LE CODE FAIT LA GUERRE

LE 3 JUIN 2011 ***OLIVIER TESQUET***

Déconcertés par la puissance de feu d'Internet, plusieurs Etats affinent leur doctrine militaire pour l'adapter au champ numérique. Une nouvelle forme de contrôle de la gouvernance?

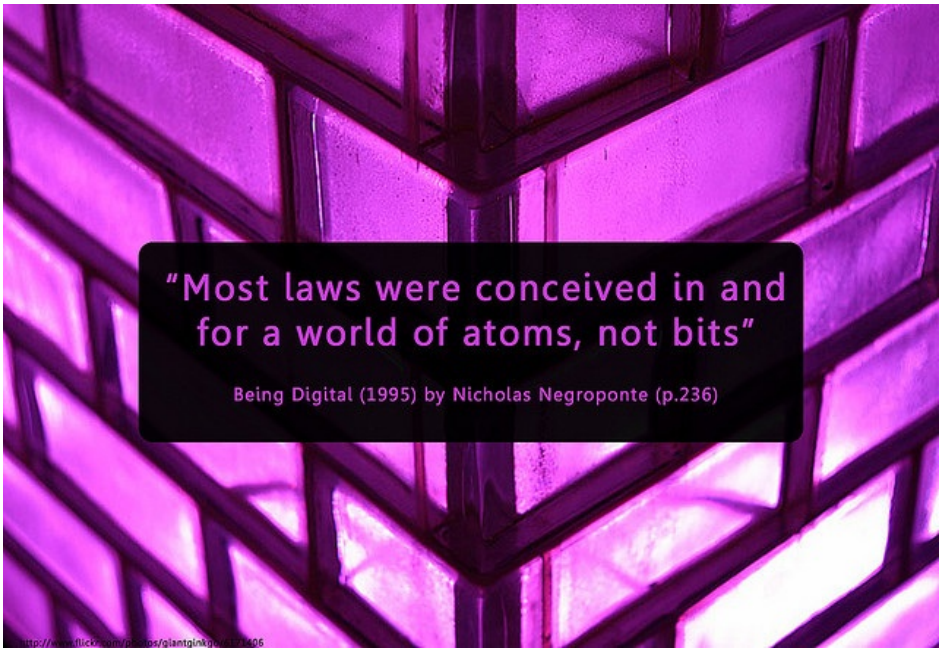
Le Pentagone s'apprête à publier un document à l'en-tête duquel devrait figurer cette recommandation: désormais, les attaques informatiques pourront être considérées comme **"des actes de guerre"**. Quinze jours après avoir annoncé leur **nouvelle stratégie** en matière de cybersécurité par le biais d'Howard Schmidt, le "cyber tsar" de la Maison-Blanche, les Etats-Unis s'apprêtent ainsi à briser un tabou ultime. Le *Wall Street Journal* , qui a révélé l'information, cite d'ailleurs les propos d'un officiel, dénués d'ambiguïté:

> ***Si vous éteignez notre réseau électrique, nous nous réservons le droit d'envoyer un missile sur l'une de vos cheminées.***

Dix ans après *Code is Law* ("le code fait loi", **traduit ici par Framasoft**) de Lawrence Lessig, formulons une nouvelle hypothèse: et si le code faisait la guerre? En 2000, sur le campus d'Harvard, l'éminent professeur de droit planche sur un article universitaire qui fera date chez les penseurs d'Internet. En définissant le code informatique comme nouvelle architecture de nos sociétés démocratiques, il interpelle tout un chacun sur la nature éminemment modifiable de cette norme.

