Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

	Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

A ce jour, il existe certains exemples de moyens, usités par les terroristes, permettant de contourner une mesure de blocage d'un site, notamment, l'utilisation d'un « Virtual Private Network » (Réseau Privé Virtuel).

Ce dernier établi un réseau fictif, reliant un ordinateur (celui du client VPN) à un serveur (le serveur VPN), afin de permettre une connexion à Internet de manière anonyme.

De cette façon, les échanges de données sont cryptés et sont protégés par des clés de chiffrement. De plus, ce système permet d'utiliser une adresse IP différente de celle réellement utilisée par un ordinateur, ce qui complique considérablement la localisation de cette machine. De même, le logiciel « Tor » permet de se connecter à Internet par le biais de serveurs répartis dans le monde dans l'anonymat. Il convient de noter que ces procédés cryptologiques sont parfaitement légaux, effectivement, l'article 30 de la loi LCEN du 21 juin 2004 érige en principe que « l'utilisation des moyens de cryptologie est libre ». Dès lors, peut-on envisager l'introduction d'un contrôle par l'autorité administrative, sous forme d'autorisation préalable, lorsque l'utilisation de tels procédés est faite à des fins de provocation au terrorisme ?

Enfin, ces mesures de blocage de sites peuvent sembler illusoires étant donné que celles-ci ne s'appliquent qu'à des FAI et hébergeurs situés sur le territoire français. D'autant que de telles mesures drastiques ne sont pas exemptes de risques de « surblocage ». En 2013, l'Australie a pu en faire les frais en bloquant par accident 250 000 sites sur sa toile.

En conséquence, loin d'être la panacée, cette nouvelle disposition, faussement pragmatique, semble foncièrement superfétatoire.

Sur la conformité de la loi par rapport au bloc de constitutionnalité ?

A titre liminaire, il importe de se poser la question de savoir si la loi du 20 novembre 2015 est susceptible d'être déclarée non conforme à la constitution compte tenu de l'absence de consécration constitutionnelle du statut de l'état d'urgence. A cette fin, il conviendra d'appliquer mutatis mutandis le raisonnement adopté par le Conseil Constitutionnel dans deux décisions : celle du 10 juin 2009 concernant la loi HADOPI et celle relative à la loi sur la pédopornographie du 10 mars 2011.

Dans sa décision du 10 juin 2009, le Conseil en raison du caractère disproportionné du blocage et de sa contrariété avec l'article 11 de la DDHC censure la loi HADOPI soumise à son contrôle « considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins ».

En substance, les Sages expliquent que l'octroie par la loi à une autorité administrative du pouvoir de suspendre l'accès à internet est une entorse à la « la libre communication des pensées et des opinions ». L'autorité administrative n'ayant pas le statut de juridiction, elle ne peut se voir octroyer ce pouvoir exorbitant de bloquer un site illicite.

A rebours, dans sa décision du 10 mars 2011, les Sages valident l'article 4 de la loi Loppsi 2 permettant de procéder au blocage administratif de sites pédopornographiques « considérant, en second lieu, que les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile ; que la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé ; que, dans ces conditions, ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 ».

Dans cette décision, la mesure de blocage est déclarée conforme à l'article 11 de la DDHC de 1789 au motif qu'il existe un recours au fond ou en référé des décisions de blocage et qu'il est consacré un objectif à valeur constitutionnelle de sauvegarde de l'ordre public (ici l'exploitation sexuelle des mineurs).
En ce qui concerne la conformité du nouveau dispositif, il est à noter que ce nouvel article 11 de la loi de 1955 énonce que « le ministre de l'Intérieur peut prendre toute mesure » de blocage de sites faisant l'apologie du terrorisme. La large marge d'appréciation laissée à l'exécutif amène à s'interroger sur le caractère proportionné de cette disposition. Ainsi, un parallèle peut être opéré avec l'article L. 336-2 du CPI prévoyant des mesure de blocage en cas de violation d'un droit d'auteur ou d'un droit voisin. Celui-ci met en évidence l'éventuel caractère excessif du nouveau dispositif. Si ce dernier rend possible « toutes mesures », l'article L. 336-2 du CPI autorise seulement « toutes mesures propres » en vue de bloquer un site.

