Cyberattaques : la protection de la France passe désormais par les ordinateurs | Le Net Expert Informatique

	Cyberattaques : la protection de la France passe désormais par les ordinateurs

Après la multiplication des cyberattaques en France, le gouvernement a mis le paquet sur la cyberdéfense : un budget de près d'un milliard d'euros et un premier colloque international organisé à Paris.

C'est un champ de bataille très particulier. Pas de chars, de canons ou d'avions. Pourtant, les victimes peuvent être très nombreuses. Nous voilà dans le monde de la cyberdéfense. Jeudi 24 septembre à Paris se tenait à l'École militaire le premier colloque international consacré au sujet. La France n'est évidemment pas à l'abri. Il faut donc trouver la parade. Le combat numérique, c'est la guerre du XXIème siècle à gagner.

Rappelez-vous du chaos provoqué par l'attaque informatique contre TV5 : des hackers (russes certainement) ont contraint la chaîne de télévision à interrompre ses programmes pendant plusieurs heures après avoir propager par e-mail un virus. En 2010, les services spécialisés américains et israéliens ont créé Stuxnet. Le « ver », le « tenia » informatique, sournois, a été capable d'embrouiller les meilleurs cerveaux iraniens en charge du programme nucléaire, en multipliant les bugs sur les centrifugeuses du site de Natanz. À la clé, Téhéran a perdu deux ans de recherche.

400 anomalies depuis le début de l'année

Aujourd'hui, si Daesh occupe l'espace numérique plutôt comme vecteur de propagande, dans un futur proche avec les moyens dont disposent les djihadistes pourquoi ne pas se lancer dans de telles attaques ? D'autant qu'il a du monde prêt à se vendre au diable, souligne le vice-amiral Arnaud Coustillière, patron de la cyberdéfense française.

« Cet espace numérique a été complètement investi par des pirates informatiques. Je vous parle de mercenaires informatiques. Les mafias se structurent, elles ont des capacités importantes. Il faut donc que les militaires trouvent leur juste place pour être capable d'identifier nos ennemis », dit-il.

On a trouvé plus de 45 virus sur le PC portable d'un sous-traitant

Arnaud Coustillière, patron de la cyberdéfense française

L'an dernier, notre ministère de la Défense a été le théâtre de 780 incidents. On ne parle pas d'attaques. Depuis le début de l'année, on tourne déjà autour de 400 anomalies identifiées, principalement sur les sites de communication (comme celui de la Dicod ou de l'état-major). Pour le reste, le ministère est plus discret. Mais il ne faut pas oublier les industriels de la défense : les grands groupes, comme les plus petites société. Là le bât blesse : la vulnérabilité est de tous les jours.

« Ce qui nous préoccupe également c'est, comme dans toutes les sociétés, les interventions dans l'environnement des plateformes de nos sous-traitants. On a trouvé plus de 45 virus sur le PC portable d'un sous-traitant qui venait faire une maintenance sur un système d'arme qui devait tirer en exercice quelques jours après. C'est inadmissible », relate Arnaud Coustillière.

Un drone Harfang avait connu des problèmes avant son décollage d'Afghanistan, justement parce qu'un serveur en France était contamine. La mission avait été retardée. Ce qui fait désordre, mais surtout peut coûter la vie à des militaires non protégés.

Maîtres en logiciels

Il ne faut pas se priver d'attaquer. Mais il faut d'abord se défendre. Au moins la menace a été prise en compte en 2009. Il y a eu la création de l'Agence nationale de la sécurite des systèmes d'information (Anssi), avec son groupe d'intervention. Il y a aussi un centre opérationnel 7 jours sur 7, 24 heures sur 24 qui apporte son expertise : il veille, détecte et alerte.

La nouvelle loi de programmation militaire vient apporter un milliard d'euros supplémentaires dans l'escarcelle et 1.000 spécialistes de plus, à recruter dans les écoles d'ingénieurs notamment. Il y a également ces compagnies cyber, maîtres en logiciels, qui sont formées. Il y en a une déployée à Abou Dhabi dans le cadre de l'operation « Chamal », et bientôt une autre sur le Charles-de-Gaulle qui doit appareiller en novembre. Avec, c'est certain, une double priorite pif-paf attaque-défense.

Source :
http://www.rtl.fr/actu/societe-faits-divers/cyberattaques-la-protection-de-la-france-passe-desormais-par-les-ordinateurs-7779843074

Replay de l’émission Infrarouge du 22 septembre : On nous écoute : Cyberguerre, l’arme fatale ? – 1ère partie | Le Net Expert Informatique

ON EST EN DIRECT	Replay de l’émission Infrarouge du 22 septembre : On nous écoute : Cyberguerre, l’arme fatale ? – 1ère partie

« Plus rien ne peut rester secret, même nos vies. Parano de grande ampleur ? Complot d'état ?

Quelle est la réalité de la plus grande campagne de surveillance jamais élaborée ? » Edward Snowden, est interviewé en exclusivité à Moscou pour le documentaire. Pour faire suite à notre article « Emission Infrarouge sur France 2 ce mardi à 22h50 : On nous écoute : Cyberguerre, l'arme fatale ? – 1ère partie » du 21 septembre dernier, nous vous mettons à disposition le replay de cette superbe émission.

A l'heure où la France vient de voter la très contestée Loi sur le Renseignement, où le hacking, le tracking et la cyber-surveillance font partie des grands débats de nos sociétés, où les révélations d'Edward Snowden ont enflammé la planète, les questions que posent ces 2 films deviennent incontournables.
Sommes-nous tous des coupables potentiels à surveiller ? Faudra-t-il abandonner notre présomption d'innocence pour une sécurité dont tout le monde sait qu'elle ne peut pas être totale ? Comment contrôler les services de renseignements sans les empêcher de travailler efficacement ? Et sommes-nous prêts à protéger nos propres lanceurs d'alerte face aux pressions récurrentes d'un Etat-surveillance de plus en plus puissant ?

Une série documentaire inédite (2X52′) écrite et réalisée par Pierre-Olivier François
Une coproduction Artline Films, WGBH Frontline et NOVA
Produit par Olivier Mille
Avec la participation de France Télévisions
Avec le soutien du Centre National du Cinéma et de l'Image Animée
Unité de programmes documentaires de France 2 : Fabrice Puchault et Barbara Hurel
La case Infrarouge invite les téléspectateurs à réagir et commenter les documentaires en direct sur twitter via le hashtag #infrarouge

---

Source : http://www.france2.fr/emissions/infrarouge/diffusions/22-09-2015_341460

Emission Infrarouge sur France 2 ce mardi à 22h50 : On nous écoute : Cyberguerre, l'arme fatale ? – 1ère partie | Le Net Expert Informatique

Emission Infrarouge sur France 2 ce mardi à 22h50 : On nous écoute : Cyberguerre, l'arme fatale ? – 1ère partie

« Plus rien ne peut rester secret, même nos vies. Parano de grande ampleur ? Complot d'état ? Quelle est la réalité de la plus grande campagne de surveillance jamais élaborée ? »
Edward Snowden, est interviewé en exclusivité à Moscou pour le documentaire.A l'heure où la France vient de voter la très contestée Loi sur le Renseignement, où le hacking, le tracking et la cyber-surveillance font partie des grands débats de nos sociétés, où les révélations d'Edward Snowden ont enflammé la planète, les questions que posent ces 2 films deviennent incontournables.

Sommes-nous tous des coupables potentiels à surveiller ? Faudra-t-il abandonner notre présomption d'innocence pour une sécurité dont tout le monde sait qu'elle ne peut pas être totale ? Comment contrôler les services de renseignements sans les empêcher de travailler efficacement ? Et sommes-nous prêts à protéger nos propres lanceurs d'alerte face aux pressions récurrentes d'un Etat-surveillance de plus en plus puissant ?

