Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 13802
08 juin 2015

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

Rapport[1]
Commission de la culture, de la science, de l'éducation et des médias
Rapporteur: M. Hans FRANKEN, Pays-Bas, Groupe du Parti populaire européen

Résumé

Considérant qu'il y a un impact positif des nouvelles technologies de l'information sur tous les aspects des sociétés modernes et de la vie humaine, le développement d'internet et des autres réseaux informatiques fait apparaître de nouvelles fragilités dans nos sociétés. C'est pourquoi il est nécessaire de poursuivre les travaux contre 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.

L'entraide judiciaire entre les services répressifs devrait être améliorée et adaptée en fonction du développement technologique. Les mesures de sécurité devraient être développées pour protéger les services et infrastructures essentiels. 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.

Sur la base de ses conventions, le Conseil de l'Europe devrait répondre à ce problème croissant, à l'échelle mondiale, pour la sécurité des réseaux informatiques.

1. Renvoi en commission: Doc. 13319, Renvoi 4008 du 22 novembre 2013.

Sommaire **Page**

A. Projet de résolution[2]

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. 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.

3. 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 et la coordination de divers aspects juridiques et pratiques internationaux, notamment pour ce qui est des principes suivants:

3.1. 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;

3.2. 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;

3.3. les Etats membres devraient s'entendre sur un niveau commun 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.

4. 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^{o} 5) et de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n^{o} 108).

5. 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:

5.1. 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;

5.2. 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;

2. Projet de résolution adopté à par la commission le 2 juin 2015.

5.3. 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;

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

5.5. 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;

5.6. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

B. Projet de recommandation[3]

1. L'Assemblée parlementaire se réfère à sa Résolution …. (2015) «Renforcer la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet»;

2. Elle souligne qu'il est important que le Conseil de l'Europe apporte des réponses au problème croissant que posent pour la sécurité des réseaux informatiques, à l'échelle mondiale, le cyberterrorisme et d'autres formes d'attaques de grande ampleur commises contre les systèmes informatiques ou au moyen de ces derniers, lesquels constituent une grave menace pour la sécurité nationale, la sécurité publique et le bien-être économique des Etats;

3. L'Assemblée recommande au Comité des Ministres:

3.1. d'inviter les Parties à la Convention sur la cybercriminalité et à son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n^{os} 185 et 189):

3.1.1. à élaborer un protocole additionnel définissant un niveau commun 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;

3.1.2. à élaborer un autre protocole additionnel sur l'entraide en matière de pouvoirs d'investigation, qui étende en particulier le champ d'application de l'article 32 de la convention, conformément à la note d'orientation correspondante du Comité de la Convention Cybercriminalité qui représente les Parties à la convention;

3.2. d'inviter le Groupe sur les preuves dans le nuage établi par le Comité de la Convention Cybercriminalité à étudier la faisabilité d'un protocole additionnel à la Convention sur la cybercriminalité relatif à l'accès de la justice pénale aux données stockées sur des serveurs d'hébergement dans le nuage;

3.3. d'élaborer des normes juridiques sur la responsabilité internationale qui revient aux Etats de prendre toutes les mesures raisonnables pour prévenir que des cyberattaques de grande ampleur soient lancées par des personnes relevant de leur juridiction ou à partir de leur territoire national contre des systèmes informatiques dans un autre Etat;

3.4. de renforcer les actions d'assistance et de contrôle relatives à l'application de la Convention sur la cybercriminalité dans le droit et la pratique internes ainsi que les mesures et la coopération pratiques contre les cyberattaques de grande ampleur, en particulier au bénéfice des Etats membres dans lesquels la mise en œuvre pratique de la Convention sur la cybercriminalité est confrontée à des difficultés;

3.5. d'appeler l'Autriche, la Bosnie-Herzégovine, la République tchèque, la Grèce, la Hongrie, l'Islande, l'Irlande, l'Italie, Malte, Monaco, le Portugal, Saint-Marin, la Suède et le Royaume-Uni à signer et/ou ratifier sans délai le Protocole de 2003 portant amendement à la Convention européenne pour la répression du terrorisme (STE n^{os} 90 et 190), ce qui est nécessaire pour que ce Protocole entre en vigueur;

3.6. de transmettre à leurs autorités et ministères nationaux compétents cette recommandation et la Résolution … (2015) «Renforcer la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet».

3. Projet de recommandation adopté par la commission le 2 juin 2015.

C. Exposé des motifs, par M. Franken, rapporteur

1. Introduction

1. Le présent rapport a été rédigé à la suite d'une proposition de résolution «Renforcer la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet» (Doc. 13319). La proposition se concentre sur le défi consistant à trouver un équilibre entre, d'une part, les efforts accrus nécessaires de la part des Etats membres du Conseil de l'Europe pour lutter contre le cyberterrorisme et les menaces de grande ampleur sur internet, et d'autre part le respect des libertés et droits fondamentaux. Afin de contribuer au débat, le présent rapport étudie les réponses juridiques que les pays pourraient apporter à de telles attaques. Il pose à cette fin les questions suivantes:

– Que sont les cyberattaques de grande ampleur et les réseaux zombies, quels liens ont-ils avec le cyberterrorisme et quelles sont leurs répercussions sur le fonctionnement de la société?

– Face à de telles attaques, quels textes réglementaires existent à ce jour au niveau international?

– Quelles approches, juridiques ou non, peuvent être suggérées pour améliorer les efforts de réglementation contre les cyberattaques de grande ampleur?

2. Il ne suffit pas d'inscrire une infraction dans le Code pénal pour lutter contre la cybercriminalité, et encore moins contre les réseaux zombies. Pour atténuer réellement les menaces, il faut coopérer pour échanger et analyser les données virales, inciter les fournisseurs de services internet à informer les autorités des risques significatifs, examiner les limites juridiques aux mesures de lutte et d'atténuation et rechercher des mesures non juridiques, améliorer les possibilités d'enquêtes transfrontières sur les cyberattaques, pouvoir traiter avec diligence les demandes urgentes de coopération et promouvoir les solutions de désinfection et les campagnes ciblant les utilisateurs. Le présent rapport ne peut traiter exhaustivement de tous ces thèmes. Il offre en revanche un aperçu des évolutions actuelles au niveau international et une présentation de quelques défis juridiques parmi ceux posés par les cyberattaques de grande ampleur. Il avance également des recommandations visant à améliorer le cadre juridique actuel en matière de cybercriminalité et des suggestions de mesures non juridiques, dont les programmes de renforcement des capacités et les partenariats public–privé. Il souligne, enfin, la nécessité de reconsidérer le type de réponse apportée par les autorités de régulation aux cyberattaques de grande ampleur.

2. Travaux préparatoires

3. Nommé rapporteur par la commission de la culture, de la science, de l'éducation et des médias le 4 décembre 2013, j'ai participé au Dialogue européen sur la gouvernance de l'internet (EuroDIG) des 12 et 13 juin 2013, à Berlin. Les 16 et 17 avril 2015, j'ai participé à la Conférence mondiale 2015 sur le cyberespace, organisée à La Haye, et au cours de laquelle a été lancé le Forum mondial d'expertise pour la cybersécurité, la cybercriminalité, la protection des données et la gouvernance en ligne[4].

4. Pour l'étude du sujet du présent rapport, la sous-commission des médias et de la société de l'information a entendu le professeur Yaman Akdeniz, de l'université Bilgi d'Istanbul, lors de sa réunion à Istanbul, les 12 et 13 mai 2014. A la suite des contacts que j'avais pris avec lui, le professeur Bert-Jaap Koops, de l'université de Tilburg, aux Pays-Bas, a préparé un rapport d'information qui a été présenté à la commission le 29 janvier 2015, à Strasbourg, et sur lequel s'appuie l'essentiel du présent exposé des motifs. Le 12 mars 2015, la commission de la culture, de la science, de l'éducation et des médias a tenu une audition au Sénat des Pays-Bas, à La Haye, avec M. Jacob Kohnstamm, Président de l'Autorité néerlandaise de protection des données, M. Olivier Burgersdijk, Directeur de la stratégie du European Cybercrime Centre (EC3), Europol, M. Menno van der Marel, PDG de Fox-IT, Delft, le professeur Bart Jacobs, Professeur de sécurité et d'exactitude des logiciels à l'université de Nimègue, ainsi qu'avec M^{me} Gabriella Battaini-Dragoni, Secrétaire Générale adjointe du Conseil de l'Europe.

5. Je suis très reconnaissant à tous les experts, en particulier le professeur Koops, pour leurs contributions substantielles, qui ont souligné et défini l'importance et l'urgence de l'action du Conseil de l'Europe visant à accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet.

4. https://www.gccs2015.com/.

3. Généralités

6. Le rapport Norton 2013[5], fondé sur l'observation d'un échantillon de 24 pays de différents continents, constate que la cybercriminalité fait chaque jour plus d'un million de victimes parmi les consommateurs et en estime le coût global dans le monde à $US 113 milliards par an. Ces chiffres restent modestes au regard de ceux de l'étude *Net Losses* de McAfee, parue en juin 2014[6]. L'entreprise de sécurité en ligne y évalue le coût global de la cybercriminalité à $US 400 milliards par an, avec un total de 800 millions de victimes pour la seule année 2013. Ces chiffres sont à prendre avec un certain recul, car les méthodes de calcul sont floues et les rapports sur la cybercriminalité souvent influencés par les intérêts privés d'entreprises qui en tirent un bénéfice. Néanmoins, il est partout admis que la cybercriminalité est en expansion et rapporte de plus en plus à ses auteurs à l'échelle mondiale. Il est à redouter, pour la sécurité nationale, que les attaques cyberterroristes ne deviennent plus nombreuses et sophistiquées et que les cyberterroristes ne lancent des attaques de grande ampleur contre des services et infrastructures essentiels. Afin de discerner les problèmes de réglementation liés à cette question particulière, il faut d'abord définir la cybercriminalité, le cyberterrorisme et les implications des attaques de grande ampleur.

