CSV
FRAKTIOUN

Monsieur Mars Di Bartolomeo
Président de la Chambre des Députés

Luxembourg, le 11 janvier 2017

Monsieur le Président,

Par la présente, nous avons l'honneur de vous informer que, conformément à l'article 80 du Règlement de la Chambre des Députés, nous souhaiterions poser une question parlementaire à Monsieur le Premier Ministre, Ministre d'Etat, à Monsieur le Ministre de la Justice, à Monsieur le Ministre de la Sécurité intérieure et à Monsieur le Ministre des Médias et Communications au sujet de la cybercriminalité.

Dans leur réponse commune à la question parlementaire n°466 du 14 août 2014, Messieurs les Ministres des Communications et des Médias et de la Justice ont indiqué qu'il n'y avait pas de nouvelles mesures à envisager pour une lutte efficace contre la cybercriminalité, tout en soulignant que les nouveaux outils mis à disposition des autorités de poursuite via la loi du 18 juillet 2014 portant approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001 peuvent toujours être utilement mis en pratique.

Au vu des récentes attaques informatiques dans le contexte des élections présidentielles américaines, les experts en cybersécurité s'alarment et mettent en garde contre des actions similaires lors des prochaines élections ayant lieu en Europe (France, Pays-Bas etc.). Même si les piratages ne sont pas nouveaux, les mobiles à la base des opérations semblent avoir changés et viser à déstabiliser nos démocraties.

C'est ainsi que nous aimerions poser les questions suivantes à Messieurs les Ministres :

- Le gouvernement maintient-il sa position de septembre 2014 ? Les services de renseignement et les autorités de poursuite luxembourgeoises sont-elles suffisamment outillés (en ressources humaines et expertise) pour lutter efficacement contre ce dernier type de cybercriminalité ?

- A défaut, quelle est la stratégie du gouvernement pour empêcher une immixtion extérieure dans le processus démocratique de notre pays ?

- Le gouvernement envisage-t-il des adaptations législatives ou réglementaires en la matière ?

- Le gouvernement peut-il nous renseigner sur d'éventuels mécanismes de coopération

mis en place à l'échelle européenne pour faciliter les échanges d'informations, aider les États Membres à renforcer leurs capacités de cyberdéfense et identifier des réponses coordonnées ? A défaut de mise en place de tels mécanismes au niveau européen, le gouvernement luxembourgeois entend-il prendre les devants pour initier un tel processus ?

Nous vous prions d'agréer, Monsieur le Président, l'expression de notre très haute considération.

Laurent Mosar
Député

Serge Wilmes
Député

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Monsieur
Fernand ETGEN
Ministre aux Relations avec le Parlement
LUXEMBOURG

Luxembourg, le 7 février 2017

Objet : Réponse commune de Monsieur le Premier ministre, ministre d'État, de Monsieur le Ministre de la Sécurité intérieure et de Monsieur le Ministre de la Justice et de Monsieur le Ministre des Médias et des Communications à la question parlementaire N° 2660 du 11 janvier 2017 de Messieurs les Députés Laurent MOSAR et Serge WILMES concernant la « cybercriminalité ».

Monsieur le Ministre,

J'ai l'honneur de vous faire parvenir la réponse commune de Monsieur le Ministre de la Sécurité intérieure, de Monsieur le Ministre de la Justice, de Monsieur le Ministre des Médias et des Communications et du soussigné à la question parlementaire N° 2660 du 11 janvier 2017 de Messieurs les Députés Laurent MOSAR et Serge WILMES.

Veuillez agréer, Monsieur le Ministre, l'expression de ma haute considération.

Le Premier ministre
Ministre d'État

Réponse commune de Monsieur le Premier Ministre, Ministre d'Etat, Monsieur le Ministre de la Justice, Monsieur le Ministre de la Sécurité Intérieure et Monsieur le Ministre des Médias et Communications
à la question parlementaire n° 2660 du 11 janvier 2017 des honorables députés Laurent MOSAR et Serge WILMES

Le gouvernement maintient-il sa position de septembre 2014? Les services de renseignement et les autorités de poursuite luxembourgeoises sont-elles suffisamment outillés (en ressources humaines et expertise) pour lutter efficacement contre ce dernier type de cybercriminalité ?