Une guerre d'un nouveau genre a vu le jour, qui bouleverse les règles et les enjeux des conflits traditionnels. Internet est en train de modifier totalement les champs de bataille, de brouiller les frontières entre alliés et ennemis, entre espionnage et sabotage, entre guerre et paix. Pas avec des armes lourdes mais avec des codes et des virus de plus en plus sophistiqués pour déstabiliser, prendre le contrôle ou détruire des centrales électriques ou nucléaires, un réseau ferroviaire, un ministère, des ordinateurs de guidage …

Nos armées se dotent de moyens toujours plus sophistiqués pour lutter contre un ennemi inconnu, invisible et imprévisible. Comment se défendre ? Comment attaquer ?

De nos choix dépendra la société dans laquelle nous vivrons à l'avenir.

Une série documentaire inédite (2X52′) écrite et réalisée par Pierre-Olivier François
Une coproduction Artline Films, WGBH Frontline et NOVA
Produit par Olivier Mille
Avec la participation de France Télévisions
Avec le soutien du Centre National du Cinéma et de l'Image Animée
Unité de programmes documentaires de France 2 : Fabrice Puchault et Barbara Hurel
La case Infrarouge invite les téléspectateurs à réagir et commenter les documentaires en direct sur twitter via le hashtag #infrarouge

---

Source : http://www.france2.fr/emissions/infrarouge/diffusions/22-09-2015_341460

Les Etats Unis devraient avoir peur des prochaines cyber-attaques ? | Le Net Expert Informatique

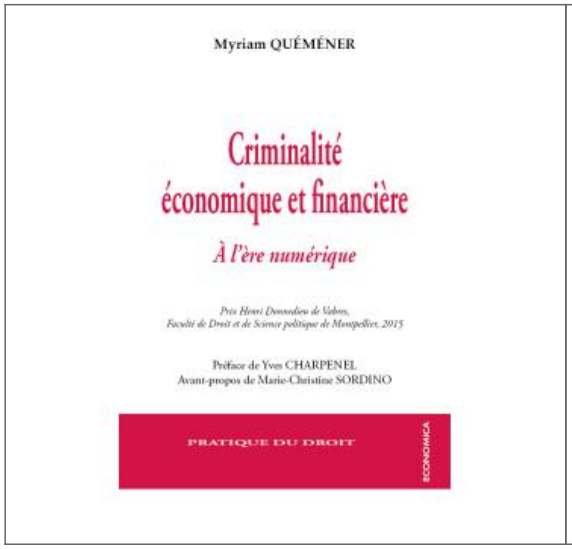
Le nouvel Economiste	Les Etats Unis devraient avoir peur des prochaines cyber-attaques ?

Mercredi dernier, la Bourse de New York et United Airlines ont suspendu leurs activités pendant plusieurs heures en raison de problèmes informatiques mystérieux, tandis que le site Internet du 'Wall Street Journal' a brièvement disparu.

Tous trois ont insisté pour dire qu'il s'agissait de problèmes techniques, et non d'attaques malveillantes. Mais l'inquiétude monte après des agressions contre de puissantes entreprises et agences américaines.
En février dernier, la compagnie d'assurance Anthem révélait que des pirates informatiques avaient volé les données de plus de 80 millions de clients. L'Office of Personnel Management, basé à Washington, révélait que des hackers avaient subtilisé des données de millions d'employés fédéraux. Commerçants ou banques, plusieurs entreprises ont aussi été attaquées.
Mercredi, au moment où la Bourse de New York était suspendue, l'université de Cambridge et le groupe d'assurances Lloyds publiaient un rapport affirmant que si une cyber-attaque s'en prenait au réseau électrique américain, les dommages pourraient s'élever à mille milliards de dollars. Quelques minutes plus tard, le directeur du FBI, James Comey, déclarait devant le Congrès qu'il avait des difficultés à venir à bout des systèmes de chiffrage des djihadistes. En mai, M. Comey expliquait que les terroristes islamiques avaient adopté l'idée d'utiliser des logiciels malveillants contre les infrastructures stratégiques. La chose est plutôt effrayante.
La question clé que les investisseurs, les politiciens et les électeurs doivent se poser est non seulement d'envisager qui pourrait être la prochaine cible, mais aussi de savoir si Washington est capable de face à ces attaques. La réponse est certainement non.
Sur le papier, les ressources ne manquent pas. En début d'année, le président Barack Obama a par exemple affecté 14 milliards de dollars à la lutte contre le cyberterrorisme. Mais le principal problème n'est plus tant un manque d'argent que de coordination : alors que la peur se propage, un nombre ahurissant d'organismes et de groupes de travail différents se sont lancés dans la lutte contre le cyberterrorisme, souvent en collaborant très peu entre eux. L'institution censée être en charge des menaces est le Département de la Sécurité nationale, mais ses compétences laissent sceptiques les responsables militaires. Le Pentagone a son propre personnel affecté aux cyberattaques, tout comme les services secrets.
"Certains pays ont trouvé des réponses : l'Australie possède un niveau impressionnant de coordination entre les secteurs public et privé sur les défenses cybernétiques. Mais avec le tribalisme exacerbé qui sévit à Washington, la triste vérité est qu'il faudra une crise majeure avant que quiconque puisse cogner sur les têtes des bureaucrates de manière efficace"
La Maison-Blanche a tenté d'obliger ces organismes à travailler ensemble. De leur côté, des organismes civils comme la Commission de réglementation nucléaire ont aussi commencé à tenir des réunions discrètes avec d'autres organismes cet automne sur ces questions. Mais la collaboration entre les secteurs reste inégale. "Le niveau de préparation des différents organismes varie énormément" admet un haut responsable de Washington au centre de cette mission. De plus, y ajouter des organismes du secteur privé entraînera une dégradation plus profonde de la situation : non seulement le Pentagone se méfie du partage de données avec d'autres institutions, mais les entreprises sont souvent terrifiées à l'idée de révéler les attaques dont elles ont fait l'objet.
Existe-t-il une solution ? Une réponse sensée pourrait être de créer une nouvelle entité qui serait l'entité centrale de lutte contre le cyberterrorisme. Il existe des précédents, la plupart des régulateurs de Washington ayant été créés pour répondre à une nouvelle menace. La Securities and Exchange Commission, par exemple, a été créée après le krach de 1929 ; la Food and Drug Administration, après des scandales concernant des médicaments dangereux. Une deuxième option serait de relancer le DHS (Department of Homeland Security) afin que celui-ci se focalise sur la lutte contre les cyberattaques. Il pourrait, par exemple, s'appeler ministère de la Sécurité Intérieure et Cybernétique.
Quoi qu'il en soit, Washington a besoin de répondre à la question qu'Henry Kissinger posait pour l'Europe : en temps de crise, "Qui dois-je appeler ?" Certains pays ont trouvé des réponses : l'Australie possède un niveau impressionnant de coordination entre les secteurs public et privé sur la défense cybernétique. Mais avec l'esprit de clan exacerbé qui sévit à Washington, la triste vérité est qu'il faudra une crise majeure avant que quiconque puisse cogner sur les têtes des bureaucrates de manière efficace. Il faut juste espérer que ce "quelque chose" ne sera pas trop dévastateur, comme une attaque réelle des transports ou des marchés.

Source : http://www.lenouveleconomiste.fr/financial-times/les-prochaines-cyber-attaques-contres-les-etats-unis-seront-terribles-27703/
Par David Pilling

La criminalité économique et financière à l’ère numérique | Le Net Expert Informatique



La criminalité économique et financière à l’ère numérique

Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle « la » solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique*.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Godfrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXIe siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (Darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement.
Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérives : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-krach de mai 2010 à Wall Street.
Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !

L'ouvrage en vente ici

Source : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php

---

Denis JACOPINI questionné par un journaliste de l'Express | Le Net Expert Informatique

L'EXPRESS L'Expansion

que faire

Denis JACOPINI questionné par un journaliste de l'Express

Le site d'actualité de jeux vidéo Nintendojo.fr a faussement annoncé mercredi 1er avril avoir été bloqué par le ministère de l'Intérieur. Une blague douteuse qui, par l'absurde, révèle néanmoins certains écueils de la loi Cazeneuve. Explications.

