CHAMBRE DES DEPUTES

Session ordinaire 2010-2011

AT/vg

Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace

Procès-verbal de la réunion du 18 juillet 2011

ORDRE DU JOUR :

1. Adoption des projets de procès-verbal des réunions des 27 juin et 4 juillet 2011

2. Présentation du CERT luxembourgeois (Computer Emergency Response Team) par Monsieur le Ministre

3. Prise d'une décision au sujet des motions figurant au rôle des affaires de la Commission (cf. lettre de Monsieur le Président de la Chambre des Députés du 5 juillet 2011)

4. COM (2011) 402 : Proposition de REGLEMENT DU PARLEMENT EUROPEEN ET DU CONSEIL concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union (Refonte)
Présentation et examen du respect des principes de subsidiarité et de proportionnalité (délai de réaction: 6 octobre 2011)

5. Divers

*

M. Claude Adam, Mme Diane Adehm, M. Eugène Berger, Mme Anne Brasseur, M. Fernand Kartheiser en remplacement de M. Jean Colombera, Mme Claudia Dall'Agnol, Mme Christine Doerner, M. Ben Fayot, M. Claude Haagen, M. Norbert Haupert, M. Lucien Thiel

M. Charles Goerens, membre du Parlement européen

M. François Biltgen, Ministre des Communications et des Médias

M. Jeannot Berg, M. Pierre Goerens, M. Jean-Paul Zens, du Ministère d'Etat *(Service des Médias et des Communications)*

M. Jean-Marie Laures, du Ministère d'Etat *(Centre de Communications du Gouvernement)*

M. Roland Bombardella, du Ministère d'Etat *(Haut-Commissariat à la Protection nationale)*

M. François Thill, du Ministère de l'Economie et du Commerce extérieur

(Direction du commerce électronique et de la sécurité informatique)

M. Patrick Houtsch, M. Pierre Zimmer, du Ministère de la Fonction publique et de la Réforme administrative *(Centre des Technologies de l'Information de l'Etat)*

Mme Anne Tescher, de l'Administration parlementaire

Excusés : M. Jean Colombera, M. Marcel Oberweis

*

Présidence : M. Lucien Thiel, Président de la Commission

*

1. Adoption des projets de procès-verbal des réunions des 27 juin et 4 juillet 2011

Les projets de procès-verbal sous rubrique sont adoptés.

2. Présentation du CERT luxembourgeois (Computer Emergency Response Team)[1]

Contexte

Les infrastructures critiques de l'Etat et des secteurs sensibles sont de plus en plus exposées aux nouvelles formes de cybercriminalité. Pour faire face à ces menaces, il semble essentiel que le Luxembourg dispose d'une force de réaction pour la détection et la réponse aux incidents de sécurité informatique et pour coordonner l'ensemble des acteurs.

Les infrastructures et réseaux de communications électroniques sont aujourd'hui le moteur principal de la croissance économique. Le Luxembourg étant un important centre financier international et un lieu attractif pour les entreprises actives dans le domaine des nouvelles technologies, la qualité et la sécurité des infrastructures de communications sont vitales pour le pays, tout comme la protection des données privées des citoyens est essentielle dans une société numérique. De plus, les réseaux de communications constituent également une infrastructure de base pour de nombreux autres secteurs et services et leur non-fonctionnement causerait d'importants dommages pour la population et l'économie.

Voilà pourquoi le Gouvernement a décidé la mise en place, sous l'autorité du Premier Ministre, des structures suivantes:

- un Cybersecurity board luxembourgeois

- un CERT gouvernemental (Computer Emergency Response Team)

Le CERT.lu est une structure publique capable de prendre en charge la prévention et la réponse aux incidents pour les systèmes d'informations publics et les infrastructures critiques. Le Cybersecurity board luxembourgeois aura la mission d'élaborer le plan stratégique nationale de lutte contre les cyberattaques et de veiller à la bonne exécution de ce plan.

