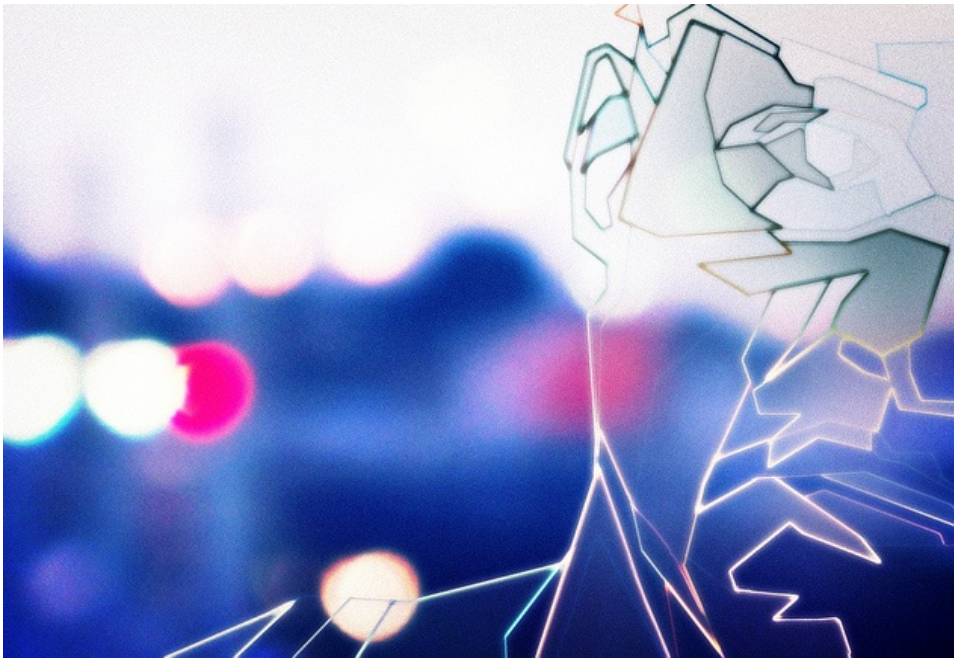
BIG (BUSINESS) BROTHER

LE 25 JUIN 2012 ***THOMAS DESZPOT***

Depuis quelques mois, le gouvernement britannique tente de renforcer la sécurité du Net. Pour connaître le véritable coût de la cyberdélinquance, il a fait appel à un groupe de chercheurs qui rendent leurs conclusions dans un rapport. Beaucoup d'argent et de mesures sont déployés, mais pas toujours à bon escient.



Bien décidé à renforcer le contrôle d'Internet, le gouvernement britannique souhaite s'attaquer à la cyberdélinquance. Problème, son coût est difficile à évaluer, et les quelques études sur le sujet laissent perplexes face aux résultats. La **dernière en date**, réalisée par le cabinet ***Detica***, l'estimait à environ 33,5 milliards d'euros par an. Ce coût se répartit comme suit : 3,75 milliards pour les particuliers, autant pour l'État, et 26 milliards pour les entreprises.

Pour y voir plus clair, le ministère de la Défense à mandaté le professeur **Ross Anderson**, expert en sécurité informatique, assisté de sept autres spécialistes universitaires. Ils avaient pour mission de chiffrer le coût réel des délits commis sur le net, un travail dont ils ont présenté les résultats sous forme d'un rapport d'une trentaine de pages.

Dans le **billet** publié pour annoncer cette étude, Anderson entend *"démystifier"* la cyberdélinquance. Concernant les fraudes traditionnelles par exemple, les experts soulignent que des fraudes "traditionnelles" -comme le resquillage aux impôts ou aux aides sociales- s'effectuent de plus en plus par le biais de l'informatique. Il s'agit là de sommes considérables, mais les dépenses consenties pour s'en prémunir reste raisonnables pour les citoyens.

