LA CYBERGUERRE SANS Y TOUCHER

LE 19 JANVIER 2011 ***OLIVIER TESQUET***

Deux chercheurs britanniques publient une étude détaillée sur la réalité de la cyberguerre, pour le compte de l'OCDE. Leurs conclusions? "Fortement improbable".

> ***Très peu d'événements en lien avec le cyberespace disposent d'une réelle capacité à causer un choc global.***

C'est le **constat sans appel** que dressent deux chercheurs britanniques dans un rapport de 120 pages (**PDF**) commandé par l'OCDE (Organisation de coopération et de développement économiques). Comme le rappelle **avec sagacité** le New York Times, on recense aujourd'hui pas moins de 270 ouvrages sur *"la cyberguerre"*, formule consacrée. Avant d'éplucher les quintaux de pages que représente cet imposant corpus, il était plus que temps de fourbir les armes théoriques pour comprendre – et dédramatiser – le **"jour d'après"** que nous promettent certains experts.

En renversant la boîte de pétri des laborantins de la cyberfin du monde, Peter Sommer, professeur à la **London School of Economics**, et Ian Brown, de l'**Oxford Internet Institute**, vont-ils également renverser la hype, remplaçant les mines affolées par une moue dubitative? La tâche s'annonce ardue: sur les douze derniers mois, le même New York Times **a parlé 90 fois** de cyberguerre en utilisant le mot *"cyberwar"*, (**101** pour le Washington Post, et **240** pour le Wall Street Journal – même caché derrière un paywall).

Et les articles ne sont pas les seuls à se multiplier comme des petits pains. Aujourd'hui, les États-Unis disposent d'un **Cyber Command** et d'un *"cybertsar"* à la Maison-Blanche, **Howard Schmidt**; le Royaume-Uni possède un **Office for Cyber Security and Information Assurance**; l'Union européenne a l'**ENISA**, son agence dédiée mais **esseulée**; l'Estonie a hérité d'un **Cooperative Cyber Defence Centre of Excellence** après les **incidents de 2007**; l'OTAN réfléchit à son propre quartier général (que voudrait récupérer la Corée du Sud); et on ne compte plus les **CERT**, ces centres d'urgence chargés de répondre aussi vite que possible aux tentatives d'intrusion dans les systèmes d'information.

Le but de la commande de l'OCDE est clair: *"Dans quelle mesure des dangers numériques peuvent-ils être aussi destructeurs que des pandémies mondiales ou la crise bancaire?"* Pourtant, derrière ses atours prospectifs, l'étude britannique s'appuie sur des structures et des protocoles préexistants. Aussi ses deux auteurs identifient-ils les deux points cruciaux qui régentent l'analyse en vogue. D'un côté, la création du **World Wide Web** au début des années 90, qui a sensiblement modifié les usages en les fluidifiant. De l'autre, le tournant des années 2000, quand une bonne part (50%, avancent les chercheurs) du PIB des États occidentaux s'est mis à reposer sur les NTIC. Loin des **préceptes de la nouvelle économie**, ce second élément vise surtout à démontrer la porosité des systèmes gouvernementaux, qui prêtent de facto le flanc aux cyberattaques.

Harder, Better, Faster, Stronger?

"Il y a cette espèce de compétition entre les auteurs, pour dire 'mon histoire est plus effrayante que la tienne'", **regrette** Peter Sommer. Avec son acolyte Brown, il préfère questionner la notion de persistance. Est-ce que les risques pointés par certains auteurs tels que le très médiatisé **Richard Clarke**, ancien conseiller à la sécurité de trois présidents américains successifs, sont vraiment des chausse-trappes dans lesquels nous sommes susceptibles de tomber à tout moment? Et pour y répondre, rien de mieux qu'un peu de dialectique issue de ce bon vieux Clausewitz, inventeur de la notion de *"friction"* et géniteur de la fameuse citation *"la guerre n'est que la continuation de la politique par d'autres moyens"* :

> ***La plupart des cyberattaques seront ciblées et courtes dans le temps [...] Finalement, comme dans toutes les guerres, vous devez penser à la finalité: comme les analystes thermonucléaires pendant la Guerre froide, vous devez vous demander, que restera-t-il?***

Plutôt que de répondre à cette épineuse question, les deux chercheurs dégonflent l'hystérie ambiante en énonçant une lapalissade qui arrache un sourire:

> ***A une échelle moindre, si vous voulez que votre ennemi capitule – comment pourra-t-il le faire si vous avez coupé tous ses moyens de communication et son système de décision?***

Le retour de Stuxnet

L'étude soulève un deuxième point, encore plus complexe et lourd de conséquences: celui de l'attribution. Il y a quelques jours, en prenant sa retraite, l'ancien chef du Mossad Meir Dagan a relancé le débat sur **Stuxnet**, en suggérant très fortement qu'il s'agissait d'une **arme de conception israélienne**, développée avec l'aide des États-Unis et de certains pays européens dont l'Allemagne. *"L'Iran ne sera pas en mesure d'avoir l'arme nucléaire avant 2015"*, se félicitait-il. Dans la foulée, le New York Times **y allait de son affirmation**, en titrant *"le ver Stuxnet utilisé contre l'Iran a été testé en Israël"* . Étayé, cet article n'en reste pas moins déclaratif, comme les allégations israéliennes. D'ailleurs, selon certains spécialistes, le régime des mollahs pourrait *"fabriquer une bombe d'ici trois mois"* .