3.1. Cybercriminalité

7. L'usage de réseaux informatiques à des fins illégales a donné lieu à un type de criminalité distinct, généralement nommé cybercriminalité. Cependant, les infractions commises dans le cyberespace peuvent revêtir des formes variées, et les systèmes informatiques peuvent être aussi bien les cibles que les instruments de telles infractions. Les premières typologies en la matière identifiaient trois catégories d'infractions[7]:

– les ordinateurs comme instruments d'une infraction (infractions utilisant l'informatique);

– les ordinateurs comme cibles d'actes malveillants (atteintes à l'intégrité de systèmes informatiques ou cybercriminalité *stricto sensu*);

– les ordinateurs comme environnement dans lequel est commise une infraction (infractions liées à l'informatique).

8. Bien que ces trois catégories se recoupent souvent, l'idée générale sous-jacente à cette distinction classique est importante pour montrer que les infractions traditionnelles, telles que la fraude, le blanchiment d'argent ou le racisme, n'ont pas été nécessairement redéfinies par les systèmes d'information mais ont migré dans un nouveau contexte, prenant ainsi une nouvelle ampleur – sinon une nouvelle nature.

3.2. Cyberterrorisme

9. Le terme de terrorisme connaît des emplois si variés, dans des contextes si différents, qu'on peut se demander si «terrorisme» constitue une notion homogène. Définir le terrorisme demeure un défi; or, les lois antiterroristes ont des conséquences bien réelles, puisqu'elles soumettent généralement les «terroristes» à un régime plus strict: peines plus lourdes, droits amoindris. La classification d'un acte répréhensible comme «cyberterrorisme» apporte aussi son lot de difficultés conceptuelles et de nouveaux défis. En effet, pour qu'un crime cyberterroriste soit commis, il faut d'abord qu'il y ait un acte de cybercriminalité. Le problème consiste alors à démêler les deux concepts. Par exemple, si l'on considère que les crimes terroristes sont nécessairement liés à une cause politique, religieuse ou sociale, le cyberterrorisme se compose de deux éléments: un élément objectif, la perpétration d'une infraction informatique, plus un élément subjectif, les motivations et intentions de l'auteur. En l'absence d'élément subjectif, une infraction susceptible de relever du cyberterrorisme ne pourra être considérée que comme une atteinte à la législation contre la cybercriminalité.

10. La question de la qualification est particulièrement importante, en outre, pour établir le droit applicable. Retrouver les auteurs de cyberattaques est un processus complexe, parfois encore compliqué par les technologies employées par les auteurs pour effacer leurs traces et dissimuler leur identité et qui requiert une solide coopération internationale. Prenons par exemple une attaque lancée depuis des ordinateurs d'un Etat A contre les systèmes d'information d'un aéroport situé dans un Etat B. Ici, les frontières entre cybercriminalité, cyberterrorisme et guerre cybernétique dépendent non seulement de l'étude des données numériques, mais aussi d'une évaluation subjective des intentions de l'agresseur ainsi que de la présence ou

---

5. www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pptx.
6. www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf.
7. Koops et Robinson, Cybercrime law: A European perspective, E. Casey (Ed.), *Digital evidence and computer crime* (p. 123-183), Waltham, MA: Academic Press (2011).

non d'une responsabilité juridique attribuable à un Etat à l'origine de l'attaque. Cette difficulté à qualifier l'infraction est nettement apparue en Estonie en 2007, lorsque plusieurs systèmes d'information des secteurs public et privé ont été visés par une attaque par DDoS (déni de service distribué). Comme l'a remarqué le Groupe de travail des Nations Unies sur la lutte contre l'utilisation d'Internet à des fins terroristes, même si l'attaque contre l'Estonie était patente, il était difficile de savoir s'il s'agissait d'un cas de cybercriminalité, de cyberterrorisme ou de guerre cybernétique.

11. En raison de la difficulté à distinguer le cyberterrorisme de la cybercriminalité, ainsi qu'à déterminer si telle ou telle attaque comporte l'élément subjectif d'un objectif terroriste, nous nous concentrerons ici sur les cyberattaques de grande ampleur en général, qu'elles revêtent ou non un caractère terroriste. Nous nous pencherons avant tout sur les effets de telles attaques sur les infrastructures et services essentiels à la société, qui appellent de sérieuses mesures de lutte indépendamment des motivations de leurs auteurs.

3.3. Attaques de grande ampleur et réseaux zombies

12. Bien qu'un petit nombre d'ordinateurs puisse causer d'importants dommages au système visé, les cyberattaques utilisant un large réseau d'ordinateurs s'avèrent plus rentables. Les attaques massives sont plus agressives et donc plus susceptibles de causer des dommages sérieux. Aujourd'hui, certaines des cyberattaques les plus rentables passent par la manipulation d'armées de machines infectées, dites «réseaux zombies».

13. Le terme de réseau zombie – en anglais *botnet*, pour «roBOT NETwork – désigne un ensemble de systèmes (zombies) infectés par un logiciel partiellement autonome qui peut être contrôlé à distance par un *botmaster* gérant le serveur de commande et contrôle (C&C)[8]. Parmi les usages illégaux des réseaux zombies figurent actuellement la fraude au clic, les attaques DDoS, les enregistreurs de frappe (qui interceptent la frappe sur un clavier pour capter des données personnelles ou financières), les warez (œuvres diffusées sans autorisation des auteurs) et les pourriels.

14. Cependant, la définition traditionnelle des réseaux zombies comme réseaux d'ordinateurs infectés contrôlés par un botmaster ne reflète plus le degré de complexité qu'ils ont atteint aujourd'hui. Selon une définition plus récente, un réseau zombie est «un réseau de logiciels malveillants avancés qui intègrent souvent un ou plusieurs virus, vers, chevaux de Troie et programmes furtifs hostiles destinés à se propager et à s'intégrer dans un système étranger, puis à se reconnecter à un serveur central ou à d'autres systèmes infectés, permettant à l'auteur de l'attaque de contrôler le fonctionnement du système touché»[9]. Bien que les réseaux zombies centralisés n'aient pas disparu, de plus en plus d'entre eux diffusent des protocoles de communication via des structures décentralisées, gagnant en résilience en évitant qu'une seule défaillance ne les compromette. Aujourd'hui, il existe des réseaux zombies complexes fondés sur des réseaux de pair à pair (botnets p2p) où l'activité n'est pas contrôlée par un seul serveur C&C mais par des systèmes infectés faisant à la fois office de zombies et de serveurs C&C. Parmi les nouvelles formes de réseaux zombies figurent aussi les *botclouds*, qui lancent des attaques via des service d'hébergement dans les nuages, transformant l'informatique dans les nuages en vecteur d'agression. Si l'informatique décentralisée remplit plusieurs fonctions utiles, elle a aussi largement alimenté les activités des réseaux zombies. Les botclouds répandent l'agent malveillant sans grand effort de la part de l'auteur de l'attaque: ils peuvent être mis en place à la demande, de grande ampleur et à faible coût. En outre, ils ne dépendent pas de l'activité des usagers: les botclouds sont en permanence en ligne et ne craignent pas les interruptions.

15. Peu d'obstacles techniques s'opposent à ce que les capacités de ces réseaux soient utilisées pour des attaques de grande ampleur. Comme l'a relevé le Groupe de travail des Nations Unies sur la lutte contre l'utilisation d'Internet à des fins terroristes, les infrastructures essentielles, comme le secteur de l'énergie, l'approvisionnement en eau, les réseaux de télécommunication, l'administration publique, les transports, le secteur de la santé et les banques, constituent des cibles attrayantes pour des attaques puissantes et très nocives[10]. Cet inquiétant scénario appelle un cadre efficace et proportionné de lutte contre les cyberattaques de grande ampleur.

---

8. Kassidy *et al*. (2011), BOTCLOUDS: The Future of Cloud-based Botnets?: http://homepage.tudelft.nl/68x7e/Papers/botclouds.pdf.
9. Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), Botnets: detection, measurement, disinfection & defence (2011).
10. Counter-Terrorism Implementation Task Force (CTITF), Working Group Report «Countering the Use of the internet for Terrorist Purposes», New York, mai 2011, www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_2011.pdf.

3.4. Réglementation au niveau international

16. Les politiques et règles internationales en matière de cybercriminalité et de terrorisme sont traditionnellement énoncées dans des instruments distincts. Néanmoins, les récents événements montrant les liens entre ces deux domaines appellent de plus en plus une stratégie combinée de lutte contre le cyberterrorisme. On trouvera en annexe un bref aperçu des mesures juridiques et non juridiques les plus pertinentes au niveau supranational, concernant en particulier la cybercriminalité, le cyberterrorisme et les attaques de grande ampleur.

