Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Résolution 2070 (2015)[1]
Version provisoire

Renforcer la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet

Assemblée parlementaire

1. L'Assemblée parlementaire est consciente de l'impact positif d'époque des nouvelles technologies de l'information sur tous les aspects des sociétés modernes et de la vie humaine. Au-delà de ces effets positifs, le développement d'internet et des autres réseaux informatiques fait apparaître de nouvelles fragilités dans nos sociétés. L'Assemblée est alarmée par le nombre et l'ampleur des attaques criminelles perpétrées dans le cyberespace ces dernières années, qui mettent à mal la confiance du public à l'égard du développement technologique.

2. Profondément préoccupée par les cyberattaques apparemment de nature politique perpétrées récemment contre une compagnie aérienne polonaise et contre le Parlement allemand, contre des sites internet en Ukraine au lendemain du conflit militaire qui s'y déroule depuis 2014, contre des sites internet en Géorgie au lendemain de la guerre entre la Russie et la Géorgie en 2008, ainsi que contre l'infrastructure du web en Estonie en 2007, l'Assemblée rappelle sa Résolution 1565 (2007) «Comment prévenir la cybercriminalité dirigée contre les institutions publiques des Etats membres et observateurs?» et souligne l'urgence de réagir à ces attaques de grande ampleur et d'obtenir des éléments de preuve afin de déterminer les origines, les auteurs et les instigateurs politiques de ces attaques.

3. Le Conseil de l'Europe a édicté des règles juridiques internationales importantes dans ce domaine avec ses conventions sur l'entraide judiciaire en matière pénale (STE n^{os} 30, 99 et 182), sur la répression du terrorisme (STE n^{os} 90 et 190), sur la prévention du terrorisme (STCE n^{o} 196) et sur la cybercriminalité (STE n^{os} 185 et 189). Cependant, d'importants obstacles entravent encore les enquêtes et les poursuites relatives aux cyberinfractions, en particulier dans le cadre des réseaux transfrontaliers, et les peines prévues par les législations nationales ne sont pas toujours adaptées. C'est pourquoi l'Assemblée estime qu'il est nécessaire de poursuivre les travaux au niveau européen et international pour apporter une réponse satisfaisante aux problèmes posés par le cyberterrorisme et d'autres formes d'attaques de grande ampleur visant les systèmes informatiques ou commises par leur intermédiaire et qui menacent la sécurité nationale, la sécurité publique et le bien-être économique des Etats.

4. Vu la législation correspondante de l'Union européenne, en particulier la Convention de l'Union européenne relative à l'entraide judiciaire en matière pénale, l'Assemblée souligne la nécessité de poursuivre le développement de divers aspects juridiques et pratiques internationaux, notamment pour ce qui est des principes suivants:

4.1. les demandes d'entraide devraient être exécutées par l'Etat requis dès que possible, en tenant compte au mieux des échéances indiquées par l'Etat requérant. Si une requête ne peut pas être pleinement exécutée conformément aux exigences de l'Etat requérant, les autorités de l'Etat requis devraient indiquer sans délai le temps nécessaire à son exécution et les conditions dans lesquelles elle pourrait être exécutée;

1. *Discussion par l'Assemblée* le 26 juin 2015 (27^{e} séance) (voir Doc. 13802, rapport de la commission de la culture, de la science, de l'éducation et des médias, rapporteur: M. Hans Franken). *Texte adopté par l'Assemblée* le 26 juin 2015 (27^{e} séance).
Voir également la Recommandation 2077 (2015).

4.2. chaque Etat membre devrait veiller à ce que les systèmes de services de télécommunications qui opèrent sur son territoire via une station terrestre et qui, aux fins de l'interception légale des communications d'une cible présente dans un autre Etat, ne sont pas directement accessibles sur le territoire de ce dernier, puissent être rendus directement accessibles pour les besoins de l'interception légale par ledit Etat par l'intermédiaire d'un fournisseur de services désigné présent sur son territoire. Cette procédure devrait s'accompagner de protections contre l'espionnage par des pays tiers;

4.3. les Etats membres devraient définir un niveau minimum d'incrimination des cyberattaques de grande ampleur, y compris pour ce qui est des circonstances aggravantes en la matière, ainsi que sur des normes minimales pour les peines applicables à ces attaques.

