Image not found or type unknown

Cyberguerre, cyberattaques et cybersurveillance : le monde 2.0

publié le **18/01/2015**, vu **2760 fois**, Auteur : Dalila MADJID Avocat

Nietzsche disait que : "la réalité, est mon système neuronal". Nous pouvons le transposer au monde virtuel ou au cybermonde, qui est devenu le système neuronal de tout internaute. Au 21e siècle, "le cybermonde est bien réel". Comme le relève justement certains, il prend la densité du réel. Il est, en effet, aussi réel que le monde réel. Internet était utilisé principalement comme un ins

Nietzsche disait que : "*la réalité, est mon système neuronal".*

Nous pouvons le transposer au monde virtuel ou au cybermonde, qui est devenu le système neuronal de tout internaute.

Au 21e siècle, "*le cybermonde est bien réel*". Comme le relève justement certains, il prend la densité du réel. Il est, en effet, aussi réel que le monde réel.

Internet était utilisé principalement comme un instrument de partage de connaissance. Il en est devenu une arme géopolitique par ses frontières translucides.

Ces derniers temps, le cybermonde est menacé. La cyberguerre est déclarée.

1- Les menaces du cybermonde : la cyberguerre, les cyberattaques

Selon le Robert, est une cyberguerre :"*une agression électronique contre les systèmes informatiques perpétrée dans le but de les utiliser comme moyen de propagande et de désinformation ou de paralyser les activités vitales d'un pays".*

Les affrontements ont trouvé un nouveau terrain sur le web. On est passé d'une guerre terrestre, physique, à une guerre virtuelle, sournoise, ayant comme armes, l'utilisation de logiciels malveillants programmés pour récolter des informations ou ralentir des systèmes.

Ces nouveaux moyens de déstabilisation de l'ennemi trouvent plusieurs exemples dans l'actualité.

Fin de l'année 2014, la panne de 9 heures sur l'internet nord Coréen ainsi que la nouvelle interruption subie par le réseau nord Coréen qui a duré 5 heures. Un porte-parole non identifié du gouvernement nord Coréen aurait accusé les Etats-Unis d'être à l'origine des attaques internet.

Les studios Sony, ont fait l'objet d'une attaque informatique massive, que le FBI aurait attribué après enquête à la Corée du Nord. Pyongyang qui s'était déclaré hostile à la sortie du film " *l'interview qui tue*", comédie sur un complot fictif de la CIA pour assassiner le leader nord-Coréen Kim Jong-Un a nié être à l'origine de l'attaque.

Mais encore, le web et les réseaux sociaux sont devenus les supports d'une forme de terrorisme,

avec les attaques de cyber-djihadistes. Ces terroristes maîtrisent ces nouveaux codes et outils de communications, en utilisant une propagande 2.0.

Ainsi, des centaines de sites d'institutions françaises ont été piratés depuis l'attentat contre Charlie Hebdo par des hackers se revendiquant comme terroristes.

Comme l'a précisé l'agence nationale de la sécurité des systèmes d'information (ANSSI), la très grande majorité de ces attaques sont, des "défigurations" des sites internet, appelées aussi "défacement", ou des dénis de service (*denial of service*, DDOS), "qui explorent les failles de sécurité des sites vulnérables".

Selon l'ANSSI:

- la défiguration d'un site est :"*le résultat d'une activité malveillante visant à modifier l'apparence ou le contenu d'un serveur internet. Cette action malveillante est souvent porteuse d'un message politique et d'une revendication".*

- les denis de service est :"*une action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. Dans le cas d'un site internet, celui-ci devient inaccessible à la consultation".*

L'ANSSI rappelle qu'il est possible de se prémunir de ces types d'attaques:

- 1/ en utilisant des mots de passe robustes

-2/ les modifications ou l'ajout de contenu sur les sites internet et réseaux sociaux, doivent être effectués exclusivement depuis un poste informatique maîtrisé par le service informatique de l'internaute lui-même. Il ne doit pas être effectué à distance depuis le domicile, une tablette ou un smartphone. Et la connexion doit être réalisée uniquement à partir d'un réseau maîtrisé et de confiance.

-3/ avoir un système d'exploitation et des logiciels à jour: navigateur, antivirus, bureautique, etc.

-4/ Et enfin, réaliser une surveillance du compte et des publications.

Il y a lieu de rappeler que l'ANSSI, créée par le décret n°2009-834 du 7 juillet 2009, est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Elle a pour principales missions d'assurer la sécurité des systèmes d'information de l'Etat, entre autres.

Par ailleurs, les cyberattaques touchent également les entreprises.

En effet, les hackers cyberattaquent les PME. Ces dernières sont, par exemple, victimes de racket, de vol de brevet.

Certaines entreprises françaises sont extrêmement vulnérables à la cybersurveillance et certaines sous-estiment le danger du cyberespionnage.

A l'heure actuelle, il n'existe pas de loi qui protège le patrimoine intellectuel des entreprises, notamment contre le vol de brevet.

Et décider de supprimer internet pour se prémunir du cyberespionnage, ne peut nullement être une solution pour ces entreprises.