Voici l'écran qui s'affiche ce mercredi lorsque l'on tente de se connecter au site Nintendojo.fr

Ministère de l'Intérieur

Enfin, les détracteurs de la loi Cazeneuve tiennent leur martyr! Jugez donc: Nintendojo.fr, un simple site consacré à l'actualité des jeux Nintendo, est inaccessible ce mercredi. Il renvoie vers une page du ministère de l'Intérieur qui explique que le contenu a été bloqué. Une mesure qui est autorisée depuis le vote de la loi Cazeneuve fin 2014, avec de premiers cas en mars dernier, mais en principe réservée aux sites terroristes ou pédophiles.

Rassurez-vous tout de suite. « Il s'agit d'une blague de mauvais goût et ça nous a bien fait rigoler », explique à L'Express Mortal, l'administrateur du site. Il ne faut donc pas voir la main du ministère de l'Intérieur derrière ce faux blocage, mais un poisson d'avril qui aura trompé des dizaines d'internautes et quelques sites d'information.

Pourquoi ce gag?

« Ce n'est pas un geste politique, mais nous estimons quand même que la loi qui permet le blocage de certains sites internet est mauvaise, justifie Mortal, qui se revendique de la Quadrature du Net, association de défense des libertés sur internet hostile au dispositif. On avait envie de piquer les gens pour que ça éveille un peu les consciences sur le sujet. Cela pourrait arriver pour de vrai à d'autres demain, c'est ça le problème », tranche-t-il.

De la difficulté de distinguer « vrai » et « faux » blocage

Qu'on le juge drôle ou pas, le poisson d'avril de Nintendojo.fr pose de sérieuses questions sur le principe même de bloquer certains sites Internet. Est-il possible pour un internaute face à une page qui affiche le fameux message du ministère de l'Intérieur de savoir avec certitude que le site a été bloqué? « La réponse est simple: c'est non », estime **Denis Jacopini**, consultant en cybersécurité. Point de vue partagé par plusieurs observateurs interrogés ce mercredi.

« **Rien est impossible, poursuit l'analyste. Cela peut être un vrai message, bien sûr. Mais cela peut aussi être une blague de l'administrateur du site, ou l'oeuvre d'un hacker qui a modifié le site**« , avance-t-il.

Qu'en pense l'Intérieur? Contactés par L'Express, les services du ministère n'ont pas donné suite à nos sollicitations. A ce jour, les services de la Place Beauvau n'ont pas mis en place de dispositif pour informer sur de telles situations. Il ne serait pas étonnant, dans ce contexte, de voir fleurir les farces voire de réelles arnaques du même tonneau dans les semaines qui viennent.

Attention, arnaques à prévoir…

Dans le cas de Nintendojo.fr, l'artifice était plutôt élaboré. Le message affiché sur la page d'accueil du site reprenait, aussi bien graphiquement qu'au niveau du contenu, celui affiché en cas de blocage. Ce n'est pas tout. Un utilisateur de Twitter a comparé le code HTML de la page vers laquelle redirigeait Nintendojo.fr avec celui d'une page affichée via un site réellement bloqué par l'Intérieur, et ils étaient bien identiques.

Mais Nintendojo.fr est allé encore plus loin. « Nous avons vraiment procédé à un blocage DNS » (domain name system, nom de domaine) explique Mortal. Ce qui a pu donner l'illusion a certains que le site avait bel et bien été « bloqué ». « Techniquement, le dispositif de censure fait appel à un résolveur DNS menteur, c'est-à-dire qu'il ne renvoie pas le résultat correct, mais un mensonge tel que demandé par le gouvernement », explique nextinpact.com.

Concrètement, le gouvernement n'efface pas les sites bloqués: l'internaute qui essaye de s'y connecter est simplement redirigé vers la fameuse page ministérielle. Un mécanisme que Nintendojo.fr a plutôt bien singé ce mercredi.

« On aurait pu faire encore plus sophistiqué »

Les bons connaisseurs, eux, ont néanmoins pu déjouer la supercherie en testant d'autres DNS. Ils ont alors observé que tous renvoyaient vers la page du ministère de l'Intérieur, ce qui n'aurait pas été le cas pour un « vrai » blocage gouvernemental. En situation réelle, les fournisseurs d'accès à Internet (FAI) bloquent le site concerné au fur et à mesure, ce qui prend du temps. De plus, il existe des DNS publics, gérés par d'autres acteurs du Web (par exemple, Google), qui peuvent ne pas faire l'objet de blocage. Changer de résolveur DNS est d'ailleurs précisément l'une des solutions pour ceux qui souhaitent contourner la censure.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://lexpansion.lexpress.fr/high-tech/les-vraies-questions-que-pose-le-faux-blocage-de-nintendojo-par-le-gouvernement_1667195.html

Les facilités pour contourner la loi Renseignement | Le Net Expert Informatique

Les facilités pour contourner la loi Renseignement

Le Projet de loi relatif au Renseignement impose aux hébergeurs et FAI d'installer un dispositif de surveillance de leurs communications, désigné sous le terme générique « boîte noire », pour recueillir les informations et documents « relatifs à des personnes préalablement identifiées comme présentant une menace ». Selon un article du JournalDuNet daté du 30 avril 2015, se référant à l'article 6 de la LCEN, le terme « hébergeur » désigne l'intermédiaire technique qui met à la disposition des tiers les outils permettant de communiquer des informations en ligne. Il peut donc désigner des éditeurs dès lors qu'ils mettent à disposition des espaces de publication « participatifs », édités par les internautes (forums, réseaux sociaux, espaces de commentaires, chronique ou tribune telle que celle-ci, etc.).
Les avis ci-dessous sont rédigés à titre personnel et ne sauraient engager ceux du groupe CCM Benchmark que je dirige (NDLA: société éditrice des sites Journaldunet, CommentCaMarche, Linternaute, etc.).

Jusqu'à ce jour, lorsque des échanges entre individus ont lieu sur un espace de publication hébergé en France, la justice peut à tout moment demander à l'éditeur, sur simple réquisition judiciaire, de lui fournir les données de connexion de l'utilisateur (adresse IP et horodatage) afin de demander l'identification de l'individu auprès de son fournisseur d'accès. Dans la pratique, cela se pratique parfois sans réquisition dans des cas de force majeure, en infraction avec la loi. A partir du moment où il est de notoriété publique que les sites hébergés en France sont équipés d'une boîte noire, il faudrait être un terroriste idiot pour utiliser un espace de discussion hébergé dans un pays ayant installé de tels dispositifs, alors même qu'il existe un grand nombre de services similaires dans des pays n'en ayant pas déployé. Ainsi, l'information qui était jusqu'ici la plupart du temps accessible risque de devenir petit à petit inaccessible aux services de renseignement.
Il restera malgré tout une trace de la connexion chez le FAI me direz-vous ? A partir du moment où des personnes ayant des choses à se reprocher auront besoin de communiquer, pensez-vous qu'ils le feront à découvert ? Evidemment non, il est à la portée de tout le monde d'ouvrir un tunnel crypté vers une connexion située à l'étranger. Toute communication chiffrée (y compris légalement) est dès lors suspecte, ce qui signifie qu'il sera nécessaire de mettre en oeuvre des moyens pour décrypter toutes les communications chiffrées afin d'en vérifier le contenu. Les moyens de cryptologie utilisables en France sont certes soumis à une réglementation spécifique (http://www.ssi.gouv.fr/administration/reglementation/controle-reglementaire-sur-la-cryptographie), encore faut-il qu'elle soit respectée et on imagine mal des terroristes appliquer à la lettre la réglementation française…
Ainsi, en mettant en place un tel niveau de contrôle des communications, le risque est de faire monter le niveau de sophistication des échanges entre terroristes. Pour peu que la loi soit votée, on peut compter sur le gouvernement pour médiatiser rapidement quelques prises afin d'illustrer la pertinence de la loi. Il est toutefois évident, à terme, que les premières mesures des organisations terroristes consisteront à former leurs membres aux techniques de chiffrement, afin de devenir invisibles sur la toile, alors même que la formation des agents de la force publique prendra des années. L'agilité joue là encore en la faveur des extrémistes.
Il est vrai que l'on ne peut pas rester inactifs face à la menace terroriste, mais une solution clé-en-main basée uniquement sur le numérique et votée en urgence est-elle la meilleure solution ? Certes le projet de Loi permet de mieux encadrer des pratiques qui existaient déjà sans support légal, mais cette Loi risque bien de rendre ces pratiques plus difficiles à mettre en oeuvre, voire caduques. Enfin, sur le fond, la réaction du public suite à l'affaire Charlie Hebdo était sur le thème « Nous n'avons pas peur, nous continuerons à être libre ». Avec ce projet de loi, le message me semble plutôt être « Nous avons peur, mais nous sommes prêts à être moins libres pour y remédier, quitte à ce que cela ne serve à rien ».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.journaldunet.com/ebusiness/expert/60824/la-loi-renseignement-sera-contournee.shtml
Par Jean- François Pillou – CCM Benchmark