5. Bien que l'entraide judiciaire entre les services répressifs doive être améliorée et adaptée en fonction du développement technologique, l'Assemblée est consciente que cela ne doit pas compromettre les autres droits fondamentaux, en particulier le droit au respect de la vie privée et à la protection des données personnelles découlant de l'article 8 de la Convention européenne des droits de l'homme (STE n° 5) et de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108).

6. Consciente que certains services et infrastructures sont essentiels pour la sécurité nationale, la sécurité publique et le bien-être économique des Etats, l'Assemblée recommande aux Etats membres:

6.1. d'établir des plans d'urgence ne dépendant pas d'internet en cas de cyberattaques visant des services et infrastructures essentiels, comme les services d'électricité, les gazoducs et oléoducs, les centrales électriques, les ouvrages hydrauliques, les réseaux de télécommunication, les aéroports, les voies ferrées, les hôpitaux, les casernes de pompiers, les services de sécurité et l'armée;

6.2. de mettre en place des mesures de sécurité d'ordre technique pour protéger les services et infrastructures essentiels sur leur territoire, comme des systèmes et réseaux informatiques de sauvegarde en circuit fermé qui puissent être utilisés au cas où les connexions ouvertes à internet seraient attaquées ou bloquées;

6.3. de conclure des accords d'urgence bilatéraux avec les Etats voisins afin de s'assurer une entraide en cas de cyberattaques visant des services ou infrastructures essentiels;

6.4. d'établir un cadre juridique adapté à la coopération public–privé pour la protection contre les cyberattaques de grande ampleur;

6.5. de reconnaître que les Etats ont la responsabilité, au niveau international, de prendre toutes les mesures raisonnables pour empêcher que des cyberattaques de grande ampleur soient menées par des personnes relevant de leur juridiction ou à partir de leur territoire national;

6.6. d'incriminer la production, la diffusion et l'utilisation de logiciels malveillants dont le but est de permettre à des individus de préparer ou lancer des cyberattaques de grande ampleur.

7. Les fournisseurs de services ou d'infrastructures essentiels devraient être tenus de signaler sans délai toute cyberattaque de grande ampleur dont ils sont la cible aux autorités répressives compétentes de l'Etat où ils ont leur siège ainsi qu'à celles de l'Etat où cette attaque a lieu. De plus, toute personne physique ou morale devrait être informée des modalités à suivre pour signaler les cyberattaques dont elle fait l'objet à ses autorités répressives compétentes.

8. Les fabricants de logiciels et matériel informatiques devraient informer leurs clients sans délai en cas de découverte de failles systémiques permettant des cyberattaques de grande ampleur, notamment au moyen de botnets (réseaux zombies), de virus électroniques ou autres logiciels malveillants.

9. Les fournisseurs de services informatiques hébergés dans le nuage devraient prendre des mesures de sécurité pour protéger leurs services contre les attaques visant leur sécurité et leur intégrité et qui peuvent déboucher sur des cyberattaques de grande ampleur, de type botclouds.

10. Les fournisseurs de sites web publics devraient veiller à ce que leurs sites ne contiennent pas de virus électroniques ou autres logiciels malveillants pouvant entraîner des cyberattaques de grande ampleur. A cette fin, leurs administrateurs de site devraient appliquer régulièrement des dispositifs techniques pour lutter contre ces logiciels malveillants.

11. Les fabricants et vendeurs d'ordinateurs et de logiciels devraient informer régulièrement les possesseurs d'ordinateurs des possibilités de ces derniers et de la responsabilité qui leur incombe au final de veiller à la sécurité technique de leurs ordinateurs lorsqu'ils les connectent à internet ou à d'autres réseaux informatiques publics.

12. Les Etats membres devraient développer des normes de sécurité contraignantes pour la protection contre les cyberattaques de grande ampleur et obtenir la certification publique de ces normes, si possible au niveau européen ou international.

13. L'Assemblée invite le Secrétaire Général du Conseil de l'Europe à engager et coordonner une action intergouvernementale du Conseil de l'Europe, à établir des programmes de coopération avec l'industrie des technologies de l'information et les fournisseurs de services internet et à assurer une coopération plus étroite avec l'Union européenne et les Nations Unies dans ce domaine de la plus haute importance.