17. Cet aperçu montre que les organisations dotées de la plus importante réglementation en matière de cybercriminalité sont le Conseil de l'Europe et l'Union européenne. Les Conventions n^{os} 185 (sur la cybercriminalité) et 196 (pour la prévention du terrorisme) orientent la réaction du Conseil de l'Europe dans ces domaines. Cependant, la cybercriminalité a considérablement évolué depuis l'adoption de ces deux textes. De nouvelles formes d'infractions sont apparues et les formes anciennes sont devenues plus élaborées. On peut donc se demander si des activités criminelles telles que les réseaux zombies et les cyberattaques de grande ampleur sont aujourd'hui suffisamment couvertes par la Convention n^{o} 185. De plus, les procédures pénales en vigueur entravent sérieusement les enquêtes et les poursuites dans ce domaine, en particulier dans le contexte des réseaux transfrontaliers.

18. L'Union européenne a récemment adopté la Directive 2013/40/UE relative aux attaques contre les systèmes d'information, remplaçant la décision-cadre précédente sur le même thème. La directive suit de près les dispositions de fond de la Convention n^{o} 185 tout en ajoutant des normes minimales pour la fixation des peines, dont des circonstances aggravantes. Elle ne réglemente cependant pas les pouvoirs d'enquête. La proposition de directive de l'Union européenne sur la sécurité des réseaux et de l'information («directive sur la cybersécurité») représente une autre initiative importante, mais elle doit encore être finalisée et adoptée.

19. Au sein des Nations Unies, il faut citer le Groupe de travail sur la lutte contre l'utilisation d'Internet à des fins terroristes, sous l'égide de l'Equipe spéciale de lutte contre le terrorisme. Dans un rapport consacré aux défis, aux bonnes pratiques et aux recommandations sur des aspects juridiques et techniques, le Groupe de travail pointe les réseaux zombies comme sources de préoccupation particulière et souligne plusieurs problèmes de droit procédural gênant les enquêtes sur les attaques de grande ampleur par réseaux zombies. Dans ses recommandations, le Groupe de travail souligne l'importance de garantir la protection des droits de l'homme, le rôle clé des partenariats public–privé (PPP) et la nécessité d'une approche diversifiée.

20. L'Organisation internationale de police (INTERPOL), l'Organisation de coopération et de développement économiques (OCDE) et l'Organisation du Traité de l'Atlantique Nord (OTAN) mènent aussi d'importants travaux sur les cyberattaques, qui sont cependant davantage axés sur le renforcement des capacités et les orientations pratiques que sur la recherche de nouvelles approches réglementaires.

4. Approches législatives

4.1. Droit matériel

21. Pour pouvoir effectivement poursuivre les auteurs de cyberattaques de grande ampleur dans les Etats membres, un degré minimal d'harmonisation de la qualification pénale des infractions s'impose, notamment parce que l'entraide judiciaire suppose une double incrimination. Cependant, cette harmonisation *a minima* pourrait s'avérer insuffisante. Les Conventions n^{os} 185 et 196 ont jeté les bases d'une réglementation du Conseil de l'Europe en matière de cybercriminalité et de terrorisme, offrant des mécanismes précieux pour répondre aux actes répréhensibles. Bien que la Convention n^{o} 185 s'applique aux infractions informatiques commises au travers d'attaques de grande ampleur, elle ne classe pas les attaques selon leur degré de gravité. Or, il serait judicieux d'établir une classification plus fine des infractions, en prévoyant des peines plus lourdes pour les formes d'attaques les plus graves.

4.1.1. L'ampleur, circonstance aggravante pour une infraction informatique

22. Au regard du cadre réglementaire du Conseil de l'Europe, une infraction donnée peut aboutir aux mêmes peines indépendamment de son mode opératoire: attaque via un point unique ou via un réseau zombie. Pourtant, compte tenu des dommages que les attaques de grande ampleur peuvent causer aux systèmes visés et du préjudice subi par les propriétaires des terminaux infectés, il serait raisonnable de sanctionner les attaques de grande ampleur par des peines plus lourdes, proportionnées à la menace représentée par le comportement illicite du ou des botmasters. L'ampleur d'une cyberattaque pourrait ainsi

être interprétée comme une circonstance aggravant l'infraction car elle augmente la gravité et la culpabilité de l'acte criminel. Le cadre actuel du Conseil de l'Europe gagnerait donc à prévoir un renforcement des sanctions en cas d'attaques de grande ampleur. Bien que la Convention n° 185 évite de fixer des peines minimales ou maximales pour les infractions pénales qu'elle mentionne, une note d'orientation sur la mise en œuvre d'une disposition supplémentaire considérant l'utilisation de réseaux zombies comme une circonstance aggravante pourrait aider les Etats membres à appliquer efficacement cette disposition.

23. La directive européenne 2013/40/UE relative aux attaques contre les systèmes d'information pourrait servir d'exemple pour cet affinement du droit pénal au moyen d'instaurer des sanctions plus élevées en raison de circonstances aggravantes. Par rapport au texte précédent (la décision-cadre 2005/222/JAI relative aux attaques visant les systèmes d'information), la directive établit en général des peines plus lourdes, prévoyant en particulier des circonstances aggravantes pour les infractions d'atteintes illégales à l'intégrité d'un système et à l'intégrité des données. En vertu de l'article 9.3 de la directive, l'atteinte illégale à l'intégrité d'un système ou de données devrait être passible d'une peine d'emprisonnement maximale d'au moins trois ans lorsqu'elle est commise au moyen d'un réseau zombie[11]. L'article 9.4 de la directive prévoit une peine d'emprisonnement maximale d'au moins cinq ans lorsque les atteintes illégales à l'intégrité d'un système ou de données sont commises dans le cadre d'une organisation criminelle, lorsqu'elles causent un préjudice grave ou lorsqu'elles sont commises contre un système d'information d'une infrastructure critique.

24. Ces nouvelles dispositions inscrites dans la Directive 2013/40/UE constituent un bon exemple d'initiatives supranationales contre les attaques de grande ampleur. Toutefois, la restriction des circonstances aggravantes aux atteintes illégales à l'intégrité des systèmes et des données signifie que toutes les infractions informatiques commises via des réseaux zombies ne sont pas passibles d'une peine aggravée. Par exemple, dans le cas d'un enregistreur de frappe[12], un logiciel surveille les activités de la victime pour repérer certaines données personnelles, telles que mots de passe ou numéros de comptes bancaires. Cette surveillance permet d'accéder à des données mais ne constitue pas nécessairement une atteinte au système ou aux données, si bien qu'on pourrait considérer qu'elle échappe aux circonstances aggravantes prévues à l'article 9, paragraphes 3 et 4 de la Directive 2013/40/UE. Néanmoins, du fait de leur caractère automatisé, les logiciels malveillants qui consultent ou interceptent illégalement des données constituent une infraction informatique de grande ampleur, et ce type d'infraction pourrait aussi être considéré comme une attaque de grande ampleur contre des systèmes d'information. Puisque les réseaux zombies peuvent être utilisés à de nombreuses étapes différentes d'une infraction pénale et pour de multiples fins, il serait envisageable d'inscrire l'utilisation de réseaux zombies pour des attaques de grande ampleur parmi les circonstances aggravantes, justifiant une peine plus lourde, au-delà des seules atteintes illégales à des systèmes ou à des données.

4.1.2. Le préjudice grave, circonstance aggravante pour une infraction informatique

25. Comme déjà constaté, la Directive 2013/40/UE classe aussi le préjudice grave parmi les circonstances aggravantes en cas d'atteinte illégale à un système ou à des données. D'après le considérant n° 5, «[l]es Etats membres peuvent déterminer, en fonction de leur droit national et de leur pratique nationale, ce qui constitue un préjudice grave, comme le fait d'arrêter des services de réseau présentant un intérêt public important, ou de causer des coûts financiers majeurs ou la perte de données à caractère personnel ou d'informations sensibles». Cette approche réglementaire peut être considérée comme répondant aux attaques cyberterroristes, puisque ces dernières visent généralement à causer d'importants dommages, du fait de leur coût financier ou, au moins, de leur impact plus large sur la société. Le Conseil de l'Europe pourrait donc envisager, à travers une note d'orientation, d'instaurer une circonstance aggravante similaire pour les infractions informatiques (articles 4 et 5, plus éventuellement articles 2 et 3 de la Convention n° 185) qui causent un préjudice grave.

26. La même approche pourrait être adoptée lorsqu'une attaque vise des infrastructures essentielles, ce qui constitue également un motif d'aggravation des peines dans la directive UE. Bien que ce critère offre l'avantage d'être clair et de souligner l'importance de la protection des infrastructures essentielles, on pourrait aussi avancer qu'il est déjà compris dans celui du préjudice grave, puisque les atteintes aux infrastructures essentielles ont de grandes chances de causer de sérieux dommages (si tel n'est pas le cas, l'attaque ne doit pas nécessairement être considérée comme particulièrement grave pour justifier des peines aggravées). Prendre en compte la gravité du préjudice plutôt que le type d'ordinateur attaqué a l'avantage de remédier aux problèmes d'interprétation – quels ordinateurs appartiennent aux infrastructures essentielles au sens de

11. Ou au moyen d'un nombre important de systèmes d'information affectés par des programmes informatiques malveillants (tels que décrits à l'article 7 de la directive, comparable à l'article 6 de la Convention n° 185).
12. https://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets.

l'article 9.4 de la directive? En effet, tous les ordinateurs utilisés au sein d'une infrastructure essentielle ne sont pas reliés aux systèmes essentiels en jeu, et on peut se demander si une attaque contre un ordinateur utilisé par les services des ressources humaines ou de fidélisation des clients d'un fournisseur d'électricité doit être considérée comme visant un «système d'information d'une infrastructure critique».