Les particuliers, les internautes sont, eux aussi, victimes de cyberattaques, qui passent soit par la naïveté de l'utilisateur ou d'une mauvaise manipulation. Par exemple, le téléchargement d'une

Copyright © 2025 Légavox.fr - Tous droits réservés

application malveillante sur un smartphone, qui pourrait surveiller le contenu d'un SMS ou accéder aux données personnelles.

2- Les solutions contre les menaces du cybermonde : la cybersurveillance

- Dans le cadre de la lutte contre le terrorisme, les enquêtes dans l'environnement numérique

Au-delà de la géolocalisation, la cyber-surveillance tend à se généraliser.

- Le décret n°2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion des internautes, texte publié au journal officiel du 26 décembre 2014 et qui est entré en vigueur le 1er janvier 2015, a pour objet l'application de l'article 20 de la loi de programmation militaire (LPM) du 18 décembre 2013.

Ainsi, l'article 20 précise dorénavant le cadre juridique de la procédure d'accès des services de renseignement aux données de connexion circulant sur internet.

La CNIL évalue à 30 000 le nombre de demandes annuelles de communication de données formulées par les services de renseignement, demandes qui n'avaient pas de fondement juridique.

Ce décret dresse la liste des services dont les agents habilités peuvent demander à accéder aux données et détermine les données pouvant être recueillies.

Il prévoit aussi les conditions de désignation de la personnalité qualifiée placée auprès du premier ministre à laquelle sont soumises les demandes d'accès.

Le décret précise enfin les modalités de présentation des demandes d'accès et de conservation de ces demandes.

En outre, pour lutter contre les sites internet faisant l'apologie du terrorisme, l'autorité administrative peut demander à l'éditeur ou l'hébergeur d'en retirer le contenu.

En effet, la loi du 13 novembre 2014 n°2014-1353, publiée au journal officiel le 14 novembre 2014, renforce la répression de l’apologie du terrorisme et de la provocation à des actes de terrorisme. Il permet le blocage administratif et le référencement de sites internet faisant l’apologie du terrorisme ou y provoquant.

La loi prévoit que les délits de provocation à la commission d’actes terroristes et d’apologie du terrorisme soient désormais inclus dans le Code pénal et assimilés à des délits terroristes pour étendre les moyens d’enquête.

"Le Sénat a estimé que seuls les délits d’apologie du terrorisme et de provocation au terrorisme commis sur internet devaient être assimilés à des délits terroristes et figurer dans le Code pénal, le régime spécial de la loi de 1881 devant continuer à s’appliquer à la commission des mêmes infractions sur les supports de presse traditionnels".

En effet, il est inséré un article 421-2-5 du Code pénal ainsi rédigé :

" *Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.*
« Les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne (...). "

La loi étend également à l’apologie du terrorisme des exigences imposées aux fournisseurs

Copyright © 2025 Légavox.fr - Tous droits réservés

d’accès à internet (FAI), déjà astreints par la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 qui réprime déjà les contenus faisant l'objet d'apologie de crimes contre l'humanité, des crimes de guerre, d'incitation à la haine raciale ou de pédopornographie.

Les enquêteurs, s'adaptant aux nouvelles techniques de stockage,
pourront dorénavant perquisitionner les "clouds". Ils auront également le droit d’intercepter les discussions sur les logiciels d’appels téléphoniques sur Internet.

- Par ailleurs, et autre solution, par un arrêté, la direction générale de la sécurité intérieure (DGSI) est autorisée à consulter les signalements de contenus illégaux.

En effet, un arrêté du 4 novembre 2014, publié le 28 décembre 2014, permet à la DGSI ayant pour mission la lutte anti-terroriste, d'accéder à la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS).

Cet arrêté modifie ainsi l'arrêté du 16 juin 2009 portant création du système PHAROS à travers lequel les opérateurs et internautes peuvent prévenir les autorités des infractions en ligne.

3- La difficile question de l'atteinte à la vie privée et aux libertés

Certains soulèvent le contour flou des dispositions du décret qui a pour objet l'application de l'article 20 de la loi de programmation militaire, qui a des répercussions sur la vie civile, notamment de l'accès par les autorités administratives sans décision judiciaire aux données de connexion des internautes.

Etant plus conscients des atteintes portées à leur vie privée, certains parlent de "*big brother à la française*".

Un avis consultatif, rendu par la commission nationale de l'informatique et des libertés (CNIL) le 4 décembre 2014, a été publié en même temps que le décret du 24 décembre 2014 qui a créé un chapitre intitulé:"accès administratif aux données de connexion".

Suite à l'avis de la CNIL du 4 décembre 2014, le texte final restreint aux simples données de connexion (identité de la personne, date et heure de connexion...) les informations qui pourront être collectées.

Le texte de loi qui mentionnait "des informations et documents" faisait craindre un élargissement de la collecte à tous les documents concernant les internautes au détriment de la vie privée et des libertés.

La CNIL a obligé le gouvernement à définir cette formulation et à la restreindre au cadre de loi existant.

Elle met en garde le gouvernement sur les risques du texte pour la vie privée et la protection des données personnelles et appelle à une adaptation des régimes sur la conservation des données.

Toutefois, au nom de la lutte contre le terrorisme et suite aux derniers événements, les atteintes portées à la vie privée sont considérées comme acceptables.

Dalila MADJID- Avocat au Barreau de Paris

Blog: https://dalilamadjid.blog

Copyright © 2025 Légavox.fr - Tous droits réservés