Les 5 dangers du projet de loi sur le renseignement | Denis JACOPINI

	**Les 5 dangers du projet de loi sur le renseignement**

Dernière ligne droite pour le projet de loi sur le renseignement. Le vote solennel du texte est prévu ce mardi 5 mai à l'Assemblée, malgré une mobilisation des opposants, lundi soir au Trocadéro, à Paris.
Que dit le texte ? Au fil des débats, les députés ont fait évoluer le projet de loi. « Il a été considérablement enrichi », estime son rapporteur, Jean-Jacques Urvoas (PS), dans une note envoyée aux députés dont « l'Obs » a eu connaissance. Au total, 260 amendements ont été adoptés. Cela répond en partie aux demandes des adversaires du texte, mais ne lève pas toutes les inquiétudes, loin de là.

Ce que l'Assemblée a modifié :
Une commission de contrôle renforcée
Est surtout renforcé « la composition, l'indépendance et les pouvoirs de la [nouvelle] Commission nationale de contrôle des techniques de renseignements » (CNCTR). Celle-ci remplacera l'actuelle Commission nationale des interceptions de sécurité (CNCIS) et, comme réclamé dans « l'Obs » par son actuel président, cette nouvelle instance disposera d'un « accès aux locaux des services, aux dispositifs de traçabilité, aux opérations de transcription, d'une saisine élargie du Conseil d'Etat ». De plus, les renseignements collectés seront bien centralisés par le Groupement interministériel de contrôle (GIC), que « l'Obs » a pu visiter en exclusivité.

Des professions moins exposées
Le texte exclut désormais certaines professions de la procédure d'urgence. Pour les magistrats, les avocats, les journalistes et les parlementaires, les écoutes ne peuvent être mises en œuvre que sur autorisation du Premier ministre, après avis de la commission. (Art. L. 821-7)

Un statut de lanceur d'alerte
De même, un « statut de lanceur d'alerte a été créé afin d'apporter une protection juridique à tout agent souhaitant révéler des illégalités commises ». N'est en revanche pas précisé si ce statut pourra être étendu à tous ceux qui révèlent des illégalités, à la manière d'Edward Snowden sur la NSA.

Les hackers plus fortement sanctionnés
Les députés ont également profité du texte pour renforcer l'arsenal de sanctions contre les hackers. Dans le sillon de la cyberattaque contre TV5 Monde, ils ont décidé de doubler les sanctions pécuniaires pour tout piratage (actuellement puni au maximum de 75.000 euros), voire de les tripler s'il s'agit d'un service de l'Etat.

Un fichier des personnes mises en cause pour terrorisme
Le gouvernement a également profité de cette loi pour créer un nouveau fichier (FIJAIT) qui recensera les noms et adresses de toutes les personnes condamnées ou mises en examen pour terrorisme.

Malgré des améliorations notables du texte, certains points continuent de poser problème.

1 – Le Premier ministre, seul maître à bord
La loi dote les six services de renseignement français de nombreux moyens supplémentaires pour enquêter, et la plupart n'auront plus besoin de l'aval d'un juge. En effet, le Premier ministre se positionne comme seul décisionnaire.
Les autorisations sont délivrées, après avis de la CNCTR, par le Premier ministre », pointe le texte.
Surtout que le Premier ministre pourra passer outre l'avis de la CNCTR, mais devra alors motiver sa décision (et risquer une saisine du Conseil d'Etat). Et tout ceci s'applique, sauf « en cas d'urgence absolue »…

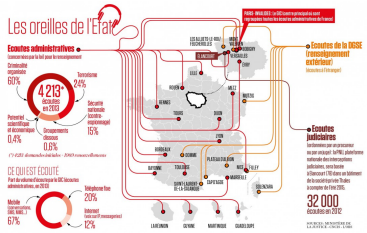
2 – Des données conservées longtemps
Afin de surveiller une personne, le projet de loi prévoit de nombreuses interceptions à distance (e-mails, conversations téléphoniques, SMS…) mais aussi la pose de micros et caméras dans des lieux ou des véhicules. Le texte prévoit que l'ensemble des renseignements ainsi collectés seront détruits au terme de certaines durées :
• 30 jours pour les correspondances,
• 90 jours pour les sonorisations, les géolocalisations et les images vidéo,
• 5 ans pour les données de connexion, aussi appelées métadonnées (qui donnent le détail de qui écrit un e-mail à qui, à quelle heure, etc.).
Et, en cas de cryptage des données, ces délais ne s'appliquent qu' »à compter de leur déchiffrement ».

3 – Eviter de croiser la route d'un suspect
Le projet de loi prévoit que les mesures de surveillance seront utilisées à la fois pour les suspects, mais aussi pour les « personnes appartenant à [son] entourage » s'il « existe des raisons sérieuses de croire [qu'elles ont] joué un rôle d'intermédiaire, volontaire ou non ». En somme, n'importe qui se trouvant au mauvais endroit, au mauvais moment, et ayant croisé une mauvaise route, pourra être mis sous surveillance.

Lors de la manifestation contre le projet de loi sur le renseignement, le 13 avril (CITIZENSIDE/ANTHONY DEPERRAZ/AFP)

4 – Tous suspects sur internet
Le projet de loi entend mettre à profit les opérateurs internet. Fournisseurs d'accès, moteurs de recherche, réseaux sociaux… Tous pourront fournir « en temps réel » les données techniques de connexion des internautes suspectés de terrorisme. Concrètement, il s'agit de pister une connexion (exprimée par une adresse IP) pour savoir quel site elle a visité, à quelle heure, si elle a envoyé un message Facebook à telle personne, si elle a tapé tel mot clef sur Google…
Le texte souhaite aussi contraindre les opérateurs internet à « mettre en œuvre sur leurs réseaux un dispositif destiné à détecter une menace terroriste sur la base de traitements automatisés ». Concrètement, les services de renseignement installeront une « boîte noire » dotée d'un algorithme qui passera au crible l'ensemble du trafic internet pour détecter automatiquement des internautes soupçonnés d'être des terroristes. A terme, cette boîte noire pourra être mise en place chez les fournisseurs d'accès à internet, mais aussi les Américains Google, Facebook, Apple ou Twitter.
L'ensemble du système surveille l'ensemble des internautes de manière anonyme pour détecter des « signaux faibles ». Et, en cas de suspicion, les opérateurs devront dénoncer la personne correspondant aux enquêteurs.
La CNCTR aura accès « au code source » de cette boîte noire afin de limiter la collecte des données aux seuls terroristes. Du moins, tant qu'un décret n'a pas étendu le champ d'action de ce dispositif qui s'apparente à « une surveillance de masse » inspirée par l'agence de renseignement américaine NSA.