27. Un autre argument plaide en faveur de circonstances aggravantes englobant le «préjudice grave». L'internet des objets est en passe de devenir une réalité. Aujourd'hui, ce ne sont plus seulement les ordinateurs et smartphones qui sont connectés à internet, mais aussi tout un éventail d'objets: des appareils domestiques comme les réfrigérateurs, machines à laver, téléviseurs et thermostats, des voitures et des appareils surveillant par exemple les conditions environnementales, les opérations sur les infrastructures ou les applications industrielles. Bien que la plupart de ces appareils ne fassent pas partie des infrastructures classiquement considérées comme essentielles, des attaques dirigées contre eux peuvent entraîner de graves dysfonctionnements et donc un préjudice grave, non seulement pour l'appareil lui-même, mais aussi pour son environnement et les personnes qui s'y trouvent (que se passerait-il si quelqu'un, au moyen d'un logiciel malveillant, prenait le contrôle de la navigation d'une voiture intelligente?). En outre, bien que l' «internet des personnes» soit encore une perspective très lointaine, les êtres humains eux-mêmes deviennent de plus en plus connectés, via des appareils enregistrant le fonctionnement du corps ou via divers implants, allant du pacemaker à l'implant cochléaire en passant par les implants cérébraux et les membres bioniques reliés au système nerveux. Ces implants exposent aussi leurs utilisateurs à des cyberattaques, qui ne seraient pas nécessairement de grande ampleur mais causeraient indéniablement un préjudice grave. La perspective d'attaques pilotées à distance contre des objets de notre environnement immédiat et contre des personnes elles-mêmes semble particulièrement effrayante – et donc particulièrement attrayante pour les cyberterroristes une fois que l'internet des objets et les implants humains connectés seront devenus plus courants. Bien que les attaques soient en principe suffisamment couvertes par la Convention n° 185, qui donne une liste complète des différents types d'attaques possibles contre des systèmes d'information, l'approche générale adoptée par les articles 2 à 6 de la Convention n° 185 risque de ne pas refléter, dans un monde où tout est connecté, la diversité des attaques et leur nature très différente de celle des attaques traditionnelles contre des PC[13]. Prévoir des circonstances aggravantes pour les infractions informatiques causant un préjudice grave pourrait apporter une réponse fructueuse aux nouvelles menaces représentées par les cyberattaques, qu'il s'agisse d'attaques de grande ampleur, visant des infrastructures essentielles ou visant des objets ou personnes rendus vulnérables par leur connexion.

4.2. Droit procédural

28. Bien que quelques améliorations puissent être apportées au droit matériel pour répondre aux cyberattaques de grande ampleur, c'est le droit procédural qui pose le plus de difficultés. La plupart des cyberattaques tombent sous le coup d'une disposition pénale dans la plupart des systèmes juridiques, mais c'est généralement au niveau de l'enquête que le bât blesse – lorsqu'il s'agit d'identifier les suspects et de recueillir suffisamment de preuves. Les raisons en sont multiples; nous nous concentrerons ici sur trois aspects que nous jugeons particulièrement importants.

4.2.1. Mise en œuvre des dispositions procédurales de la Convention n° 185

29. La Convention n° 185 présente une liste assez complète[14] de pouvoirs d'enquête que les Etats membres sont invités à prévoir dans leur législation. Les pouvoirs les plus importants, à savoir l'injonction de produire (article 18), la perquisition et saisie (article 19) et l'examen des télécommunications (articles 20-21), y figurent, ainsi que d'importants pouvoirs accessoires facilitant la conservation rapide de données susceptibles de perte (articles 16-17). En général, les Parties à la convention ont appliqué les dispositions de droit matériel de la Convention n° 185 dans leur droit national de façon plus systématique et complète que les dispositions procédurales. Par exemple, le pouvoir de perquisitionner un système informatique prévu à l'article 19.2, extension d'une perquisition *in situ* à celle de données stockées dans un autre système situé sur le territoire

13. Gasson et Koops (2013), Attacking human implants: a new generation of cybercrime, 5 Law, Innovation and Technology (2), p. 248-277.

14. Assez complète seulement car la convention ne couvre pas certains pouvoirs qui peuvent s'avérer importants, comme la perquisition à distance (visant des ordinateurs via internet de façon indépendante, sans lien avec une perquisition déjà lancée dans un lieu donné au sens de l'article 19 de la Convention n° 185). Nous ne pouvons examiner plus avant dans le présent rapport l'opportunité de créer des pouvoirs d'enquête supplémentaires, une question complexe, notamment en raison de l'équilibre délicat à trouver entre l'autorisation de nouvelles formes très intrusives d'enquêtes pénales et la préservation de la protection des droits fondamentaux. La question des pouvoirs d'enquête devrait être abordée dans le cadre des activités de suivi sur la réglementation en matière de lutte contre les cyberattaques de grande ampleur.

de l'Etat qui perquisitionne et légalement accessibles à partir du système initial, figure expressément dans la législation de pays comme l'Allemagne (article 110.3 du Code de procédure pénale allemand), les Pays-Bas (article 125.j du Code de procédure pénale néerlandais) et le Royaume-Uni (article 20 de la loi de 1984 sur la police et les preuves pénales), mais on ne trouve aucune disposition expresse équivalente en droit bulgare, croate, italien ou slovène par exemple. Point à noter, les Philippines, qui ne sont pas Parties à la Convention n° 185 mais l'ont utilisée comme modèle de législation, ont repris presque tels quels les articles 19.1, 19.3 et 19.4 de la Convention dans l'article 15 de leur loi de prévention de la cybercriminalité mais n'ont pas transposé l'article 19.2. Il serait selon nous utile de disposer d'une étude complète de l'application de la Section 2 (droit procédural) dans les législations nationales, afin de savoir s'il existe bel et bien des lacunes importantes dans la mise en œuvre de la Convention n° 185 et, si oui, d'en analyser les raisons.

4.2.2. Harmonisation de l'entraide

30. Le chapitre III de la Convention n° 185 comprend des mesures importantes pour harmoniser l'entraide en matière pénale, cruciale pour enquêter sur des infractions informatiques qui ont très souvent une composante internationale et concernent des données particulièrement sensibles aux risques de perte si elles ne sont pas rapidement conservées. Outre les dispositions réglementant les différents cas de recours à l'entraide, la mise en place d'un Réseau 24/7 (article 35) est particulièrement importante pour permettre des contacts rapides entre Etats et faciliter l'entraide. Il semble que les procédures d'entraide, malgré les efforts d'harmonisation existants et les nombreux contacts de qualité entre Etats et entre acteurs de terrain, restent souvent lentes, du moins en ce qui concerne les enquêtes sur la cybercriminalité. Il faut toujours facilement une ou plusieurs semaines, sinon plus, pour obtenir des preuves à la suite d'une demande d'entraide, intervalle pendant lequel les données recherchées peuvent être déplacées ou supprimées. Ce point n'est pas facile à résoudre. Dans tous les cas, le fonctionnement rapide et sans heurts des procédures d'entraide est vital pour assurer une réponse effective aux cyberattaques de grande ampleur.

31. L'intérêt de mesures juridiques allant plus loin, comme l'instauration d'un délai maximal pour répondre à une demande d'entraide judiciaire, pourrait être étudié[15]. Cependant, les obstacles aux procédures d'entraide rapide sont probablement de nature plus organisationnelle. Des mesures visant à stimuler l'investissement dans des moyens de traitement des demandes d'entraide, à sensibiliser à l'importance de réponses rapides à de telles demandes pour la lutte contre la cybercriminalité en général, et peut-être à donner des directives claires aux autorités nationales pour qu'elles puissent définir, compte tenu de leurs ressources limitées, leurs priorités en matière de traitement des demandes, pourraient s'avérer plus judicieuses que des obligations légales qui resteront lettre morte en l'absence de moyens suffisants ou d'accueil favorable de la part des acteurs chargés de les appliquer sur le terrain. Etant donné que les difficultés à assurer une entraide satisfaisante sont reconnues depuis longtemps mais que les procédures, à notre connaissance, restent trop lentes, des recherches supplémentaires pourraient être entreprises pour comprendre les raisons du problème et trouver des solutions novatrices.

4.2.3. Accès transfrontalier aux données

32. Compte tenu des limites de l'entraide et, parfois, des difficultés à déterminer le territoire sur lequel les données sont stockées, par exemple dans le contexte de l'informatique décentralisée, il est urgent d'autoriser les enquêteurs chargés d'affaires de cybercriminalité à accéder à distance à des données y compris lorsque ces dernières sont stockées sur le territoire d'autres pays. Ce thème est examiné au sein du Conseil de l'Europe par le «Groupe sur l'accès transfrontalier», sous-groupe ad hoc du Comité de la Convention sur la cybercriminalité travaillant sur la compétence et l'accès transfrontalier aux données. Il étudie la possibilité d'un protocole additionnel ou d'une recommandation et a proposé plusieurs solutions possibles susceptibles d'être retenues dans un protocole:

«1. Accès transfrontalier avec consentement, mais non limité aux données stockées «sur le territoire d'une autre Partie» (...).