La référence au principe de proportionnalité, tangible dans cet article du CPI, ne l'est pas en ce qui concerne cette nouvelle mesure. Dans le cadre d'un raisonnement analogue à celui employé dans la décision du 10 juin 2009, on peut appréhender une potentielle censure par les Sages. En effet, la loi du 20 novembre 2015, compte tenu de sa rédaction large et générale, peut habiliter le ministre de l'Intérieur à « restreindre ou à empêcher l'accès à Internet ». De ce fait, un accroc à l'article 11 de la DDHC peut être redouté. D'ailleurs, le rapporteur au Sénat énonçait que « la disposition proposée [la loi lopssi 2] présente une portée beaucoup plus restreinte [que la loi HADOPI] puisqu'elle tend non à interdire l'accès à internet mais à empêcher l'accès à un site déterminé en raison de son caractère illicite ». Ainsi, le nouveau texte de 2015 risque de connaître le même sort que celui donné à la loi HADOPI, en ce que rien n'interdit au ministre de l'Intérieur de prendre des mesures bloquant l'accès à un site sans pour autant bloquer un site en particulier.
Par ailleurs, une autre incertitude juridique semble planer sur cette loi du 20 novembre 2015 au regard de la décision du 10 mars 2011. S'il est vrai que la suppression du délai de 24 heures ne semble pas impacter la conformité de ce texte, il en va autrement de l'éviction du rôle de contrôle de la CNIL. En effet, l'article 66 de la Constitution dispose que l'autorité judiciaire est « gardienne de la liberté individuelle ». Auparavant, la loi de 2014, chargeait la CNIL d'assurer ce rôle de gardien a posteriori, c'est-à-dire, en actionnant en aval les recours nécessaires devant la juridiction compétente. De même, la CNIL détenait la faculté de contrôler le bien fondé des demandes de retrait de l'autorité administrative. La nouvelle loi éludant cet encadrement exercé par la CNIL, peut laisser sceptique sur sa conformité au texte constitutionnel. D'autant que la loi ancienne (de 2014) n'a jamais fait l'objet d'un contrôle, que ce soit de manière a priori ou a posteriori, devant le Conseil Constitutionnel !

Sur le risque de contrariété de la loi avec la Convention Européenne des Droits de l'Homme ?

Dans un récent arrêt CEDH du 1er décembre 2015, la Cour censure des mesures de blocage de sites pratiquées par le gouvernement turc. En l'espèce, les autorités turques avaient ordonné le blocage de Youtube en raison de dix vidéos accusées de faire outrage à la mémoire d'Atatürk, fondateur de la République laïque turque. Des mesures de blocage ont été ordonnées entre 2008 et 2010.
La Cour reconnait une ingérence de l'autorité publique dans l'exercice des droits garantis par l'article 10 de la convention portant sur la liberté d'expression. De la même façon, la loi de novembre 2015 n'excluant pas la possible coupure d'un site Internet, elle encourt le risque d'être déclarée disproportionnée au regard de l'intérêt légitime poursuivi, à savoir, la lutte contre l'apologie du terrorisme.
Toutefois, l'article 15 de la CEDH autorise dérogation aux obligations de cette convention dans une situation d'état d'urgence, excepté pour les principes non dérogeables, dont ne fait pas partie l'article 10 de la CEDH. Mais un prolongement durable de l'état d'urgence posera nécessairement une difficulté relative à sa compatibilité avec l'article 15 de la CEDH. A moins, (ce que le gouvernement envisage) d'établir un socle juridique solide de l'état d'urgence, au sein de la constitution. En conséquence, de lege lata, la conformité de ce nouveau dispositif semble loin d'être évidente au regard d'un certain nombre de droits fondamentaux garantis.
Somme toute, est-ce qu'« à force de sacrifier l'essentiel pour l'urgence, on finit par oublier l'urgence de l'essentiel » ? (Edgar Morin)

Réagissez à cet article

Source : *Utilité et conformité des mesures de blocage de sites Internet faisant l'apologie du terrorisme dans le cadre de l'état d'urgence. Par Dan Scemama.*

Faut-il avoir peur des cyberdjihadistes ?

Faut-il avoir peur des cyberdjihadistes ?

Des pirates informatiques se présentant comme des hackers de Daesh multiplient les actions sur le Web. Les spécialistes tirent la sonnette d'alarme.

Depuis l'attaque du site internet de la chaîne de télévision TV5 Monde, en avril dernier, la France a essuyé des dizaines d'attaques informatiques émanant de prétendus cyberbataillons de l'organisation État islamique. Mardi matin, au cours d'une visite au QG d'interception des services de renseignements britannique à Cheltenham, George Osborne, chancelier de l'Échiquier (l'équivalent de notre ministère de l'Économie) du Royaume-Uni, a déclaré redouter des attentats numériques d'ampleur de la part de Daesh. « Ce mouvement terroriste utilise déjà Internet pour ses hideux objectifs de propagande, pour la radicalisation, pour la gestion de ses opérations », a déclaré George Osborne.