5 – Surveiller les terroristes, mais pas seulement
Finalement, il convient de rappeler que, malgré les présentations du texte par François Hollande ou Manuel Valls, il ne s'agit pas d'une loi anti-terroriste, mais bien d'un texte sur le renseignement. Le projet prévoit sept finalités pour recourir aux diverses techniques de renseignement :
• l'indépendance nationale, l'intégrité du territoire et la défense nationale,
• les intérêts majeurs de la politique étrangère et la prévention de toute forme d'ingérence étrangère,
• les intérêts économiques, industriels et scientifiques majeurs de la France,
• la prévention du terrorisme,
• la prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale ou de la reconstitution de groupements dissous,
• la prévention de la criminalité et de la délinquance organisées,
• la prévention de la prolifération des armes de destructions massives.
Pour rappel, en 2014, 60% des écoutes administratives visaient la criminalité organisée, 24% le terrorisme, 15% la sécurité nationale (contre-espionnage), 0,6% les groupements dissous, et 0,4% la protection du potentiel scientifique et économique. Depuis l'attaque meurtrière contre « Charlie Hebdo », la part dédiée au terrorisme est montée à 48%.



Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Note de Jean-Jacques Urvoas publié par NouvelObs.com

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://tempsreel.nouvelobs.com/loi-renseignement/20150504.OBS8368/les-5-dangers-du-projet-de-loi-renseignement.html?cm_mmc=EMV-_-NO-_-20150505_NLNOACTU08H-_-les-5-dangers-du-projet-de-loi-renseignement##xtor=EPR-1-Actu8h-20150505
Par Boris Manenti

Loi sur le renseignement : Les coulisse d’un algorithme intrusif | Le Net Expert Informatique

Un chaton travaillant sur un algorithme (Mr Thinktank/Flickr/CC)	Loi sur le renseignement : Les coulisse d’un algorithme intrusif

On a demandé à des spécialistes en informatique s'il était possible de concevoir un programme répondant aux attentes du gouvernement en matière de renseignement. Résultat : techniquement, c'est très foireux.

Vous ne savez sans doute pas de quoi il s'agit. Pour être francs, nous non plus, nos élus non plus, et même nos contacts les plus calés en informatique nous répondent que ce domaine est trop pointu pour eux.
Pourtant, ce sujet est l'un des points les plus controversés du projet de loi sur le renseignement, discuté à l'Assemblée nationale depuis lundi : l'algorithme que le gouvernement, à la demande des services secrets, souhaite faire tourner au cœur de l'Internet français.

Programmé au sein des fameuses « boîtes noires » que l'exécutif veut installer sur les tuyaux des opérateurs (Orange, Free, Numericable…) et des hébergeurs (Google, Facebook, et autres), cet algorithme a pour but de détecter, avant même la commission d'actes terroristes, d'éventuels suspects.

On a déjà beaucoup parlé des similitudes entre cette ambition et la science-fiction. Mais concrètement, comment fonctionnera cet « algorithme » que tous les députés, tous les ministres, tous les conseillers, et donc tous les médias, ont à la bouche ces derniers jours ?
Nous sommes allés poser la question à des chercheurs en informatique, qui réfléchissent à la question de la vie privée, du stockage des données, ou bien encore à l'intelligence artificielle.
Croisées avec les rares explications fournies par le gouvernement (secret-défense oblige), les réflexions de nos interlocuteurs nous permettent d'affirmer qu'en l'état, quelle que soit la forme de l'algorithme choisie, le dispositif sera coûteux, intrusif et inefficace.

1. Un algorithme, c'est d'abord des humains
Ce n'est pas une formule magique, mais du code informatique créé par des êtres humains
« Quand les gens du gouvernement en parlent, on a l'impression qu'il s'agit d'une formule d'Harry Potter ! »
A l'instar de ce docteur en intelligence artificielle (IA), qui a souhaité garder l'anonymat, les personnes qui bossent quotidiennement sur des algorithmes sont aujourd'hui un peu désolées de voir leur outil de travail autant malmené.
Car si le terme revient souvent ces derniers temps, il est très rarement défini. Et devient l'objet d'une fascination béate, ou, à l'inverse, d'une peur irrationnelle.

Ni magique, ni diabolique : une recette de cuisine
Instant définition donc, histoire de lever le brouillard. Comme nous l'explique notre interlocuteur :
• « *Un algorithme, c'est simplement une suite d'opérations définies très strictement, que l'ordinateur, parfaitement stupide, exécute.* »
Un simple bout de code informatique (voir exemple ci-dessous), parfois court, parfois très long, qui vise à accomplir quelque chose. Pour cette raison, on compare souvent les algorithmes à une recette de cuisine : une série d'ingrédients précis qui aboutissent à un plat. L'analogie est plutôt bonne. Car si certaines recettes peuvent facilement être déduites de l'assiette posée devant soi (par exemple, un croque-monsieur), d'autres sont bien plus difficiles à cerner.

Un algorithme, ça ressemble en partie à cela. Extrait de Scikit-learn, qui donne des outils de data-mining (Scikit-learn)
Comme l'explique Gilles Dowek, chercheur à l'Institut national de recherche en informatique et en automatique (Inria), par e-mail :
• « Vous avez sans doute déjà mangé dans un restaurant un plat qui vous a plu que vous avez tenté de reproduire dans votre cuisine en essayant d'imaginer la recette qui y a conduit (pour ma part, j'essaie souvent avec un succès inégal). »

Avant, après : il y a des êtres humains
Autre corolaire de cette définition : si l'ordinateur exécute, c'est bien l'être humain qui définit ce qu'il doit exécuter. Et ce qu'il attend de cette opération. Notre spécialiste de l'IA explique :
• « En informatique, il y a toujours une entrée et une sortie. Au milieu, il y a une boîte, dans laquelle on entre une série d'opérations à faire, pour lesquelles on attend un résultat. »

Pour ce chercheur, les limites de l'opération sont déjà nettes :
• « La sortie attendue ici n'est pas très claire : il s'agit de dégager des comportements atypiques de la population qui seraient aussi typiques du terrorisme. »

Problème : comment définir des comportements atypiques ? Et typiques ? Le fait d'aller regarder une vidéo de décapitation de l'organisation Etat islamique est-il déjà un acte suspect ? On vous renvoie à la lecture de cet entretien très éclairant avec la chercheuse Antoinette Rouvroy.

Gilles Dowek pousse la démonstration un peu plus loin, en imaginant un système s'appuyant sur une liste de mots utilisés par des terroristes :
• « Que faire par exemple, si on s'aperçoit que cette liste contient le mot "banane" ? Cela signifie que statistiquement, les criminels utilisent fréquemment le mot "banane". Doit-on supprimer ce mot qui, manifestement, n'est pas suspect ? Ou alors considérer comme suspecte toute personne qui utilise ce mot ? »

Pour notre spécialiste de l'intelligence artificielle, on demande ici à un ordinateur une tâche bien trop fine : celle de catégoriser des êtres humains.
• « Or, ce système d'étude est hyper compliqué. Les ordinateurs n'ont qu'un modèle simplifié de l'humain. Par exemple, un humain vu par Amazon sera l'ensemble des bouquins qu'il a achetés sur un an. »

Or, à la différence d'Amazon et de tous les autres géants du Web, l'algorithme voulu par ce projet de loi ne recommandera pas des livres ou des sites internet, mais des humains.

Le gouvernement a beau jeu de dire que ces acteurs appliquent déjà, sur nous et avec notre accord, ces mêmes règles. Ce n'est pas tout à fait la même chose. Et par ailleurs, comme le note Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (Cnil), la puissance publique a d'autres prérogatives (et responsabilités) que les entreprises privées.

2. Quel que soit l'algorithme choisi, la surveillance est massive
Manuel Valls et Bernard Cazeneuve ont beau répéter que ce n'est pas la cas, la technique les fait mentir.
Passées ces précisions, entrons dans le dur : comment les services vont-ils s'y prendre avec cet algorithme ? Ou plus précisément, avec ces algorithmes qui, enchaînés entre eux, aboutiront au résultat voulu ?
« Il y a des tas de façons de faire », nous rétorquent l'ensemble des chercheurs que nous avons interrogés. Néanmoins, trois options se dégagent nettement. Et chacune, pour être efficace, nécessite de surveiller tout le monde.