2. Accès transfrontalier sans consentement mais par des moyens obtenus légalement (…).

3. Accès transfrontalier sans consentement de bonne foi ou dans des situations urgentes ou exceptionnelles (…).

15. On trouve une timide tentative en ce sens dans la directive 2013/40/UE, qui demande aux Etats, à l'article 13.1, d'indiquer «dans un délai de huit heures à compter de la réception de la demande, au moins si la demande sera satisfaite, et la forme et le délai estimé pour cette réponse». Si cette disposition peut aider l'autorité requérante à mieux planifier ses activités, elle ne constitue en rien l'obligation de coopérer rapidement.

4. Extension des perquisitions [du système initialement perquisitionné aux systèmes connectés] sans la limite au territoire de la Partie qui perquisitionne prévue à l'article 19 [paragraphe 2] (...).

5. Le pouvoir d'utilisation comme critère de légalité des recherches (...)[16]».

33. Aucune de ces propositions (sauf peut-être la deuxième) ne donne d'orientation claire pour traiter le problème, en raison des strictes limites que le droit international pose à l'accès à des données sur le territoire d'un autre Etat sans le consentement préalable de cet Etat. Un tel accès n'est licite en droit international que lorsque les Etats se sont accordés sur certaines formes d'accès unilatéral, comme prévu par exemple à l'article 32.*b* de la Convention n° 185 (qui autorise l'accès transfrontalier à des données avec le consentement volontaire de l'usager ou de prestataire si cette personne est légalement autorisée à divulguer les données); de plus, l'article 32.*b* a un champ d'application limité et ne fait pas l'unanimité.

34. On pourrait considérer que l'article 32.*b* englobe déjà la proposition n° 2, c'est-à-dire la possibilité de mener une perquisition transfrontalière par des moyens obtenus légalement (c'est-à-dire l'identifiant de connexion et le mot de passe d'un compte, s'il a été légalement fourni par le suspect ou par le prestataire de services ou trouvé, par exemple, sur un post-it sur le bureau du suspect au cours d'une perquisition légale), si l'Etat qui perquisitionne sait que les données sont stockées dans un Etat qui est partie à la convention. Une telle interprétation doit encore recueillir l'assentiment des Etats Parties à la Convention sur la cybercriminalité pour pouvoir être considérée comme légitime; mais elle pourrait prendre la forme d'une note d'orientation plutôt que d'un protocole, qui suppose un long processus de ratification.

35. En dehors de cette proposition, il est peu probable que les Etats parviennent à s'entendre dans de brefs délais sur des formes plus poussées d'accès transfrontalier aux données. A notre époque de plus en plus mobile et connectée, les autorités répressives n'auront donc toujours que des moyens très limités d'enquêter sur la cybercriminalité. Cette difficulté ne pourra être correctement levée qu'au prix de considérables travaux préliminaires, qui devraient passer par la reconnaissance formelle du problème par les représentants des Etats dans des forums internationaux et par le rapprochement des acteurs des enquêtes sur la cybercriminalité et de ceux du droit international, qui se rencontrent rarement et manquent souvent des connaissances de base sur les aspects et évolutions clés de l'autre domaine. Le Conseil de l'Europe pourrait jouer un rôle important à cet égard en accueillant des manifestations réunissant les deux communautés pour discuter de cette question, contribuant ainsi à sensibiliser à la nécessité que les autorités répressives puissent accéder d'une manière ou d'une autre à des données à l'étranger tout en restant dans les limites du droit international. Une fois le problème suffisamment reconnu et correctement cerné, les Etats pourront entreprendre de le résoudre en s'appuyant sur les régimes juridiques internationaux existants dans des domaines atypiques (tels que l'imagerie spatiale et satellitaire, la haute mer, la piraterie et la compétence de l'Etat du port) pour tenir compte du cyberespace et de l'informatique décentralisée, autorisant une certaine forme d'action unilatérale acceptable dans un tel espace.

5. Mesures non juridiques

5.1. Renforcement des capacités

36. Le Conseil de l'Europe a soutenu plusieurs activités de formation et de renforcement des capacités des autorités répressives dans le domaine de la cybercriminalité. De 2006 à 2011, le Projet global sur la cybercriminalité (phase 1) s'est concrétisé dans plusieurs pays du monde, avec plus de 110 activités visant à renforcer la justice pénale et à améliorer la mise en œuvre de la Convention n° 185 et la coopération dans ce cadre. Les programmes de renforcement des capacités, en rapprochant des professionnels de différents pays, offrent aux forces de l'ordre et aux autres acteurs concernés l'occasion d'améliorer leurs connaissances et d'actualiser leurs techniques en entrant en contact avec d'autres experts. Les cyberattaques de grande ampleur, qui ne sont pas les infractions informatiques les plus fréquentes, demandent à ce que les autorités répressives disposent de la formation et des équipements suffisants pour faire face à des criminels organisés ou ayant des motivations politiques et aux techniques modernes de diffusion de logiciels malveillants. Cela suppose aussi davantage de coopération car les attaques de grande ampleur, par leur nature même, entraînent presque toujours des infections transfrontalières. Le renforcement des capacités, en vue d'améliorer les compétences et la résilience face à la cybercriminalité, est inscrit dans les politiques de cybersécurité de nombreux pays et entre désormais dans la Stratégie de cybersécurité de l'Union européenne[17].

16. Comité de la Convention sur la cybercriminalité, document T-CY(2013)14, (Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data (Strasbourg, Conseil de l'Europe).

37. Néanmoins, nous n'avons pas trouvé de programmes de formation spécifiquement consacrés au cyberterrorisme ou aux attaques de grande ampleur au niveau du Conseil de l'Europe[18], ce qui montre la nécessité d'encourager les formations ciblant ce domaine. Au vu des risques particuliers liés à cette menace potentielle et de l'étendue de ses conséquences, les activités de renforcement des capacités sur les cyberattaques de grande ampleur sont de la plus haute importance. Le Conseil de l'Europe, compte tenu de son histoire et de son expérience en matière de promotion de la prééminence du droit, serait bien placé pour lancer un programme spécifique sur les cyberattaques de grande ampleur et l'utilisation des réseaux zombies, mettant l'accent sur la protection des infrastructures essentielles, l'internet des objets et l'informatique décentralisée, et pour inscrire ces thèmes à l'ordre du jour des réunions et ateliers des initiatives de lutte contre le terrorisme et la cybercriminalité.

5.2. Partenariats public–privé

38. En matière de lutte contre la cybercriminalité, les partenariats public–privé (PPP) ont le vent en poupe, puisqu'ils permettent de rapprocher différents acteurs des secteurs public et privé, de mettre en commun les informations et les expériences concernant les menaces et d'élaborer de meilleures stratégies de lutte contre la cybercriminalité. Le secteur privé ne saurait être tenu à l'écart de la lutte contre la cybercriminalité, puisque les entreprises qui assurent l'infrastructure d'internet et différents services en ligne sont les mieux placées pour, par exemple, repérer le lancement d'une attaque DDoS ou un usage malveillant de leur infrastructure. En outre, les entreprises de sécurité des technologies de l'information, fortes d'une longue expérience, sont les acteurs les plus compétents pour mener une analyse approfondie des données après une infection et mieux comprendre les caractéristiques des menaces, et pourraient pousser à des travaux de recherche et développement en vue d'améliorer les outils de protection contre les failles. Pour être efficace, le cadre de lutte contre les cyberattaques de grande ampleur requiert l'existence d'un réseau collaboratif transversal, solide et hyper-compétent. Bien qu'il n'y ait pas à notre connaissance de PPP spécifiquement consacré aux cyberattaques de grande ampleur, on rencontre plusieurs exemples de PPP mis en place pour lutter contre la cybercriminalité ou contre le terrorisme[19], dont certains consacrés aux réseaux zombies[20].

39. Les PPP sont une affaire de confiance et fonctionnent bien mieux lorsqu'ils reposent sur des organisations fiables, jouissant d'un certain crédit auprès de leurs partenaires et du grand public. Fort de sa réputation en matière de lutte contre la cybercriminalité et le cyberterrorisme, le Conseil de l'Europe peut jouer un rôle important dans la promotion des PPP ainsi que dans le rapprochement des initiatives existantes. La collaboration et les échanges rendus possibles par un réseau coopératif de partenariats public–privé sur les questions de cybercriminalité, de terrorisme et de réseaux zombies peuvent livrer d'importants éléments de réponse aux cyberattaques de grande ampleur. Ce cadre se nourrirait des connaissances et des efforts déjà déployés par de nombreuses équipes nationales et organisations régionales sur différents aspects de la criminalité.

6. Inverser la perspective

40. La menace de cyberattaques de grande ampleur paraît importante – nous ne connaissons pas son niveau réel, faute de statistiques fiables. La difficulté de répondre à la cybercriminalité réside en partie dans la mythologie qui l'entoure, fondée sur une image souvent influencée par les personnages de hackers au

---

17. Sur ce sujet, voir les travaux de l'ENISA et les supports de formation destinés aux équipes d'intervention en cas d'urgence informatique concernant la réponse aux incidents de grande ampleur: https://www.enisa.europa.eu/activities/cert/support/exercise.

