s'attelle pour l'instant au lancement d'un système européen d'information et d'alerte (EISAS), qui devrait être opérationnel fin 2008. La Belgique a besoin d'un point de contact national qui dispose de suffisamment de savoir-faire et de capacités techniques pour pouvoir coopérer avec ce système.

Le *European Governmental CERT Group* comprend actuellement sept États européens (la Belgique n'en fait pas partie) et deux États de l'Association européenne de libre-échange, mais il devrait idéalement être étendu à tous les États membres de l'Union européenne.

L'orateur évalue la capacité actuelle de l'IBPT en matière de sécurisation de réseaux: pour le contrôle des réseaux, la collecte d'informations et la sécurisation de réseaux, l'institution dispose de très peu d'effectifs,

bestand, waardoor ze haar opdrachten niet ten volle kan vervullen. Om een gouvernementele CSIRT te kunnen opstarten, is er nood aan een versterking van de technische ploeg van het BIPT, een belangrijke inspanning voor opleiding en een groter budget voor de aankoop van materiaal. Daarnaast heeft het BIPT nog andere, meer klassieke taken: het opstellen van technische regels en voorschriften voor een bescherming van de kritische infrastructuur, de verlening van medewerking aan de Gemengde Commissie Telecommunicatie en nationale crisisplanning. Ook de controle op de toepassing van die regels en voorschriften behoort tot zijn opdrachten.

2. Uiteenzetting van mevrouw Cécile Coppin, verantwoordelijke van de dienst «Internetbewaking» van de Algemene Directie Controle en Bemiddeling van de Federale Overheidsdienst Economie

Internet is een machtig medium. Aldus hoeft het niet te verbazen dat het door professionelen wordt misbruikt. Ingeval geen economische inbreuk wordt geconstateerd of de verkoper te goeder trouw is, kan de overheidsdienst alternatieve geschillenbeslechting bevorderen. Maar hij kan ook als economische politie repressief optreden. Daartoe beschikt de dienst over 200 beëdigde enquêteurs, verdeeld over zeven regionale directies, drie secties naargelang van de te handhaven reglementering. Op de hoofdzetel gebeuren de elektronische opzoekingen, worden de nodige instructies verstrekt en worden de verzoeken tot internationale samenwerking verstuurd. De gerechtelijke politie komt tussenbeide ingeval van misdrijven van welke aard ook begaan via het internet, inzonderheid wanneer oplichting, misbruik van vertrouwen, valsheid in geschrifte, witwaspraktijken of informaticacriminaliteit in het spel is. De economische politie daarentegen houdt zich uitsluitend bezig met de economische inbreuken via het internet die worden begaan door een professionele verkoper of een dienstenaanbieder, behalve als de toevallige verkoper de koper heeft misleid (artikel 498 van het Strafwetboek), aan een buitensporige prijs heeft verkocht of een kettingverkoop heeft teweeggebracht. De gerechtelijke politie (FCCU) en de economische politie (algemene directie Controle en Bemiddeling van de FOD) werken regelmatig samen, onder meer binnen eCops. De enquêteurs van de FOD Economie hebben uitgebreide bevoegdheden die vergelijkbaar zijn met die van officieren van gerechtelijke politie in de specifieke reglementeringen die ze moeten controleren.

Iedere enquête wordt op gang gebracht door een klacht, hetzij via «*eCops*» (het uniek loket om misbruiken op het internet aan te klagen sedert 23 januari 2007) of door benadeelde consumenten, concurrenten, of nog via apostilles van de procureur des Konings. Af en toe worden op eigen initiatief controles uitgevoerd, waarvan

ce qui l'empêche de remplir pleinement ses missions. Pour pouvoir lancer une CSIRT gouvernementale, il est nécessaire de renforcer l'équipe technique de l'IBPT, de fournir un effort important en matière de formation et de consacrer un plus gros budget à l'achat de matériel. En outre, l'IBPT a encore d'autres tâches, plus classiques celles-là: l'élaboration des règles et prescriptions techniques pour protéger les infrastructures critiques, la coopération avec la Commission mixte des télécommunications et la planification nationale de crise. Il lui incombe également de veiller à l'application de ces règles et prescriptions.

2. Exposé de Mme Cécile Coppin, responsable de la cellule «Veille sur internet» de la Direction générale Contrôle et Médiation du Service public fédéral Economie

L'internet est un média puissant. Il n'est donc pas étonnant que des professionnels en usent et abusent. Si aucune infraction économique n'est constatée ou si le vendeur est de bonne foi, le service public peut favoriser le règlement alternatif des litiges. Mais il peut aussi intervenir sur le plan répressif en tant que police économique. A cet effet, le service dispose de 200 enquêteurs assermentés, répartis en sept directions régionales et trois sections en fonction de la réglementation à surveiller. Au siège central, on effectue les recherches digitales, on fournit les instructions nécessaires et on envoie les demandes de collaboration internationale. La police judiciaire intervient lorsque des infractions, de quelque nature que ce soit, sont commises via internet, en particulier lorsqu'il est question d'escroquerie, d'abus de confiance, de faux en écriture, de pratiques de blanchiment ou de criminalité informatique. La police économique, par contre, s'occupe exclusivement des délits économiques commis via internet par un vendeur professionnel ou un prestataire de services, sauf lorsque le vendeur occasionnel a trompé l'acheteur (article 498 du Code pénal), a vendu un bien à un prix abusif ou a provoqué une vente en chaîne. La police judiciaire (FCCU) et la police économique (Direction générale du Contrôle et de la Médiation du SPF Economie) collaborent régulièrement, notamment au sein du système eCops. Les enquêteurs du SFP Economie ont des pouvoirs étendus comparables à ceux des officiers de police judiciaire dans les réglementations spécifiques qu'ils sont chargés de contrôles..

Toute enquête démarre à la suite d'une plainte, déposée soit via «*eCops*» (le guichet unique pour dénoncer les abus sur internet depuis le 23 janvier 2007), soit par des consommateurs lésés ou des concurrents, soit par le biais d'apostilles du procureur du Roi. De temps en temps, des contrôles d'initiative sont organisés.

«*Sweepday*» het treffendste voorbeeld is: op dergelijke dag wordt een bepaalde sector helemaal doorgelicht, in samenspraak met andere landen (een recent voorbeeld daarvan is de «*Sweepday*» met betrekking tot de verkoop van vliegtuigbiljetten). Deze laatsten kunnen ook om medewerking verzoeken in het raam van het Europees Reglement 2006/2004 van 27 oktober 2004 dat de samenwerking inzake consumentenbescherming regelt.

Het internet creëert een virtuele economische markt zonder dat men zich moet verplaatsen, met tal van opties en verleidelijke reclames. Het heeft geleid tot een groot aantal technieken die voorheen niet bestonden: links in zoekmotoren, gewenste en ongewenste e-mails en virusmarketing, pop-upberichten die een valse bedreiging doen vrezen, onder meer om antivirusprogramma's te promoten.

Om de consumenten te beschermen maar ook om de concurrentie eerlijk te laten verlopen, hebben de professionele verkopers een aantal basisverplichtingen: ze moeten zich correct identificeren, de reclame mag niet misleidend zijn, het verkoopaanbod op afstand niet dubbelzinnig en het verkoopcontract moet te goeder trouw worden uitgevoerd.

Om misbruiken te voorkomen zijn een bepaald aantal handelspraktijken gereglementeerd en andere dan weer helemaal verboden. De niet-eerbiediging van voorgeschreven regels kan een inbreuk impliceren, maar daarom is niet noodzakelijk sprake van kwade trouw. De geviseerde praktijken worden slechts dan als malafide beschouwd als zij om winst te maken, wat het doel is van alle handelstransacties, de consumenten willen misleiden.

Dit gebeurt vaak door misbruik van het woordje «gratis», «promotie» of «bedreiging» (om antivirusprogramma's te slijten die men helemaal niet nodig heeft). Vaak wordt men naar betalende telefoonnummers doorverwezen waar men, zonder dat men enige kwaliteitsvolle dienst aangeboden krijgt, een buitensporig tarief voor betaalt. Er zijn de aanbiedingen in verband met de «beltonen» voor mobieltjes. Men wordt als winnaar uitgeroepen van onbestaande wedstrijden (de wettelijkheid hiervan moet bovendien met de Kansspelcommissie worden bekeken). De malafide dienstenaanbieders zijn vaak niet of zeer moeilijk traceerbaar. ze zijn alleen bereikbaar via een telefoonnummer of geven een vals adres op en verschuilen zich achter kredietwaardig geachte sites.

De meest kwetsbare doelgroep is de categorie «zwakke internetgebruiker»: zij die op zoek zijn naar een partner of naar een job, jongeren die onbezonnen via

«*Sweepday*» en est l'exemple le plus frappant: ce jour-là, un secteur particulier est entièrement passé au peigne fin, en concertation avec d'autres pays (un exemple récent est le «*Sweepday*» concernant la vente de billets d'avion). Ces derniers peuvent également demander une collaboration dans le cadre du Règlement européen 2006/2004 du 27 octobre 2004 qui règle la coopération en matière de protection des consommateurs.

L'internet crée un marché économique virtuel qui ne demande aucun déplacement, avec de nombreuses options et des publicités attrayantes. Il a donné naissance à un grand nombre de techniques qui n'existaient pas auparavant: le référencement dans les moteurs de recherche, les e-mails et sms non solliicités, le marketing viral, les popups intempestifs faisant craindre une fausse menace, notamment pour promouvoir des anti-virus.

Pour protéger les consommateurs mais également pour permettre à la concurrence de s'exercer loyalement, les vendeurs professionnels sont soumis à un certain nombre d'obligations de base: ils doivent s'identifier correctement, la publicité ne peut être mensongère, l'offre en vente à distance ne peut pas être équivoque et le contrat de vente à distance doit être exécuté loyalement.

Afin d'éviter les abus, certaines pratiques commerciales sont réglementées, tandis que d'autres sont totalement interdites. Le non-respect des règles prescrites peut impliquer une infraction, mais n'est pas nécessairement synonyme de mauvaise foi. Les pratiques en question ne sont considérées comme malhonnêtes que si elles procèdent de la volonté de réaliser des bénéfices, en dehors du but lucratif inhérent à son activité commerciale, en trompant le consommateur.

Cela passe souvent par l'utilisation du petit mot «gratuit», des termes «promotion» ou «menace» (afin de vendre des logiciels antivirus dont on n'a aucun besoin). Souvent, l'on est orienté vers des numéros de téléphone payants pour lesquels on paiera un tarif excessif sans obtenir en retour quelque service de qualité que ce soit. Il y a aussi les offres de «sonneries» gsm. L'on est présenté comme le gagnant d'un concours fictif (la commission des jeux de hasard doit en outre se pencher sur la légalité de cette pratique). Souvent, il est difficile voire impossible de retrouver la trace des fournisseurs de services malhonnêtes. Ils ne sont joignables que par téléphone ou donnent une fausse adresse et se cachent derrière des sites réputés.

Le groupe-cible le plus vulnérable est la catégorie des «internautes faibles»: ceux qui sont à la recherche de l'âme sœur ou d'un emploi, les jeunes qui achètent en

het internet dingen kopen waarvan de prijs buitensporig is, worden gemakelijker het slachtoffer van malafide praktijken.

De malafide dienstenaanbieder heeft krachtige middelen te zijner beschikking die hem door de nieuwe technologische toepassingen worden aangereikt, voornamelijk inzake publiciteit en betaling (meer en meer via betalende sms'en). Hij kan zich in het labyrint van het internet ook beter verschuilen dan iemand die fysiek ergens gevestigd is. De verbeelding van de bedriegers kent geen grenzen: men doet geloven dat een bepaalde dienst kosteloos is, terwijl men intussen een langjarig abonnement aansmeert. details over prijzen worden in dezelfde kleur weergegeven als die van het scherm. de aanbiedingen zijn buitenmaats ten opzichte van het scherm zodat essentiële informatie buiten het scherm valt. Ook worden via pop-ups en spam en zelfs spyware valse bedreigingen verspreid, zodat men om zich te beschermen zich een antivirusprogramma aanschaft dat men helemaal niet nodig had.