La méthode déjà possible : les relations sociales
L'une des options possibles est de s'appuyer sur un objet mathématique bien connu, le graphe. Concrètement, il s'agirait de regarder les relations des « 3 000 personnes engagées de près ou de loin dans la mouvance terroriste », dont parlait le Premier ministre lundi.
De cette façon, on établit rapidement une cartographie de potentiels terroristes. En présumant, bien sûr, que le simple fait d'être en relation avec un terroriste identifié suffit à faire un suspect. Or, même en étant un véritable proche d'un terroriste, on peut ne rien savoir de ses activités. Il suffit de prendre le cas d'Amedy Coulibaly, en rupture avec certaines de ses sœurs.
Avec cet outil, la surveillance est massive. Peut-être connaissez vous la théorie des six degrés de séparation, selon laquelle chaque personne sur Terre est à six relations d'une autre ? Avec Internet, ce chiffre serait passé à quatre. Et la NSA, par exemple, va étudier jusqu'à deux degrés de séparation… Et espionne donc, grosso modo, des centaines de millions d'individus.
Néanmoins, on voit mal pourquoi les services français auraient attendu ce texte pour mettre en place ce dispositif, il suffit qu'il l'appliquent sur les 3 000 personnes déjà connues. Et il ne leur permettra pas de repérer les futurs éventuels coupables, ce qui est le but de cette loi.

La méthode basique : définir un ensemble de règles
Une autre option serait de demander à l'ordinateur de signaler les internautes qui font un ensemble de choses sur Internet considérées comme suspectes. Se connecter à tel et tel site djihadiste, utiliser régulièrement sur Internet une série de mots (par exemple « bombe », « arme », « explosion », « tirer », « tuer »), vérifier qu'une vidéo de propagande a bien été mise en ligne.
Ce scénario est l'un des plus crédibles. Il correspond aux rares exemples fournis par les ministres et leurs conseillers. Et a le caractère « rustique » que dépeignait, à l'occasion d'une conférence le 9 avril sur le sujet, l'un des conseillers de Manuel Valls, Renaud Vedel.
Néanmoins, là encore, pour être efficace, cette méthode nécessite de scruter l'ensemble des communications internet pour repérer ce que l'on recherche.

La méthode plus fine : un algorithme qui apprend
Ici, l'ordinateur apprend d'un jeu de données — on parle d'apprentissage automatique ou statistique.
Concrètement, la méthode consisterait, pour les services, à soumettre à la machine les habitudes de navigation des 3 000 personnes qui sont aujourd'hui dans leur radar. A partir de ces données, l'ordinateur détecte des particularités (des motifs), qui lui permettront par la suite de dire si oui ou non, tel ou tel internaute correspond à un profil de suspect.

Deux chercheurs de l'Inria, là encore sous couvert d'anonymat, nous alertent alors sur un point précis :
• « Pour détecter les motifs, l'algorithme a besoin des données d'un ensemble d'individus ayant le profil recherché que l'algorithme analyse (apprentissage) au regard des données d'individus ne correspondant pas au profil (pris au hasard). »

Traduction : là encore, pour que la méthode fonctionne, il faut surveiller non seulement des gens dont on ne sait pas s'ils sont suspects, mais dont on est certain qu'ils ne le sont pas. Non seulement cela confine à l'absurde, mais signifie que tout le monde peut être surveillé.

3. Quel que soit l'algorithme choisi, il sera inefficace
Faux positifs, faible nombre de suspects, limites du programme…

Une quantité astronomique de faux positifs
Les chercheurs sont également unanimes sur ce point : même si l'algorithme concocté par les services est hyper-balèze, il ne pourra échapper à une quantité considérable de faux positifs (en l'occurrence, des gens identifiés comme potentiellement suspects et qui se révèlent non coupables).

Pire, comme le dit notre spécialiste de l'intelligence artificielle :
• « Même avec un système d'une performance extrêmement élevée, il y aura toujours beaucoup plus d'innocents que de coupables accusés. »

Nos interlocuteurs de l'Inria confirment. Et déploient une démonstration implacable :
• « Supposons un algorithme d'une super-qualité qui n'a qu'une chance sur 100 de se tromper. Sur 60 millions de personnes, ça fait 600 000 personnes détectées à tort, plus les 1 000 "vrais positifs" qu'on a bien détectés. Donc l'algorithme détecte 601 000 personnes, parmi lesquelles en réalité 1 000 seulement sont de vrais terroristes. L'algorithme détecte alors les terroristes avec une probabilité de 1 000/601 000, soit 1/600, soit 0,02%… Tout ça pour ça ?

Par e-mail, Marc Schoenauer, directeur de recherche à l'Inria, évoque par exemple la possibilité de prendre dans ces filets "les créatifs d'avant-garde" (les gens qui ont des comportements "anormaux"). On peut aussi penser à tous ceux qui vont voir les vidéos de l'Etat islamique. Aux journalistes, aux chercheurs qui travaillent sur ces sujets.

Le problème des signaux faibles, c'est qu'on ne les voit pas
A cause des faux positifs, et parce que rapporté à des dizaines de millions de personnes, les terroristes sont très rares, les algorithmes auront du mal à les détecter.
Là encore, les chercheurs sont formels : cela revient à chercher une goutte dans l'océan que vous ciblez. A étendre la taille de la meule de foin dans laquelle vous recherchez l'aiguille, pour reprendre une expression de Pierre Lellouche, élu UMP opposé au texte.
Or, si des techniques permettent de repérer ce genre de signaux sur Internet, les chercheurs estiment que ces derniers ne sont pas assez fiables en l'espèce. Encore loupé.

La solution du gouvernement : encore moins efficace
Quand on leur demande, les conseillers du gouvernement sont formels : l'algorithme en question n'adaptera pas seul ses paramètres. C'est en effet une possibilité technique : certains algorithmes, à partir des données de départ, évoluent, apprennent en fonction des nouveaux usages observés.
Or, selon l'exécutif, chaque modification du code source de l'algorithme sera soumis au contrôle de la commission prévue à cet effet, la CNCTR. Ce qui est très inquiétant en termes de garanties pour les citoyens (on voit mal en effet comment la commission pourrait contrôler effectivement un algorithme qui change sans cesse), mais qui rend le dispositif bien précaire.

Si le but est de détecter de nouveaux terroristes, et qu'il faut modifier, à la main, le code de l'algorithme à chaque fois qu'une nouvelle pratique propre aux mouvements terroristes est détectée sur Internet, on voit mal comment on pourra les identifier à l'avance.

Ou, comme le résume notre expert en intelligence artificielle :
• "J'ai la crainte que quelque chose comme ça soit toujours en retard d'une guerre."

4. Un stockage incontournable, un anonymat tout relatif

Le stockage de nos données : nécessaire et faisable
De l'aveu même du gouvernement, les données observées par ce dispositif seront stockées, quelque part en France. Néanmoins, il assure que seules les informations intéressantes (les données qui correspondraient à un profil suspect) seront entreposées dans des disques durs.
Qu'il soit partiel ou intègre l'ensemble du trafic internet français, ce stockage pose déjà un énorme enjeu de sécurité. Sans mettre en doute la bonne foi des espions, le risque d'intrusion informatique existe.
Par ailleurs, nos interlocuteurs doutent de la possibilité de ne pas stocker du tout, même brièvement, les données de tout le monde.
Certes, des systèmes existent pour se débarrasser des informations parasites, du bruit, que peuvent brasser d'énormes détecteurs de données. C'est par exemple le cas au Cern, le fameux accélérateur de particules, qui se fiche bien (comme les services, on le suppose), de stocker toutes les données de toutes les particules. Mais comme le dit notre spécialiste de l'intelligence artificielle :
• "Même s'il y a une élimination du signal, ça veut tout de même dire qu'à un moment, ils ont les données."

