

Doc. 11335
27 juin 2007

Comment prévenir la cybercriminalité dirigée contre les institutions publiques des Etats membres et observateurs ?

Avis¹

Commission des questions politiques

Rapporteur pour avis: M. Pedro AGRAMUNT, Espagne, Groupe du parti populaire européen

I. Conclusions de la commission

1. La Commission des questions politiques soutient pleinement le rapport de M. Sasi, Rapporteur de la Commission des questions juridiques et des droits de l'homme. A ce stade de l'ère de l'information, nos sociétés dépendent des technologies et y sont vulnérables :

- Les cyber-attaques sont de plus en plus fréquentes et de plus en plus perfectionnées ;
- beaucoup d'entre elles ont des motifs politiques visent, outre les entreprises privées, les sites Internet gouvernementaux et militaires ;
- elles sont capables de perturber l'offre de services essentiels ainsi que de nuire à la vie et à la sécurité des citoyens ordinaires ;
- leurs auteurs peuvent être des particuliers exprimant une opposition à la politique de tel ou tel pays et essayant de faire progresser leur propre agenda politique ;
- jusqu'à présent cela n'a jamais été le cas, mais il est concevable que des États sponsorisent des cyber-attaques.

2. Compte tenu de cela, la cyber-sécurité doit être un objectif primordial de nos gouvernements. Ce qui est en jeu, ce n'est pas seulement la criminalité économique, c'est également la sécurité nationale. Cette question doit sortir du domaine réservé de quelques spécialistes et faire l'objet d'un débat politique, car elle nécessite l'adoption d'une nouvelle manière d'aborder les relations internationales, de même que les relations entre l'État et les particuliers et la menace du terrorisme.

3. Le Conseil de l'Europe est en mesure de contribuer à soutenir l'harmonisation d'un cadre législatif contre la cybercriminalité. L'Assemblée doit donc réitérer son appel en faveur de la plus large adhésion possible aux traités pertinents du Conseil de l'Europe, en particulier la Convention pour la prévention du terrorisme et la Convention sur la cybercriminalité.

4. Les États doivent trouver des moyens appropriés de faire participer des acteurs privés – par exemple les industries des ordinateurs, des réseaux et des logiciels – à l'élaboration d'une stratégie exhaustive contre la cybercriminalité.

¹ Voir Doc. 11325 déposé par la Commission des questions juridiques et des droits de l'homme.

II. Amendements au projet de Résolution proposés par la Commission

Amendement A :

Au paragraphe 2, remplacer « la démocratie, les droits de l'homme et l'État de droit, et que » par :

« la stabilité démocratique et la sécurité nationale et qu'elle pose des problèmes fondamentaux quant au respect des droits de l'homme et de l'État de droit ; par conséquent, »

Amendement B :

Au paragraphe 3, avant « Pour la première fois », ajouter la phrase suivante :

« Les attaques à motifs politiques contre des sites militaires ou gouvernementaux de plusieurs États membres et observateurs du Conseil de l'Europe sont de plus en plus fréquentes et sophistiquées. »

Amendement C :

«Au paragraphe 4, à la fin du paragraphe, ajouter la phrase suivante :

« Cette menace peut provenir de particuliers, de groupes organisés ou d'États. »

Amendement D :

Après le paragraphe 6, insérer le nouveau paragraphe suivant :

« L'Assemblée rappelle aussi qu'avec la Convention du Conseil de l'Europe pour la prévention du terrorisme, on dispose d'un instrument supplémentaire dans la lutte contre le cyber-terrorisme, ainsi que contre l'utilisation de l'Internet à des fins terroristes. »

Amendement E :

Au paragraphe 7, remplacer « n'aient pas encore ratifié cette importante Convention » par :

« et observateurs n'aient pas encore ratifié ces importantes Conventions. »

Amendement F :

À la fin du paragraphe 13, ajouter la nouvelle phrase suivante :

« En outre, ils devraient faire participer à cet effort des acteurs privés, y compris les industries des ordinateurs, des réseaux et des logiciels. »

Amendement G :

Au paragraphe 14, alinéa 2, insérer entre « sans tarder » et « la Convention sur la cybercriminalité » :

« la Convention du Conseil de l'Europe pour la prévention du terrorisme, ainsi que »

* * *

III. Exposé des motifs, par M. Pedro Agramunt, Rapporteur pour avis

1. Introduction

1. À ce stade de l'ère de l'information, nos sociétés dépendent des technologies et y sont vulnérables. Actuellement, le réexamen des notions traditionnelles que sont la souveraineté, la sécurité nationale et la guerre s'impose de lui-même, à la lumière du fait que des individus peuvent paralyser le fonctionnement normal d'un Etat sans même bouger de leurs postes informatiques, où qu'ils se trouvent sur la planète.

2. Les cyber-attaques ne sont pas seulement les actes de quelques jeunes gens qui piratent « pour s'amuser », mais peuvent être une décision délibérée de certains individus de lancer une attaque de nature politique contre un Etat. Etant donné la rapidité avec laquelle les informations circulent sur Internet, ils n'ont même pas besoin de former un groupe longtemps avant le début de la cyber-attaque : à travers des réseaux sociaux et des blogs, des inconnus de différents pays peuvent se rencontrer et s'unir derrière le même objectif politique en l'espace de quelques minutes. Que ces individus agissent spontanément ou sous l'influence d'un groupe terroriste, criminel ou autre, ou encore sous l'égide d'un Etat, demeure une question ouverte et la réponse peut varier au cas par cas. Les trois scénarios sont possibles.

3. En outre, à l'heure actuelle, des outils d'attaque automatisés sont en libre accès sur Internet. Dès lors que la vulnérabilité d'un système d'exploitation donné ou d'une application particulière est connue, la mise à disposition sur Internet d'outils exploitant cette vulnérabilité se fait en l'espace de quelques heures. Ces *armes* sont donc accessibles à tous.

4. Ce pouvoir perturbateur – et, dans le pire des cas, destructeur – des individus devrait être pris très au sérieux par les responsables politiques car il peut affecter la sécurité de nos citoyens. Comme je l'explique plus précisément dans mon avis, la cybercriminalité est une question de défense et de sécurité nationales. Il est question des libertés civiles et de la liberté d'expression sur Internet, et de leurs limites légitimes. Par ailleurs, c'est incontestablement une question de coopération internationale, car les pirates opèrent par delà les frontières, et les lacunes en matière de prévention et de criminalisation de leurs activités dans un pays auront des répercussions dans d'autres.

5. Il était donc grand temps que notre Assemblée consacre son attention à la question de la cybercriminalité dans sa globalité, impliquant la Commission des questions politiques et la Commission des questions économiques, en plus de la Commission des questions juridiques et des droits de l'homme. J'aimerais saluer l'excellent rapport de M. Kimmo Sasi et je félicite ce dernier d'avoir pris l'initiative de mettre la question de la cybercriminalité à l'ordre du jour de l'Assemblée.

2. Formes de cyber-attaques

6. Dans la plupart des cas, les cyber-attaques n'ont pas un but politique mais économique, et elles s'en prennent à des petites et moyennes entreprises mal préparées, ayant de faibles capacités de défense. Toutefois, des attaques de nature politique peuvent aussi avoir lieu et incluent, parmi leurs cibles les plus fréquentes, les chaînes de télévision et les radios, les journaux en ligne et les sites web liés à l'Etat.

7. Les vastes réseaux bien protégés du gouvernement et militaires, en revanche, nécessitent beaucoup plus de temps, de savoir-faire et d'expérience pour être piratés. Cependant, les cyber-attaques deviennent de plus en plus sophistiquées et sont capables de toucher aussi ces sites sensibles. Parmi les cibles principales, il y a les Etats-Unis, la Chine, le Brésil, l'Australie, le Royaume Uni et la Turquie.²

8. Les différentes formes de cyber-attaques incluent :

- le piratage clandestin d'un système ;
- le « déni de service » ;
- la destruction ou le vol d'informations sensibles ;
- la pénétration d'un réseau ;
- le « craquage » de la protection par logiciel, et
- le sabotage ou le piratage téléphoniques (« phreaking »).

3. Cyber-attaques à motifs politiques

9. En matière de cyber-attaques, la tendance est le reflet des tensions politiques dans le monde entier. Depuis la moitié des années 90, époque à laquelle on commençait de collecter des informations sur ce phénomène, une corrélation directe est perceptible entre l'éclatement de crises politiques et la fréquence des cyber-attaques.

² <http://www.mi2g.com/>.

10. Ce qu'a subi dernièrement l'**Estonie** n'est que la dernière en date de ces cyber-attaques à motifs politiques. L'opération a été particulièrement virulente, puisque ses auteurs ont réussi à mettre en panne l'infrastructure numérique du pays, à saturer les sites Internet des principales institutions étatiques et agences gouvernementales, à ébranler Hansabanka, la plus grande banque d'Estonie, et à submerger les sites des principaux quotidiens du pays. Les attaquants sont passés par un réseau géant d'ordinateurs asservis allant de l'Amérique du Nord à l'Extrême-Orient, afin d'engendrer d'énormes paquets de flux d'informations provoquant des dénis de service. Si cette attaque a été tellement réussie, c'est parce qu'en Estonie, la première infrastructure critique est l'Internet lui-même ; en effet, l'Estonie est l'un des pays du monde les plus connectés à l'Internet, chaque aspect ou presque de la vie des citoyens ordinaires y étant géré par des infrastructures informatiques.

11. Il existe des indices clairs de l'existence d'un lien entre l'action des pirates informatiques et la décision du gouvernement estonien d'ôter la statue dite du Soldat en Bronze du centre-ville de Tallin, où elle se trouvait depuis soixante ans, pour la replacer dans le cimetière militaire³.

12. Il existe beaucoup d'autres exemples de cyber-attaques à motifs politiques, les principaux étant :

- la **cyber-attaque contre l'OTAN d'avril 1999**, après le commencement des frappes aériennes de l'OTAN sur la Serbie : selon les déclarations de la personne qui était alors le porte-parole de l'OTAN, il semblait que certaines attaques de Belgrade opposés aux bombardements avaient piraté le site Internet de l'OTAN et provoqué la saturation du serveur ; ils avaient aussi infiltré et saturé le système informatique de l'alliance de défense⁴ ; le mois suivant, en représailles contre le bombardement accidentel de l'ambassade de Chine à Belgrade par l'OTAN, des **pirates informatiques chinois** prenaient pour cibles des sites Internet du gouvernement américain⁵ ;
- depuis 2000, **des sites arméniens et azerbaïdjanais** ont été affectés par plusieurs séries de cyber-attaques motivées par le conflit du Haut-Karabakh⁶ ;
- La publication des **caricatures danoises** sur le prophète Mahomet a suscité en février 2006 une campagne mondiale de protestations en ligne contre le Danemark. Les cibles visées alors ont été surtout le journal qui avait publié les dessins pour la première fois et d'autres sites danois importants⁷.

4. Une nouvelle forme de guerre ?

13. La possibilité d'une guerre numérique à grande échelle a été envisagée et annoncée il y a longtemps déjà par plusieurs groupes de réflexion et experts en sécurité. Or, la récente cyber-attaque contre l'Estonie a conduit de nombreuses personnes à penser que les temps étaient mûrs pour l'avènement d'une telle forme de guerre. Cela oblige donc toutes les parties concernées, en particulier les milieux politiques, à redéfinir la notion même de guerre.

a. Particuliers livrant une guerre aux États ou attaques chapeautées par des États ?