[1] Pour de plus amples détails, il est renvoyé au document gouvernemental au sujet de l'étude CERT.lu, lequel a été diffusé le 18 juillet 2011 par courrier électronique aux membres de la Commission et qui ne peut être annexé au présent procès-verbal pour des raisons de confidentialité.

Gouvernance du CERT.lu

Le CERT.lu, compte tenu de sa mission sensible concernant les intérêts vitaux de l'Etat, est placé sous l'autorité du Ministère d'Etat. Les instances suivantes sont étroitement associées dans la gouvernance du CERT.lu : le Centre de technologies de l'information de l'Etat (CTIE), le Haut-commissariat à la protection nationale (HCPN), le Service de renseignement (SRE) ainsi que le Centre de Communications du Gouvernement (CCG) notamment par le biais de l'Agence nationale de sécurité des systèmes d'informations (ANSSI) laquelle sera créée par voie législative sous peu.

En termes de ressources humaines, un fonctionnaire du CTIE a été nommé en tant que coordinateur du CERT.lu. Il est prévu de recruter encore 6 personnes, notamment des analystes, un développeur ainsi qu'un assistant.

Missions

Le CERT.lu a pour vocation avant tout la protection des intérêts nationaux contre des attaques provoquant des dommages substantiels à son économie ou privant le pays de fonctionner normalement.

A noter que la majorité des CERTs des autres pays réalise des missions de prévention des incidents tels que la détection d'attaques, la sensibilisation, le conseil, et plus spécifiquement l'alerte sur les vulnérabilités et les attaques virales.

Actuellement, plusieurs structures de prévention et de réponse aux incidents coexistent au Luxembourg. Les domaines de compétences et les responsabilités sont variés, mais ne correspondent pas aux besoins nationaux principaux que sont :

- la nécessité d'avoir une structure publique capable de prendre en charge la prévention et la réponse aux incidents pour les systèmes d'informations du Gouvernement et des infrastructures critiques qui touchent à la sécurité nationale et représentent un enjeu majeur ;
- la nécessité d'avoir un acteur global ayant à la fois les compétences, mais également les accréditations, permettant la coordination d'attaques majeures ;
- le besoin d'avoir un acteur principal responsable, reconnu comme point de contact au niveau international, pouvant coordonner toutes les autres structures locales de réponse aux incidents, et pouvant jouer le rôle de redistribution des incidents pour les différents CERTs nationaux ayant des vocations et des périmètres précis.

Ainsi, il existe au Luxembourg des structures telles que CIRCL, CASES et SMILE, qui réalisent notamment des missions de sensibilisation et de réponse aux incidents dont le périmètre d'intervention sont les entreprises de manière générale ainsi que le grand public et les communes.

Le CERT.lu n'a pas pour vocation de remplacer ces structures dans les domaines où elles sont efficaces. Ainsi le CERT.lu n'interviendra pas au niveau des campagnes de sensibilisation qui sont réalisées par CASES auprès des services de l'Etat, des infrastructures critiques et des secteurs et organisations sensibles. Cependant, ces structures ne peuvent répondre à tous les besoins, notamment

- parce qu'elles ne sont pas exclusivement financées par le Gouvernement ou parce que leur financement nécessite la commercialisation des services, ces structures ne peuvent concentrer leurs investissements et leurs compétences sur des problématiques critiques du fait de logiques économiques divergentes ;

- parce que ces structures reposent en majeur partie sur des salariés aux contrats de travail privés, ils ne peuvent avoir accès aux informations hautement confidentielles nécessaires pour la gestion des incidents sur des infrastructures critiques et classifiées;

- parce que les besoins de prévention et de réponse aux incidents touchant les infrastructures vitales de l'Etat nécessitent un accès direct aux réseaux gérés par le Centre de technologies de l'information de l'Etat (CTIE) et le Centre de Communications du Gouvernement (CCG).

Le périmètre d'action du CERT.lu comprend en premier lieu l'administration gouvernementale, ainsi que les infrastructures critiques (p.ex. Luxtrust, EPT, Luxconnect, LU-CIX, Restena, ou encore les opérateurs du secteur de l'énergie) et les secteurs sensibles (p.ex. les opérateurs de télécommunications, le secteur financier, les hôpitaux, le secteur industriel notamment avec Goodyear, Dupont de Nemour et Arcelor, l'aéroport, Cargolux, les chambres professionnelles, la CSSF, l'Université, les centres de recherches publics etc.)