Les deux chercheurs de l'Inria nous font par ailleurs remarquer que l'argument selon lequel stocker toutes ces données serait très difficile, du fait du volume que cela représenterait, n'est pas valable :
• "Le volume n'est pas si conséquent que ça : par exemple, la liste des sites web (juste l'adresse du site, pas le contenu, soit de l'ordre de 100 octets par site) visités par jour, avec éventuellement le temps resté sur chaque page. Le nombre de sites différents visités par jour n'est pas si important par personne (disons 100 par jour)". En imaginant qu'on trace 60 000 000 de personnes, […] ça ferait soit moins d'un terra octet… Ça tient sur un disque dur et c'est faisable de les traiter. Donc en gros, sur un disque dur, nous avons l'ensemble des métadonnées françaises pour la journée (qu'on pourrait même compresser)."

Anonymat des données : illusoire
Là encore, grand scepticisme. Le gouvernement assure que l'anonymat des données collectées selon ce dispositif ne sera levé qu'après avis de la commission de contrôle.
Sauf que pour être efficace, l'algorithme devra savoir que telle ou telle donnée correspond à la même personne. Pour nos deux experts de l'Inria :
• "C'est un contresens juridique de définir la possibilité de retirer l'anonymat : l'anonymat est le fait que rien ni personne ne puisse nous identifier, quelque soit les mesures mises en œuvre (loi informatique et libertés)."

Au passage, cet enjeu pose une autre difficulté : comment les services vont-ils faire pour savoir qu'une même personne se connecte sur un site suspect de chez elle, sur un autre site suspect depuis son téléphone ou depuis un cyber-café ? A l'heure des écrans multiples, des bornes wifi, comment repérer un seul et même individu ?

5. Un contrôle délicat
Il faut des moyens humains et financiers à la hauteur du défi
On l'a déjà vu, en fonction du type d'algorithme choisi par les services, le contrôle prévu dans le projet de loi sera plus ou moins effectif. Ainsi, si l'algorithme évolue sans cesse, on voit mal comment les experts pourront aller vérifier qu'il fonctionne bel et bien uniquement pour détecter d'éventuels terroristes.

De même, certains algorithmes sont par nature très opaques : on parle alors de "boîtes noires". Eh oui ! L'expression utilisée par des conseillers gouvernementaux renvoie aussi à un type d'algorithme très précis. Dans ces cas-là, un peu comme avec un plat très élaboré dont il n'est pas évident de reproduire la recette, ou avec notre réseau de neurones, on sait que ça marche, mais on ne sait pas bien comment…

Le gouvernement rassure en affirmant que le code source de l'algorithme sera remis à la commission de contrôle. Un conseiller parlant même, dans un sourire, "de logiciel libre dans un monde de secret-défense".

L'initiative est louable, mais même en ayant écrit le code source, il arrive que les chercheurs n'arrivent pas à comprendre comment l'algorithme aboutit à un résultat précis. Ce n'est pas donc pas forcément suffisant !

Par ailleurs, le contrôle de cet algorithme sera de toute manière très complexe. Et lourd. Comme le confie notre docteur en intelligence artificielle :
• "Relire le code écrit par quelqu'un d'autre, croyez-moi, c'est l'enfer !"

A l'en croire, des théories mathématiques existent aujourd'hui pour vérifier qu'un algorithme ne sorte pas de son domaine. Problème : elles s'appliquent sur des codes assez limités, comme sur un avion de ligne.

• "C'est valable dans l'aviation, mais le code d'un Airbus est petit par rapport à ce qu'il y a sur votre Windows !" »

La qualité de contrôle de l'algorithme dépendra donc de la quantité et de la qualité des données à dispositions des experts, des moyens humains et financiers à leur disposition, du délai dont ils disposeront… Le tout pour trancher si oui ou non, pour citer le texte, ces données reflètent une réelle menace terroriste.
• « Oppenheimer devant la bombe atomique »

La responsabilité est donc colossale. Et renvoie, selon les chercheurs, toujours au même problème : la question fondamentale n'est pas un enjeu technique mais un enjeu social. Comme le dit Gilles Dowek :

• « Acceptons-nous ou non d'être observés en permanence afin que quelques criminels soient arrêtés au moment où ils en sont encore à préparer un crime ? »

Colin de la Higuera, membre du laboratoire informatique de l'université de Nantes, regrette pour sa part que le sujet, aux « vraies répercussions pour la société », ne fasse pas l'objet d'un débat public avec les chercheurs compétents.

De son côté, notre spécialiste de l'intelligence artificielle se définit « comme Oppenheimer devant la bombe atomique ! ». Et ajoute :

• « J'ai l'impression que les politiques viennent me raconter mon boulot alors qu'ils ne le connaissent pas mieux que moi. […] Ils parlent d'algorithme avec un grand A, comme s'il s'agissait d'un archange tombé du ciel pour arrêter les méchants… Non ! Un algorithme ne sort que des cerveaux humains. Et je vous en conjure : méfiez-vous de ce qui sort de mon cerveau ! »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://rue89.nouvelobs.com/2015/04/15/lalgorithme-gouvernement-sera-intrusif-inefficace-prouve-258672
Par Andréa Fradin

Une loi pour nous espionner sous couvert de la peur du terrorisme | Le Net Expert Informatique

Des manifestants contre le projet de loi sur le renseignement devant l'Assemblée nationale, à Paris, le 13 avril 2015. (MAXPPP)

Une loi pour nous espionner sous couvert de la peur du terrorisme…

Selon le projet de loi, le renseignement sera désormais autorisé à récupérer les "métadonnées" des échanges électroniques, soit les informations qui entourent une conversation : qui envoie un message, à qui, quand, par quel support. (MAXPPP)

C'est un texte qui agite les défenseurs des droits et des libertés depuis sa présentation, le 19 mars dernier. Le projet de loi sur le renseignement déchaîne les passions entre le gouvernement et les opposants à ces dispositions.
Le texte, qui arrive lundi 13 avril en première lecture à l'Assemblée nationale, dispose d'un vaste soutien politique. Le PS comme l'UMP sont décidés à le voter, dans un réflexe d'union nationale après les attentats des 7 et 9 janvier. Mais au vu du peu de temps disponible pour lire ce projet très technique, les opposants craignent que peu de députés comprennent véritablement ce qu'ils s'apprêtent à voter. Francetvinfo a fait ce travail d'éclairage pour vous.

Pourquoi une nouvelle loi ?
Après les attentats de Charlie Hebdo, Montrouge, et porte de Vincennes, le gouvernement a insisté sur le manque de moyens donnés aux services de renseignement. Plus particulièrement, le projet de loi sur le renseignement veut mettre en place un cadre légal sur des pratiques des services qui étaient illégales. Si un rapport parlementaire a été publié en 2013, proposant des réformes des services de renseignement, les attentats de janvier ont tout accéléré. Au point que le gouvernement souhaite voir sa copie adoptée d'ici l'été.
Pour le gouvernement et les partisans de ce texte, il s'agit de réformer la dernière loi antiterroriste, qui date de 1991. Il est à noter que les services disposent déjà de moyens étendus depuis la loi de programmation militaire votée en décembre 2013, mais aussi depuis la loi de lutte contre le terrorisme en 2006, qui permet déjà aux services de procéder à des écoutes des communications dites "administratives", c'est-à-dire uniquement du ressort du Premier ministre. Aujourd'hui, environ 6 000 écoutes sont demandées chaque année.

Qu'y a-t-il de plus dans cette nouvelle loi ?
Cette loi autorise les services de renseignement à faire des écoutes bien plus intrusives que précédemment. Si ce projet est adopté en l'état par le Parlement, les services pourront poser des micros dans un appartement ou un véhicule, installer des balises GPS ou écouter des communications téléphoniques, sans l'accord d'un juge. Ils pourront également utiliser des IMSI-catchers, un dispositif qui permet d'écouter toutes les communications (téléphoniques comme électroniques) dans un rayon de 500 mètres à un kilomètre.