De vuistregel van het bedrog is eenvoudig: de internetgebruiker zou niet met een bepaalde dienst hebben ingestemd indien hij de exacte reikwijdte – zowel qua inhoud, als die er al is, als qua tarief – had gekend. De betaling gebeurt steeds vaker via een telecomoperator. Anderzijds kan men ingeval van klacht bij niemand terecht.

Wanneer dergelijke ontoelaatbare praktijken worden geconstateerd, wordt opgetreden, tenminste als de bedrieger in België is gevestigd. Naargelang van de ernst van de inbreuk, kan een waarschuwing worden gegeven, kan de staking van geconstateerde praktijk worden bevolen of een boete worden opgelegd.

Wanneer de bedrieger niet in België is gevestigd, wordt een verzoek tot samenwerking gericht aan het Europees land waar hij gevestigd is via het voornoemde Europees Reglement 2006/2004, of via de OESO-kanalen voor consumentenbescherming als hij buiten de Europese Unie is gevestigd.

3. Uiteenzetting van de heer Michel De Coster, ICT-verantwoordeling van de Federale Overheidsdienst Financiën

De heer Michel De Coster beschrijft de ICT-infrastructuur van de FOD Financiën:

– Het systeem «Atlas», bedoeld voor de massale gecentraliseerde opslag van gegevens, wordt gebruikt door de toepassingsservers.

ligne, sans discernement, des articles à prix prohibitif, sont plus facilement victimes de pratiques malhonnêtes.

Les nouvelles applications technologiques dotent le fournisseur de services malhonnête d'outils efficaces, essentiellement en matière de publicité et de paiement (de plus en plus souvent par sms payants). Il peut également mieux se dissimuler dans le labyrinthe de l'Internet qu'une personne qui est physiquement domiciliée quelque part. L'imagination des fraudeurs est sans limite: l'on fait croire qu'un service donné est gratuit, alors que l'on refile au consommateur un abonnement de longue durée; les informations sur le prix figurent en caractères de même couleur que celle du fond d'écran; la taille des offres est démesurée par rapport à la résolution d'écran si bien que les informations essentielles ne se voient pas sur l'écran; via les pop-ups et le spam, voire les logiciels espions, l'on diffuse également de fausses menaces, de telle sorte que le consommateur achète, pour s'en prémunir, un logiciel antivirus parfaitement inutile.

La règle cardinale de l'arnaque est simple: l'utilisateur d'Internet n'aurait pas souscrit à un service déterminé s'il en avait connu la portée exacte – tant en ce qui concerne le contenu, quand il y en a un, qu'en ce qui concerne le tarif. Le paiement se fait de plus en plus souvent par le biais d'un opérateur de télécommunications. Par ailleurs, en cas de plainte, il n'y a personne à qui s'adresser.

Lorsque de telles pratiques inadmissibles sont constatées, on intervient, du moins si l'arnaqueur est établi en Belgique. En fonction de la gravité de l'infraction, on peut donner un avertissement, ordonner la cessation de la pratique constatée ou infliger une amende.

Si l'arnaqueur n'est pas établi en Belgique, une demande de collaboration est adressée au pays européen dans lequel il est établi, via la base de données commune en vertu du Règlement CE 2006/2004 précité ou via le Réseau international de Contrôle et de Protection des consommateurs de l'OCDE, s'il est établi dans un pays hors Union européenne.

3. Exposé de M. Michel De Coster, responsable TIC du SPF Finances

M. Michel De Coster décrit l'infrastructure TIC du SPF Finances:

– Le système «Atlas», destiné au stockage massif centralisé de données, est utilisé par les serveurs d'application.

– De verschillende gegevensbanken zijn met elkaar verbonden.

– Het Communicatiecentrum voor de Federale Fiscaliteit (CCFF) integreert een groot aantal applicaties in een gemeenschappelijk architecturaal kader en standaardiseert de interfaceclient voor gebruikers. Het centrum integreert ook gestandaardiseerde veiligheidsfuncties: identificatie bij aanmelding (al dan niet met een elektronische identiteitskaart), registratie van het internetverkeer, opstelling van een journaal van legaliseringen en toegangverleningen. Het CCFF wordt geïdentificeerd door een certificaat, dat door elke gebruiker kan worden geraadpleegd.

– De infrastructuur van een groot aantal gebouwen van de FOD Financiën, die over het gehele grondgebied van België zijn verspreid, wordt beheerd. Zij neemt de vorm aan van een groot privaat netwerk, dat van de infrastructuur «Balans» van Belgacom gebruik maakt.

– Een systeem staat in voor de identificatie van gebruikers en de controle op toegang tot het netwerk.

Om verlies van de beschikbare informatie te vermijden, zijn de meeste informaticasystemen van de FOD Financiën ontdubbeld en zijn de twee grote systemen («*production*» en «*disaster recovery*») verdeeld over twee geografisch onderscheiden sites. Van alle gegevens wordt een automatische kopie gemaakt, zowel op harde schijven als op externe dragers. Verder worden de beide sites beveiligd en bestaat er een opstartplan bij incidenten.

Het netwerk van de FOD wordt beschermd tegen de mogelijke bedreigingen uit de buitenwereld, met name internet, Fedman (de interface die de FOD Financiën toegang tot internet verleent) en verschillende gespecialiseerde verbindingen. Om de continuïteit van de openbare dienst te verzekeren, wordt de beveiliging verzekerd door de volgende functies van de infrastructuur:

– De *firewall* met twee lagen wordt beschermd door een DMZ (een zogenaamde «*demilitarized zone*», een netwerksegment dat zich tussen het interne en het externe netwerk bevindt), die zowel omgeven is door een interne firewall (tussen de DMZ en het netwerk van de FOD Financiën) als door een externe firewall (tussen de DMZ en de buitenwereld). Een DMZ reageert op binnendringing van instanties die geen toegang tot het netwerk hebben.

– De antivirusbescherming functioneert voor drie protocollen: http, https en ftp. Voor https-protocollen bestaat de mogelijkheid om de informatiestromen te controleren.

– Ambtenaren krijgen toegang tot een webapplicatie via een proxy, die over de functionaliteit beschikt om toegang tot verdachte websites te weigeren.

– Les différentes banques de données sont reliées entre elles.

– Le Centre de Communication de la Fiscalité fédérale (CCFF) intègre un grand nombre d'applications dans un cadre architectural commun et standardise l'interface client pour les utilisateurs. Le centre intègre également des fonctions de sécurité standardisées: identification à l'entrée (au moyen ou non d'une carte d'identité électronique), enregistrement du trafic Internet, établissement d'un journal de légalisations et d'autorisations d'accès. Le CCFF est identifié par un certificat, qui peut être consulté par chaque utilisateur.

– L'infrastructure d'un grand nombre de bâtiments du SPF Finances, répartis sur l'ensemble du territoire belge, est gérée sous la forme d'un grand réseau privé, qui utilise l'infrastructure «Bilan» de Belgacom.

– Un système assure l'identification des utilisateurs et le contrôle de l'accès au réseau.

Pour éviter la perte des informations disponibles, la plupart des systèmes informatiques du SPF Finances ont été dédoublés et les deux grands systèmes («production» et «*disaster recovery*») ont été répartis sur deux sites géographiquement distincts. Une copie automatique de toutes les données est réalisée, tant sur disques durs que sur supports externes. Les deux sites sont en outre sécurisés et un plan de démarrage est prévu en cas d'incidents.

Le réseau du SPF est protégé contre les menaces provenant du monde extérieur, à savoir Internet, Fedman (l'interface qui fournit l'accès à Internet au SPF Finances) et différentes connexions spécialisées. Pour garantir la continuité du service public, la sécurisation est assurée par les fonctions suivantes de l'infrastructure:

– Le pare-feu à deux couches est protégé par une DMZ (une zone «démilitarisée», un segment de réseau qui se situe entre le réseau interne et le réseau externe), qui est entourée à la fois d'un pare-feu interne (entre la DMZ et le réseau du SPF Finances) et d'un pare-feu externe (entre la DMZ et le monde extérieur). Une DMZ réagit à l'intrusion d'instances qui n'ont pas accès au réseau.

– La protection antivirus fonctionne pour trois protocoles: http, https et ftp. Pour les protocoles https, la possibilité de contrôler les flux d'informations existe.

– Les fonctionnaires accèdent à une application web par le biais d'un *proxy*, qui dispose de la fonctionnalité de refuser l'accès aux sites Internet suspects.

– Het automatisch scannen van de berichtenstroom zorgt voor bescherming tegen virussen en spam. verdachte berichten worden vervolgens in een afzonderlijke map geplaatst.

– Er is voldoende capaciteit om weerstand te bieden tegen aanvallen van het type DOS (weigering van dienst).

– Een gespecialiseerd bedrijf waakt permanent over het veiligheidssysteem.

De bevolking kan niet rechtstreeks de interne systemen van de FOD Financiën raadplegen: zij heeft enkel toegang tot bepaalde gelocaliseerde systemen in de DMZ, die communiceren met de interne servers van de FOD en die een door DNS toegekende domeinnaam hebben (bijvoorbeeld www.taxonweb.be of www.myminfin.be.

Het beheer van het computerpark verloopt volledig op gecentraliseerde wijze. Dit geldt voor de aankoop, de verdeling en het onderhoud van PC's en software, de standaardisering van de PC's, de verdeling van veiligheidsstrips en de activering van antivirusbescherming die *up-to-date* is.

Eveneens door een centraal beheer hebben ambtenaren van de FOD Financiën de mogelijkheid om te werken vanaf om het even welke post, terwijl de toegang tot gevoelige interne gegevens wordt gecontroleerd. Elke ambtenaar beschikt ook over een e-mailadres voor professionele doeleinden en heeft toegang tot een beperkt aantal websites, die zich op een zogenaamde «white list» bevinden. Een algemene toegang tot het internet wordt enkel toegekend aan ambtenaren voor wie dit wegens hun functie verantwoord is.

Alle gebruikers van het netwerk van de FOD worden geïdentificeerd:

– Burgers krijgen toegang op basis van een Token, dat door Fedict wordt gecreëerd, of aan de hand van een elektronische identiteitskaart.

– Ambtenaren moeten zich aanmelden met een login en een wachtwoord. In de toekomst zou de controle nog kunnen worden verbeterd door het aanloggen met elektronische identiteitskaart.

– In sommige gevallen verloopt de toegang via een vertrouwenspartner, die zelf een beveiligde verbinding tot stand brengt (bijvoorbeeld de Kruispuntbank voor de Sociale Zekerheid).

– In andere gevallen maakt een vertrouwenspartner gebruik van een SAML-procedure om zich te identificeren (dat geldt bijvoorbeeld voor mandatarissen van belastingplichtigen).

– Le scannage automatique du flux de messages assure la protection contre les virus et les spams. Les messages suspects sont ensuite placés dans un répertoire distinct.

– La capacité est suffisante pour résister aux attaques du type DOS (refus de service).

– Une entreprise spécialisée surveille en permanence le système de sécurité.

La population ne peut pas consulter directement les systèmes internes du SPF Finances: elle a uniquement accès à certains systèmes localisés dans la DMZ, qui communiquent avec les serveurs internes du SPF et ont un nom de domaine attribué par DNS (par exemple, www.taxonweb.be ou www.myminfin.be).

Le parc informatique est géré de façon complètement centralisée, tant pour l'acquisition, la distribution et l'entretien des ordinateurs et des logiciels que pour la standardisation des ordinateurs, la distribution de bandes de sécurité et l'activation de la protection antivirus actualisée.

C'est également par le biais d'une gestion centrale que les agents du SPF Finances ont la possibilité de travailler à partir de n'importe quel poste, tandis que l'accès aux données internes sensibles est contrôlé. Chaque fonctionnaire dispose également d'une adresse électronique à des fins professionnelles et a accès à un nombre limité de sites Internet figurant sur une «liste blanche». L'accès généralisé à l'Internet n'est octroyé qu'aux agents dont la fonction le justifie.

Tous les utilisateurs du réseau du SPF sont identifiés:

– Les citoyens ont accès sur la base d'un token, qui est créé par Fedict, ou par le biais d'une carte d'identité électronique.

