DE LA CYBERGUERRE À LA SURVEILLANCE

LE 3 JANVIER 2011 ***PHILIPPE QUÉAU***

Tandis que la suspicion autour d'un espionnage industriel basé sur le hacking s'accentue, Philippe Quéau pointe l'enjeu plus vaste de cette cyberguerre: celui d'une nouvelle société de la surveillance.

Le mois dernier, **Richard A. Clarke,** "tsar du contre-terrorisme" et conseiller à la Maison Blanche pour les trois derniers présidents, déclarait que le projet d'avion de combat F-35 Lightning II **avait été l'objet de cyber-attaques**. Le paragraphe le plus intéressant de son interview est le suivant:

> ***Les Etats-Unis et plusieurs de ses alliés travaillent à la construction d'un nouvel avion de chasse de cinquième génération, le F-35 Lightning II, un bijou de technologie. Il y a de bonnes raisons de croire qu'un gouvernement étranger, probablement la Chine, a piraté les serveurs de l'entreprise qui le fabrique pour télécharger l'intégralité des plans. Ainsi, un ennemi potentiel connaît donc les forces et les faiblesses d'un appareil qui n'a pas encore volé.***

> ***Mais venons-en au chapitre le plus effrayant: s'ils se sont introduits dans le système, croyez-vous qu'ils ont seulement copié des informations? Ou pensez-vous qu'ils aient pu implémenter un virus dans le programme? Imaginez un futur dans lequel un F-35 américain est opérationnel au combat, dans lequel une autre nation met en service un chasseur beaucoup moins efficace, mais qui pourrait envoyer un signal révélant une faille dans le programme du F-35 et causant son crash. Les avions d'aujourd'hui, qu'il s'agisse du F-35 ou du Boeing 787, reposent sur l'informatique. L'appareil n'est qu'un gros ordinateur dont la plupart des actions sont commandées par l'électronique.***

Ce qui est intéressant ici, c'est l'admission qu'il est possible pour des groupes de cyberguerre de s'insérer dans les projets militaires les plus secrets et les plus sensibles. L'une des raisons structurelles de cet état de fait tient entre autre en ce que les composants électroniques de toutes sortes de matériels sont développés dans une vingtaine de pays. Et les logiciels correspondants à ces composants sont développés par des programmeurs répartis dans le monde entier. A l'évidence, il est impossible d'assurer une sécurité numérique dans ce type d'environnement. Selon Clarke, *"il est tellement facile d'intégrer une trappe dans 50 millions de lignes de code. Il est tellement facile d'avoir un élément microscopique sur une carte mère qui permette à quelqu'un de rentrer sans autorisation"*.

Société du contrôle numérique

Partant de ce constat simple et de bon sens, je cherche seulement à en tirer quelques possibles implications, non pas seulement pour telle ou telle industrie sensible, mais surtout pour l'ensemble de la société. Ma prédiction est que les prolégomènes de la cyberguerre

révèlent une extrême fragilité intrinsèque de l'ensemble de l'info-structure, fragilité dont **Stuxnet** ou l'attaque du début 2010 sur les comptes gmail de Google n'est qu'un simple avertissement.

Je prévois que la cyberguerre, qui a déjà commencé ses premières escarmouches sous des formes relativement modérées, ou bien alors visant des types d'adversaires très ciblés, va en fait essaimer sous des formes incontrôlables, avec sans doute deux conséquences principales:

- Un **durcissement impitoyable** des politiques de sécurisation de la Toile, par le biais législatif, technique et policier, affectant l'ensemble de la population ("transparence" accrue, info-totalitarisme).
- Une diffusion générale des techniques de cyberguerre dans de très nombreux pays, mais aussi dans les mafias et, sans doute, dans certaines entreprises très "motivées".

