Nations Unies | Union interparlementaire | Union internationale des télécommunications

Quatrième Forum parlementaire sur la société de l'information
Le triple défi de la cybersécurité: Information, citoyens et infrastructure

18-20 mai 2011
Salle II – Centre de conférences de l'OIT
Organisation internationale du Travail
Genève, Suisse

AIDE MEMOIRE

Contexte

Le nombre de délits liés à Internet a augmenté de façon spectaculaire ces dernières années. Les articles décrivant des atteintes à la vie privée et des cyber-attaques sont devenus monnaie courante dans les médias. Du fait de son expansion rapide, son ouverture et son accessibilité, le réseau planétaire se transforme rapidement en terrain de prédilection pour toutes sortes d'activités malintentionnées, telles que l'envoi de spam, la pédopornographie, les escroqueries financières et l'espionnage industriel. Le crime organisé s'est fermement implanté sur l'internet. Pour les cybercriminels, le coût d'opportunité est très bas et les bénéfices potentiels très élevés. Ils contrôlent, à l'insu de leurs propriétaires, de vastes réseaux d'ordinateurs infectés de logiciels malveillants (« botnets »). Ces réseaux peuvent être utilisés de façon anonyme pour détourner les données des utilisateurs et s'attaquer à d'autres victimes innocentes. Les cybercriminels proposent leurs services sur un marché noir prospère sur lequel s'échangent données de cartes de crédit, coordonnées bancaires, adresses de courrier électronique et autres données acquises illégalement. Selon certaines sources, l'industrie en ligne clandestine aurait connu une croissance à deux chiffres en 2010[1]. Le coût de la cybercriminalité pour les entreprises est estimé à environ € 750 milliards par an[2]. Bien qu'il soit difficile de s'en faire une idée précise, les pertes encourues par la société en général pourraient être plus élevées, car les pertes financières subies par les particuliers sont souvent sous-déclarées.

Les progrès enregistrés par les télécommunications mobiles et à haut débit permettent à un nombre croissant d'usagers d'accéder à Internet et d'opérer des transactions grâce aux nouveaux appareils mobiles tels que les « smartphones » et les tablettes électroniques. Ce sont de nouvelles plateformes informatiques, dont les dispositifs de sécurité ne sont pas encore suffisamment développés, ce qui offre aux cybercriminels un terrain propice pour accéder à des informations confidentielles et réaliser des opérations non autorisées

1 UPI.com: Cybercrime 'industry' sees double-digit growth, http://www.upi.com/Business_News/Security-Industry/2011/03/02/Cybercrime-industry-sees-double-digit-growth/UPI-66271299103546/

2 EuroPol: Cybercrime as a business: The digital underground economy http://www.europol.europa.eu/index.asp?page=news&news=pr110106.htm

aux dépens des usagers légitimes. Dans le même temps, volontairement ou non, les citoyens divulguent une quantité prodigieuse d'informations personnelles par leur usage régulier et intensif des réseaux sociaux. Ce faisant, ils laissent derrière eux un fil d'Ariane virtuel qui peut être facilement déroulé à des fins illégitimes. Peu au fait des conséquences qu'une telle attitude peut avoir sur leur vie privée, les utilisateurs des réseaux sociaux sont incités à divulguer de plus en plus d'informations personnelles, posant ainsi la question de la signification à donner, à l'ère d'Internet, à la notion même de sphère privée. Le regroupement de données privées telles que les sites Internet visités, les achats en ligne, les réseaux d'amis et les lieux géographiques fréquentés sont au cœur de modèles d'activité qui alimentent une industrie sur Internet dont le chiffre d'affaires atteint des milliards de dollars. Inévitablement, cette industrie prospère attire également la convoitise des cybercriminels.

Malgré quelques exemples très médiatisés d'arrestations spectaculaires de cybercriminels, il est clair que l'absence de cadre réglementaire internationalement reconnu en matière de cybersécurité entrave les efforts des autorités. Les récents exemples[3] de démantèlement de réseaux de pédopornographie illustrent l'étendue de la coopération internationale requise pour interpeler les coupables et mettre un terme à leurs activités criminelles, qui passe par l'intervention de plusieurs services de répression lors d'opérations étroitement coordonnées.

Dans cet environnement complexe et en rapide évolution, les autorités peinent à assurer la sécurité des citoyens, des informations sensibles et des infrastructures face à la croissance rapide de l'utilisation illicite des innovations technologiques. La nature planétaire d'Internet et le caractère transnational de la cybercriminalité leur posent des défis particuliers car les cybercriminels, libres d'agir à partir de n'importe quel point du globe, collaborent souvent à distance les uns avec les autres sans jamais s'être rencontrés physiquement. Les lois et règlements diffèrent d'un pays à l'autre, ce qui permet aux cybercriminels de jouir d'une certaine impunité dans les pays qui n'ont pas adopté les lois requises[4].