18. A l'exception du «Nouvel exercice de classification des mouvements de capitaux sur internet: méthodes, tendances et actions conjuguées de plusieurs parties prenantes», lancé par MONEYVAL (Comité d'experts du Conseil de l'Europe sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme) et par la Fédération de Russie en septembre 2009, dans le cadre du Projet global sur la cybercriminalité (phase 2): activités. Cependant, le rapport ne traite pas directement des mécanismes visant les réseaux zombies: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/all%20activities_fr.asp.

19. «L'importance des PPP dans le contexte de la lutte antiterroriste est expressément reconnue par la Stratégie antiterroriste mondiale de l'Organisation des Nations Unies, dans son chapitre III, paragraphe 13, qui encourage l'identification et le partage des bonnes pratiques pour empêcher les attentats terroristes contre des cibles particulièrement vulnérables». Institut interrégional de recherche des Nations Unies sur la criminalité et la justice, Public–Private Partnerships (PPPs) for the Protection of Vulnerable Targets Against Terrorist Attacks: Review Of Activities And Findings, janvier 2009.

20. Comme l'EP3R de l'ENISA et le projet de Centre coopératif d'excellence pour la cyberdéfense financé par l'Union européenne, ainsi que des initiatives nationales, comme Botfrei.de (Allemagne), AbuseHub (Pays-Bas), AISI (Australie), Cyber Clean Center (Japon) et l'Anti-Botnet Code of Conduct (Etats-Unis).

cinéma et dans les romans et par des chiffres gonflés tels qu'on en trouve dans les rapports des entreprises de sécurité en ligne. Il serait utile, en premier lieu, de disposer de statistiques plus fiables. Les autorités de réglementation devraient encourager les recherches indépendantes sur la prévalence de la cybercriminalité, dont les infections par réseaux zombies et les attaques de grande ampleur, afin de fonder les politiques dans ce domaine sur de meilleures bases.

41. Parallèlement, même lorsque des données fiables sont disponibles, les concepteurs des politiques ne devraient pas tomber dans le piège consistant à s'efforcer de réduire à néant les risque d'attaques de grande ampleur en adoptant des mesures de détection et de sanction des auteurs de plus en plus répressives et des mesures de sécurité de plus en plus coûteuses. Nous vivons dans une société du risque, où les problèmes sociaux sont envisagés au travers des risques qu'ils représentent et des stratégies susceptibles de les réduire. Dans ce contexte, on observe la montée d'une culture de la peur – la peur de conséquences néfastes l'emporte sur les évaluations rationnelles et désintéressées des risques réellement encourus. Comme le montrent les révélations d'Edward Snowden, les pouvoirs publics peuvent se laisser aller à appliquer des mesures antiterroristes sans s'assurer dûment que ces mesures sont vraiment nécessaires, légitimes, efficaces et rentables. Bien que ce message soit difficile à entendre dans une société qui fuit le risque, les citoyens devraient savoir qu'il est impossible de vivre dans un monde entièrement dénué de risque et que nous devons par conséquent apprendre à faire face à l'adversité, qu'il s'agisse de catastrophes naturelles, de crimes ou d'attentats terroristes. Bien sûr, le potentiel de nuisance des attentats terroristes est énorme, si bien qu'ils représentent un risque considérable même si la probabilité qu'ils ne surviennent est faible. Pour autant, toutes les mesures de réduction des risques ne se justifient pas. Les mesures destinées à prévenir ou à atténuer les effets de cyberattaques de grande ampleur peuvent avoir un coût énorme, à la fois sur le plan économique et au regard de leur impact négatif sur les libertés et droits fondamentaux.

42. Tout en évitant de tomber dans le piège consistant à viser le «risque zéro», les concepteurs des politiques devraient tenir compte d'une autre perspective. Beaucoup de politiques traitent les conséquences et les symptômes des nouveaux phénomènes mais non leurs causes. S'agissant des cyberattaques de grande ampleur, on peut facilement supposer qu'elles sont une conséquence des possibilités d'abus d'internet à des fins criminelles et terroristes, et donc concevoir des politiques visant à la fois à mieux sécuriser internet et à réprimer plus sévèrement les attaques commises via internet. Cependant, le risque représenté par les cyberattaques de grande ampleur repose aussi largement sur la dépendance croissante de la société vis-à-vis des TIC et d'internet. Aujourd'hui, les systèmes et réseaux informatiques sont utilisés pour presque toutes les activités sociétales, et passer par internet plutôt que par des moyens hors ligne présente tant d'avantages que de nombreuses activités sont en train de devenir rapidement dépendantes des systèmes d'information et de l'infrastructure internet. Nous créons ainsi une société extrêmement vulnérable. Cette vulnérabilité ne réside pas dans la menace de cyberattaques en soi, mais dans l'ampleur de l'impact et des effets en cascade que ces attaques peuvent avoir sur de nombreux secteurs, personnes et activités.

43. De ce fait, nous jugeons important d'inverser en quelque sorte la perspective sur le défi que représentent les cyberattaques de grande ampleur. En plus de s'interroger sur les mesures à prendre pour mieux protéger nos infrastructures et mieux repérer et poursuivre ceux qui les attaquent, les concepteurs des politiques devraient aussi se demander jusqu'où devrait aller la dépendance de notre société à l'égard d'internet, devenu la pierre angulaire de toutes les activités sociétales. Quel que soit l'arsenal des mesures adoptées, internet est et restera peu sûr. Quoi que nous fassions, il y aura des attaques, y compris de grande ampleur, avec parfois des effets dévastateurs. Par conséquent, toute stratégie raisonnable de gouvernance de la cybercriminalité devrait compter parmi ses éléments clés le renforcement de la résilience de la société devant une infrastructure internet inévitablement exposée aux attaques. Cette résilience suppose non seulement des systèmes d'alerte précoce et de réaction rapide, mais aussi l'atténuation des effets des attaques sur les infrastructures essentielles. Il faut pour cela disposer d'alternatives appropriées, et notamment d'infrastructures de secours fonctionnelles et éprouvées en cas de panne temporaire d'internet. Les hôpitaux ont des générateurs d'électricité en cas de coupure du réseau. De quelles solutions et infrastructures de secours les pays européens disposent-ils pour suppléer aux réseaux électriques et systèmes de transports intelligents, à l'enseignement à distance, aux e-banques, à l'e-administration, etc.? Pouvons-nous toujours, si une cyberattaque bloque temporairement l'accès à internet à grande échelle, payer en monnaie non électronique, utiliser des appareils fonctionnant hors ligne, conduire de «bêtes» voitures, consulter des livres, obtenir un passeport? Si la réponse est non, alors les stratégies de réponse aux cyberattaques de grande ampleur seront peu ou prou vouées à l'échec, ou coûteront si cher qu'aucun e-citoyen/e-consommateur ne sera prêt à en payer le prix.

7. Conclusion

44. L'une des difficultés majeures de la gouvernance de la cybercriminalité aujourd'hui réside dans la réponse aux cyberattaques de grande ampleur et notamment, quoique non exclusivement, à celles commises via des réseaux zombies (vastes réseaux d'ordinateurs infectés). Les instruments élaborés ces dernières décennies pour répondre à la cybercriminalité s'appliquent à de telles attaques mais ne sont pas particulièrement adaptés à leur ampleur et à leurs modalités nouvelles, dont les réseaux zombies. Parallèlement, les instruments élaborés pour répondre à des attentats terroristes sont susceptibles de répondre à des attaques de grande ampleur mais souvent non spécifiquement adaptés aux attaques informatiques. Il existe donc une marge d'amélioration dans la réponse aux défis que représentent les cyberattaques de grande ampleur.

45. Par conséquent, les mesures réglementaires suivantes pourraient être envisagées pour relever ces défis:

–

– Distinguer, en droit pénal, les formes communes de la cybercriminalité (déjà bien couvertes par la Convention n° 185) de ses formes aggravées, notamment les attaques commises au moyen de réseaux zombies et/ou les attaques entraînant un préjudice grave; dans le deuxième cas, une harmonisation des législations nationales pourrait être envisagée, précisant que la peine minimale pour une infraction informatique aggravée doit être d'au moins quelques années d'emprisonnement.

– Mener une enquête complète sur les mises en œuvre au niveau national des dispositions de droit procédural de la Convention n° 185, afin de repérer d'éventuelles lacunes et d'analyser les raisons d'une mise en œuvre insuffisante.

– Harmoniser encore les procédures d'entraide judiciaire, en investissant dans des ressources permettant de traiter ces demandes, en sensibilisant à leur importance, en donnant des orientations pour fixer des priorités au moment d'y répondre et éventuellement en instaurant des délais de réponse maximaux. Des recherches supplémentaires seraient souhaitables afin de comprendre pourquoi les efforts actuels d'harmonisation de l'entraide judiciaire semblent avoir globalement échoué.

– Inscrire résolument le défi de l'accès transfrontalier aux données à l'ordre du jour international et associer à la fois les acteurs des enquêtes informatiques et ceux du droit international aux discussions sur ce thème, afin de sensibiliser à la nécessité que les autorités répressives puissent accéder d'une manière ou d'une autre à des données à l'étranger tout en restant dans les limites du droit international. Une note d'orientation supplémentaire pourrait être envisagée pour que l'article 32.*b* de la Convention n° 185 soit interprété comme autorisant les perquisitions transfrontalières unilatérales par des moyens obtenus légalement. A plus long terme, il convient d'encadrer de façon réaliste les perquisitions transfrontalières dans le cyberespace sans préjudice du respect du droit international.