Notons en guise d'introduction que la cybercriminalité se décline autour de deux grands axes, à savoir :

a) Les crimes et délits dont l'objet est constitué par les technologies numériques, tels que
   - le piratage de systèmes informatiques pour vols de données,
   - la distribution massive de chevaux de Troie visant à encrypter les données sur le disque dur avec la demande de rançon pour restituer l'état initial,
   - les attaques DDOS, visant à paralyser des systèmes entiers,
   - la prise en main totale et la manipulation de systèmes informatiques.

b) Les crimes et délits qui utilisent de façon centrale les technologies numériques, tels que
   - la diffusion de contenus sur Internet,
   - les escroqueries bancaires,
   - la contrefaçon d'œuvres de l'esprit,
   - la diffamation,
   - la distribution d'idéologies et de « Fake News ».

Dans ce contexte, et comme signalé dans la réponse à la question parlementaire n° 466 du 14 août 2014, la loi du 18 juillet 2014 portant approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001 a permis de compléter les dispositions du droit pénal luxembourgeois en matière de lutte contre la cybercriminalité et de renforcer la coopération internationale en la matière. En effet, les auteurs de la Convention, conscients que la cybercriminalité ne connaît pas de frontières, ont souligné dans leur rapport explicatif que « les solutions à une lutte efficace contre la cybercriminalité relèvent du droit international ce qui nécessite l'adoption d'instruments internationaux adéquats ».

Au niveau national, la loi du 5 juillet 2016 attribue au SRE la mission de lutter contre la menace en rapport avec l'espionnage et l'ingérence, tout comme la lutte contre la menace cyber si celle-ci présente un lien avec une des missions principales du SRE. Dans le cadre de ses missions, le SRE peut ainsi accéder à des systèmes informatiques afin de rechercher de manière ciblée des renseignements ou de surveiller et contrôler des communications dans une optique de prévention.

Ce nouvel instrument légal est une des réponses à la multiplication des attaques électroniques. Dans le contexte de la prévention et de la lutte contre ces attaques, les acteurs

luxembourgeois en charge de la cyberdéfense coopèrent au niveau national et s'échangent régulièrement avec leurs homologues européens.

De son côté, le *Computer Emergency Response Team* (CERT) Gouvernemental est chargé de la prévention et de la réponse aux incidents de sécurité d'envergure liés aux réseaux et aux systèmes d'information des administrations et des opérateurs d'infrastructures critiques.

Le Parquet près du Tribunal d'arrondissement de Luxembourg dispose quant à lui de 2 substituts compétents pour la cybercriminalité. Au niveau de la Police Grand-Ducale, la section Nouvelles Technologies du Service de Police Judiciaire fait les enquêtes dans le contexte des attaques informatiques. Cette dernière dispose d'experts informatiques hautement spécialisés dans des analyses et exploitations techno-légales.

La Police est actuellement bien outillée en termes techniques. L'on peut cependant noter que la formation d'un analyste informatique en matière de cybercriminalité est complexe et s'étend sur une période d'environ 2 ans.

A défaut, quelle est la stratégie du gouvernement pour empêcher une immixtion extérieure dans le processus démocratique de notre pays ?

Un des objectifs principaux de la stratégie nationale en matière de cybersécurité approuvée et rendue exécutoire par le Conseil de gouvernement en 2015 consiste à assurer la protection opérationnelle des infrastructures et systèmes de communication et de traitement de l'information.

D'un côté, cette stratégie prévoit un volet opérationnel préventif, coordonné par le *Cyber Security Board*, et de l'autre, un volet opérationnel défensif, auquel appartient notamment le plan d'intervention d'urgence en cas d'attaque contre les systèmes d'information ou de faille technique des systèmes d'information (« PIU Cyber »). Ainsi, ce plan détermine les organes de gestion de crise, fixe le déroulement de la diffusion d'alerte des autorités et de l'information au public et détermine les actions y relatives ainsi que les responsables et acteurs respectifs.