En outre, le processus politique de négociation d'accords internationaux et d'adoption de dispositions coordonnées en matière de cybersécurité avance à un rythme plus lent que l'évolution technologique. Depuis l'adoption de la Convention sur la cybercriminalité en 2001[5], Facebook, Twitter, les smartphones, l'informatique en nuage, les réseaux de machines zombies et le filoutage (« *phishing* ») ont fait leur apparition dans le paysage technologique, ouvrant de nouveaux et délicats sujets de discussion.

D'autre part, pressés par les citoyens qu'ils représentent de résoudre les problèmes de cybersécurité, les gouvernements risquent souvent de réagir de façon excessive et de perturber le fragile l'équilibre existant entre les exigences de sécurité et les droits fondamentaux des citoyens, qui pourraient se ressentir de certaines décisions prises, volontairement ou non, par l'exécutif. Une étude publiée par le Parlement européen confirme que les TIC ouvrent de nouvelles perspectives en matière de protection et de promotion des droits de l'homme, tout en menaçant directement ces mêmes droits du fait qu'elles permettent la conception de mécanismes de surveillance et de censure de plus en plus sophistiqués[6].

---

3. V3.co.uk: Hacker arrested on Mariposa botnet charges, http://www.v3.co.uk/v3-uk/news/1950312/hacker-arrested mariposa-botnet-charges SV Mercury News: International child porn ring is broken up, http://www.mercurynews.com/california/ci_16857738

4. Par exemple, les efforts récemment mis en œuvre pour empêcher l'accès aux informations confidentielles publiées par Wikileaks ont été en grande partie voués à l'échec car le contenu a été reproduit sur des centaines de serveurs, hors de portée des accords internationaux ou bilatéraux.

5. En 2001, le Conseil de l'Europe a adopté la Convention sur la cybercriminalité, qui est entrée en vigueur en 2004. Il est à noter que la Convention est loin de bénéficier d'un soutien unanime.

6. Study: Information and Communication Technologies and Human Rights, Parlement européen, juin 2010 EXPO/B/DROI/2009/24, www.europarl.europa.eu/activities/committees/studies.do?language=EN

Dans ce contexte, les menaces en ligne ayant un impact puissant et appelant une réponse tant internationale que nationale, il est évident que la question de la cybersécurité est devenue une priorité pour un grand nombre de gouvernements et pour la communauté internationale.

Etant l'institution publique la plus directement appelée à répondre auprès de l'électorat de son action en faveur de la sécurité des citoyens, de la protection de leurs droits et de la promotion d'une société de l'information axée sur l'être humain, les parlements assument une responsabilité particulière dans le traitement réservé aux questions de cybersécurité, auquel ils doivent activement contribuer. Les parlementaires ont pour mission de veiller à ce que les lois soient réellement bénéfiques aux citoyens qu'ils représentent et il leur revient donc de trouver un juste équilibre entre des besoins divergents en défendant l'instauration d'une société de l'information réaffirmant l'importance des droits de l'homme et les renforçant, tout en garantissant la sécurité des citoyens et la protection des informations et des infrastructures. Ce faisant, le Parlement doit pleinement exercer son rôle de contrôle du pouvoir exécutif et des services de répression en examinant minutieusement la réponse qu'ils apportent aux menaces et défis posés par la technologie.

Au niveau international, les parlements peuvent apporter une contribution considérable aux progrès à réaliser en matière de coordination et d'harmonisation des lois et règlements sur la cybersécurité, grâce à la coopération et au développement des échanges entre parlementaires et commissions impliqués dans l'examen de cette question.

Objectifs du Forum parlementaire

Le Forum parlementaire sur le thème "*Le triple défi de la cybersécurité : Information, citoyens et infrastructure*" est la quatrième réunion de parlementaires à se pencher sur les questions relatives à la société de l'information. Comme les trois précédents, il est organisé dans le cadre du Centre mondial pour les TIC au Parlement, initiative lancée en partenariat par le Département des affaires économiques et sociales de l'ONU et l'Union interparlementaire (UIP) lors du Sommet mondial sur la société de l'information (SMSI) en 2005.

Ce quatrième forum portera sur les responsabilités assumées par les parlementaires en matière de représentation, d'adoption de lois et de contrôle dans le domaine de la cybersécurité. On y examinera les défis particuliers posés par l'utilisation illicite des technologies de l'information et de la communication, notamment la sécurité des citoyens dans un environnement connecté, la protection des informations, données et infrastructures nationales, et la riposte transnationale à la cybercriminalité.

Le Forum parlementaire a pour objectif de faire avancer le dialogue entre parlementaires concernant les différentes priorités stratégiques et politiques mises en œuvre à l'échelon national, de brosser un tableau général des différents engagements pris par les États pour surmonter les difficultés évoquées, de définir le rôle et les responsabilités des parlements dans le cadre des fonctions législatives et de contrôle qu'ils exercent dans ce domaine, de recenser les bonnes pratiques parlementaires et de formuler des recommandations concrètes à l'intention des parlements.