Autrement dit, des lois comme **Hadopi**, **Loppsi**, ou des accords comme ACTA, ne sont que des préfigurations d'une société du contrôle numérique poussé jusqu'au moindre bit. Ces lois et accords sont d'ailleurs déjà complètement dépassés par la dangerosité intrinsèque des formes de cyberguerre qui se déploient sous nos yeux. Il faudra donc bientôt passer à des modèles législatifs beaucoup plus inquisiteurs, et beaucoup plus destructeurs des libertés. Officiellement, il s'agira de lutter contre le cyber-terrorisme, avec sans doute comme élément déclencheur un futur virus de type Stuxnet provoquant une catastrophe impactant l'opinion publique et la réduisant au silence des agneaux.

Face à un tel pronostic, que faire?

D'abord le travail de longue haleine: éducation approfondie de tous, sensibilisation permanente aux dangers non seulement personnels mais structurels de l'info-sphère. Ensuite, il faut renforcer le développement prioritaire du "libre et de l'ouvert", avec auto-contrôle accru par les pairs. Adapter le droit de la propriété intellectuelle pour permettre l'examen par des autorités indépendantes (Une organisation mondiale du numérique?) des designs de tous les composants de la chaine numérique. Il faudra se résoudre à arbitrer entre la notion de secret industriel et celle de protection de la sécurité numérique globale.

Enfin, il y a le volet politique et démocratique. *In fine*, c'est là que réside le nœud du problème.
Il y a du pain sur la planche, et du bois à scier dans la grange.

Ce billet a initialement été publié sur Metaxu, le blog de Philippe Quéau

—

Crédits photo: Flickr CC ***laverrue***, ***fotdmike***

LATEO
le 3 janvier 2011 - 17:26 • SIGNALER UN ABUS - PERMALINK

Je ne vois pas le lien qui fait aboutir l'auteur à la société du flicage numérique.

AMHA, tout ce que l'expérience apprend c'est que « oh, surprise, il serait peut-être bon de revoir notre politique de sécurité et de former nos agents à la SSI ».

Si c'était ironique, au temps pour moi, effectivement le monde politique pourrait formuler le problème avec ce type d'éléments de langage.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PKP

le 4 janvier 2011 - 1:13 • SIGNALER UN ABUS - PERMALINK

Je me méfie de l'optimisme excessif qui va souvent de pair avec la fascination pour la technologie, mais pour le coup, j'aurais tendance à être d'accord avec J. Gilmore : "The Net interprets censorship as damage and routes around it" (Le Net interprète la censure comme un dégât et se reconstruit autour d'elle). Deux raisons à cela :
- Toutes les tentatives de filtrage du Net jusqu'à présent (à l'exception toute relative de la Chine, qui n'a pas l'inconvénient d'être une démocratie) ont lamentablement échouées (Australie, Royaume-Uni notamment).
- Les précédentes alertes à la censure d'Internet en France (Hadopi, DADVSI, etc) se sont révélées être des pétards mouillés, créés pour l'effet d'annonce et inapplicables techniquement.

L'exemple chinois est intéressant, d'ailleurs. On voit bien que même avec une censure "machine" d'un niveau technique probablement excellent, doublée d'une véritable armée de délateurs et autres "hackers-patriotes", le régime est totalement incapable de stopper complètement la diffusion de l'information. On dirait bien qu'il est réellement impossible de censurer complètement Internet.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MICHAËL

le 4 janvier 2011 - 9:26 • SIGNALER UN ABUS - PERMALINK

@pKp : sans doute est-il impossible de totalement censurer le Net mais il est tout à fait possible de le censurer suffisamment pour neutraliser une info gênante (qui a besoin d'une certaine diffusion et exposition pour avoir un impact)… On peut dresser un parallèle avec la stratégie de l'HADOPI : ils savent parfaitement que le système est contournable mais, ce qu'ils visent, c'est les 90% de madame Michu et de petits tipiaks.

Ensuite, comme l'avait souligné Bluetouff, les technologies de censure évoluent à une vitesse considérable (il faut dire qu'il y a pas mal d'acheteurs potentiels, ça motive la R&D…), au point qu'il est déjà possible, aujourd'hui, de mettre tout un pays sous deep packet inspection pour un coût réaliste (à l'échelle d'un Etat)

Et n'oublions pas que les systèmes de censure chinois et iraniens fonctionnent avec du matériel européen… (Nokia-Siemens, Alcatel-Lucent, etc.)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE