Mon point de vue sur le rapport Bockel

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 21 juillet 2012. Dernière mise à jour le 23 juillet 2012

https://www.bortzmeyer.org/rapport-bockel.html

Le monde de la sécurité informatique, notamment les gens qui travaillent sur la sécurité de l'Internet, attendait avec intérêt la publication du rapport d'information n° 681 (2011-2012) de M. Jean-Marie BOCKEL <http://www.senat.fr/rap/r11-681/r11-681_mono.html>, « La cyberdéfense : un enjeu mondial, une priorité nationale ». Il n'y a pas en France trop de documents stratégico-politiques sur les menaces liées à ce fameux « cyberespace ». Certains ont ricané de quelques maladresses du rapport mais il y a d'abord de sérieux problèmes de fond.

Donc, Jean-Marie Bockel a rédigé un rapport <http://www.senat.fr/rap/r11-681/r11-681_mono.html> sénatorial et plein de professionnels de l'Internet qui, d'habitude se moquent complètement de ce que peut faire, dire ou penser le Sénat parlent de ce rapport. Il y a pourtant de grandes chances que, comme tant d'autres rapports parlementaires, il finisse simplement enterré sous la poussière. Est-ce une mauvaise chose ?

Pourtant, le sujet est important. Une grande partie des activités humaines, qu'elles soient de nature économiques, politiques, créatrices ou personnelles, ont migré sur l'Internet (le « cyberespace » comme il faut dire pour faire croire qu'on a lu Gibson). Très logiquement, les comportements négatifs se sont donc également retrouvés sur l'Internet, de la criminalité à la guerre en passant par l'escroquerie, la répression étatique, la censure et le mensonge. C'est tout à fait normal. La société interagit via les réseaux et les aspects les plus désagréables de la société également. Il n'y a pas de spécificité de l'Internet à ce sujet. Mais cela ne veut pas dire qu'il faut baisser les bras et accepter les risques liés à ces activités. Pas mal de gens sont donc occupés à combattre les criminels, en ligne comme ailleurs, à lutter pour maintenir le réseau en fonctionnement malgré les attaques, et à tout faire pour que les salauds et les parasites n'aient pas la partie trop facile. La sécurité dans l'Internet est donc un enjeu important (ça y est, je fais mon Manuel Valls) et il est normal d'y consacrer du temps, des efforts et de l'argent. En soi, un rapport parlementaire sur ce sujet, appelant à mobiliser davantage de ressources pour la sécurité et à la prendre plus au sérieux, est donc une bonne chose.

La plupart des commentaires sur le rapport Bockel se sont focalisés sur une proposition extrêmiste (interdire les routeurs chinois, j'y reviendrais), ou sur une formulation malheureuse (l'usage incorrect du terme hacker et le mélange hollywoodien que fait l'auteur). Personnellement, j'ai bien ri en apprenant

dans le rapport que l'insécurité sur l'Internet était de la faute de Lisbeth Salander, qui représente un personnage de pirate trop sympathique (le rapporteur n'aurait pas dit cela s'il avait lu le livre de Larsson au lieu de voir une adaptation cinématographique très lissée). J'ai également pouffé en lisant que Flame était « vingt fois plus puissant que Stuxnet ». Comment mesure-t-on la puissance d'un "*malware*" ? En quelles unités ?

Mais il n'y a pas tant de bavures que cela, le texte a manifestement été relu par des gens compétents, on n'y trouve pas ces énormités qui font la joie des "*geeks*" quand ils lisent les rapports officiels. Le texte contient des informations intéressantes (par exemple l'étude de la situation chez les autres pays comme l'Allemagne), et le Sénat a au moins l'avantage de publier ses rapports sous des formats ouverts, permettant une lecture agréable même si on est attaché au logiciel libre (je l'ai lu sur une tablette, ce qui est très difficile avec la plupart des textes officiels).

Certaines recommandations de ce rapport vont d'ailleurs dans le bon sens et le principal regret sera qu'elles n'aillent pas assez loin. Bockel critique ainsi le scandaleux article 323-3-1 <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418323&cidTexte=LEGITEXT000006070719> qui empêche d'étudier les failles de sécurité (distribuer un logiciel comme hping ou scapy est officiellement un délit en France), mais sans oser en réclamer franchement l'abolition.

De toute façon, comme je l'avais déjà dit lors d'une conférence récente, on ne demande pas au sénateur d'être geek <https://www.bortzmeyer.org/pas-sage-en-seine-politiques.html>. Non, le problème avec ce rapport est un ou plutôt plusieurs problèmes de fond.

Le premier et le plus grave : Bockel ne parle que des menaces contre l'État et contre les entreprises privées (« dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates +informatiques, activistes ou organisations criminelles, est une certitude. Certaines d'entre elles pourront être de grande ampleur »). Or, comme l'a bien expliqué Schneier longtemps avant moi, les menaces les plus sérieuses aujourd'hui sont celles qui pèsent contre les citoyens. Ils sont menacés à la fois par les États (qui, démocratiques ou dictatoriaux, resserrent tous la vis de plus en plus contre l'Internet) et par les entreprises privées (collectes d'informations privées, atteintes à la liberté d'expression comme lorsqu'Amazon a coupé WikiLeaks, etc). **Aujourd'hui, le gros problème en sécurité informatique, c'est de protéger les citoyens contre ces puissances.** Faire un rapport aussi long et détaillé sur les menaces, sans mentionner une seule fois celles contre les citoyens, c'est avoir une vision très étroite... ou bien avoir un agenda politique qui n'est pas le mien. C'est ainsi que la rapport dit qu'il y a trois conceptions, « celle défendue par certains pays dits "libéraux", comme la Suède ou les Pays-Bas, qui sont très attachés à l'espace de liberté que représente l'Internet et hostiles à toute forme de réglementation du cyberespace », celle des dictatures et... celle de la France, qui « se situe dans une position médiane ». Si je comprends bien, elle a donc vocation à se tenir à mi-chemin entre les démocraties et les dictatures...

Par exemple, le rapport mentionne plusieurs fois la nécessité d'étendre les pouvoirs de l'ANSSI, qui initialement en avait très peu, mais ne parle pas une seule fois des risques associés à ces pouvoirs, ni des moyens de limiter ces risques. L'ANSSI, contrairement à toutes les organisations sociales inventées jusqu'à présent, serait-elle miraculeusement immunisée contre les tentations d'abus de pouvoir ?

La sécurité est malheureusement souvent utilisée comme argument pour restreindre les libertés. La sécurité informatique n'est pas différente des autres, de ce point de vue. C'est ainsi que le rapport Bockel, à propos du piratage de Bercy <http://owni.fr/2011/03/26/les-dessous-du-piratage-de-bercy-anss index.html>, note bien qu'il était dû à des courriers électroniques contenant le logiciel malveillant mais explique ensuite que, dans le cadre des mesures qui ont pu être imposées après ce piratage, « l'accès à Twitter a été supprimé ». Pourtant, Twitter n'était pour rien dans le piratage. Mais c'est un grand classique que de profiter d'une crise pour imposer des mesures impopulaires.

---

https://www.bortzmeyer.org/rapport-bockel.html

Alors, on va me dire qu'il est normal que ce rapport se concentre sur les risques pour l'État. C'est un rapport parlementaire, destiné à des politiques, il est normal qu'il parle de leurs problèmes, laissant ceux des citoyens à d'autres études. Sauf que le rapport Bockel ne parle pas que des risques pour l'État. Il est également très prolixe quand aux risques pour les entreprises privées et, là, il dérape sérieusement. Non seulement il ne mentionne jamais les risques que font courir ces entreprises aux citoyens, mais il propose beaucoup plus de mesures pour aider le secteur commercial privé que de mesures pour protéger l'État. Ainsi, le texte cité plus haut sur les « trois conceptions », précise la position de la France en disant qu'elle est favorable « à un minimum de régulation, par exemple pour protéger le droit d'auteur ». Ce droit n'a pourtant aucun rapport avec les cybermenaces. Mais on comprend cette mention quand on sait que « droit d'auteur » est, pour beaucoup de politiques, le terme codé pour « défense acharnée des intérêts des industries du divertissement, quelles que soient les évolutions sociales et politiques ». Ce ne sont donc plus les auteurs d'attaques par déni de service qui préoccupent le rapporteur du Sénat, ce sont les copies illégales des œuvres culturelles.

Ce choix de mettre les moyens de l'État au service de la défense d'intérêts privés apparaît à d'autres endroits. Ainsi, le rapport dit qu'il faut défendre « notre savoir-faire technologique comme nos parts de marché, dans la véritable guerre économique que nous connaissons aujourd'hui ». Plus d'intérêts nationaux menacés, uniquement du business.

Autre demande du rapport, que l'« ANSSI devrait ainsi être en mesure de répondre aux demandes des entreprises, en matière d'expertise, de conseils, d'assistance et d'offre de produits labellisés ». Un service public payé avec l'argent public se transformerait donc en SSII gratuite pour les entreprises.

Puisqu'on parle de business, c'est l'occasion de revenir sur la proposition qui a été la plus remarquée et la plus commentée dans le rapport, la proposition d'interdire les routeurs chinois (par exemple ceux de Huawei), accusés d'espionner les communications et de contenir du code permettant éventuellement de perturber les communications. D'abord, du point de vue technique, il faut rappeler qu'un routeur est un engin très complexe et qu'il n'est pas facile à auditer pour détecter d'éventuelles capacités néfastes. Mais c'est le cas de tous les routeurs. Le rapporteur sénatorial nous croit-il assez naïfs pour penser que les Cisco et les Juniper états-uniens n'ont pas exactement les mêmes capacités ? Comme les Huawei, ils ne font pas tourner du logiciel libre. On n'a pas le code source et le contrôle de leurs activités est donc encore plus complexe. (Note pour mes lecteurs techniciens : si on est sérieux en matière de sécurité, le fait d'utiliser du logiciel libre est une condition nécessaire. Mais elle n'est pas suffisante. Une porte dérobée peut être cachée à bien des endroits.)

Bockel oublie aussi, lorsqu'il cite les méchancetés dont sont capables les routeurs chinois, de rappeler que la France est un grand exportateur de technologies de surveillance et de contrôle, et qu'elle fournit les pires dictateurs comme le défunt Kadhafi, dont le système de contrôle de son peuple était mis en place par une société française, Amesys, filiale de Bull. Le fait que le rapporteur s'inquiète des capacités chinoises de DPI sans mentionner ces succès du commerce extérieur français peut permettre de douter de sa bonne foi. Ou bien cette proposition anti-chinoise était tout simplement du protectionnisme déguisé ?

Ce rapport porte aussi les marques d'une tendance très fréquente en cyber-sécurité : les discours alarmistes, non soutenus par des faits (ou par des chiffres donnés sans explications) et qui servent à justifier des augmentations de budget et de pouvoir. Ce discours cyber-guerre se retrouve dans des affirmations comme celle comme quoi Conficker aurait « perturbé le fonctionnement de plusieurs hôpitaux en France et dans le monde » (une histoire qui a souvent servi lors de rapports sur la cyber-sécurité mais dont les sources sont obscures).

Il faut savoir qu'il n'existe pas de statistiques fiables sur les attaques informatiques (une situation que le rapport Bockel dénonce à juste titre, et pour laquelle il propose entre autres des signalements

obligatoires à l'ANSSI). Contrairement aux cambriolages ou aux accidents de la route, personne ne sait exactement ce qui se passe et les chiffres les plus impressionnants sont toujours issus de généraux en retraite reconvertis « consultants en cyber-sécurité » et qu'on peut certainement soupçonner de forcer le trait. C'est ainsi que le rapport Bockel dit « les administrations françaises, les entreprises ou les opérateurs font aujourd'hui l'objet de manière quotidienne de plusieurs millions de tentatives d'intrusion dans les systèmes d'information », chiffre complètement invérifiable (la source n'est pas nommée) et qui, de toute façon, n'a aucune valeur scientifique puisqu'il ne définit pas ce qu'est une tentative d'intrusion et que la méthodologie de mesure n'est pas indiquée. Quant on sait que certains responsables sécurité comptent **chaque** paquet IP rejeté par le parefeu comme étant une tentative d'intrusion, on voit qu'on peut devenir millionaire facilement.

Pour conclure, je voudrais aussi revenir sur la sécurité informatique en général. Cela fait de nombreuses années que des experts très compétents travaillent à l'améliorer. Les résultats ne sont pas spectaculaires, en bonne partie parce que le problème est humain et pas technique. Le rapport Bockel se contente de reprendre le discours ultra-classique comme quoi c'est de la faute de l'utilisateur (il choisit des mauvais mots de passe, il clique sur les liens marqués « agrandissez votre pénis », etc). Ce n'est pas faux. Mais, en 2012, on pourrait enfin chercher à aller plus loin. Pourquoi est-ce le cas ? Pourquoi les utilisateurs préfèrent-ils accomplir leur travail plutôt que de suivre les règles de sécurité ? Pourquoi les sénateurs continuent-ils à utiliser toutes les choses que leur rapport dénonce, les logiciels non sécurisés, le nuage qui est si pratique, les "*smartphones*" et tablettes qui sont si jolis et si prestigieux ? Tant qu'on se contente d'incantations (« il faudrait que les utilisateurs fassent plus attention »), on ne risque pas d'améliorer la sécurité.

Sans compter les conseils idiots. Le rapport Bockel propose parmi « Les 10 commandements de la sécurité sur l'internet » : « tu vérifieras l'expéditeur des mails que tu reçois ». Ah bon, Jean-Marie Bockel utilise PGP ? Et comment « vérifie » t-il sinon ? Il regarde l'adresse et, plus fort que Chuck Norris, il voit si elle est fausse ? Si on reste à des slogans creux comme ces absurdes « dix commandements », on en sera encore là pour le prochain rapport parlementaire, en 2016 ou 2019.

Quelques lectures sur ce rapport :

— « Tu t'es vu quand tu parles des pirates chinois ? <http://reflets.info/tu-tes-vu-quand-tu-parles
> », sur la naissance du thème du hacker chinois,
— « Rapport Bockel : un point sur la cyberdéfense française <http://reflets.info/rapport-bockel-un-
> », qui revient notamment sur l'espionnage fait par les firmes françaises,
— « Espionnage d'Internet : des firmes chinoises bientôt bannies du marché français ? <http://
www.rue89.com/2012/07/19/espionnage-dinternet-des-firmes-chinoises-bientot-bannie
sur le cas des routeurs chinois.
— « Les hackers ont enfin fait cracker le sénat <http://owni.fr/2012/07/20/les-hackers-ont-enfin-
index.html> » sur une autre proposition du rapport, dont je n'ai pas parlé, celle d'embaucher des « hackers » (terme utilisé n'importe comment dans le rapport Bockel) à l'ANSSI,
— « Vers une super-ANSSI ? <http://www.hackersrepublic.org/cultureduhacking/vers-une%
20super-anssi> », article qui critique la tonalité caricaturalement pro-ANSSI du rapport,
— « Bockel au pays de l'ANSSI... <http://sid.rstack.org/blog/index.php/552-bockel-au-pays-de
qui fait notamment remarquer qu'on ne peut pas isoler l'informatique de l'État. De même qu'un manque d'hygiène dans les quartiers pauvres d'une ville va favoriser des épidémies qui toucheront aussi les quartiers riches, la mauvaise sécurité de tant de machines non-étatiques va permettre la constitution de puissants botnets qui pourront alors représenter une menace pour la sécurité nationale,
— « Puisqu'il faut bien en parler ... <http://news0ft.blogspot.fr/2012/07/puisquil-faut-bien-en
html> », très critique notamment sur le gaspillage d'argent public que représente en général les aides de l'État au privé « À peu près tous les financements publics alloués à des entreprises dites "innovantes" se sont avérés être du détournement de fonds » et « Toute politique industrielle qui se résume à verser un gros chèque après le montage d'un dossier kafkaïen ne peut se terminer

que dans la corruption et le détournement », phrases qui décrivent bien le système de copinage français et avec lesquelles je suis entièrement d'accord. Constructive, cette critique se termine par plusieurs recommandations. Je suis d'accord avec la plupart mais je trouve curieux que, comme le rapport Bockel, il propose que l'ANSSI aide gratuitement les entreprises (proposition 3). La suggestion d'un statut officiel de l'expert en sécurité (proposition 7) m'inquiète également, lorsque je vois les compétences de certains experts pourtant munis de tous les papiers.

---

https://www.bortzmeyer.org/rapport-bockel.html