14. Comme je l'ai déjà indiqué, derrière la cyber-attaque lancée contre l'Estonie se trouvaient des individus mus par des motifs politiques et dont l'action avait été déclenchée par le retrait du Soldat de Bronze. Malgré, quelques soupçons initiaux et l'énorme effort financier pour mettre en place une attaque à aussi large échelle, il semble que les autorités russes n'étaient pas à l'origine de leurs actions. Bien entendu, il est également concevable qu'une cyber-attaque lancée par un groupe de particuliers puisse avoir été orchestrée politiquement par un État, mais jusqu'à présent, cela n'a pu être démontré en aucun cas. En fait, il est possible aussi d'imaginer des situations dans lesquelles les

³ http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598.

⁴ « Sci/Tech Kosovo info warfare spreads » (extension de la guerre de l'information sur le Kosovo par des moyens scientifiques et techniques), BBC online, 1^{er} avril 1999.

⁵ « Kosovo cyber-war intensifies : Chinese hackers targeting U.S. sites, government says » (la cyber-guerre du Kosovo s'intensifie : des pirates informatiques chinois s'en prennent à des sites Internet américains, déclare le gouvernement), CNN online, 12 mai 1999.

⁶ « Nagorno-Karabakh dispute takes to cyber space » (le conflit du Haut-Karabakh se déplace dans le cyberspace), www.eurasia.net, 8 février 2007.

⁷ « Muslims hackers hit 3,000 Danish websites » (des pirates informatiques musulmans s'en prennent à 3.000 sites Internet danois), United Press International, 22 février 2006.

citoyens d'un pays donné décident d'adopter une position politique vis-à-vis d'un pays étranger dont la politique officielle n'est pas celle de leur pays, ou que des citoyens utilisent des cyber-attaques contre leur propre pays, en tant que moyen de pression politique.

15. À l'âge de l'information, la guerre ne se fait pas forcément entre des États, mais peut impliquer en tant que belligérant un groupe de particuliers et un État. Pour les États, le problème est de savoir comment concevoir une stratégie efficace afin de se défendre des cyber-attaques, y compris celles d'agents non étatiques, à savoir :

- comment prévenir ces attaques ;
- comment en limiter les effets ;
- comment rétablir la normale après une attaque, dans un délai acceptable et à un coût acceptable.

16. Dans l'élaboration de cette stratégie, les États doivent être conscients de la nécessité :

- de la coopération internationale,
- d'un cadre juridique approprié et harmonisé pour la pénalisation de la cybercriminalité,
- ainsi que d'un équilibre entre le respect des libertés civiles et des droits fondamentaux, d'une part, l'impératif d'assurer la sécurité publique, d'autre part, mais aussi de la nécessité
- de faire participer le grand public et des acteurs privés à l'application de la stratégie en question, car la faiblesse du système de protection de celle-ci pourrait avoir un impact négatif considérable sur la sécurité et la sûreté des citoyens ordinaires. La coopération avec les industries de l'informatique, des réseaux et des logiciels présentera une importance particulière à cet égard.

b. Les cyber-attaques dans le contexte des guerres interétatiques

17. La guerre interétatique, elle aussi, pourrait se transformer sous l'influence de la technologie numérique : des cyber-attaques pourraient servir à perturber les communications ou autres services-clés de l'ennemi, avant ou pendant des opérations purement militaires. Comme dans tous les autres domaines relatifs au cyberspace, les États-Unis d'Amérique ont été les premiers à prévoir l'intégration de ce type d'action dans leur stratégie de défense⁸. Ils ont même constitué une équipe chargée de coordonner des opérations fondées sur des réseaux informatiques offensifs (the Joint Functional Component Command for Network Warfare, JFCC-WF)⁹.