Dans ces circonstances, la cyberguerre ressemble moins à une menace armée qu'à une forme moderne de soft power, un outil utilisé dans les administrations et les états-major pour influencer les rapports de force. Meir Dagan est par exemple un opposant notoire à une attaque militaire contre l'Iran. En annonçant fièrement le terrain (supposément) gagné grâce à Stuxnet, il peut servir la position qu'il défend.

Il existe aussi une raison technique à cette difficulté d'identification et d'attribution. *"Les revendications d'attaques, par des groupes affiliés aux gouvernement chinois ou russe par exemple, peuvent être contrées en rappelant que leurs ordinateurs peuvent avoir été infiltrés par des tiers, ou qu'il s'agit de l'initiative de hackers patriotiques isolés"*, peut-on lire dans l'étude. Aux yeux de ses auteurs, *"l'attaque Stuxnet, qui visait apparemment les installations nucléaires iraniennes, pointent autant les difficultés que le futur"*.

Cinétique contre numérique

Mais l'identité de celui qui appuie sur le bouton n'est qu'une conséquence. Comme l'écrivent les chercheurs anglais, *"L'un des avantages des armes cybernétiques sur les armes conventionnelles, c'est qu'il est beaucoup plus facile de créer une ambiguïté autour de l'individu qui lance l'attaque*". Pour Sommer et Brown, il faut étudier la cyberguerre à l'aune de son aïeule sans préfixe, pour déterminer sa portée:

> ***Pour définir un acte de cyberguerre, il faut montrer qu'il était équivalent à une attaque hostile conventionnelle, dans son intensité, sa durée, son contexte [...] La première considération que nous devrions avoir, c'est la raison pour laquelle un État ou une entité voudrait partir en guerre. Dès lors que l'hostilité existe, il y a fort à parier que les pays ne se limitent pas à des armes conventionnelles. Les armes cybernétiques ne sont qu'un moyen additionnel de mener ces assauts.***

Pour l'heure, de telles armes sont encore mal maîtrisées, comme l'attestent les **dommages collatéraux** du ver Stuxnet, encore lui. C'est peut-être la raison pour laquelle, en guise de conclusion, les deux experts considèrent une *"cyberguerre pure"* comme *"improbable"*. Dans un autre cas de figure, celui populaire des **attaques par déni de service** (DDoS), elles ne sont qu'une munition supplémentaire, sûrement pas le canon de l'arme. La faute à leur faible intensité et leur courte durée de vie. Et si finalement, la fameuse cyberguerre d'après-demain, celle qui mettra les pays à genoux, résidait dans ce déséquilibre? Avant d'imaginer les **bombes informatiques**, regardons d'abord exploser quelques petits pétards.

—

Crédits photo: Flickr CC ***obeyken***, ***superfem***, ***fixedgear***

DFITZ
le 20 janvier 2011 - 13:35 • SIGNALER UN ABUS - PERMALINK

Une remarque que je crois importante, le raccourci de requête Google pour connaître le nombre de pages appartenant à un même domaine et indexées par Google comme contenant tel mot clef est site: et non in:.

Ce qui, si je ne me trompe pas, change tout, puisque le cyberwar pour le WSJ donne 240 pages, 101 pour Washington post et que lemonde.fr contient 127 pages avec le mot clef "cyberguerre".

Je ne connais pas le raccourci in: mais de toute évidence il renvoie beaucoup de pages qui ne sont pas du domaine visé.

cordialement

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OLIVIER TESQUET
le 20 janvier 2011 - 15:24 • SIGNALER UN ABUS - PERMALINK

Bonjour Dfitz,

Vous avez raison, la requête "in:" renvoie vers les contenus hébergés sur les sites en question, mais également à toutes leurs citations ailleurs sur le web. J'amende.

Cordialement
OT

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DFITZ
le 20 janvier 2011 - 16:00 • SIGNALER UN ABUS - PERMALINK

digital journalism, indeed… Ces outils ne sont pas toujours aussi évident à maîtriser qu'il n'y paraît.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI REPONDRE

1 ping

tuxnux le 29 janvier 2011 - 13:52

[...] La cyberguerre sans y toucher [...]