– Les agents doivent se connecter avec un login et un mot de passe. Dans le futur, le contrôle pourrait encore être amélioré grâce à la connexion avec la carte d'identité électronique.

– Dans certains cas, l'accès se réalise via un partenaire de confiance, qui établit lui-même une connexion sécurisée (par exemple la Banque carrefour de la Sécurité sociale).

– Dans d'autres cas, un partenaire de confiance recourt à une procédure SAML pour s'identifier (c'est notamment le cas des mandataires de contribuables).

4. Uiteenzetting van mevrouw Christiane Rouma, verantwoordelijke van het Rijksregister

Zoals de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen bepaalt, zijn in het Rijksregister alle Belgen opgenomen die in België verblijven, alsmede alle in België verblijvende vreemdelingen die toegelaten of gemachtigd zijn zich in het Rijk te vestigen of er te verblijven, en voorts alle in het buitenland verblijvende Belgen die ingeschreven zijn in de registers gehouden in de diplomatieke zendingen en consulaire posten, en alle vreemdelingen die zich vluchteling verklaren of die vragen om als vluchteling te worden erkend en die niet in een andere hoedanigheid ingeschreven zijn in de bevolkingsregisters. De wet bepaalt welke inlichtingen in verband met die personen in het Rijksregister worden opgenomen (maximum 14 gegevens). Op vraag van de gemeenten worden de andere in de bevolkingsregisters vermelde gegevens eveneens in het Rijksregister bewaard.

Het Rijksregister, dat zo'n 15 miljoen dossiers beheert, is de hoeksteen van al wat met identiteit te maken heeft, maar sedert de invoering van de elektronische identiteitskaart is het tevens het hart van de administratieve elektronische communicatie (e-government). Dankzij de elektronische identiteitskaart beschikt iedere burger over een beveiligd middel om zich – in het kader van zijn elektronische communicaties – te identificeren en zijn handtekening te plaatsen, zowel in de publieke als in de privésfeer.

Het Rijksregister beschikt over een back-up-centrum in Vilvoorde.

De gebruikers van het Rijksregister zijn op verschillende manieren met dat register verbonden ((DCS, PubliLink, Fedman, Irisnet, Vera, Cipal enzovoort). De communicatie komt tot stand in realtime of via zogeheten «batches» (uittreksel uit de gegevens dat op verschillende dragers wordt geregistreerd of op een beveiligde manier wordt overgezonden (FTP)).

De toegang in realtime tot het bestand van de natuurlijke personen gebeurt in 90 % van de gevallen via het X.25-protocol. Het IP-protocol wordt gebruikt voor de toepassingen in verband met de elektronische identiteitskaart, maar sedert 2006 ook voor de toegang tot de bestanden van de natuurlijke personen.

De externe met het Rijksregister geassocieerde netwerken zijn privénetwerken : PubliLink (netwerk van Dexia en Belgacom), *Data Communication Service* (DCS – Belgacom), abonnementscircuit (vast circuit tussen twee plaatsen), *Federal Metropolitan Network* (Fedman), Vera (netwerk van de provincie Vlaams-Brabant), Irisnet

4. Exposé de Mme Christiane Rouma, responsable du Registre national

Comme le prescrit la loi du 8 août 1983 organisant un Registre national des personnes physiques, sont inscrites au Registre national, tous les Belges, résidant en Belgique, ainsi que tous les étrangers résidant en Belgique qui sont admis ou autorisés à s'établir ou a séjourner dans le Royaume, de tous les Belges résidant à l'étranger et inscrits dans les registres tenus dans les missions diplomatiques et les postes consulaires belges à l'étranger, et de tous les étrangers qui se déclarent réfugiés ou qui demandent la reconnaissance de la qualité de réfugiés et qui ne sont pas inscrits à un autre titre dans les registres de la population. Les informations enregistrées concernant ces personnes sont déterminées par la loi (14 données maximum). Toutefois, à la demande des communes, les autres données enregistrées dans les registres de la population sont également conservées au Registre national.

Le Registre national, qui gère quelque 15 millions de dossiers, est la pierre angulaire de tout ce qui a trait à l'identité, et, depuis l'instauration de la carte d'identité électronique, il est devenu le pilier de la communication électronique (e-gouvernement). Grâce à la carte d'identité électronique, chaque citoyen dispose d'un moyen sécurisé lui permettant de s'authentifier et d'apposer sa signature – dans le cadre de ses communications électroniques, tant dans la sphère publique que privée.

Le Registre national dispose d'un centre back-up à Vilvorde.

Les utilisateurs du Registre national sont reliés à celui-ci de différentes manières (DCS, Publilink, Fedman, Irisnet, Vera, Cipal, etc.). La communication est établie en temps réel ou via «batch» [extrait de données, enregistré sur différents supports ou transmis via transfert sécurisé (FTP)].

L'accès en temps réel au fichier des personnes physiques est réalisé dans 90% des cas via le protocole X.25. Le protocole IP est utilisé pour les applications relatives à la carte d'identité électronique, et, depuis 2006, également pour l'accès au fichier des personnes physiques.

Les réseaux externes associés du Registre sont des réseaux privés : Publilink (réseau de Dexia et Belgacom), *Data Communication Service* (DCS – Belgacom), abonnement circuit (circuit fixe entre deux endroits), *Federal Metropolitan Network* (Fedman), Vera (réseau de la province du Brabant flamand), Irisnet (réseau de la

(netwerk van het Brussels Hoofdstedelijk Gewest), C-Net (netwerk van CEVI) en Ci-Port (netwerk van CIPAL).

Inzake de toegang via TCP/IP-protocol (algemene term voor een protocol dat door het gebruik ervan op internet als communicatiestandaard tussen informaticanetwerken geldt), zijn twee soorten van toegangen mogelijk :

– de eerste toegangsmogelijkheid, van het type "individuele gebruiker", maakt gebruik van een internetbrowser en is specifiek bedoeld voor gebruikers die (minder dan) het gemiddelde aantal verrichtingen uitvoeren; de gebruiker moet zich identificeren door middel van zijn elektronische identiteitskaart. Elk werkstation moet over een eID-kaartlezer beschikken. De versleutelde verbinding wordt tot stand gebracht via het SSL protocol, aan de hand van de elektronische identiteitskaart;

– de tweede toegangsmogelijkheid loopt via de webdiensten en is bedoeld voor de gemeenten, de federale overheidsdiensten, en in het algemeen voor de organen die werken met het Rijksregister voor de centrale en geautomatiseerde verwerking van gegevens (teneinde ze op lokale dan wel ruimere schaal toegankelijk te maken). Deze toegangsmogelijkheid zal geleidelijk de verbinding van computer tot computer vervangen. Om gebruik te maken van deze toegangsmogelijkheid, moeten de onder het orgaan ressorterende gebruikers hun elektronische identiteitskaart aanwenden om het Rijksregister te raadplegen en/of bij de tijd te brengen.

Het gebruiks- en toegangsbeleid kan worden weergegeven aan de hand van drie afkortingen: PEP («*Policy Enforcement Point*»), PDP («*Policy Definition Point*») en PAP («*Policy Administration Point*»).

PEP: het verzoek van de gebruiker wordt geanalyseerd aan de hand van zijn identiteit, zijn toegangsvergunning, het ingebrachte verzoek, de bestanden en de omgeving waartoe hij toegang wenst te hebben.

PDP: het verzoek wordt doorgesluisd naar de PAP om na te gaan of al dan niet toegang mag worden verleend. De toestemming heeft louter betrekking op de gevraagde toepassing.

PAP: dit is de omgeving voor het beheer en de registratie van de machtigingen voor de personen die als beheerders van de toepassing zijn aangewezen; deze omgeving stelt de machtigingsregels ter beschikking van de PDP.

In de praktijk kunnen alleen instanties die over een wettelijke machtiging beschikken, toegang hebben tot de gegevens waarvoor voornoemde machtiging werd verleend (wet van 25 maart 2003, die daartoe een sec-

Région de Bruxelles-Capitale), C-Net (réseau de CEVI) et Ci-Port (réseau de CIPAL).

En ce qui concerne l'accès en protocole TCP/IP (terme générique utilisé pour désigner un protocole qui s'est imposé comme un standard de communication entre réseaux informatiques de par son utilisation sur Internet), deux types d'accès sont possibles :

– le premier est l'accès de type client isolé par navigateur Internet, typiquement destiné à des utilisateurs effectuant un nombre faible ou moyen de transactions et pour lequel l'utilisateur doit s'authentifier au moyen de sa carte d'identité électronique. Chaque poste de travail doit être équipé d'un lecteur de cartes d'identité électroniques. La connexion cryptée est établie via le protocole SSL utilisant la carte électronique;

– le second est l'accès aux webservices; il est destiné aux communes, aux services publics fédéraux et en général aux organismes qui effectuent des transactions avec le Registre national en vue d'un traitement centralisé et automatisé de données (en vue d'une redistribution locale ou plus étendue de celles-ci). Ce second type d'accès est amené à remplacer progressivement l'accès ordinateur-ordinateur. Dans ce second type d'accès, les utilisateurs relevant de l'organisme doivent utiliser leur carte d'identité électronique pour la consultation et/ou la mise à jour du Registre national.

La politique de gestion des utilisateurs et des accès se résume en trois sigles : PEP («*Policy Enforcement Point*»), PDP («*Policy Definition Point*») et PAP («*Policy Administration Point*»).

PEP: la requête de l'utilisateur est analysée en fonction de son identité, de son autorisation d'accès et de l'action demandée, des ressources et de l'environnement auxquels il souhaite avoir accès.

PDP: la demande est transférée vers la PAP pour obtenir la décision concernant la demande d'autorisation d'accès ; une réponse positive ne s'applique qu'à l'accès à l'application demandée.

PA : est l'environnement pour la gestion et l'enregistrement des autorisations pour les personnes désignées gestionnaires de l'application; il met les règles d'autorisation à disposition du PDP.

En pratique, seuls des organismes disposant d'une autorisation légale peuvent avoir accès aux données pour lesquelles l'autorisation précitée a été délivrée (loi du 25 mars 2003, qui a institué un comité sectoriel à

toraal comité instelde; wet tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen). Het sectoraal comité beoordeelt of de doeleinden, waarvoor de toegang tot de gegevens van het Rijksregister van de natuurlijke personen wordt gevraagd of van de vraag om mededeling ervan, welbepaald, duidelijk omschreven en wettig zijn en, in voorkomend geval, of de gevraagde gegevens uit het Rijksregister toereikend, relevant en niet overmatig zijn in het licht van die doeleinden.

Vooraleer het sectoraal comité zijn machtiging verleent, gaat het na of de toegang of de inzageverlening geschiedt in overeenstemming met de voormelde wet van 8 augustus 1983, met de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en hun uitvoeringsbepalingen, alsook met de andere relevante normen betreffende de bescherming van de persoonlijke levenssfeer of persoonsgegevens.

Het IP-adres wordt altijd geregistreerd, ongeacht de toegangsmodus.

De wijze waarop de gebruiker wordt geïdentificeerd, hangt af van het type toegang. Bij toegang volgens het terminal-computerprotocol kent het Rijksregister een variabele sleutel toe, bestaande uit een vaste waarde (gebruikersnaam) en een variabele waarde (wachtwoord) die bij elke transactie moeten worden opgegeven. De variabele sleutel is gekoppeld aan de naam en de NIS-code van de instelling, alsmede aan de toestemming. Elke maand wordt een nieuwe sleutel toegekend.

Bij toegang volgens het computer-computerprotocol kent het Rijksregister een vaste sleutel toe, die gekoppeld is aan de naam van de verantwoordelijke van de instelling, de NIS-code van de instelling en de toestemming.

Bij toegang van een afzonderlijke cliënt (standalone) via de webbrowser wordt de gebruiker geïdentificeerd aan de hand van het certificaat dat op zijn elektronische identiteitskaart opgeslagen is.

Bij webservice-toegang wordt de gebruiker geïdentificeerd aan de hand van zijn rijksregisternummer, de naam van de applicatie waaraan de NIS-code van de instelling gekoppeld is, en de gebruikte transacties.