– Il convient d'encourager un renforcement des capacités particulièrement ciblé sur les cyberattaques de grande ampleur. Le Conseil de l'Europe pourrait lancer un programme de formation spécifique sur les cyberattaques de grande ampleur et sur l'utilisation des réseaux zombies, en insistant sur la protection des infrastructures essentielles, l'internet des objets et l'informatique décentralisée.

– Les autorités répressives et les organismes publics de cybersécurité ne peuvent lutter seuls contre les cyberattaques de grande ampleur. Cette lutte ne relève pas non plus de la responsabilité première du secteur privé. Afin de promouvoir des partenariats public–privé efficaces et légitimes, nécessaires à la lutte commune contre les cyberattaques de grande ampleur, le Conseil de l'Europe pourrait contacter et rapprocher les PPP existants dans les domaines du terrorisme et de la cybercriminalité, favoriser la création de nouveaux PPP dans le cadre de ses programmes d'information et de renforcement des capacités et adopter une recommandation appelant les Etats membres à se joindre aux efforts régionaux et à favoriser des PPP nationaux contre les cyberattaques de grande ampleur.

– Les mesures de lutte contre les cyberattaques de grande ampleur devraient reposer sur des statistiques fiables et indépendantes concernant la prévalence de telles attaques. Ces politiques ne devraient pas tenter à tout prix de réduire à néant le risque d'attaques de grande ampleur, mais en évaluer les coûts de façon rationnelle et fondée (à la fois les coûts économiques et l'impact sur les droits de l'homme et les libertés fondamentales), tout en gardant à l'esprit que le risque ne peut pas toujours être calculé et qu'il est de toutes manières impossible de l'éliminer complètement.

– Les mesures doivent s'attacher à renforcer la résilience de la société face aux cyberattaques de grande ampleur, ce qui suppose de prendre des initiatives pour éviter que la société ne devienne trop dépendante des infrastructures internet. Là où les pouvoirs publics stimulent, facilitent ou tolèrent le

remplacement des formes d'interaction hors ligne par des formes d'interaction en ligne, il convient de veiller à ce que des solutions de secours appropriées restent disponibles. internet est et restera peu sûr, et des cyberattaques – mineure ou graves – se produiront quelle que soit l'étendue des mesures prises. La société doit être préparée à surmonter les conséquences de cyberattaques de grande ampleur.

Annexe – Réglementation au niveau international

Conseil de l'Europe

1. La Convention du Conseil de l'Europe sur la cybercriminalité (STE n° 185), largement connue sous le nom de «Convention sur la cybercriminalité» (ci-après: «Convention n° 185»), présente quatre catégories d'infractions de cybercriminalité, à savoir: 1. les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques; 2. les infractions informatiques; 3. les infractions se rapportant au contenu, c'est-à-dire la pornographie enfantine (catégorie complétée par le Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, STE n° 189), et 4. les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes. Comme le précise le rapport explicatif de la Convention n° 185, les dispositions de droit matériel de la Convention visent à harmoniser les législations nationales en fixant des normes minimales communes sur la cybercriminalité. Les Etats membres et les autres Parties à la convention sont libres de s'appuyer sur ces normes communes pour renforcer leur droit national en matière de cybercriminalité. En fait, la Convention n° 185 a été utilisée comme modèle de loi, plusieurs signataires optant pour une approche nationale de la cybercriminalité plus large et plus complète, comme on le voit par exemple dans les codes pénaux de l'Allemagne, des Etats-Unis et de la Suisse.

2. En outre, la Convention du Conseil de l'Europe pour la prévention du terrorisme (STCE n° 196) (ci-après: «Convention n° 196») opte pour un large champ d'application et ne donne pas de définition précise du terme de terrorisme. La définition est à rechercher dans les instruments énumérés en annexe à la convention. Toutefois, ces instruments eux-mêmes ne livrent pas de définition du terrorisme complète et reconnue au plan international; cette définition est donc avant tout laissée à la discrétion des Etats au niveau national.

3. Le Conseil de l'Europe a érigé le cyberterrorisme et l'utilisation d'internet à des fins terroristes en domaines de travail prioritaires. Ils figurent à l'ordre du jour du Comité d'experts sur le terrorisme (CODEXTER) depuis 2006. Un rapport d'experts, *Cyberterrorism – the use of the Internet for terrorist purposes* souligne trois usages potentiels des systèmes d'information par des terroristes, conformément à la typologie utilisée dans la Convention n° 185: a) attaques en ligne visant des infrastructures essentielles et des vies humaines; b) diffusion de contenus à caractère terroriste (exposé d'idées, de menaces et de propagande à caractère terroriste, recrutement et formation, financement et levée de fonds); et c) autres usages logistiques des systèmes d'information par des terroristes (communication en ligne et analyse des cibles). Comme déjà relevé, un acte de cyberterrorisme peut être difficile à reconnaître en tant que tel, puisqu'il entre aussi presque inévitablement dans le champ de la cybercriminalité au sens de la Convention n° 185, avec les conséquences déjà évoquées.

4. La contribution du Conseil de l'Europe et des Conventions nos 185 et 196 à l'élaboration d'une réponse à la cybercriminalité et au terrorisme est indéniable. Cependant, la cybercriminalité a considérablement évolué depuis l'adoption des Conventions nos 185 et 196. De nouvelles formes d'infractions sont apparues et les formes anciennes sont devenues plus élaborées. On peut donc se demander si des activités criminelles telles que les réseaux zombies et les cyberattaques de grande ampleur sont aujourd'hui suffisamment couvertes par la Convention n° 185. De plus, les procédures pénales en vigueur entravent sérieusement les enquêtes et les poursuites dans ce domaine, en particulier dans le contexte des réseaux transfrontaliers. Enfin, le cadre réglementaire du Conseil de l'Europe sur le terrorisme et la cybercriminalité n'offre aucune disposition spécifique sur la protection des infrastructures essentielles.

Union européenne

5. La Communication de 2004 de l'Union européenne sur la protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme reflète les préoccupations régionales sur une éventuelle utilisation terroriste des systèmes d'information contre des infrastructures essentielles. La Communication signale que des attaques cybernétiques et physiques combinées pourraient interrompre le fonctionnement d'infrastructures essentielles, causant d'importants dommages à la société. Comme le souligne la Communication, les infrastructures critiques des Etats membres de l'Union européenne sont de plus en plus dépendantes des systèmes d'information et les unes des autres. Cette dépendance technologique rend les infrastructures essentielles plus exposées aux ingérences, coupures et destructions, et l'interdépendance des infrastructures fait craindre des défaillances en cascade. La Stratégie de lutte contre le terrorisme de l'Union européenne inscrit parmi les priorités en la matière l'élaboration d'approches communes pour détecter les comportements posant problème, en particulier l'utilisation abusive d'internet, et prendre des mesures pour

les combattre. La Communication sur la protection des infrastructures critiques a abouti en 2006 au Programme européen de protection des infrastructures critiques (EPCIP), puis à l'adoption de la Directive 2008/114/CE, qui érige en priorité la lutte contre les menaces terroristes.

6. Plus récemment, la Stratégie de cybersécurité de l'Union européenne, publiée en 2013, a souligné la nécessité d'améliorer les outils et les instruments de lutte contre les activités cyberterroristes. Dans le cadre des efforts pour renforcer la cybersécurité dans l'Union européenne, une proposition de directive concernant des mesures destinées à assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union (ci-après: «directive sur la cybersécurité») a été lancée, suivie de près par l'adoption de la Directive 2013/40/UE relative aux attaques contre les systèmes d'information. En outre, le cadre réglementaire de l'Union européenne en matière de cybersécurité a chargé Europol avec son Centre européen de lutte contre la cybercriminalité (EC3) et l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) d'agir pour améliorer les mesures de prévention, de résilience et de lutte face à la cybercriminalité. En décembre 2013, Europol et le Federal Bureau of Investigation (FBI) des Etats-Unis, en s'associant au secteur privé et aux autorités répressives nationales, sont parvenus à stopper le botnet ZeroAccess, qui aurait infecté quelque deux millions de systèmes dans le monde entier.

7. Le texte original de la proposition de directive sur la cybersécurité prône un cadre renforcé dans les cas où les incidents contre des systèmes d'information sont liés à des actes de cyberespionnage ou à des attaques favorisées par un Etat, ou s'ils ont des conséquences sur la sécurité nationale. Dans ces cas, des mécanismes d'alerte précoce permettraient aux autorités nationales de sécurité et de défense de signaler rapidement la menace aux acteurs concernés afin de leur permettre de gérer le risque et la crise et d'y apporter des réponses appropriées. En outre, la Directive 2013/40/UE relative aux attaques contre les systèmes d'information («Directive Botnet») introduit la notion d'attaques de grande ampleur, érige en infraction pénale l'usage illégal de logiciels malveillants et renforce les sanctions pour certaines infractions spécifiques commises via des réseaux zombies. Dans ce texte, deux critères amènent à considérer qu'une attaque est «de grande ampleur»: la taille du système visé et le préjudice qu'il subit. En vertu de la Directive 2013/40/UE, une attaque de grande ampleur est donc une attaque qui affecte un grand nombre de systèmes ou qui cause des dommages économiques notables. Quoi qu'il en soit, il n'a été fixé ni nombre minimum de systèmes ni montant minimum de pertes économiques, ce qui laisse la porte ouverte aux interprétations dans les cas concrets. La Directive 2013/40/UE constitue un instrument novateur de lutte contre les cyberattaques de grande ampleur, qui ouvre la voie à des sanctions appropriées.