« Ils n'ont pas encore pu l'utiliser pour tuer, en s'en prenant à notre infrastructure. Mais nous savons qu'ils souhaitent le faire et font tout leur possible pour y parvenir », a-t-il ajouté.

Après l'intrusion en octobre dernier d'un hacker pro-palestinien dans la boîte mail de plusieurs officiels américains, à commencer par le directeur de la CIA, la menace d'attaques numériques est prise très au sérieux par les spécialistes de cybersécurité. « Cette réalité est considérée avec gravité depuis plusieurs années en Israël.

L'Europe commence à s'en préoccuper », confie Guy-Philippe Goldstein, l'un de ces consultants qui intervient au sein de l'Institute for National Security Studies (INSS), un think tank basé à Tel-Aviv. « Le niveau d'expertise des hackers djihadistes ne leur a permis jusque-là que de perturber temporairement le fonctionnement de sites officiels, mais on sait qu'ils peuvent sous-traiter certaines missions en recourant à des savoir-faire disponibles sur le dark web [la partie du réseau qui n'est accessible que par les pirates informatiques, NDLR] », poursuit Guy-Philippe Goldstein. Combien d'hommes comptent les cyberbataillons djihadistes ? La question reste en suspens, mais agite nombre de conversations dans les travées du Milipol, le salon professionnel dédié à la sécurité intérieure des États, qui s'est ouvert la semaine dernière à Villepinte. Quel que soit leur nombre, les membres de l'équipe qui s'est autoproclamée Cybercalifat réalisent des intrusions de plus en plus profondes dans nos systèmes de défense. La plus sérieuse a eu lieu en décembre dernier aux États-Unis. À cette occasion, des données confidentielles concernant des officiers supérieurs de l'armée américaine ont été subtilisées, qui ont ensuite été postées sur le compte Twitter de plusieurs sympathisants du groupe État islamique. Une menace prise au sérieux « En marge de ces opérations de déstabilisation psychologique que constituent la prise de contrôle et la dégradation de sites d'administration, et en dehors du coût que ces dégâts engendrent, d'autres interventions sont à craindre », indique Solange Ghernaouti, professeur à l'université de Lausanne, sollicitée par l'état-major suisse pour des missions de conseil. Cette enseignante en informatique, diplômée de l'université Paris-VI et ancienne auditrice de l'Institut de hautes études en défense nationale (IHEDN), a elle-même vu le site de l'équipe de recherche qu'elle dirige être attaqué en mars dernier. « Il m'a fallu trois jours pour tout remettre en état », indique-t-elle. En affirmant que les autorités britanniques surveillent attentivement 450 sites internet de « services sensibles » (énergie, distribution et traitement de l'eau, défense) susceptibles d'être visés par des interventions de pirates informatiques de Daesh, George Osborne accrédite l'idée que ces hackers auraient atteint une capacité de nuisance inquiétante. « Probablement liée au rapprochement qu'ont effectué les terroristes avec le monde très fermé de la cybercriminalité », estiment conjointement Guy-Philippe Goldstein et Solange Ghernaouti.

Réagissez à cet article

Source : http://www.lepoint.fr/high-tech-internet/faut-il-avoir-peur-des-cyberdjihadistes-17-11-2015-1982367_47.php

Attentats à Paris : les Anonymous promettent une riposte « massive »

Attentats à Paris : les Anonymous promettent une riposte « massive »

Comme après les attentats de Charlie Hebdo en janvier dernier, le collectif Anonymous promet de se venger sur le Web.

Sur une vidéo, un internaute qui se réclame de la nébuleuse de hackers promet une riposte « massive » suite aux attentats qui ont ensanglanté la capitale ce vendredi.

« Ces attentats ne peuvent pas rester impunis. C'est pourquoi les Anonymous du monde entier vont vous traquer. Oui, vous les vermines qui tuent les pauvres innocents, nous allons vous traquer, comme nous avons pu le faire depuis les attentats de 'Charlie Hebdo'. », déclare ce « représentant », caché derrière le fameux masque de V pour Vendetta.

« Attendez-vous donc à une réaction massive d'Anonymous. Sachez que nous vous trouverons et que nous ne lâcherons rien. Nous allons lancer l'opération la plus importante jamais réalisée contre vous, attendez-vous à de très nombreuses cyberattaques. La guerre est déclenchée, préparez-vous. Le peuple français est plus fort que tout et se relèvera de cette atrocité encore plus fort, sachez-le. », peut-on encore entendre.