18. Mais les États-Unis ne sont pas seuls à agir ainsi, car selon un rapport militaire américain sur les futures relations géopolitiques avec la Chine, le gouvernement chinois serait en train de créer une division de guerre cybernétique en vue d'éventuels conflits à venir¹⁰. Il est d'ailleurs légitime de se demander si la cyber-dominance ne va pas devenir bientôt le principal élément de la puissance militaire.

5. L'utilisation d'Internet à des fins terroristes et le cyber-terrorisme

19. Les réseaux terroristes exploitent à fond l'Internet depuis ses débuts, et ils se sont révélés être de remarquables experts en la matière : ils sont versés dans la sécurité opérationnelle et savent masquer leurs véritables situations géographiques en utilisant des serveurs relais. Voici quelques-unes des activités auxquelles ils se livrent sur l'Internet :

- **Recrutement, formation et propagande** : on trouve sur l'Internet des instructions pour la fabrication de bombes, des forums de discussion appelant au djihad et des informations sur

⁸ « The White House, The National Strategy to Secure Cyberspace, February 2003 ; US ponders cyber war plans » (Maison Blanche – Stratégie nationale de sécurisation du cyberspace, février 2003 ; les États-Unis élaborent des plans de guerre cybernétique), BBC online, 7 février 2003 – « Pentagon plans cyber-insect army » (Le Pentagone prépare une armée de cyber-insectes), BBC online, 16 mars 2006.

⁹ « U.S. Military's Elite Hacker Crew » (l'équipe de pointe de pirates informatiques militaires américains), www.wired.com, 18 avril 2005 ; voir également http://www.stratcom.mil/organization-fnc_comp.html.

¹⁰ Department of Defence of the United States, Annual Report to Congress, The Military Power of the People's Republic of China, 2007.

les camps de formation au terrorisme ; certains vont même jusqu'à planifier des opérations sur des sites Internet confidentiels. A ce propos, il faudrait mentionner que la Convention de 2005 du Conseil de l'Europe sur la prévention du terrorisme criminalise les actes qui peuvent porter à commettre des actions terroristes, y inclus la provocation publique ou l'incitation indirecte, le recrutement et la formation à des fins terroristes, la justification et glorification du terrorisme, etc.¹¹

- **retrait d'informations sensibles** : il n'est pas inhabituel de constater que certains individus passent par l'Internet pour dénicher des informations sur une infrastructure critique ; des recherches conduites par les services de sécurité ont permis, à la suite d'attaques de ce genre menées en 2002, de remonter jusqu'à des adresses IP d'Indonésie, du Koweït, du Pakistan et d'Arabie Saoudite ; des programmes informatiques hautement perfectionnés dont on se sert en ingénierie pour déceler les points de tension et les faiblesses des bâtiments, des ponts et des barrages ont été retrouvés en 2001 et 2002 dans des ordinateurs appartenant à des membres d'Al Qaida, en Afghanistan¹².

20. Par cyber-terrorisme, par contre, on entend l'utilisation d'Internet et de la communication électronique en tant que cibles pour les terroristes. Il représente une menace réelle, en soi comme en association avec d'autres formes d'attaque : il est possible d'imaginer des attaques numériques capables de paralyser les réactions à une situation d'urgence, les transports et les communications, l'objectif étant de magnifier l'impact d'un attentat matériel commis par ailleurs.

* * *

Commission chargée du rapport: Commission des questions juridiques et des droits de l'homme

Commission saisie pour avis: Commission des questions politiques

Renvoi en commission: Demande de débat d'urgence, renvoi n°3365 du 25 juin 2007

Avis approuvé par la commission le 27 juin 2007

Secrétariat de la commission: M. Perin, Mme Nachilo, M. Chevtchenko, Mme Sirtori-Milner, Mme Pieter, M. Alarcon

¹¹ A ce jour, cette convention, qui est ouverte à l'adhésion des Etats non-membres, a été signée par 39 Etats membres et ratifiée par 7 Etats. Les procédures nationales de ratification sont en cours dans 10 autres Etats membres.

¹² <http://www.mi2g.com/>