> ***Ce code, ou cette architecture, définit la manière dont nous vivons le cyberespace. Il détermine s'il est facile ou non de protéger sa vie privée, ou de censurer la parole. Il détermine si l'accès à l'information est global ou sectorisé. Il a un impact sur qui peut voir quoi, ou sur ce qui est surveillé. Lorsqu'on commence à comprendre la nature de ce code, on se rend compte que, d'une myriade de manières, le code du cyberespace régule.***

Pris au dépourvu par les **attaques DDoS des Anonymous**, traumatisés par le mystérieux **virus Stuxnet**, exposés à un risque toujours plus important **d'espionnage industriel**, les pays du G8 – les premiers concernés – sont à la recherche d'un cadre légal (un code) aujourd'hui inexistant. A tel point que Lord Jopling, le rapporteur général de l'OTAN, a commencé à rédiger **un rapport** sur cette nouvelle guerre de l'information, qui brasse WikiLeaks, hacktivisme et coopération internationale. Soumis à la lecture, ce document pourrait être approuvé avant la fin de l'année.



Nouvelle doctrine

Ce coup de grisou en accompagne bien d'autres. En moins d'un mois, plusieurs puissances mondiales sont sorties du bois. La Chine a reconnu l'existence d'une **cellule de guerre électronique**, tandis que le Royaume-Uni a annoncé son intention de se doter d'un **arsenal offensif** pour défendre ses infrastructures critiques. C'est un secret de Polichinelle, certains gouvernements se sont déjà livrés à des attaques qui n'étaient pas des ripostes pour sauvegarder leurs intérêts. En septembre 2007, lors de l'opération Orchard, Israël n'a pas hésité à **court-circuiter les défenses aériennes syriennes** pour mener un raid contre la centrale nucléaire d'Al-Kibar.

Dans le monde militaire "ouvert", la cyberguerre n'était jusqu'à présent qu'un levier à crédits actionné par les acteurs du complexe militaro-industriel américain. Des poids lourds comme **Raytheon**, **Northtrop Grumman** ou **Lockheed Martin**, directement affectés par l'arrêt programmé de la production de certains appareils comme **le chasseur F-22**, ont tous développé une gamme de conseil technologique, jusqu'à en tapisser les couloirs du métro de Washington D.C.

Désormais, non seulement d'autres pays placent leurs pions sur l'échiquier, mais c'est un véritable changement de doctrine qui se dessine à l'horizon. Dans une tribune pour le *Guardian*, Lord John Reid, ancien secrétaire à la Défense de Tony Blair, appelle de ses voeux **une véritable révolution**, en insistant sur le fait que les structures d'aujourd'hui ne sont pas suffisamment résilientes pour absorber les chocs du réseau:

> ***Il y a toujours un certain degré de continuité dans le changement, même radical. Mais la nature du cyberespace signifie que nos vieilles doctrines de défense ne marcheront pas. Tant que nous n'aurons pas reconnu ça, nous risquons de succomber à une dangereuse cyber-complaisance.***

Sur qui tire-t-on?

De la bulle économique, la "cyberguerre" est en train de glisser vers la gouvernance, un ajustement politique qui n'est pas sans risque. Derek E. Bambauer, de la Brooklyn Law School, **s'est récemment penché** sur les défis posés aux Etats par la cybersécurité, qu'il considère comme une "énigme" (*conundrum* en anglais). A ses yeux, les recommandations de l'administration Obama – fondées sur l'identification de l'agresseur pourraient *"mettre en péril l'architecture générative d'Internet mais aussi des engagements clés par rapport à la liberté d'expression".*

Bambauer touche ici un point critique: les attaques informatiques ne disent presque jamais leur nom. Leurs commanditaires choisissent cette méthode précisément parce qu'elle offre le triple confort de la rapidité, de la volatilité et de l'anonymat. Dès lors, selon la rhétorique américaine, à qui déclarer la guerre? Au botnet russe par lequel a transité le virus? Au serveur chinois identifié par le **Cyber Command**?

Le G8 s'intéresse depuis de nombreuses années à ces questions. Elles ont longtemps été traitées – de façon très confidentielle – au sein du **Groupe de Lyon** (après le G8 de Lyon de 1996) consacré aux échanges informels sur la grande criminalité organisée. À l'intérieur du Groupe de Lyon, un Sous-groupe lié aux risques technologiques s'était créé en réunissant notamment le **SGDSN** (France), le **GCHQ** (UK) la **NSA** (US) où en réalité les uns et les autres discutaient beaucoup de façon informelle des armes de la cyberguerre et de leurs "partenariats" avec les industriels et les réseaux de logiciels libres afin d'harmoniser ces moyens, pour qu'un jour ils répondent aux impératifs normatifs de l'OTAN.