De bestanden van het Rijksregister worden door een hele waaier van klassieke middelen beveiligd, onder meer applicaties die zwakke plekken en eventuele pogingen tot hacking detecteren.

cette fin : loi modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques). Le Comité sectoriel juge si les finalités en vue desquelles l'accès aux données du Registre national des personnes physiques ou la communication de certaines de ces données a été demandé, sont déterminées, explicites et légitimes, et, le cas échéant, si les données du Registre national demandées sont adéquates, pertinentes et non excessives par rapport à ces finalités.

Avant de donner son autorisation, le Comité sectoriel vérifie si l'accès ou la communication se fait en conformité avec la loi du 8 août 1983 précitée, avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et leurs dispositions d'exécution, ainsi qu'avec les autres normes pertinentes en matière de protection de la vie privée ou des données à caractère personnel.

Pour tous les modes d'accès, il est procédé à un enregistrement de l'adresse IP.

L'identification de l'utilisateur se fait de différentes façons selon le type de connexion. Pour les connexions, terminal-ordinateur, des clefs variables sont attribuées par le Registre national -comprenant une partie fixe (login) et une partie variable (mot de passe) qui doit être incrémentée à chaque transaction- associées au nom de l'organisme, au code INS de celui-ci et à la permission. De nouvelles clefs sont attribuées chaque mois.

Pour les connexions ordinateur-ordinateur, il s'agit de clefs fixes attribuées par le Registre national et qui sont associées au nom du responsable de l'organisme, au code INS de l'organisme et à la permission.

Pour l'accès de type client isolé par navigateur Internet, l'utilisateur est identifié via le certificat qui est stocké sur sa carte d'identité électronique.

Pour l'accès au webservices, l'utilisateur est identifié par son numéro d'identification au Registre national, par le nom de l'application auquel est associé le code de l'organisme et les transactions utilisées.

Les fichiers du Registre national sont protégés par tout un éventail de mesures de sécurisation classiques, y compris des programmes de détection des vulnérabilités et des tentatives de piratage.

Bestanden die via een extern netwerk worden verstuurd, worden versleuteld. De fysieke toegang tot de gebouwen en de lokalen wordt gecontroleerd en centraal beheerd. Alle personeelsleden moeten over een toegangsbadge beschikken. Bezoekers moeten zich laten registreren en krijgen een bezoekersbadge.

In opdracht van de FOD Economie vond een audit plaats, in uitvoering van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten. Op 27 april 2006 keurde de FOD Economie het actieplan goed dat een antwoord moest bieden op de aanbevelingen in het auditverslag.

Kortom, het Rijksregister is toegankelijk via het internet, maar alleen via de versleutelde SSL-verbinding en met gebruik van de elektronische identiteitskaart; dat geldt niet alleen voor de gebruiker die gemachtigd is het Rijksregister te raadplegen, maar ook voor de burger die van zijn wettelijk recht gebruikmaakt de hem betreffende Rijksregistergegevens te raadplegen en te vragen wie zijn gegevens de jongste zes maanden heeft opgevraagd of bijgewerkt.

Andere gebruikers kunnen alleen toegang krijgen via een erkend netwerk of het netwerk van de federale besturen.

5. Uiteenzetting van de heer Marc Van Wesemael, general manager van de vzw «DNS.BE»

De heer Marc Van Wesemael situeert DNS: het is de Belgische vereniging voor internetdomeinregistratie. De rol van DNS kan als het ware omschreven worden als die van een telefooncentrale van het internet. Elke computer die op het internet is aangesloten, heeft een uniek IP-adres met cijfers (bijvoorbeeld 195.22.138.102), dat kan worden vervangen door een domeinnaam (wat niet hetzelfde is als een website).

In vergelijking met een IP-adres heeft een domeinnaam verschillende voordelen:

– De beheerder kan de naam, onder voorbehoud van beschikbaarheid, zelf kiezen;
– De naam wordt gebruikt voor verschillende diensten (websites, e-mailadressen);
– Het betreft meestal een gemakkelijke referentie, die door een surfer vlot wordt gevonden;
– De transparantie blijft bij verandering van computer of website verzekerd (enkel het cijferadres moet dan worden gewijzigd, niet de domeinnaam).

Les fichiers qui sont transférés via un réseau externe sont cryptés. L'accès physique aux bâtiments et aux locaux est contrôlé et les accès sont gérés par un système centralisé. Les membres du personnel doivent disposer d'un badge d'accès. Les visiteurs occasionnels doivent s'enregistrer et porter un badge.

Un audit a été effectué par une équipe d'auditeurs, à la demande du SPF Economie, en exécution de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification. Un plan d'actions a été établi en vue de rencontrer les recommandations formulées dans le rapport d'audit. Le SPF Economie a approuvé ce plan d'actions le 27 avril 2006.

En résumé, le Registre national est accessible par Internet mais uniquement par le biais d'une connexion cryptée SSL et en utilisant la carte d'identité électronique et tant en ce qui concerne les utilisateurs habilités à consulter le Registre national qu'en ce qui concerne le citoyen, lorsqu'il exerce le droit qui lui est reconnu par la loi, de consulter les informations le concernant enregistrées au registre national et de demander qui a consulté ou mis à jour ses données au cours des six derniers mois.
Pour les autres utilisateurs, un réseau agrée ou le réseau des administrations fédérales est exigé.

5. Exposé de M. Marc Van Wesemael, directeur général de l'asbl «DNS.BE»

M. Marc Van Wesemael situe DNS: c'est une association belge spécialisée dans l'enregistrement de noms de domaines sur Internet. Le rôle de DNS peut en quelque sorte être décrit comme celui d'un central téléphonique de l'internet. Tout ordinateur connecté à Internet possède une adresse IP unique composée de chiffres (par exemple 195.22.138.102), qui peut être remplacée par un nom de domaine (ce qui n'est pas la même chose qu'un site web).

Comparé à une adresse IP, un nom de domaine présente divers avantages:

– Le gestionnaire peut choisir lui-même le nom, pour autant qu'il soit disponible;
– Le nom est utilisé pour divers services (sites web, adresses de messagerie électronique);
– Il s'agit généralement d'une référence facile que le cybernaute trouve rapidement;
– La transparence reste garantie en cas de changement d'ordinateur ou de site web (seule l'adresse chiffrée doit être remplacée, et pas le nom du domaine).

De toekenning van domeinnamen is hiërarchisch georganiseerd in zones met een gedistribueerde verantwoordelijkheid:

– RFC-documenten (*Requests for Commons*) beschrijven de protocollen en andere aspecten van het internet en zijn derhalve de technische wetten van het internet, die ervoor zorgen dat computers met elkaar over het internet kunnen communiceren;
– ICANN (*Internet Corporation for Assigned Names and Numbers*) is de instantie die de zogenaamde «*Top level domains*» beheert, het eerste organisatieniveau van het internet (.be, .com, .org, .net, .eu,…);
– De toekenning van domeinnamen die op .be eindigen is de opdracht van DNS;
– Het beheer van een bepaalde domeinnaam is de verantwoordelijkheid van de beheerders zelf (instellingen, bedrijven, particulieren).

Sinds 1989 worden domeinnamen die op .be eindigen geregistreerd:

– Vanaf 1989 gebeurde dit door het departement Computerwetenschappen van de KULeuven, waar professor P. Verbaeten als eerste administrator optrad;
– Door de commerciële doorbraak van het internet nam het aantal aanvragen toe en werd door de toenmalige beheerder gevraagd een oplossing te vinden. In samenspraak met het BIPT werd door ISPA, Agoria en Beltug in 1999 DNS opgericht, een vzw waarin ook vertegenwoordigers van de overheid, academici en experten zitting hebben.

Het beheer van de .be-zone door DNS houdt de volgende opdrachten in:

– voorzien in de technische infrastructuur die nodig is voor het bereikbaar maken van websites en e-mailadressen in de .be-zone;
– instaan voor een goed beheer van de infrastructuur en voor de vervanging, *upgrading* en ontdubbeling ervan;
– voorzien in een efficiënt en kwalitatief technisch platform voor het beheer van de .be-domeinnamen (zodat registratie van een domeinnaam vlot kan gebeuren);

– promotie maken voor domeinnamen in de .be-zone, registratie en verlenging van namen, overdracht en schrapping van bestaande domeinnamen;
– ontwikkelen van een niet-discriminatoire en transparante aanpak bij de vervulling van die verschillende opdrachten.

L'attribution de noms de domaine est organisée hiérarchiquement en zones avec une responsabilité distribuée:

– Les documents RFC (*Requests for Commons)* décrivent les protocoles et d'autres aspects relatifs à Internet et constituent dès lors les lois techniques de l'Internet, qui font en sorte que les ordinateurs peuvent communiquer entre eux sur l'Internet;
– ICANN (*Internet Corporation for Assigned Names and Numbers*) est l'instance qui gère les «*Top Level domains*», le premier niveau organisationnel d'Internet (.be, .com, .org, .net, .eu,…);
– DNS est chargée d'attribuer les noms de domaine qui se terminent par .be;
– La gestion d'un nom de domaine particulier relève de la responsabilité des gestionnaires eux-mêmes (institutions, entreprises, particuliers).

Depuis 1989, les noms de domaine se terminant par .be sont enregistrés:

– À partir de 1989, par le département informatique de la KULeuven, où le professeur P. Verbaeten occupait la fonction de premier administrateur;
– En raison de la percée commerciale d'Internet, le nombre de demandes a augmenté et le gestionnaire de l'époque a demandé qu'une solution soit trouvée. En concertation avec l'IBPT, ISPA, Agoria et Beltug ont fondé en 1999 DNS, une asbl où siègent également des autorités publiques, des universitaires et des experts.

La gestion de la zone .be par DNS comprend les tâches suivantes:

– fournir l'infrastructure technique nécessaire pour rendre les sites internet et les adresses e-mail accessibles dans la zone .be;
– garantir une bonne gestion de l'infrastructure ainsi que son remplacement, son *upgrading* et son dédoublement;
– fournir une plate-forme technique efficace et de qualité pour la gestion des noms de domaine .be (afin que l'enregistrement d'un nom de domaine puisse se dérouler facilement);
– promotionner les noms de domaine dans la zone .be, l'enregistrement et la prolongation de noms, le transfert et la suppression de noms de domaine existants;
– développer une approche non discriminatoire et transparente pour effectuer ces différentes tâches.

De volgende zaken behoren niet tot de opdrachten van DNS:

– de keuze van een geschikte domeinnamen is de verantwoordelijkheid van de gebruiker, die onderhevig is aan de diverse wetten. DNS heeft geen politionele noch rechterlijke bevoegdheden en de volgende zaken horen daarom niet tot haar opdrachten :
– evaluatie van de inhoud van websites (een domeinnaam is geen website – een domeinnaam op zich is zelden onwettig)
– het voeren van een onderzoek naar inbreuken op copyright, Intellectuele eigendomsrechten en informatica criminaliteit;
– het uitspreken van een waardeoordeel over de toelaatbaarheid van de registratie van domeinnamen;
_ de evaluatie van de rechten van derden op een bepaalde domeinnaam.

Het beleid inzake de registratie van domeinnamen is in 2000 fundamenteel veranderd. Vóór 11 december 2000 was de situatie als volgt:

– Het registratiebeleid was restrictief: het verband tussen een domeinnaam en de aanvrager moest worden aangetoond, toegang voor particulieren was uitgesloten en er waren geen generieke, regionale of sectorgebonden namen;
– Registratie was relatief duur: een nieuwe registratie kostte 2.500 frank (62 euro), voor een vernieuwing moest 2.000 frank (50 euro) worden neergeteld;
– De registratieprocedure verliep traag door een zware administratieve procedure en de verplichting om rechtvaardigingsstukken toe te voegen;
– De procedure was inefficiënt: meer tijd ging naar de weigering van aanvragen dan naar de goedkeuring ervan;
– Weigeringen om een domeinnaam toe te kennen werden aangevochten voor de rechterlijke macht;
– Het starre beleid zorgde ervoor dat Belgische gebruikers een domeinnaam in de .com- of .org-zone verkozen boven een naam in de .be-zone;
– Zowel overheid als bedrijfswereld formuleerden kritiek op het beleid van DNS;
– Opportunisten slaagden er in om het registratiebeleid te omzeilen.