Et comme le terrorisme se développe de plus en plus sur internet, le renseignement sera désormais autorisé à récupérer les "métadonnées" des échanges électroniques, soit les informations qui entourent une conversation : qui envoie un message, à qui, quand, par quel support. Ces métadonnées sont différentes du contenu explicite des messages, qui ne sera pas collecté. Une surveillance du clavier d'un suspect, ou keylogger, pourra également être demandée, ce qui permettra aux services de tout savoir de ce que l'on tape sur son clavier. Enfin, l'internet français pourra être espionné à la source, chez les fournisseurs d'accès et hébergeurs, à l'aide de « boîtes noires ».

Concrètement, les services pourront ainsi surveiller physiquement et électroniquement des individus particuliers : d'une voiture au téléphone en passant par les communications électroniques.

Attendez, ça veut dire que tout internet sera espionné ?
De fait, oui. Car la surveillance à la source d'internet se fera à l'aide de « boîtes noires », ce qui pose le plus problème. Le projet de loi prévoit d'installer des boîtiers chez les fournisseurs d'accès internet et les hébergeurs de données pour surveiller l'ensemble du trafic internet qui transite par la France. Ces boîtes noires auront comme objectif de détecter des "comportements suspects" en analysant les comportements des citoyens français sur la toile. La détection se fera au moyen d'un algorithme, soit un mécanisme élaboré par des humains mais mis en œuvre par des machines. Si ce type de comportement est remarqué, une alerte sera envoyée aux services de renseignement. On ne sait pas encore ce à quoi correspond un "comportement suspect".

Un comportement suspect est-il forcément celui de quelqu'un qui veut commettre un acte terroriste ?
Non, pas seulement. Contrairement à ce qui dit la communication gouvernementale, le projet de loi ne concerne pas uniquement la lutte antiterroriste. Le renseignement, c'est la recherche d'informations et leur analyse. On y inclut les domaines économique, financier ou scientifique. Concrètement, l'espionnage industriel, la lutte contre le blanchiment ou la veille scientifique font partie du renseignement.

Cette dimension très large est présente noir sur blanc dans le projet de loi. De fait, les moyens ne s'appliqueront pas uniquement au terrorisme, mais dans sept domaines définis par le projet de loi, dont « l'indépendance nationale », « les intérêts majeurs de la politique étrangère », les « intérêts économiques industriels et scientifiques majeurs de la France », ou même « la prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale, de la reconstitution ou d'actions tendant au maintien de groupements dissous ». Les motifs se révèlent particulièrement vastes.

Et je peux être surveillé, moi ?
Malgré les dénégations du gouvernement qui jure qu'il ne s'agit pas d'une surveillance de masse, la formulation extrêmement vague du comportement suspect ou même des motifs de surveillance possibles font craindre aux opposants que cette loi puisse être utilisée pour surveiller l'ensemble de la population. Car si les « boîtes noires » ne font remonter que les comportements suspects, elles analyseront tout le trafic internet.

De plus, si des communications chiffrées sont interceptées sur internet ou par les écoutes des services, les données pourront être conservées indéfiniment, afin de laisser du temps aux services de décrypter les échanges. Si ces données ne sont pas chiffrées, elles pourront être conservées entre 12 mois et 5 ans. Mais rien ne décrit dans la loi comment ces données seront utilisées ou contrôlées. Nos confrères de Libération ont, à ce propos, réalisé un questionnaire qui vous permet d'estimer à quel point vous êtes concerné.

Mais si je n'ai rien à me reprocher ?
Comme expliqué précédemment, l'ensemble du trafic internet français sera espionné d'une manière ou d'une autre par les « boîtes noires ». Donc, même si vous n'avez rien à vous reprocher, il y a des chances que vous puissiez être espionné sur internet. Un autre point clé de cette loi est qu'elle cherche à « prévenir » le terrorisme.

En passant, elle s'inspire de la NSA américaine, l'agence de sécurité des Etats-Unis, en prévoyant de surveiller les personnes à N+1, le N étant le suspect. Si vous entrez en contact avec lui d'une manière ou d'une autre, vous pourrez être espionné. Au-delà des spécificités techniques, le projet cible le « préterrorisme », fondé sur une présomption de culpabilité, qui abaisse considérablement le seuil de la détection.

C'est pour cela que des opposants manifestent ?
Cette surveillance de masse est précisément un des points clés de la manifestation organisée lundi 13 avril par les opposants à cette loi devant l'Assemblée nationale. Ils vont, a recensé Le Monde, du juge antiterroriste Marc Trevidic à l'association de défense des libertés individuelles sur internet la Quadrature du net en passant par la Ligue des droits de l'homme, la Cnil ou Reporters sans frontières. Ils craignent que ce projet de loi soit une atteinte irrémédiable à la vie privée des individus surveillés, et globalement une perte de sécurité dans les communications. Les « boîtes noires » ou les IMSI-catchers sont particulièrement combattus, car ils sont très intrusifs. Face à l'importance de ce texte, les opposants réclament plus de temps, alors que le projet de loi est examiné en « procédure accélérée », soit une seule lecture par l'Assemblée nationale et le Sénat.

Ils luttent également pour obtenir des garanties plus importantes face à l'étendue des nouveaux moyens confiés aux services. Et notamment qu'un juge procède au contrôle des écoutes. Car, dans le projet de loi actuel, les nouveaux moyens des services de renseignement pourront être mis en œuvre sans le contrôle d'un juge. Plus précisément, le contrôle est laissé à la Commission nationale de contrôle des techniques de renseignement (CNCTR) qui ne dispose que d'un avis consultatif. Le vrai pouvoir de décision reste entre les mains du Premier ministre.

Et si jamais les services se trompent ?
Le gouvernement a bien insisté sur le contrôle du processus par la CNCTR. Concrètement, les services font une « demande motivée » au Premier ministre pour utiliser un moyen de surveillance. Cette demande est examinée par la commission, qui rend un avis. Mais en cas d'urgence décrétée par le Premier ministre, aucun avis n'est requis, et aucun contrôle n'est possible pendant 48 heures. Ainsi, le chef du gouvernement a toute latitude pour autoriser ou non les écoutes.

Cependant, si la CNCTR s'oppose à une écoute, elle peut saisir le Conseil d'État. Innovation du texte, un citoyen pourra également saisir directement cette institution s'il pense être surveillé. Si le Conseil d'État considère que l'écoute a été réalisée sans motifs réels, il ordonne la suppression des données collectées. Le citoyen ne pourra cependant pas savoir comment il a été surveillé, ni même ce qui a été surveillé.

En résumé
Après les attentats de janvier en France, le gouvernement a voulu réagir et a présenté un projet de loi de renseignement, qui est examiné le 13 avril à l'Assemblée nationale. Le gouvernement veut le voir adopté d'ici à l'été prochain. Ce texte étend les moyens des services de renseignements, qui pourront écouter une personne dans sa voiture, son appartement, lors de ses appels téléphoniques et sur internet. Tout cela sans le contrôle d'un juge. De plus, le projet de loi prévoit l'installation de « boîtes noires » qui pourront espionner l'ensemble du trafic internet en France à la recherche de « comportements suspects » qui seront ensuite remontés aux services. Le projet de loi n'est pas uniquement destiné à la lutte antiterroriste, mais également au renseignement économique, technique et scientifique.

Côté politique, le PS et l'UMP soutiennent le texte, qui a de grandes chances d'être adopté en l'état. Cependant, les opposants sont nombreux, du juge antiterroriste Marc Trevidic à l'association de défense des libertés individuelles sur internet la Quadrature du net en passant par la Ligue des droits de l'homme, la Cnil ou Reporters sans frontières. Ils réclament plus de contrôle sur les nouveaux moyens accordés aux services et l'abrogation de la partie du projet de loi sur les boîtes noires. Pour l'instant, le Premier ministre a toute latitude, selon le texte, pour autoriser ou non les écoutes. Une commission est chargée de contrôler a priori et a posteriori, mais elle ne dispose que de pouvoirs consultatifs.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.francetvinfo.fr/politique/loi-sur-le-renseignement/larticle-a-lire-pour-comprendre-le-projet-de-loi-sur-le-renseignement_875623.html
Par Etienne Combier