On se souviendra que les Anonymous ont transmis à Twitter 9.200 comptes liés au groupe Etat islamique et ont lancé l'opération OpCharlieHebdo visant à faire tomber des sites proches de la mouvance islamiste. Des actions qui ont parfois été critiquées par certains observateurs, le risque étant de rendre encore plus discrète la présence en ligne de ces terroristes.

Rappelons que la loi antiterroriste récemment adoptée en France pénalise l'apologie du terrorisme sur Internet et permet un blocage administratif des sites concernés.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

http://www.zdnet.fr/actualites/attentats-a-paris-les-anonymous-promettent-une-riposte-massive-39828172.htm

---

Les armées dans le monde ont de plus en plus recours aux

cyberattaques | Le Net Expert Informatique

Les armées dans le monde ont de plus en plus recours aux cyberattaques

Les armées utilisent de plus en plus l'arme informatique de manière offensive, pour déstabiliser l'adversaire, et non plus seulement de manière défensive pour parer à des cyberattaques, a déclaré jeudi le ministre français de la Défense Jean-Yves Le Drian.

« La cyber n'est plus seulement un enjeu défensif (…) Pour nos forces armées, le premier enjeu est désormais d'intégrer le combat numérique et de le combiner avec les autres formes de combat », a expliqué M. Le Drian à l'ouverture d'un colloque consacré à la cyberdéfense à Paris.

« La lutte informatique offensive n'est pas un tabou (…) Les effets opérationnels de la cyber peuvent largement se comparer à ceux de certaines armes conventionnelles », a-t-il ajouté devant la presse.

L'arme informatique peut ainsi neutraliser des « dispositifs très fortifiés », a-t-il dit, rappelant l'exemple du virus STUXNET qui avait perturbé le fonctionnement de sites nucléaires iraniens.

Elle peut aussi offrir un « appui tactique » aux combattants, par exemple « perturber les défenses antiaériennes en leurrant ou en neutralisant des systèmes radars », a expliqué le ministre.

« La France dispose de capacités offensives. Elles sont encore limitées, mais la voie est tracée pour leur développement », a souligné Jean-Yves Le Drian.

Le ministre français et son homologue britannique, Michael Fallon, présent au colloque, ont souhaité une intensification de la coopération internationale et des échanges d'informations face à la recrudescence des cyberattaques, y compris dans le secteur militaire.

« Nous sommes victimes de cyberattaques que nous contenons au mieux mais elles croissent en ampleur et en sophistication et nos armées-mêmes le vivent sur les théâtres d'opérations », a souligné Jean-Yves Le Drian.

Il a cité l'exemple d'une cyberattaque dont l'armée française a été la cible en Afghanistan et « qui a temporairement perturbé les liens » entre ses drones et l'état-major à Paris. « Nos équipes ont très vite réagi » et l'attaque a pu être contrecarrée, a-t-il assuré, sans plus de précisions.

« Il y a 100 ans, nous étions ensemble sur le front de la Grande Guerre. Aujourd'hui nous sommes ensemble en première ligne d'une guerre virtuelle », a souligné M. Fallon.

« La menace cyber est tout sauf théorique. Nos adversaires, que ce soit Daech (acronyme du groupe Etat islamique) ou une Russie revancharde, sont de plus en plus déterminés à utiliser le cyber pour forcer leur avantage », a-t-il dit, citant les cyberattaques contre la chaîne de télévision française TV5Monde ou l'Estonie.

Les responsables de la cyberdéfense dans les pays participant au colloque, la France, les Etats-Unis, la Grande-Bretagne, l'Espagne et les Pays-Bas notamment, ont décidé de constituer un « forum » informel qui se réunira tous les six mois pour des échanges sur ces questions, a annoncé l'amiral Arnaud Coustillière, officier général cyberdéfense auprès de l'état-major français.

« Nous sommes tous à la tête de chaînes récentes », a-t-il expliqué, la plus ancienne, le Cyber Command américain, datant de 2009 et la française, qu'il commande, de 2011.

En France, « nous disposons de capacités offensives et défensives et notre travail aujourd'hui est de les intégrer pleinement aux capacités militaires », a-t-il ajouté.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
https://www.45enord.ca/2015/09/les-armees-dans-le-monde-ont-de-plus-en-plus-recours-aux-cyberattaques/

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.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

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

	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

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

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