Cybersecurity board luxembourgeois

Un cybersecurtiy board sera mis en place ayant pour mission d'élaborer une stratégie nationale de lutte contre les cyberattaques. Contrairement au CERT.lu, le cybersecurity board n'a donc pas de missions opérationnelles. La stratégie devrait être finalisée en novembre 2011, lors d'une conférence des pays du Benelux au sujet de la cybersécurité.

M. le Ministre propose de présenter cette stratégie à la commission parlementaire suite à sa finalisation fin 2011.

Echange de vues

De l'échange de vues, il y a lieu de retenir succinctement les éléments suivants :

- M. le Ministre précise que le Luxembourg est bien placé pour faire de la cybersécurité un avantage compétitif.

- M. le Ministre souligne l'importance de la coopération avec le Centre interdisciplinaire SnT (*Security and Trust*) de l'Université du Luxembourg afin de soutenir et de renforcer les efforts de recherche en matière de cybersécurité.

- Un groupe de travail interministériel au sujet du *cloud computing* a été mis en place. Il s'agit d'offrir des mesures de sécurité de haute qualité au niveau du *cloud computing* ce qui attribuerait un avantage compétitif au Luxembourg.

- Le représentant du CERT.lu précise que les cyberattaques à destination de l'administration gouvernementale sont connues. Cependant, la situation des attaques au niveau du secteur secteur privé n'est pas assez connue. Voilà pourquoi il est prévu que le CERT.lu analysera dans son rapport annuel l'évolution des menaces à la cybersécurité.

- Un expert gouvernemental explique que le niveau des mesures de protection que les acteurs du secteur privé ont mis en place contre des cyberattaques est très hétérogène.

- Le CCG s'occupe de la gestion et de l'exploitation des informations classifiées et non classifiées destinées au Gouvernement luxembourgeois ou générées à son niveau. Le CCG est donc responsable tant de l'acheminement que de la sécurité des informations, que celles-ci transitent de et vers les organismes internationaux dont fait partie le Grand-Duché (OTAN, Union européenne, OSCE) ou à l'intérieur du réseau du Gouvernement ainsi que les ambassades et les représentations permanentes du Luxembourg.

3. Prise d'une décision au sujet des motions figurant au rôle des affaires de la Commission

M. le Président informe la Commission au sujet du courrier de M. le Président de la Chambre des Députés invitant les commissions parlementaires à épurer le rôle des affaires des motions et résolutions qui seraient caduques et de discuter d'une éventuelle mise à l'ordre du jour d'une séance publique de celles qui seraient d'actualité.

Il est décidé de reporter ce point à l'ordre du jour de la réunion du 15 septembre 2011.

4. COM (2011) 402 : Proposition de REGLEMENT DU PARLEMENT EUROPEEN ET DU CONSEIL concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union (Refonte)

Résumé du document

Le règlement proposé, directement applicable, introduirait pour la première fois des mesures structurelles de stimulation de la concurrence en permettant aux consommateurs qui le souhaitent, de souscrire, dès le 1er juillet 2014, à un contrat d'itinérance moins cher. Ce contrat sera distinct de leur contrat national, mais permettra au consommateur de conserver le même numéro de téléphone. La proposition prévoit une baisse progressive des plafonds actuels pour les tarifs de détail des services vocaux et de SMS et l'introduction d'un nouveau plafond pour les tarifs de détail des services de données en itinérance. D'ici au 1er juillet 2014, les consommateurs en itinérance paieraient tout au plus 24 cents la minute pour émettre un appel, 10 cents la minute pour recevoir un appel, 10 cents pour l'envoi d'un SMS et 50 cents par mégaoctet (MB) pour le téléchargement de données ou la navigation sur l'internet pendant leurs voyages à l'étranger (facturation au kilooctet utilisé).
La proposition de la Commission permettrait de remédier au manque de concurrence et de choix pour les consommateurs de la manière suivante:

- en facilitant l'entrée d'autres opérateurs sur les marchés de l'itinérance, notamment des opérateurs qui n'ont pas de réseau propre, en imposant aux opérateurs des autres Etats membres de leur ouvrir l'accès à leurs réseaux à des tarifs de gros réglementés. Cela permettrait d'intensifier la concurrence sur les marchés de l'itinérance et d'inciter ainsi les opérateurs à offrir des prix et des services plus attractifs à leurs clients.