Sinds de belangrijke hervorming van 2000 is de situatie totaal anders:

– Het registratiebeleid is geliberaliseerd: naar analogie met andere landen wordt een domeinnaam in principe toegekend aan wie het eerst een aanvraag indient, wat tot een aanzienlijke vereenvoudiging aanleiding heeft gegeven;

Les matières suivantes ne font pas partie des missions de DNS:

– la responsabilité du choix des noms de domaine appropriés incombe à l'utilisateur, qui est soumis à plusieurs lois. DNS n'a pas de compétences policières ou juridictionnelles et les matières suivantes ne font pas partie de ses tâches :
– l'évaluation du contenu des sites internet (un nom de domaine n'est pas un site internet – en soi, un nom de domaine est rarement illicite)
– la réalisation d'une enquête pour rechercher les infractions en matière de copyright, de droits de propriété intellectuelle et de criminalité informatique ;
– le fait de porter un jugement de valeur sur l'admissibilité de l'enregistrement des noms de domaine ;
– l'évaluation des droits de tiers sur un nom de domaine particulier.

La politique en matière d'enregistrement des noms de domaine a changé fondamentalement en 2000. Avant le 11 décembre 2000, la situation était la suivante:

– La politique d'enregistrement était restrictive: le lien entre un nom de domaine et le demandeur devait être prouvé, l'accès aux particuliers était exclu et il n'y avait pas de noms génériques, régionaux ou liés à un secteur;
– L'enregistrement était relativement cher: un nouvel enregistrement coûtait 2.500 francs (62 euros), un renouvellement coûtait 2.000 francs (50 euros);
– La procédure d'enregistrement était lente en raison de la lourdeur de la procédure administrative et de l'obligation de joindre des pièces justificatives;
– La procédure était inefficace: le refus de demandes prenait davantage de temps que l'approbation de demandes;
– Les refus d'accorder un nom de domaine étaient contestés en justice;
– La rigidité de la politique a amené les utilisateurs belges à préférer un nom de domaine situé dans la zone .com ou .org plutôt qu'un nom dans la zone .be:
– Tant les pouvoirs publics que les entreprises ont critiqué la politique de DNS;
– Les opportunistes sont parvenus à contourner la politique d'enregistrement.

Depuis la réforme importante opérée en 2000, la situation a complètement changé:

– La politique d'enregistrement est libéralisée: à l'instar de ce qui se fait dans d'autres pays, le nom de domaine est en principe accordé à celui qui en fait la demande en premier lieu, ce qui a permis une simplification considérable;

– De registratie verloopt geautomatiseerd en is toegankelijk via een softwareplatform, waardoor er een onmiddellijke beschikbaarheid is;

– Ter bevordering van de mededinging gebeurt de registratie via een netwerk van professionele tussenpersonen (agenten);

– Om de belangen (bijvoorbeeld het recht op een merknaam) van rechthebbenden te beschermen, is een procedure van alternatieve geschillenbeslechting ingevoerd: Cepina, dat in de schoot van het VBO functioneert, staat hiervoor in.

De liberalisering heeft belangrijke positieve effecten gesorteerd:

– de kostprijs van een registratie daalde onmiddellijk van 2500 frank (62 euro) naar 25 euro (ondertussen na enkele bijkomende prijsdalingen is dit 3 euro);

– de registratie gebeurt ogenblikkelijk (volledig automatisch)

– de gelijkheid onder de aanvragers is hersteld;

– er is toegang tot een domeinnaam voor nieuwe categorieën, onder meer particulieren;

– de .be-zone is opnieuw aantrekkelijk, waardoor het Belgische stukje van het internet groeit.

De invoering van een open en transparant systeem impliceert niet dat er geen regels zouden zijn:

– Bepaalde algemene voorwaarden zijn van toepassing op iedere houder van een domeinnaam;

– Een agentencontract bevat waarborgen;

– Wie van oordeel is dat zijn rechten worden aangetast, kan een beroep instellen in het kader van een alternatieve geschillenbeslechting;

– De wet van 26 juni 2003 betreffende het wederrechtelijk registreren van domeinnamen sluit aan bij de algemene voorwaarden die DNS oplegt, maar is ook van toepassing op domeinnamen met andere extensies (bijvoorbeeld .com);

– Er geldt een technische bescherming tegen onvrijwillige vrijgave («*quarantaine*») of overname («*trade*»).

– Alle andere wetten: wet eerlijke handelspraktijken, wetten inzake intellectuele eigendom.

Het doel van alternatieve geschillenbeslechting is de verlening van de mogelijkheid aan een benadeelde derde om via een snelle en professionele juridische procedure de domeinnaam waarop hij aanspraak maakt te recupereren. Elke houder van een domeinnaam moet zich aan die procedure onderwerpen en de gevolgen van de beslissing die wordt genomen aanvaarden. De

– L'enregistrement est à présent automatisé et est accessible via un logiciel, la disponibilité étant dès lors immédiate;

– Afin de promouvoir la concurrence, l'enregistrement s'effectue via un réseau d'intermédiaires professionnels (agents);

– Dans le souci de protéger les intérêts (par exemple, le droit à un nom de marque) des ayants droit, une procédure de règlement alternatif des litiges a été prévue: c'est le Cepani, qui fonctionne sous l'égide de la FEB, qui s'en charge.

La libéralisation a eu d'importants effets positifs:

– le coût d'un enregistrement est passé d'emblée de 2 500 francs (62 euros) à 25 euros (dans l'intervalle, après quelque baisses de prix supplémentaire, le prix est de 3 euros);

– l'enregistrement est instantané;

– l'égalité entre les demandeurs est rétablie;

– les noms de domaine sont accessibles à de nouvelles catégories, notamment aux particuliers;

– la zone .be est à nouveau attrayante, si bien que le territoire belge de l'internet grandit.

L'instauration d'un système ouvert et transparent n'implique pas qu'il n'y a plus de règles:

– Certaines conditions générales s'appliquent à tout titulaire d'un nom de domaine;

– Un contrat d'agent est assorti de garanties;

– Une personne qui estime que ses droits sont lésés peut introduire un recours dans le cadre d'un règlement alternatif de litiges;

– La loi du 26 juin 2003 relative à l'enregistrement abusif des noms de domaine est conforme aux conditions générales imposées par la DNS, mais elle est également applicable aux noms de domaines ayant d'autres extensions (par exemple, .com);

– Une protection technique est prévue contre la libération («quarantaine») ou la reprise («*trade*») involontaire;

– Toutes les autres lois: la loi sur les pratiques de commerce loyales, les lois relatives à la propriété intellectuelle.

Le règlement alternatif des litiges vise à permettre à un tiers lésé de récupérer, par une procédure juridique rapide et professionnelle, le nom de domaine qu'il revendique. Chaque titulaire d'un nom de domaine est tenu de se soumettre à cette procédure et d'accepter les conséquences de la décision qui est prise. L'appréciation est confiée à un juriste professionnel spécialisé en droits

beoordeling gebeurt door een professionele jurist specialist in het intellectuele eigendomsrecht met kennis van de ICT-wereld, die binnen een termijn van zes weken uitspraak doet.

De .be-zone is bij de allereerste met een land verbonden extensies die een systeem van arbitrage heeft ingevoerd. Om de drempel voor de instelling van een beroep te verlagen, betaalt DNS bovendien sinds 2007 50% van de gemaakte kosten terug indien de klager het pleit wint.

De spreker somt de prioriteiten van DNS.BE op:

– De robuustheid van de systemen moet worden gehandhaafd en verbeterd: de nameservers (telefooncentrale) worden zoveel mogelijk geografisch verspreid, aanvallen worden gelocaliseerd, het registratiesysteem is permanent beschikbaar en heeft zeer veel bandbreedte en back-upsites;

– Externe controle en toetsing moeten het behoud van kwaliteit waarborgen: een externe firma (Deloitte) voert technische audits uit, in het strategisch comité van DNS hebben experts zitting en er wordt aan benchmarking met andere landen gedaan;

– Het vertrouwen dient te worden bevorderd door volledige transparantie, die op de website en in jaarverslagen tot uiting komt; op financieel vlak gebeurt dat door de publicatie van resultaten en via een audit.

Het door DNS uitgetekende model is succesvol, wat blijkt uit de keuze van de Europese Commissie voor een soortgelijk beheer van de .eu-zone en uit het feit dat de .be-extensie de voorkeur van bedrijven geniet. Belangrijke beleidsopties zijn ook de uitsluiting van «*domain name tasting*» (het gratis ter beschikking stellen van domeinnamen gedurende enkele dagen, wat in andere landen tot misbruik leidt door het tijdelijk gebruiken van een naam met malafide bedoelingen) en de grote toegankelijkheid (het behoud van een domeinnaam kost amper 3 euro per jaar).

6. Uiteenzetting van de heer Pierre Bruyère, directeur van «Belnet»

«Belnet» is oorspronkelijk het netwerk van de onderzoeksinstellingen (momenteel zijn er 165 aangesloten instellingen van alle aard met in totaal meer dan 600.000 gebruikers). Belnet is sedert 1993 een pionier van het internet in België. De wet van 7 mei 1999 heeft er een Staatsdienst met afzonderlijk beheer van gemaakt die ressorteert onder de programmatorische overheidsdienst Wetenschapsbeleid. Er werken 35 personen, waarvan een beetje minder dan de helft zich bezighoudt met netwerken en met internetdiensten.

de propriété intellectuelle qui connaît le monde de la TIC et qui se prononce dans un délai de six semaines.

La zone .be est l'une des toutes premières extensions liées à un pays à avoir instauré un système d'arbitrage. Pour abaisser le seuil d'introduction d'un recours, depuis 2007, DNS rembourse de surcroît 50% des frais exposés si le plaignant obtient gain de cause.

L'orateur énumère les priorités de DNS.BE:

– La robustesse des systèmes doit être maintenue et renforcée: les serveurs de nom (centrales téléphoniques) sont autant que possible répartis géographiquement, les attaques sont localisées, le système d'enregistrement est accessible en permanence et dispose d'une très grande largeur de bande et de sites de secours;

– Le contrôle et la surveillance externes sont là pour garantir le maintien de la qualité: une entreprise externe (Deloitte) effectue les audits techniques, des experts siègent au comité stratégique de DNS et un benchmarking est réalisé avec les autres pays;

– La confiance doit être renforcée par une transparence totale, qui s'exprime sur le site internet et dans les rapports annuels; sur le plan financier, cette transparence s'exprime par la publication des résultats et la réalisation d'un audit.

Le modèle élaboré par DNS remporte un franc succès, comme le démontre le choix de l'Union européenne pour une gestion similaire de la zone .eu et le fait que l'extension .be remporte les faveurs des entreprises. Parmi les options politiques importantes, on soulignera encore l'exclusion du «*domain name tasting*» (la mise à disposition gratuite de noms de domaine pendant quelques jours, qui donne lieu à des abus dans d'autres pays du fait de l'utilisation temporaire d'un nom par des personnes malintentionnées) et la grande accessibilité (la conservation d'un nom de domaine coûte à peine 3 euros par an).

6. Exposé de M. Pierre Bruyère, directeur de «Belnet»

«Belnet» est initialement le réseau des instituts de recherche (pour l'instant, 165 instituts de tout type, totalisant plus de 600.000 utilisateurs, y sont affiliés). Depuis 1993, Belnet est un pionnier de l'Internet en Belgique. La loi du 7 mai 1999 en a fait un service de l'État à gestion séparée qui relève du service public de programmation politique scientifique. Il emploie 35 personnes, dont un peu plus de la moitié s'occupe des réseaux et services en ligne.

Belnet heeft zijn eigen noodinterventieteam CERT («*Computer Emergency Response Team*»), dat in juli 2004 werd opgericht en bemand wordt door twee personen. Deze laatsten houden zich bezig met alle veiligheidsincidenten die de gebruikers signaleren. Zij staan ook te hunner beschikking inzake technische bijstand en als veiligheidsexperts. Zowel preventie als vorming zijn een zeer belanrijk aspect van dit CERT. De jongste jaren is het aantal incidenten haast verdubbeld. Het CERT van Belnet is lid van de internationale gemeenschap van noodinterventieteams (op Europees niveau, «*Trusted Introduced*», op mondiaal niveau, «*FIRST*»). Het heeft een bevoorrechte relatie met de FCCU. Behalve het CERT van de Navo, is het CERT van Belnet het enige publieke CERT. Tijdens de recente aanval op Estland heeft het CERT van Belnet als Belgisch contactpunt gefungeerd.