Lieu de la réunion et modalités

Le Forum parlementaire se tiendra les 18, 19 et 20 mai 2011 au Siège de l'Organisation internationale du Travail à Genève, en Suisse. La cérémonie d'ouverture aura lieu à 15 h.00 le mercredi 18 mai et le Forum se terminera à 13 h.00 le vendredi 20 mai 2011.

Il s'articulera autour d'une série de séances plénières, auxquelles contribueront experts et parlementaires. Une bonne part de chaque séance sera réservée aux interventions des participants, au dialogue interactif et à la libre discussion entre parlementaires.

Participation

Le Forum parlementaire devrait rassembler quelque 150 parlementaires du monde entier chargés des questions relatives à la société de l'information. Des présidents de commissions parlementaires chargées des questions relatives aux sciences et aux technologies, à l'information et aux télécommunications et/ou à la sécurité devraient conduire les délégations et participer activement aux débats avec leurs pairs d'autres pays et régions.

Le Forum parlementaire accueillera en outre de hauts représentants et fonctionnaires d'organisations internationales, ainsi que des experts représentant les institutions internationales, les gouvernements, le secteur des TIC et le monde universitaire.

Les contributions des parlements

Pour que le Forum soit l'occasion d'en savoir plus sur les expériences nationales, les délégations sont vivement encouragées à soumettre à l'avance des contributions écrites décrivant les différentes mesures prises à l'échelon national par le parlement pour remédier aux problèmes mondiaux de cybersécurité. Ces contributions devraient porter sur la façon dont parlements, commissions parlementaires et parlementaires ont représenté les points de vue de l'électorat, facilité l'élaboration des lois et la définition des politiques et contrôlé les activités entreprises par le gouvernement.

Les contributions devront être soumises en anglais, français ou espagnol en suivant les directives figurant en annexe, également reprises sur la page Web du Forum.

Langues

Les langues de travail de la réunion seront l'anglais, l'espagnol et le français. L'interprétation simultanée sera assurée dans ces trois langues.

Organisateurs

Le Quatrième Forum parlementaire sera organisé conjointement par le Département des affaires économiques et sociales de l'ONU, l'Union interparlementaire (UIP) et l'Union internationale des télécommunications (UIT), par le truchement du Centre mondial pour les TIC au Parlement.

<u>Département des affaires économiques et sociales de l'ONU</u>

Le Département des affaires économiques et sociales de l'ONU (DESA) encourage et soutient la coopération internationale afin que le développement devienne une réalité pour tous. Il aide les gouvernements à établir leur ordre du jour et à définir leurs politiques sur les questions de développement au niveau mondial. Il propose une large gamme de produits — analyses et conseils — dont pays développés et pays en développement se servent comme d'outils

de référence et d'aide à la prise de décision, en particulier pour traduire les engagements pris au niveau mondial en politiques et mesures nationales et pour évaluer les progrès accomplis dans la réalisation des objectifs de développement adoptés par la communauté internationale, notamment des Objectifs du Millénaire pour le développement.

Union internationale des télécommunications (UIT)

L'UIT est l'institution spécialisée des Nations Unies pour les technologies de l'information et de la communication. Pôle de convergence mondial où se retrouvent pouvoirs publics et secteur privé pour développer réseaux et services, l'UIT coordonne depuis près de 145 ans le partage du spectre des radiofréquences au niveau mondial, favorise la coopération internationale en assignant des orbites aux satellites, s'emploie à améliorer l'infrastructure des télécommunications dans le monde en développement, établit au plan mondial les normes techniques qui permettent l'interconnexion harmonieuse des systèmes de communication les plus divers et s'attache à relever des défis mondiaux en s'efforçant d'atténuer les changements climatiques, par exemple, et de renforcer la cybersécurité. L'UIT a son siège à Genève, en Suisse, et compte 191 Etats Membres.

Union interparlementaire (UIP)

L'Union interparlementaire est l'organisation internationale des parlements. Foyer de la concertation interparlementaire depuis 1889, date de sa fondation, elle œuvre en vue de la paix et de la coopération entre les peuples, ainsi que du renforcement des institutions représentatives. L'UIP a son siège à Genève et compte actuellement 151 Membres et huit Membres associés.

Centre mondial pour les TIC au Parlement

Le Centre mondial pour les TIC au Parlement est une initiative conjointe du Département des affaires économiques et sociales de l'ONU, de l'Union interparlementaire et d'un groupe de parlements nationaux et régionaux prise en novembre 2005 dans le cadre du Sommet mondial sur la société de l'information. Ses objectifs sont : a) d'encourager parlements et parlementaires à jouer un rôle accru dans la promotion de la société de l'information, et b) de renforcer la capacité des parlements à se servir des outils offerts par les TIC pour mieux remplir leurs fonctions démocratiques et améliorer le fonctionnement des institutions et la coopération interparlementaire.