En sus, le Conseil de gouvernement a décidé en 2015 la création d'une Agence nationale de la sécurité des systèmes d'information (ANSSI). L'ANSSI assure la fonction de CERT national et gouvernemental et collabore étroitement avec les autres acteurs dans le public et le privé.

Finalement, la stratégie précitée met un accent particulier sur l'information, la formation et la sensibilisation des secteurs privé et public sur les risques encourus et les moyens de se protéger.

Le gouvernement envisage-t-il des adaptations législatives ou réglementaires en la matière ?

Suite aux attentats de Paris, le gouvernement luxembourgeois a déposé en 2015 le projet de loi 6921 qui renforce l'arsenal législatif en matière de lutte contre le terrorisme. Ainsi, en matière de terrorisme, le projet permet notamment d'étendre la surveillance et le contrôle de

toutes les formes de communication à la captation de données informatiques[1] et de participer à des échanges électroniques à des fins d'enquête (technique dite de la cyberinfiltration).

De même, le projet de loi 6976 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres de l'Union européenne (transposition décision-cadre 2006/960/JAI) a été déposé.

Les mesures proposées dans les deux projets de loi sont très importantes pour une lutte efficace contre les attaques informatiques d'envergure et notamment celles qui présentent un lien avec une activité terroriste. Ces mesures ont à la fois un caractère préventif en contribuant à éviter des attaques informatiques, qu'un caractère réactif en facilitant ainsi l'identification des auteurs et l'échange d'informations entre les pays sachant que ce type de cybercriminalité a toujours un volet international.

Le gouvernement peut-il nous renseigner sur d'éventuels mécanismes de coopération mis en place à l'échelle européenne pour faciliter les échanges d'informations, aider les États Membres à renforcer leurs capacités de cyberdéfense et identifier des réponses coordonnées ? A défaut de mise en place de tels mécanismes au niveau européen, le gouvernement luxembourgeois entend-il prendre les devants pour initier un tel processus ?

La coopération internationale en matière cyber s'est fortement développée ces dernières années. Pour ne citer que quelques exemples :

- Le Luxembourg participe depuis 2010 activement aux exercices Cyber Europe organisés par l'ENISA (*European Union Agency for Network and Information Security*). Ces exercices ont pour objectif de passer au crible l'échange d'informations au niveau européen en cas d'attaque cyber.

- Par le biais du CERT Gouvernemental, le Luxembourg participe à une multitude d'échange d'informations. Les informations partagées ont trait aux spécificités techniques d'attaques et sont échangées de façon automatisée entre des cercles de CERTs. Au niveau européen, le CERT Gouvernemental adhère depuis plusieurs années à un cercle de confiance dénommé *Trusted Introducer*.

- En matière pénale, il convient de citer la participation luxembourgeoise à Eurojust (niveau judiciaire) et Europol/ Interpol (niveau policier). En sus, les experts européens se réunissent dans le cadre du *European Cybercrime Task Force* (EUCTF ; réunion d'experts qui facilite la lutte contre la cybercriminalité) et du *Expert meeting on Cross-border access to electronic evidence*.

- Finalement, la directive NIS[2] prévoit plusieurs mécanismes de coopération destinés à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, à savoir :

[1] La captation de données informatiques consiste à placer un dispositif technique aux fins d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données.

[2] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

- le réseau des CSIRT (*Computer Security Incident Response Team*), qui a pris ses fonctions en février 2017, promeut l'échange d'informations relatives aux incidents et aux menaces potentielles entre les CERTs nationaux permettant ainsi de prendre des mesures adéquates afin d'empêcher ou de limiter les impacts d'une cyberattaque ;

- un groupe de coopération visant à faciliter la coopération stratégique entre Etats membres ;

- la désignation d'un point de contact unique national par Etat membre servant d'interlocuteur avec les autres points de contacts nationaux et avec le groupe de coopération.