Lorsqu'il concerne les autres types de fraude en ligne, le bilan s'inverse. Avec le phishing, le spam ou les malwares, spécifiques à Internet, le coût direct est relativement faible. Bien inférieur en tout cas aux dépenses indirectes et de défense. Celles-ci incluent la sécurisation des réseaux et des ordinateurs, à grand renfort d'antivirus et de mesures de prévention des risques. Le chercheur regrette les investissements massifs dans ces dispositifs onéreux, menés en parallèle des politiques de surveillance de la population. Son conseil : donner à la police les moyens de s'attaquer directement aux délinquants qui sévissent sur le Net.

Riposte

Ce rapport intervient alors qu'outre-Manche, un projet de loi pour surveiller Internet est à l'étude. Ce que **soulignait** *Owni* début avril :

> ***L'idée est de mettre en pratique le rêve de toute agence de renseignement qui se respecte : un dispositif de surveillance généralisée et permanente de l'ensemble des communications électroniques et téléphoniques d'une population.***

Cette initiative s'inscrit dans la continuité des politiques menées par nos voisins britanniques. En 2011, un **plan d'investissement** pour la cybersécurité a été lancé. Ce sont 810 millions d'euros qui sont alloués jusqu'en 2015, avec l'objectif afficher de *"protéger et promouvoir le Royaume-Uni au sein du monde numérique."* Cette somme a été divisée comme suit :

Selon les chercheurs, cette répartition s'avère peu judicieuse. Favoriser le **Government Communications Headquarters** (GCHQ), l'une des trois agences de renseignement britannique au détriment de la police ne devrait permettre aucune avancée significative dans la lutte contre la cyberdélinquance.

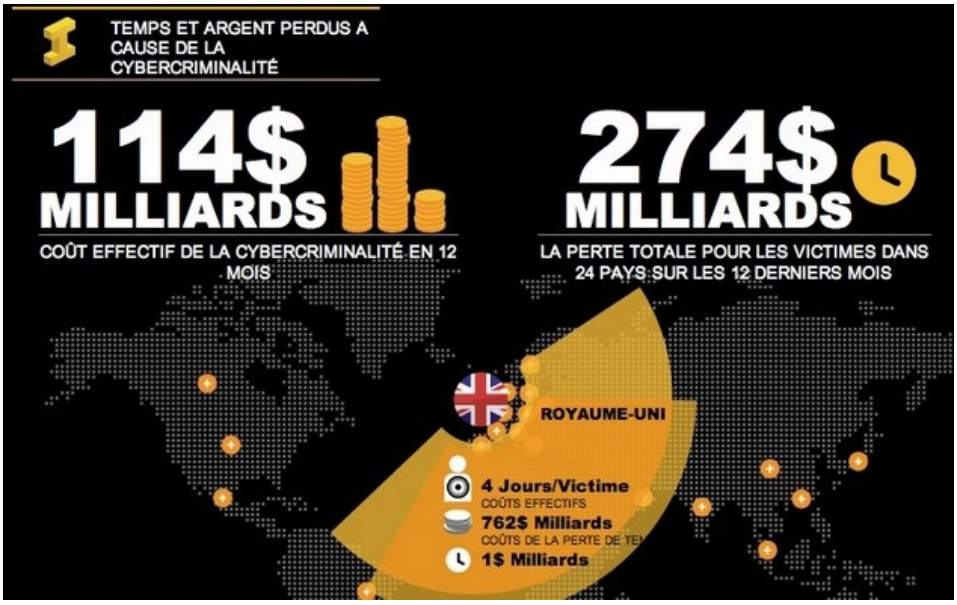
> ***Le nombre de pirates informatiques, de sites de phishing ou de malwares est sans cesse surévalué. Cela conduit certains services de police à croire que le problème est trop vaste et diffus pour s'y attaquer. En fait, seules quelques bandes sont à l'origine de la majorité des incidents. Une réponse de la police serait bien plus efficace que d'inciter le public à s'équiper de barres d'outils anti-phishing ou de logiciels antivirus.***

Une riposte plus ciblée, voilà la solution avancée par le groupe d'universitaires. De l'autre côté de l'Atlantique par exemple, le gouvernement américain a pris des résolutions drastiques. En faisant pression sur les organismes bancaires, il avait **fait interdire** les dons d'argent à WikiLeaks.