Le Pentagone prépare depuis près de 8 ans ces évolutions. En 2002, le US Space Command a été intégré au US Strategic Command car, précisément, le Space Command, en raison de son importance sur la gestion de la guerre de l'information avait vocation à devenir un centre de décision stratégique.

En France, lors du **piratage de Bercy** – qui constitue difficilement un *casus belli* - le patron de l'Agence nationale de sécurité des systèmes d'information (**ANSSI**), Patrick Pailloux a lourdement insisté sur la difficulté de l'attribution des attaques. Dès lors, on imagine mal un Etat s'affranchir des conventions de Genève pour riposter de manière conventionnelle et aveugle à un hacker dont il ignore tout. Dans la dialectique de Lessig, le code est une loi, il ne s'en affranchit pas.

Crédits photo: Flickr CC ***zanaca***, ***:ray***, ***Will Lion***

ELOINA DIAZ
le 4 juin 2011 - 9:33 • SIGNALER UN ABUS - PERMALINK

a serious problem already here, In Mexico Sony got hacked today! June 4, 2011

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

22DECEMBRE
le 4 juin 2011 - 17:44 • SIGNALER UN ABUS - PERMALINK

Chaque étape de l'évolution humain ajoute un degré dans la guerre :
nous avions l'épée.
Puis nous avons ajouté vaisseaux de guerre et avions. Et c'est avec ces armes que nous avons gagné nos dernières guerres. Pourtant nous avons gardé les fantassins, parce que l'avion ne permet pas de protéger le coeur du pays (industries, tribunaux, casernes…).

Bientôt, ce sera le tour de l'avion d'être obsolète, puisque la guerre se jouera sur le réseau ! Et pourtant nous garderons toujours les fantassins et les avions, puisqu'eux seuls permettent de protéger les infrastructures ! Ce serait dommage de perdre la guerre sous prétexte qu'un missile a détruit un nœud du réseau…

De même des révolutions : aujourd'hui, elles se jouent sur les réseaux, sur internet, plus seulement dans la rue. Et bientôt, les hackers eux-aussi rentreront dans la danse pour promouvoir leurs valeurs (partage et liberté…)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LEPIGEON
le 15 mai 2012 - 8:38 • SIGNALER UN ABUS - PERMALINK

Une fois de plus les mathématiciens et tous les spécialistes en cybernétique sont en première ligne pour donner les moyens à l'utilisateur lambda les moyens de ne pas être (trop) le dindon de la farce. qu'ils le veuillent ou non, ils ont sur les épaules la redoutable charge d'empêcher que des systèmes robotisés, contrôlés par une minorité, n'établissent une surveillance systématique et opaque sur les sociétés civiles qui seraient ainsi pilotées par des minorités politiques non élus; le lobbying n'en est-il pas déjà le paradigme ?
Nulle doute que la "cybercriminalité" et la "défense militaires" offrent le prétexte idéal pour justifier la mise en place d'un monde soumis à la surveillance automatiques et systématiques par des robots sans état d'âme et par conséquent prompt à "liquider" ce que son programme lui indique comme étant un obstacle au système qui le dirige.

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

2 pings

#FrenchRevolution #WorldRevolution La fin du monde, "made in China" par Owni.fr : #FrenchRevolution le 5 août 2011 - 1:39

[...] guerre des codes" était sur le point d'éclater (une terminologie que nous utilisions déjà début juin, avec une lecture sensiblement [...]

Les Etats-Unis s'autorisent les cyberattaques » revue du web, Just another weblog le 12 janvier 2012 - 14:15

[...] les actions offensives, les États-Unis viennent de franchir un nouveau cap dans la cyberguerre. Plusieurs États avaient déjà annoncé leur intention de se doter de forces offensives et plusieurs opérations ont déjà [...]