De veiligsheidsketen is maar zo sterk als de zwakste van zijn schakel, met name de individuele gebruiker. Er is nood aan sensibilisering en vorming van deze laatste. Ingeval van bedreiging, aanval of panne, moet zeer vlug worden gereageerd. Het aantal actoren (de telecombedrijven, de internetaanbieders, enz.) is talrijk. Ze moeten in een mum van tijd zowel nationaal als internationaal gecoördineerd worden.

De oprichting van een nationale CERT is daarom een prioriteit.

Dit nationale noodinterventieteam moet echter neutraal zijn omdat het gebruikers heeft die zowel uit de openbare als uit de commerciële sector komen. Het moest vierentwintig uur per dag en zeven dagen per week paraat staan. Het moet echte veiligheidsspecialisten hebben die ervaring hebben met een echt operationeel netwerk en internationaal erkend zijn. Alle voornoemde actoren moeten een contactpunt leveren.

7. Vragen en opmerkingen van de leden

A. Vragen aan de heer Rudi Smit

De heer Roel Deseyn (CD&V – N-VA) onderschrijft het pleidooi voor meer aandacht en middelen voor de beveiligingsopdrachten van het BIPT. Is de heer Smet van oordeel dat de coördinatie van de ICT-beveiliging in België het best onder het BIPT ressorteert? Is samenwerking met Belnet, dat over een eigen CERT-groep beschikt, raadzaam? Zal België tijdig klaar zijn voor de nieuwe verplichtingen die de EU zal opleggen? Dient DNS zorgvuldiger te werk te gaan bij de toekenning van .be-domeinnamen?

Belnet dispose de sa propre équipe d'intervention CERT («*Computer Emergency Response Team*»), qui a été créée en juillet 2004 et se compose de deux personnes. Ces dernières s'occupent de tous les incidents de sécurité signalés par les utilisateurs et se tiennent également à la disposition de ces derniers pour leur fournir une assistance technique et en tant qu'experts en matière de sécurité. La prévention comme la formation constituent un élément très important de ce CERT. Ces dernières années, le nombre d'incidents a pratiquement doublé. Le CERT de Belnet est membre de la communauté internationale des équipes d'intervention d'urgence («*Trusted Introduced*» au niveau européen, «*FIRST*» à l'échelle mondiale). Il entretient des relations privilégiées avec la FCCU. À l'exception du CERT de l'OTAN, le CERT de Belnet est le seul CERT public. Lors de la récente attaque contre l'Estonie, le CERT de Belnet a fait office de point de contact belge.

La résistance de la chaîne de sécurité est à l'image de celle de son maillon le plus faible, c'est-à-dire l'utilisateur individuel. Il est nécessaire de sensibiliser et de former ce dernier. En cas de menace, d'attaque ou de panne, la réaction doit être très rapide. Le nombre d'acteurs (les entreprises de télécommunication, les fournisseurs Internet, etc.) est considérable. En un clin d'œil, il faut coordonner leur action, tant à l'échelle nationale qu'internationale.

La création d'un CERT national est par conséquent une priorité.

Cette équipe nationale d'intervention d'urgence doit toutefois être neutre parce qu'elle compte des utilisateurs issus du secteur public et du secteur commercial. Elle doit être opérationnelle vingt-quatre heures sur vingt-quatre, sept jours sur sept et se composer de vrais spécialistes en matière de sécurité qui ont de l'expérience en matière de réseau opérationnel et sont reconnus comme tels à l'échelle internationale. Tous les acteurs précités doivent fournir un point de contact.

7. Questions et observations des membres

A. Questions à M. Rudi Smit

M. Roel Deseyn (CD&V – N-VA) réclame, lui aussi, davantage d'attention et de moyens pour les missions de sécurisation de l'IBPT. M. Smit estime-t-il préférable que la coordination de la sécurisation TIC en Belgique relève de l'IBPT? La collaboration avec Belnet, qui dispose d'un groupe CERT propre, est-elle opportune? La Belgique sera-t-elle prête dans les temps pour les nouvelles obligations qui seront imposées par l'Union européenne? DNS doit-il faire preuve de plus de rigueur en accordant des noms de domaine .be?

De heer Guido De Padt (Open Vld) hekelt de grote versnippering van het beleid inzake ICT-veiligheid. Zou er niet beter één instantie bevoegd worden gemaakt voor een volledige coördinatie of integratie van het beleid? Zou het uittekenen van het beleid niet best door slechts één minister gebeuren?

De heer François Bellot (MR) verdedigt de oprichting van één agentschap, dat als platform voor alle aspecten van het veiligheidsbeleid kan fungeren.

B. Vragen aan mevrouw Cécile Coppin

De heer Guido De Padt (Open Vld) vraagt of er een overzicht bestaat van het aantal acties dat door de eenheid «Internetbewaking» is doorgevoerd. Worden de operatoren – die uiteraard zoveel mogelijk omzet nastreven – verzocht om op te treden tegen malafide dienstenaanbieders? Bestaan er wettelijke mogelijkheden om operatoren te dwingen een eind te maken aan de oplichtingspraktijken?

De heer Roel Deseyn (CD&V – N-VA) wenst te vernemen of met de Ombudsdienst voor de telecommunicatie een protocol is afgesproken. Zal de Ethische Code aan alle operatoren kunnen worden opgelegd?

Mevrouw Valérie De Bue (MR) vraagt of de FOD Economie de Ethische Code zal opstellen?

De heer François Bellot (MR) vraagt hoe men in het raam van de «e-commerce» enige vorm van controle kan opleggen, desnoods door de dienstenaanbieder zelf, om frauduleuze praktijken tegen te gaan. Hoe kunnen toevallige van professionele verkopers worden onderscheiden? Wanneer men via een Duitse internetsite in de Verenigde Staten een goed besteld dat in Italië moet geleverd worden door een Duitse transporteur, welke autoriteit is dan gemachtigd om op te treden? Hoe wordt in zo'n geval de bestemmeling geïdentificeerd?

C. Vragen aan de heer Michel De Coster

De heer Roel Deseyn (CD&V – N-VA) vraagt of de FOD Financiën voldoende maatregelen neemt om de persoonlijke levenssfeer van burgers te beschermen. Dreigt het systematisch bijhouden van de gegevens van wie op het netwerk van de FOD inlogt niet aanleiding te geven tot misbruiken? Wordt de toegang tot die gegevens strikt beperkt tot personen die in het kader van hun functie bevoegd zijn om er kennis van te nemen?

M. Guido De Padt (Open Vld) fustige le grand morcellement de la politique en matière de sécurité TIC. Ne serait-il pas plus opportun de charger une seule instance de l'ensemble de la coordination ou de l'intégration de la politique? Ne serait-il pas préférable qu'un seul ministre définisse la politique?

M. François Bellot (MR) défend l'idée de la création d'une seule agence, pouvant fonctionner comme plateforme pour l'ensemble des aspects de la politique de sécurité.

B. Questions à Mme Cécile Coppin

M. Guido De Padt (Open Vld) demande s'il existe un relevé du nombre d'actions menées par la cellule «Veille sur Internet». Les opérateurs – qui cherchent bien entendu à réaliser un chiffre d'affaires maximum – sont-ils priés d'agir contre les fournisseurs de services malhonnêtes? Est-il légalement possible de contraindre des opérateurs à mettre un terme à des pratiques d'escroquerie?

M. Roel Deseyn (CD&V – N-VA) demande si un protocole a été conclu avec le service de médiation des télécommunications. Le Code éthique pourra-t-il être imposé à tous les opérateurs?

Mme Valérie De Bue (MR) demande si le SFP Économie élaborera le Code d'éthique.

M. François Bellot (MR) demande comment on peut imposer une forme quelconque de contrôle dans le cadre de l'«e-commerce», fût-ce exercé par le fournisseur de services même, afin de contrer les pratiques frauduleuses. Comment distinguer les vendeurs occasionnels des professionnels? Lorsque l'on commande, sur un site internet allemand, une marchandise aux États-Unis, qui doit être livrée en Italie par un transporteur allemand, quelle est l'autorité habilitée à intervenir? Comment identifie-t-on, en pareilles circonstances, le destinataire?

C. Questions à M. Michel De Coster

M. Roel Deseyn (CD&V – N-VA) demande si le SPF Finances prend suffisamment de mesures pour protéger la vie privée des citoyens. La conservation systématique des données des personnes qui se connectent sur le réseau du SPF ne risque-t-elle pas de donner lieu à des abus? L'accès à ces données est-il strictement limité aux personnes qui sont habilitées à en prendre connaissance dans le cadre de leur fonction?

D. Vragen aan mevrouw Christiane Rouma

De heer Roel Deseyn (CD&V – N-VA) wenst te vernemen op welke wettelijke grondslag de facturatie aan administraties en grootgebruikers in het raam van «*e-government*» stoelt.

De heer François Bellot (MR) maakt de bedenking dat ook een vertegenwoordiger van de Kruispuntbank voor de Sociale Zekerheid uitgenodigd had moeten worden. Wie is belast met de coördinatie? Het Rijksregister of het Platform?

E. Vragen aan de heer Marc Van Wesemael

De heer Roel Deseyn (CD&V – N-VA) vraagt wat de geplande investeringen van DNS in de nabije toekomst zijn. Strekt het tot aanbeveling dat er een korte preventieve controle bij de aanvraag van een domeinnaam plaatsvindt om misbruiken te verhinderen? Zo zou het onder meer mogelijk worden om de problematiek van onlinegoksites in beeld te brengen. Beschikt DNS over een toetsingspanel met vertegenwoordigers van internetorganisaties?

De heer Guido De Padt (Open Vld) wijst op de kritische opmerkingen van Len Lavens over het beleid van DNS tijdens de hoorzitting in de commissie op 16 januari 2008. Is DNS van oordeel dat sommige van zijn voorstellen overweging verdienen, bijvoorbeeld de jaarlijkse overzending van een activiteitenverslag aan het federaal parlement?

De heer Rudi Smit, uitgenodigd spreker die bet BIPT vertegenwoordigt, verwijst naar lopende projecten die ertoe strekken telefoonnummers naar adressen op het internet te vertalen. Hij is van oordeel dat de .be-zone moet worden beschouwd als een nationaal nummeringsplan, waarover de overheid strikt toezicht moet uitoefenen om misbruiken tegen te gaan. De bevoegdheid om domeinnamen aan organisaties en particulieren toe te kennen mag bij een instantie buiten de overheid berusten, althans op voorwaarde dat die instantie aan duidelijke regels wordt onderworpen en kan worden gecontroleerd. In dat kader kan worden verwezen naar de evolutie in Denemarken, waar de nationale regulator voor de telecommunicatiesector een strengere controle in het vooruitzicht stelt. Is DNS voorstander van de afsluiting van een beheerscontract met de overheid om zo de controle te versterken? DNS is een vzw, wat impliceert dat de raad van bestuur wordt aangesteld door de algemene vergadering van de leden. Wie zijn die leden? De spreker vermoedt dat de overheidsvertegenwoordigers in de raad van bestuur van DNS bij het nemen

D. Questions à Mme Christiane Rouma

M. Roel Deseyn (CD&V – N-VA) souhaiterait savoir sur quelle base légale repose la facturation aux administrations et aux gros utilisateurs dans le cadre de l'«*e-government*».

M. François Bellot (MR) fait observer qu'un représentant de la Banque-carrefour de la sécurité sociale aurait aussi dû être invité. Qui est chargé de la coordination? Le Registre national ou la Plate-forme?

E. Questions à M. Marc Van Wesemael

M. Roel Deseyn (CD&V – N-VA) demande quels sont les investissements prévus par DNS dans un futur proche. Est-il recommandé d'effectuer un bref contrôle préventif lors de la demande d'un nom de domaine pour éviter les abus? Ainsi, il serait notamment possible de cerner la problématique des sites de jeux de hasard en ligne. DNS dispose-t-il d'un panel de contrôle comprenant des représentants des organisations internet?