Pour conclure son billet de présentation, Anderson privilégie une action à la source et préconise d'éviter la surenchère dans les dispositifs de prévention.

> ***Plutôt que d'augmenter le budget du GCHQ alloué à la cybersécurité, le gouvernement devrait améliorer les moyens de lutte et d'expertise de la police face à la cyberdélinquence. Cela doit aussi s'accompagner mesures plus strictes pour la protection des internautes.***

Ce constat ne fait bien sûr pas les affaires des éditeurs de logiciels spécialisés dans la sécurité. D'ordinaire, les **données** concernant la cyberdélinquance sont communiquées par les entreprises privées du secteur, à l'instar de Symantec, qui édite l'antivirus Norton. Comme on peut le constater sur la capture d'écran ci-dessous, les chiffres avancés semblent démesurés, pour ne pas dire fantaisistes.



Contradiction

Le renforcement de la sécurité sur Internet est un véritable enjeu pour nos voisins anglais, comme le rappelle l'équipe de chercheurs :

> ***Le Royaume-Uni se place au second rang des pays qui enregistrent le plus de pertes causées par le phishing et le pharming*** **(attaque via les serveurs DNS NDLR)*. Il est aussi le plus touché par les fraudes à la carte bancaire, qui touche 5% des internautes britanniques.***

Au regard de ces chiffres, la lutte contre la cyberdélinquance a de beaux jours devant elle. Quand déjouer les actions menées par de petits groupes de pirates semble envisageables, réguler les agissements des états paraît bien plus hypothétique.

Internet est désormais utilisé dans le cadre de certains conflits. Pour freiner la course vers l'énergie atomique entamée par l'Iran, les États-Unis n'ont par exemple pas hésité à **s'en prendre** aux systèmes informatiques chargés de la gestion des programmes d'enrichissement d'uranium.

Barack Obama poursuit en ce sens la politique menée par son prédécesseur Georges W. Bush, ce qui n'est pas sans inquiéter outre-Atlantique. La directrice executive du *Bulletin of the Atomic Scientists* faisait part il y a peu de **ses craintes**. Kennette Benedict redoute que les armes informatiques deviennent les armes nucléaires du 21e siècle.

> ***Nous avons pris conscience peu à peu du danger que pouvaient faire peser les armes nucléaires sur nos sociétés et notre civilisation, mais nous n'avons pas encore compris comment des cyberguerres pourraient détruire notre mode de vie. Nous savons pourtant que les É tats-Unis ont beaucoup à perdre de ces attaques. A bien y regarder, ils sont hautement dépendants de l'information et des technologies de communications, et ce, dans tous les secteurs de la société. C'est pourquoi nous avons besoin d'engager un vaste débat public sur cette nouvelle classe d'armes.***

A mesure qu'il lutteront face à la cyberdélinquance, les gouvernements devront prendre des précautions. De victime à coupable, il n'y a parfois qu'un clic.

Illustration par **Surian Soosay [CC-by]**

FRANCK
le 25 juin 2012 - 22:02 • SIGNALER UN ABUS - PERMALINK

J'ai repéré une erreur dans votre article:
"Le préjudice du resquillage aux impôts ou aux aides sociales -qui s'effectue de plus en plus par le biais de l'informatique- est en effet bien supérieur aux frais de défense pour s'en prémunir." Il faut lire bien inférieur non ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

THOMASDESZPOT
le 25 juin 2012 - 23:27 • SIGNALER UN ABUS - PERMALINK

Effectivement, la fatigue pousse à quelques erreurs. Merci pour le signalement, j'éditerai ce para demain matin /-)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

1 ping

Semaine #26 – News | Grokuik le 2 novembre 2012 - 0:25

[...] une sorte de billard à 3 bandes dont nous sommes les dindons de la farce comme le démontre très bien OWNI surtout quand on balance des chiffres qui font [...]