- en laissant aux consommateurs la liberté de choisir un autre opérateur pour les services d'itinérance, quel que soit leur opérateur national. Chaque fois qu'un client passerait une frontière, il basculerait d'office sur le fournisseur de services d'itinérance choisi tout en conservant le même numéro de téléphone et le même module d'identification de l'abonné (carte SIM). Cela favoriserait la transparence et permettrait aux clients de comparer les prix pour trouver la meilleure offre d'itinérance et inciterait les opérateurs à offrir des formules d'itinérance plus concurrentielles.

En attendant que ces solutions structurelles portent tous leurs fruits, la proposition prévoit les mesures suivantes:

- l'introduction d'un nouveau plafond pour les prix de détail des services de données en itinérance ;

- le maintien des plafonds pour les prix de détail des communications vocales et des SMS en itinérance ;

- le maintien de la protection contre les «mauvaises surprises» à la réception des factures pour les services de données en itinérance ;
- le maintien des plafonds applicables aux prix de gros entre les opérateurs jusqu'en 2022 pour tous les services d'itinérance.

Conclusions de la Commission

La Commission est d'avis qu'il s'agit d'une bonne initiative législative et décide de ne pas émettre d'avis.

5. Divers

Le calendrier provisoire des réunions de la Commission pour la session 2011-2012 est distribué et repris en annexe du présent procès-verbal.

Luxembourg, le 18 juillet 2011

La secrétaire,
Anne Tescher

Le Vice-Président,
Ben Fayot

Annexe :

Calendrier provisoire des réunions de la Commission pour la session 2011-2012

Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace

Calendrier provisoire des réunions en 2011-2012

<u>En principe plage fixe jeudi à 14h30</u>

Sauf pour les semaines des séances publiques: lundi à *10h30 (en italique)*

- <u>Lundi 19 septembre</u> (évaluation CRP – suite)
- <u>Jeudi 22 septembre</u>

  - 9h : réunion jointe (commissions travail, DD, aff. int. et santé) : émetteurs d'ondes électromagnétiques

  - 10h30 : réunion jointe (commission éducation nationale) : rôle de l'Université dans le processus de réforme du système éducatif luxembourgeois

- **Jeudi 29 septembre**
- **Jeudi 6 octobre**
- *Lundi 10 octobre*
- <u>Jeudi 20 octobre</u> (Visite « journée de l'Espace » prévue pour le <u>matin)</u>
- *Lundi 24 octobre*
- **Jeudi 10 novembre**
- *Lundi 14 novembre*
- **Jeudi 24 novembre**
- *Lundi 28 novembre*
- *Lundi 5 décembre*
- *Lundi 12 décembre*
- **Jeudi 5 janvier**
- **Jeudi 12 janvier**
- *Lundi 16 janvier*
- **Jeudi 26 janvier**
- **Jeudi 2 février**
- *Lundi 6 février*
- **Jeudi 16 février**
- **Jeudi 1 mars**
- *Lundi 5 mars*
- *Lundi 12 mars*
- **Jeudi 22 mars**
- **Jeudi 29 mars**
- **Jeudi 19 avril**
- *Lundi 23 avril*

- **Jeudi 3 mai**
- *Lundi 7 mai*
- *Lundi 14 mai*
- **Jeudi 24 mai**
- **Jeudi 7 juin**
- *Lundi 11 juin*
- **Jeudi 21 juin**
- *Lundi 25 juin*
- *Lundi 2 juillet*
- *Lundi 9 juillet*