M. Guido De Padt (Open Vld) attire l'attention sur les observations critiques de Len Lavens sur la politique de DNS lors de l'audition en commission du 16 janvier 2008. DNS estime-t-il que certaines de ses propositions méritent d'être prises en considération, par exemple la transmission annuelle d'un rapport d'activités au parlement fédéral?

M. Rudi Smit, orateur invité représentant l'IBPT, renvoie aux projets en cours qui visent à traduire les numéros de téléphone en adresses Internet. Il estime que la zone .be doit être considérée comme un plan national de numérotation, sur lequel les pouvoirs publics doivent exercer un contrôle strict, afin de lutter contre les abus. Le pouvoir d'attribuer des noms de domaine à des organisations et des particuliers peut être confié à une instance extérieure aux autorités, à condition du moins que cette instance soit soumise à des règles claires et puisse être contrôlée. Dans ce cadre, on peut référer à l'évolution observée au Danemark, où le régulateur national du secteur des télécommunications prévoit un contrôle plus strict. DNS est-il partisan de la conclusion d'un contrat de gestion avec les pouvoirs publics afin de renforcer ainsi le contrôle? DNS est une ASBL, ce qui implique que le conseil d'administration est désigné par l'assemblée générale des membres. Qui sont ces membres? L'orateur suppose que les représentants des pouvoirs publics au conseil d'administration n'ont pas de voix prépondérante lors de la prise de décisions. Les

van beslissingen geen doorslaggevende stem hebben. Kunnen particulieren in het kader van de alternatieve geschillenbeslechting een beroep instellen bij Cepina, een onderdeel van het VBO, of wordt die mogelijkheid voorbehouden aan bedrijven?

F. Vragen aan de heer Pierre Bruyère

De heer Roel Deseyn (CD&V – N-VA) wenst te vernemen of de sterstructuur – die de acties moet coördineren ingeval van problemen – niet onder de voogdij van het BIPT behoort te staan. Hoe kan worden vermeden dat twee noodinterventieteams (CERT's), een bij Belnet en een ander die nationaal is, operationeel worden? Volgens de telecomwet van 13 juni 2005 moeten de internetdienstenaanbieders (ISP's) de gebruikers zoveel mogelijk middelen aanreiken om zich te beschermen? Zijn deze voorwaarden wel realistisch of moeten ze nog worden bijgeschaafd?

De heer Guido De Padt (Open Vld) vraagt of bij Belnet geen investerings- en actieplan nodig is om het hoofd te bieden aan toekomstige veiligheidsincidenten?

8. Antwoorden van de genodigde sprekers

A. Antwoorden van de heer Rudi Smit

De snelle oprichting van een gouvernementele CERT in België, die onafhankelijk van alle betrokken partijen moet kunnen optreden, is een must. Belnet beschikt over een beperkt CERT-team, dat zich enkel inlaat met de problemen van de eigen klanten. In Finland slaagt de nationale regulator van de telecommunicatiesector, die voor het gouvernementele CERT bevoegd is, er in om bij incidenten in zeer korte tijd actie te ondernemen; zo kan een website met illegale inhoud, anders dan in België, binnen een tijdsbestek van 30 minuten worden afgesloten. De integratie van de CERT en netwerkbeveiliging is wenselijk omdat daardoor veiligheidsincidenten in bedrijven buiten het kader van een strafrechtelijk onderzoek kunnen worden behandeld; de CERT moet dan ook de bevoegdheid krijgen om bepaalde maatregelen daadwerkelijk af te dwingen, maar blijft daarnaast vooral een coördinerende rol vervullen.

Het CERT kan het best worden ondergebracht bij het BIPT omdat dat instituut thans reeds kan steunen op een ruime nationale en internationale samenwerking en

particuliers peuvent-ils, dans le cadre du règlement alternatif de litiges, introduire un recours auprès du Cepani, une composante de la FEB, ou cette possibilité est-elle réservée aux entreprises?

F. Questions à M. Pierre Bruyère

M. Roel Deseyn (CD&V – N-VA) demande si la structure en étoile – qui doit coordonner les actions en cas de problèmes – ne doit pas être placée sous la tutelle de l'IBPT. Comment éviter que deux équipes d'intervention d'urgence (CERT), une chez Belnet et une autre, nationale, deviennent opérationnelles? En vertu de la loi du 13 juin 2005 relative aux communications électroniques, les fournisseurs de services Internet (ISP) doivent, dans la mesure du possible, donner aux utilisateurs le plus possible de moyens de se protéger. Ces conditions sont-elles effectivement réalistes ou doivent-elles encore être adaptées?

M. Guido De Padt (Open Vld) demande s'il n'est pas nécessaire de prévoir, chez Belnet, un plan d'action et d'investissement pour faire face à de futurs incidents de sécurité.

8. Réponses des orateurs invités

A. Réponses de M. Rudi Smit

La création rapide d'un CERT gouvernemental en Belgique, qui puisse intervenir indépendamment de toutes les parties concernées, est indispensable. Belnet dispose d'une équipe CERT limitée, qui s'occupe uniquement des problèmes de ses propres clients. En Finlande, le régulateur national du secteur des télécommunications, qui a compétence en ce qui concerne le CERT gouvernemental, parvient à entreprendre des actions à très court terme en cas d'incident; ainsi, contrairement à ce qui se passe en Belgique, un site Internet à contenu illégal peut être fermé dans un délai de trente minutes. L'intégration du CERT et de la sécurisation de réseaux est souhaitable, car cela permet de traiter les incidents de sécurité survenus dans les entreprises en dehors du cadre d'une enquête pénale; le CERT doit par conséquent être habilité à imposer réellement le respect de certaines mesures, mais il continuera à se charger principalement de la coordination.

Il est préférable d'intégrer le CERT dans l'IBPT, parce que cet institut peut déjà s'appuyer sur une vaste coopération, tant nationale qu'internationale, et qu'il dispose

over de meeste expertise beschikt. Het huidige wettelijke kader van het BIPT veroorzaakt echter moeilijkheden: het instituut is enkel bevoegd voor netwerken en diensten van elektronische communicatie die moeten worden aangemeld, terwijl sommige netwerken (bijvoorbeeld Swift) van die meldingsplicht zijn vrijgesteld en ook niet aan de regelgeving op het vlak van beveiliging onderworpen zijn. Een verruiming van de bevoegdheden van het BIPT is derhalve noodzakelijk, maar dit impliceert ook een uitbreiding van mensen en middelen.

Het ICT-beleid ressorteert thans onder de bevoegdheid van elf departementen en vijf ministers, waardoor er «gaten» in het beleid ontstaan, aspecten die door geen enkele instantie worden geregeld. De bevoegdheid voor ICT zou het best aan één enkele minister worden toevertrouwd omdat dat de ontwikkeling van een integraal en samenhangend beleid zou bevorderen. Omdat telecommunicatie een transversaal gegeven in de samenleving is, zou het anderzijds niet verstandig zijn om de volledige beveiliging op het terrein door één instantie te laten uitwerken; een poging van de EU om dergelijke concentratie tot stand te brengen, is trouwens mislukt. Wel strekt het tot aanbeveling dat een bepaalde instantie de residuaire bevoegdheid inzake ICT-veiligheid krijgt (om te vermijden dat reactie op een incident of crisis uitblijft).

Elk overheidsdepartement behoudt voor het overige een eigen verantwoordelijkheid, maar het zwaartepunt van de actie moet liggen bij de FOD Fedict, de instantie die verantwoordelijk is voor het ICT-beleid in de federale departementen, en bij het BIPT, dat vooral waakt over private actoren.

B. Antwoorden van mevrouw Cécile Coppin

b.1 Cijfers acties

Eventuele cijfers over de acties ondernomen door de eenheid «Internetbewaking» kunnen apart worden meegedeeld.

b.2 Waaier acties

De economische politie heeft een hele waaier van acties ter beschikking: bevel tot staking van de frauduleuze praktijk, voorstel tot een administratief vergelijk, mededeling van het proces-verbaal aan de procureur des Konings. Als gevolg van het optreden van de FOD Economie bij de operatoren wordt de benadeelde consument over het algemeen vergoed.

b.3 Houding operatoren

Inzake dienstverlening van het informatiebedrijf voorziet de reglementering in een vrijstellingsregeling met betrekking tot de verantwoordelijkheid van de tussenoperatoren zolang zij niet actief weet hebben van

de la plus grande expertise. Le cadre légal actuel de l'IBPT est toutefois source de difficultés: l'institut n'a compétence que pour les réseaux et les services de communication électronique qui doivent être annoncés, tandis que certains réseaux (Swift, par exemple) sont dispensés de cette obligation de notification et ne sont pas non plus soumis à la réglementation en matière de sécurisation. Il est dès lors nécessaire d'élargir les compétences de l'IBPT, mais cela implique également une extension du personnel et une augmentation des moyens.

La politique en matière de TIC relève actuellement de la compétence de onze départements et de cinq ministres, ce qui crée des lacunes dans cette politique dont certains aspects ne sont régis par aucune instance. Il serait préférable de confier la politique en matière de TIC à un seul ministre, parce que cela favoriserait l'élaboration d'une politique complète et cohérente. Par ailleurs, étant donné que les télécommunications sont un aspect transversal de la société, il serait déraisonnable qu'une seule instance soit chargée de veiller à l'ensemble de la sécurisation sur le terrain; l'Union européenne a d'ailleurs échoué dans sa tentative de mettre en œuvre ce type de concentration. Il est néanmoins recommandé qu'une instance donnée soit investie de la compétence résiduelle en matière de sécurité des TIC (afin d'éviter l'absence de réaction à un incident ou une crise).

Chaque département public conserve du reste sa responsabilité, mais le centre de gravité de l'action doit se situer au SPF Fedict, l'instance responsable de la politique en matière de TIC des départements fédéraux, et à l'IBPT, qui surveille principalement les acteurs privés.

B. Réponses de Mme Céline Coppin

b.1 Données chiffrées des actions

Les éventuelles données chiffrées des actions entreprises par l'unité «Veille sur Internet» peuvent être communiquées séparément.

b.2 Eventail d'activités

La police économique a tout un éventail d'actions à sa disposition: injonction de cesser la pratique frauduleuse, proposition de transaction administrative, communication du procès-verbal au procureur du Roi. Suite aux interventions du SPF Economie auprès des opérateurs, le consommateur lésé est de manière générale indemnisé.

b.3 Attitude des opérateurs

En matière de services de la société de l'information, la réglementation prévoit un régime d'exonération de responsabilité des prestataires intermédiaires tant qu'ils n'ont pas effectivement connaissance d'un activité illicite

een onwettige activiteit op hun net. Nadat hij evenwel op de hoogte is gesteld van een ontoelaatbare activiteit, kan de operator beschouwd worden als medeplichtige als hij niet alles in het werk stelt om een eind te maken aan voornoemde praktijk als hij in de mogelijkheid was dat te doen.

b.4 Verschil met Ombudsdienst

De Algemene Dienst Controle en Bemiddeling van de FOD Economie heeft andere bevoegdheden dan de Ombudsdienst voor de telecommunicatie: deze laatste behandelt geschillen tussen een telecomgebruiker en een telecomoperator, daar waar voornoemde dienst van de FOD Economie ontloetbare praktijken behandeld tussen kopers en verkopers waarvoor het internet slechts een middel is waarmee het vergelijk tot stand komt. Deze dienst kan bovendien repressief optreden. Voor tarieven van betalende sms'jes is het BIPT verantwoordelijk.

b.5 Ethische Code

Bij het opstellen van deze Code zal beroep gedaan kunnen worden op de ervaring met consumentenzaken van de FOD Economie.

b.6 E-commerce

Sites als «e-Bay» zouden zelf meer de identiteit van de verkopers moeten checken. De eenheid «Internetbewaking» kan steeds een onderzoek instellen om na te gaan of de verkoper een toevallige verkoper of een regelrechte handelaar is.

b.7 Buitenlandse sites

De toepasselijke wet is die van de plaats waar de commerciële activiteit plaatsvindt.