8. De plus, la Convention d'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne du 29 mai 2000 pose la base juridique de la coopération transfrontalière des services répressifs au sein de l'Union.

Organisation internationale de police (INTERPOL)

9. L'Organisation internationale de police est l'organisation de police la plus importante au monde, avec 190 pays membres, et lutte activement contre le terrorisme et la cybercriminalité. INTERPOL et les Nations Unies coopèrent de longue date dans le domaine du maintien de l'ordre, et de nombreux instruments internationaux adoptés par les Nations Unies appellent les Etats membres à collaborer avec INTERPOL pour garantir la prééminence du droit. Le rôle d'INTERPOL dans la lutte contre la cybercriminalité est centré sur l'harmonisation, le renforcement des capacités et le soutien opérationnel et criminalistique. L'unité Criminalité de haute technologie d'INTERPOL organise des réunions de groupes d'experts et des sessions de formation au niveau mondial et régional, coopérant avec les autorités répressives, les secteurs concernés et les universités et apportant une aide aux membres en cas d'attaques ou de demandes de coopération. Dans le domaine du terrorisme, INTERPOL collecte, stocke, analyse et échange avec les pays membres et d'autres organisations internationales des données concernant des activités potentiellement terroristes.

10. Bien qu'INTERPOL n'ait pas vocation à établir une législation internationale contraignante en matière pénale, l'organisation a adopté en 2005 la Résolution AG-2005-RES-10, qui appelle entre autres les Etats membres à créer des points de contact nationaux dans leurs services chargés de l'application de la loi pour faciliter l'échange rapide d'informations, à prendre part aux enquêtes internationales et à accroître l'échange d'informations sur les réseaux terroristes internationaux et les méthodologies qui facilitent leurs activités, y compris des informations relatives à l'utilisation d'internet aux fins d'activités criminelles.

Organisation du traité de l'Atlantique Nord (OTAN)

11. L'Organisation du traité de l'Atlantique Nord, organisation militaire internationale, est active dans la lutte contre le terrorisme et dans le domaine de la cyberdéfense et de la guerre cybernétique. Les concepts stratégiques de l'OTAN visent à lutter contre le cyberterrorisme et à protéger les infrastructures essentielles et témoignent des efforts de l'organisation pour améliorer la prévention et la détection des cyberattaques et du terrorisme international et mieux lutter contre ces phénomènes. A cette fin, l'OTAN organise des ateliers et des formations de renforcement des capacités à l'attention des Etats membres. En 2013, le Centre coopératif d'excellence pour la cyberdéfense (CCDCOE) a publié le *Tallinn Manual on the International Law Applicable to Cyberwarfare*. Ce manuel passe en revue le droit humanitaire international existant pour en déterminer l'application aux conflits dans le cyberespace. Il s'agit aujourd'hui du manuel le plus complet en matière de cyberdéfense; il constitue aussi un bon exemple de la manière dont les organisations peuvent renforcer la prééminence du droit sans nécessairement créer de nouvelles législations.

Organisation de coopération et de développement économiques (OCDE)

12. L'Organisation de coopération et de développement économiques n'est pas particulièrement active dans la lutte contre le crime et le terrorisme, mais principalement dans les domaines de la croissance économique, du développement social et des défis environnementaux. Néanmoins, l'OCDE a le statut d'observateur auprès du Comité de la Convention sur la cybercriminalité (T-CY) du Conseil de l'Europe et s'est jointe aux efforts en matière de cybersécurité. Elle a publié des Lignes directrices régissant la sécurité des systèmes et réseaux d'information. En 2012, l'OCDE a publié *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. L'organisation mentionne dans ce document l'usage d'internet à des fins terroristes comme exemple de l'évolution rapide des sources, des motivations, de la nature, de l'organisation et de la complexité des menaces.

Nations Unies

13. D'importantes résolutions adoptées par le Conseil de sécurité des Nations Unies ont attiré l'attention des Etats sur les menaces cyberterroristes (Résolutions 1373/2001 et 1566/2004). La Résolution 1624/2005, en particulier, condamne l'usage d'internet pour justifier des actes terroristes ou en faire l'apologie et engage les Etats à interdire par la loi l'incitation à commettre un ou des actes terroristes. Parmi les autres instruments des Nations Unies soulignant la nécessité de mesures renforcées contre le cyberterrorisme figurent la Résolution 1963/2010 du Conseil de sécurité et le rapport de 2006 du Secrétaire général à l'Assemblée générale intitulé «S'unir contre le terrorisme: recommandations pour une stratégie antiterroriste mondiale». Le rapport insiste particulièrement sur la nécessité de promouvoir l'Etat de droit, le respect des droits de l'homme et l'instauration de systèmes de justice pénale efficaces.

14. Les Nations Unies œuvrent également à la création d'un réseau de coopération entre ses agences et d'autres acteurs et organisations importants au niveau international. Le cadre de coordination de l'Equipe spéciale de lutte contre le terrorisme (CTITF) harmonise les efforts des Nations Unies dans la lutte contre le terrorisme, soutenant la mise en œuvre de la Stratégie antiterroriste mondiale des Nations Unies, adoptée par l'Assemblée générale des Nations Unies en septembre 2006 (A/RES/60/288). Reconnaissant la menace représentée par l'usage d'internet à des fins terroristes, les Etats s'engagent (chapitre II, paragraphe 12 de la Stratégie) à «s'employer avec l'Organisation des Nations Unies, sans nuire à la confidentialité, dans le respect des droits de l'homme et conformément aux autres obligations prévues par le droit international, à explorer les moyens a) de coordonner les efforts aux échelles internationale et régionale afin de contrer le terrorisme sous toutes ses formes et dans toutes ses manifestations sur l'internet; b) d'utiliser l'internet comme un outil pour faire échec au terrorisme, tout en reconnaissant que les Etats pourront avoir besoin d'une assistance à cet égard». Comme on le voit, la Stratégie reconnaît le double rôle d'internet, à la fois moyen de répandre des manifestations de terrorisme et de lutter contre leur diffusion.

15. La CTITF a créé huit groupes de travail, correspondant aux principaux aspects de la lutte contre le terrorisme, dont un Groupe de travail sur l'usage d'internet pour la lutte contre le terrorisme. Ce groupe de travail a notamment pour mission d'identifier et de rapprocher les acteurs et partenaires concernés par le problème de l'abus d'internet à des fins terroristes, par exemple pour la radicalisation, le recrutement, la formation, la planification opérationnelle, la collecte de fonds etc. En 2011, le Groupe de travail a publié une synthèse des défis, des bonnes pratiques et des recommandations sur les aspects juridiques et techniques. Il y pointe les réseaux zombies comme sources de préoccupation particulière. Le Groupe de travail affirme que les réseaux zombies peuvent servir à lancer de puissantes attaques, telle que celle contre l'Estonie en 2007. Le Groupe de travail a jugé que l'enquête sur l'affaire estonienne avait été entravée par plusieurs problèmes de droit procédural. Il manquait en effet des instruments effectifs permettant de recueillir rapidement des

preuves, et les instruments de procédure étaient limités à des communications spécifiques. Cela a contrarié l'analyse des communications au sein du réseau zombie, qui n'ont pas nécessairement lieu entre le terminal infecté et le centre de commande et de contrôle. Le rapport avance les conclusions et recommandations suivantes:

– Importance de la protection des droits fondamentaux – la responsabilité qu'ont les Etats de respecter et de protéger les droits de l'homme, et dans ce contexte particulier le droit à la vie privée, ne doit pas s'effacer devant les impératifs de sûreté publique et de sécurité nationale. Il faut plutôt assurer un équilibre entre les mesures et techniques de lutte contre le cyberterrorisme d'une part, le droit à la vie privée d'autre part;

– Rôle clés des partenariats public–privé (PPP) – étant donné que les infrastructures de télécommunications et les systèmes d'information sont fabriqués, détenus ou diffusés par le secteur privé, et compte tenu des compétences du secteur privé en matière de lutte contre les menaces informatiques, il est de la plus haute importance d'établir des réseaux de coopération entre les pouvoirs publics et les entreprises. Les PPP peuvent rapprocher les compétences de différents secteurs et mettre en commun des informations essentielles sur la cybercriminalité afin d'améliorer la prévention, la résilience et la désinfection des systèmes d'information;

– Approche diversifiée – les mesures juridiques et techniques s'avérant peu efficaces isolément, il faut lutter contre le cyberterrorisme et toutes ses sources à travers une approche globale, comprenant des programmes de sensibilisation visant à éduquer les citoyens et à discréditer les organisations terroristes.

16. Comme nous l'avons vu, la CTITF est chargée de gérer les efforts de lutte contre le terrorisme menés par les Nations Unies. Cependant, d'autres agences des Nations Unies jouent un rôle important dans le renforcement des politiques sur les questions liées au cyberterrorisme. L'Office des Nations Unies contre la drogue et le crime (ONUDC) et l'Union internationale des télécommunications (UIT) participent à la CTITF et contribuent activement aux politiques et aux débats à haut niveau sur les questions relatives à la cybersécurité et à la cybercriminalité.