C. Antwoorden van de heer Michel De Coster

Elke ambtenaar moet zich identificeren om toegang te krijgen tot het netwerk van de FOD Financiën. De bevoegdheid om toegang te verkrijgen tot bepaalde gegevens wordt toegekend aan groepen gebruikers, die door de administratie worden afgebakend in functie van hun respectieve opdrachten. De opstelling van «journaals» van personen die bepaalde gegevens hebben geraadpleegd, creëert juist de mogelijkheid om misbruiken of een foutieve groepsafbakening op te sporen.

D. Antwoorden van mevrouw Christiane Rouma

d.1 Wettelijke basis facturatie

De wettelijke basis voor de facturatie dor het Rijksregister is het koninklijk besluit van 2 april 2003 betref-

sur leur réseau. Cependant, après avoir été informé d'une activité illicite, l'opérateur peut être considéré comme complice s'il ne met pas tout en œuvre pour faire cesser la pratique précitée alors qu'il était en mesure de le faire.

b.4 Différence avec le Service de médiation

Les compétences de la Direction générale du Contrôle et de la Médiation du SPF Économie sont différentes de celles du Service de médiation des télécommunications: ce dernier traite les litiges entre un utilisateur de télécommunication et un opérateur de télécommunication, alors que le service précité du SPF Économie traite des pratiques illicites entre des acheteurs et des vendeurs, l'Internet n'étant que l'instrument par le biais duquel se réalise la transaction. Ce service peut en outre agir de façon répressive. L'IBPT est responsable des tarifs des SMS.

b.5 Code d'éthique

L'expérience du SPF Economie dans le domaine de la protection de la consommation pourra être utilisée lors de l'élaboration de ce Code.

b.6 E-commerce

Des sites comme «e-Bay» devraient eux-mêmes vérifier l'identité des vendeurs. L'unité «Veille sur Internet» peut toujours ouvrir une enquête afin de vérifier si le vendeur est un vendeur occasionnel ou un véritable commerçant.

b.7 Sites étrangers

La loi applicable est celle du lieu de l'activité commerciale.

C. Réponses de M. Michel De Coster

Tout fonctionnaire doit s'identifier pour accéder au réseau du SPF Finances. La compétence d'accéder à certaines données est accordée à des groupes d'utilisateurs, qui sont définis par l'administration en fonction de leurs missions respectives. La tenue d'un «journal» des personnes qui ont consulté certaines données crée précisément la possibilité de dépister des abus ou des erreurs dans la définition du groupe.

D. Réponses de Mme Christiane Rouma

d.1 Fondement légal de la facturation

Le fondement légal de la facturation par le Registre national est l'arrêté royal du 2 avril 2003 relatif aux

fende de vergoedingen waartoe de prestaties van het Rijksregister van de natuurlijke personen aanleiding geven. De principes van deze regeling zijn de volgende: de actualisering van de gegevens die door de autoriteiten worden aangedragen is kosteloos; voor een hele waaier aan autoriteiten gelden degressieve tarieven naargelang van de consultaties die ze uitvoeren; specifieke verrichtingen worden aangerekend tegen een tarief waarvan zowel het minimum als het maximum is vastgelegd; een aantal organismen naargelang van het standaardvolume gegevens dat wordt opgevraagd, betalen een forfaitaire vergoeding. Het Rijksregister heeft het statuut van Staatsdienst met afzonderlijk beheer.

d.2 Wettelijke periode registratie

De toegang tot het Rijksregister is nooit automatisch. De periode waarin al de gegevens met betrekking tot de toegang en de aanvragen wordt geregistreerd, bedraagt vijf jaar.

d.3 Samenwerking Kruispuntbank

De Kruispuntbank voor de Sociale Zekerheid is de grootste klant van het Rijksregister.

d.4 Transparantie Rijksregister

Krachtens de wet van 25 maart 2003 (voluit wet tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen) heeft de burger zes maand om te checken wie zijn dossier heeft geraadpleegd.

E. Antwoorden van de heer Marc Van Wesemael

De middelen waarover DNS beschikt, worden in overeenstemming met haar statutaire doelstellingen gebruikt. De ontwikkeling en de beveiliging van een efficiënt en kwalitatief platform is haar prioritaire doelstelling.

De leden van de algemene vergadering van DNS worden vermeld in het jaarverslag.

Elke vorm van preventieve controle op de toekenning van domeinnamen door DNS of een andere instantie zou problematisch zijn: het verleden heeft aangetoond dat de regels steeds van hun ratio legis kunnen worden afgewend. De invoering van voorafgaande procedures zou dus weinig voordeel opleveren bij de strijd tegen websites met een illegale inhoud.

DNS gaat permanent het debat aan met organisaties die op het domein van ICT actief zijn:

– Bedrijvenfederaties hebben zitting in de raad van bestuur van DNS;

rétributions auxquelles donnent lieu les prestations du Registre national des personnes physiques. Les principes de cette réglementation sont les suivants: l'actualisation des données fournies par les autorités est gratuite; des tarifs dégressifs sont prévus pour toute une série d'autorités, en fonction des consultations qu'ils effectuent; les opérations spécifiques sont facturées à un tarif dont le minimum et le maximum ont été fixés; une série d'organismes payent une rétribution forfaitaire en fonction du volume standard de données sollicitées. Le Registre national a un statut de service de l'État à gestion séparée.

d.2 Période légale d'enregistrement

L'accès au Registre national n'est jamais automatique. La période d'enregistrement de toutes les données relatives à l'accès et aux demandes est de cinq ans.

d.3 Collaboration avec la Banque-carrefour

La Banque-carrefour de la Sécurité sociale est le client principal du Registre national.

d.4 Transparence du Registre national

En vertu de la loi du 25 mars 2003 (loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques), le citoyen dispose de six mois pour vérifier qui a consulté son dossier.

E. Réponses de M. Marc Van Wesemael

Les moyens dont dispose DNS sont utilisés conformément à ses objectifs statutaires. Le développement et la sécurisation d'une plate-forme efficace et de qualité constituent son objectif prioritaire.

Les membres de l'assemblée générale de DNS sont mentionnés dans le rapport annuel.

Toute forme de contrôle préventif sur l'attribution de noms de domaine par DNS ou une autre instance serait problématique: il s'est avéré dans le passé que les règles peuvent toujours être détournées de leur ratio legis. L'instauration de procédures préalables ne serait donc pas très utile dans le cadre de la lutte contre les sites internet ayant un contenu illégal.

DNS est constamment en discussion avec les organisations actives dans le domaine de la TIC:

– Des fédérations d'entreprises siègent au conseil d'administration de DNS;

– DNS is ingeschreven op de mailinglijsten van US-CERT (*United States Computer Emergency Readiness Team)* om snel toegang te hebben tot informatie over veiligheidsproblemen in de systemen die eventueel ook door haar zouden gebruikt worden.

Niet alle opmerkingen die door *securitybloggers* worden gemaakt, zijn correct; dat geldt ook voor de kritiek die door Len Lavens wordt geformuleerd, al wordt die wel steeds met de nodige aandacht geanalyseerd. DNS handelt zo transparant mogelijk, al is zij natuurlijk voorzichtig met de verspreiding van informatie over bepaalde aspecten van haar veiligheidsbeleid.

Wie zijn recht op een domeinnaam geschonden acht, kan op de website van DNS nagaan wie de domeinnaam waarop hij aanspraak maakt, heeft verkregen. Hij kan dan met de betrokken persoon of instantie contact opnemen en vervolgens eventueel een rechtszaak opstarten of opteren voor een procedure van alternatieve geschillenbeslechting, die tegen betaling van 1.600 euro (die voor de helft wordt terugbetaald als de klager het pleit wint) voor bedrijven, instellingen, verenigingen en natuurlijke personen openstaat. Als de gegevens op de website van DNS niet correct zijn, onderzoekt DNS op verzoek van de klager de identiteit van de houder van de domeinnaam.

De technologie om telefoonnummers naar internetadressen te vertalen, blijkt weinig succesvol te zijn: landen die geprobeerd hebben om die technologie te implementeren, zijn er ondertussen al mee gestopt.

Tot besluit beklemtoont de spreker dat het internet in eerste instantie een zelfregulerend organisme is. Als dat niet het geval was geweest, zou het nooit zo snel tot ontwikkeling zijn gekomen; enige terughoudendheid bij de invoering van strenge reglementering lijkt daarom raadzaam. De overheid neemt overigens thans reeds deel aan de mechanismen van zelfregulering, wat onder meer blijkt uit het feit dat het BIPT, als vertegenwoordiger van de Belgische overheid, deelneemt aan het GAC, een van de reguleringsorganen van de ICANN.

– DNS est inscrit sur les listes de diffusion de US-CERT (*United States Computer Emergency Readiness Team*) pour pouvoir accéder rapidement aux informations relatives aux probèmes de sécurité qui surviennent dans les systèmes qu'il utiliserait éventuellement également.

Toutes les remarques effectuées par les *securitybloggers* ne sont pas nécessairement correctes; il en va de même pour la critique formulée par Len Lavens, même si elle est toujours analysée avec l'attention requise. DNS agit de manière aussi transparente que possible, même s'il fait bien sûr preuve de prudence en ce qui concerne la diffusion d'informations sur certains aspects de sa politique de sécurité.

Toute personne qui estime que son droit à un nom de domaine a été violé peut vérifier sur le site internet de DNS qui a obtenu le nom de domaine qu'il réclame. Elle peut alors prendre contact avec la personne ou instance concernée et ensuite éventuellement entamer une procédure judiciaire ou opter pour une procédure de règlement alternatif des litiges, qui est ouverte aux entreprises, aux institutions, aux associations et aux personnes physiques contre paiement de 1.600 euros (remboursés pour moitié si le plaignant l'emporte). Si les données sur le site de DNS ne sont pas correctes, DNS recherche, à la demande du plaignant, l'identité du détenteur du nom de domaine.

Il s'avère que la technologie permettant de convertir des numéros de téléphone en adresses internet remporte peu de succès: les pays qui ont tenté de mettre en œuvre cette technologie l'ont entre-temps déjà abandonnée.

En guise de conclusion, l'orateur souligne que l'internet est en première instance un organisme autorégulé. Si ce n'était pas le cas, il ne se serait jamais développé aussi vite; c'est pourquoi il semble opportun de faire preuve d'une certaine réserve en ce qui concerne l'instauration d'une réglementation sévère. En effet, les autorités participent déjà actuellement aux mécanismes d'autorégulation, ce qui ressort notamment du fait que, en tant que représentant de l'autorité belge, l'IBPT participe au GAC, qui est un des organes de régulation de l'ICANN.

F. Antwoorden van de heer Pierre Bruyère

Het CERT van Belnet zou een nationale CERT kunnen bijstaan door het verzamelen en verspreiden van informatie en zich te beperken tot de eigen gebruikers. Het probleem is overigens niet alleen of de internetdienstenaanbieders meer wettelijke verplichtingen inzake beveiliging moeten krijgen. De sensibilisering van de gebruikers schiet tekort. De kritiek van de heer Len Lavens op Belnet is onterecht vermits het veiligheidsprobleem dat door hem werd aangekaart sloeg op een server van de RTBf, die niet door Belnet wordt beheerd.

De rapporteur, *De voorzitter,*

Roel DESEYN François BELLOT

F. Réponses de M. Pierre Bruyère

Le CERT de Belnet pourrait seconder un CERT national en rassemblant et en diffusant des informations et en se limitant à ses propres utilisateurs. Le problème n'est d'ailleurs pas seulement de savoir si les fournisseurs de services internet doivent être investis d'un plus grand nombre d'obligations légales en matière de sécurisation. La sensibilisation des utilisateurs n'est pas suffisante. La critique de Belnet de M. Len Lavens n'est pas fondée, étant donné que le problème de sécurité qu'il a abordé concernait un serveur de la RTBf, qui n'est pas géré par Belnet.

Le rapporteur, *Le président,*

Roel Deseyn François Bellot

Centrale drukkerij – Deze publicatie wordt uitsluitend gedrukt op volledig gerecycleerd papier
Imprimerie centrale – Cette publication est imprimée exclusivement sur du papier entièrement recyclé