Pour Nicolas Arpagian, la France doit multiplier les initiatives pour attirer des experts de haut niveau si elle veut défendre ses intérêts souverains.

NICOLAS ARPAGIAN

Sur le Net, la cyberguerre est déjà déclarée

Conflits virtuels mais dégâts réels : l'espace numérique est devenu le nouveau terrain d'affrontement des entreprises comme des Etats.

Propos recueillis par **Bernard Poulet**

AU-DELÀ DES DOUX RÊVES de démocratie universelle que propagent les nouveaux apôtres d'Internet – Twitter, Facebook... –, l'espace cybernétique ouvre sur une autre dimension : celle de vraies guerres dans les mondes virtuels. Et ce n'est plus de la science-fiction, ni une déclinaison de jeux vidéo, comme l'explique Nicolas Arpagian, qui vient de publier *La Cyberguerre* (Vuibert).

Vous dites que la guerre numérique a commencé. Qu'appelle-t-on la « cyberguerre » ?

Dans la définition classique, le terme « guerre » désigne les conflits où s'affrontent, de manière souvent directe, des armées régulières. Aujourd'hui, le cyberespace constitue un terrain d'affrontement au même titre que l'air, l'eau, la terre et l'espace. La cyberguerre repose sur deux piliers. D'une part, les tuyaux informatiques, qui peuvent être espionnés, maîtrisés ou neutralisés à distance par un ennemi. D'autre part, les informations, qui sont présentes et stockées sur le réseau informatique mondial ou dans les ordinateurs des Etats, des entreprises ou des particuliers, et qui peuvent être, toujours à distance, piratées, altérées ou détruites. Elle peut provoquer des morts, par exemple à la suite du sabotage de systèmes électriques ou nucléaires. Le FBI ne s'y est pas trompé quand il a indiqué officiellement, en janvier 2009, que la possibilité d'une « apocalypse cybernétique », ou « Cybergeddon », représentait l'une des principales menaces pour la sécurité des Etats-Unis. Les parties prenantes peuvent être des gouvernements, des sociétés ou même des individus isolés.

Les gouvernements et les populations en ont-ils vraiment conscience ?

La difficulté de la technologie est qu'elle reste pour l'essentiel l'apanage des techniciens. Or de plus en plus de particuliers sont des internautes. Ainsi, Monsieur Tout le Monde devient un acteur de ce cyberespace : son ordinateur peut être piraté ou mis à contribution pour mener des actions malveillantes après avoir été contaminé. A son insu, sa machine peut servir à diffuser un virus ou à détourner de l'argent qui, éventuellement, financera une activité terroriste. Le paradoxe d'Internet, c'est que les menaces sont multiples et en évolution constante, mais qu'il revient à chacun d'assurer sa propre sécurité, en achetant et en installant des logiciels. Il ne viendrait pourtant pas à l'idée de la plupart des gens qu'ils puissent être responsables de la pose et de la révision régulière des pare-chocs de leurs voitures. Et, avec Internet, on ignore fréquemment qu'on a fait l'objet d'une attaque.

Comment organiser l'éducation des populations ?

Pour la première fois, le savoir n'émane pas de la génération précédente. Il n'y a pas – ou peu – de transmission de la part d'anciens qui seraient en mesure d'indiquer les dangers aux plus jeunes, puisque bien souvent ils ne connaissent pas les subtilités de ces mondes numériques. Ce qui pose de vrais problèmes de management dans les structures pyramidales, en particulier les administrations et ➠

Pour le FBI, la possibilité d'une « apocalypse cybernétique » est l'une des principales menaces pour la sécurité des Etats-Unis.

JÉRÔME CHATIN

JÉRÔME CHATIN

NICOLAS ARPAGIAN
Le rédacteur en chef de la revue *Prospective stratégique* est aussi coordinateur des enseignements « Stratégies d'influence et lobbying » à l'Institut d'études et de recherche pour la sécurité des entreprises. Longtemps journaliste spécialisé dans les nouvelles technologies, il a publié avec Eric Delbecque *Pour une stratégie globale de sécurité nationale* (Dalloz).

les armées, où, traditionnellement, c'est le plus ancien dans le grade le plus élevé qui détient la connaissance. Dans le cybermonde, celui qui a l'expertise peut très bien se trouver en bas de la hiérarchie : le stagiaire ou la jeune recrue qui sait comment casser un code d'accès, ou comment propager efficacement une information sur les réseaux sociaux. Il faut savoir repérer cette compétence et l'intégrer à la stratégie de l'entreprise. C'est d'abord une affaire de management et de bonne gestion des talents, certainement pas une question 100 % technique.

Quel est le rôle de l'Etat ?

La France vient de créer une agence spécialisée dans la sécurité des systèmes d'information étatiques. Mais il va lui falloir faire preuve de créativité pour attirer et surtout pour fidéliser les spécialistes dont elle a besoin, afin que le passage par cette agence ne soit pas perçu comme un troisième cycle de luxe pour des informaticiens soucieux d'éclore dans le privé. Gare au turnover ! A priori, l'Etat n'est pas un employeur très sexy pour un jeune génie d'Internet à qui on propose un salaire calculé d'après la grille de la fonction publique. Ce cyberguerrier potentiel risque d'être attiré par de grandes entreprises qui le paieront mieux et lui accorderont des moyens matériels plus importants. Et s'il veut relever de beaux défis cybernétiques, il les trouvera en travaillant pour Areva, pour Total ou pour EDF, où il affrontera sur la Toile la fine fleur des activistes de la terre entière. Donc, quand il s'agit de défendre les intérêts souverains français, l'Etat doit relever un défi managérial. Sans doute faudra-t-il déplafonner les salaires et assurer des gestions de carrière durables.

Quelles situations de cyberguerre peut-on imaginer ?

Elles sont multiples. Cela va du simple raid informationnel, comme les campagnes de dénigrement de la France sur le Net avant les jeux Olympiques de Pékin, aux attaques informatiques qui ont cloué l'aviation géorgienne au sol lors du conflit avec la Russie, durant l'été 2008. La France n'est pas à l'abri. A la fin de l'année dernière, des dizaines d'ordinateurs du ministère de la Défense ont été victimes d'un « ver » baptisé Conficker, et les avions de l'aéronavale ont été menacés de se retrouver cloués au sol.

On peut également pirater les systèmes d'orientation des missiles ennemis afin de les amener à frapper un hôpital plutôt que la caserne visée, histoire de rallier à soi l'opinion publique internationale. Ou désorganiser les communications des services de secours après avoir commis un attentat, afin d'aggraver le bilan humain et de déstabiliser encore davantage les populations civiles. En fait, plus le pays attaqué sera numérisé, plus l'impact de ces assauts sera fort. L'Estonie, nation high-tech par excellence, a été gravement affectée par des vagues de cyberattaques – potentiellement russes – au printemps 2007. Il ne faut donc pas tomber dans une dépendance technologique trop grande. Or l'informatique est partout, en particulier quand il s'agit de réduire les coûts de fonctionnement de nombreux secteurs – transports, électricité, distribution d'eau, d'énergie, etc. C'est une source de grandes fragilités surtout quand ces échanges utilisent le banal réseau Internet. Il faudra réapprendre à fonctionner, en situation de crise, en dehors de ces systèmes sophistiqués, sans cette béquille technologique permanente.

Nicolas Sarkozy a fait savoir que la France s'autorise désormais à mener des opérations offensives de cyberguerre.

Qu'a-t-on fait en France ces dernières années ?

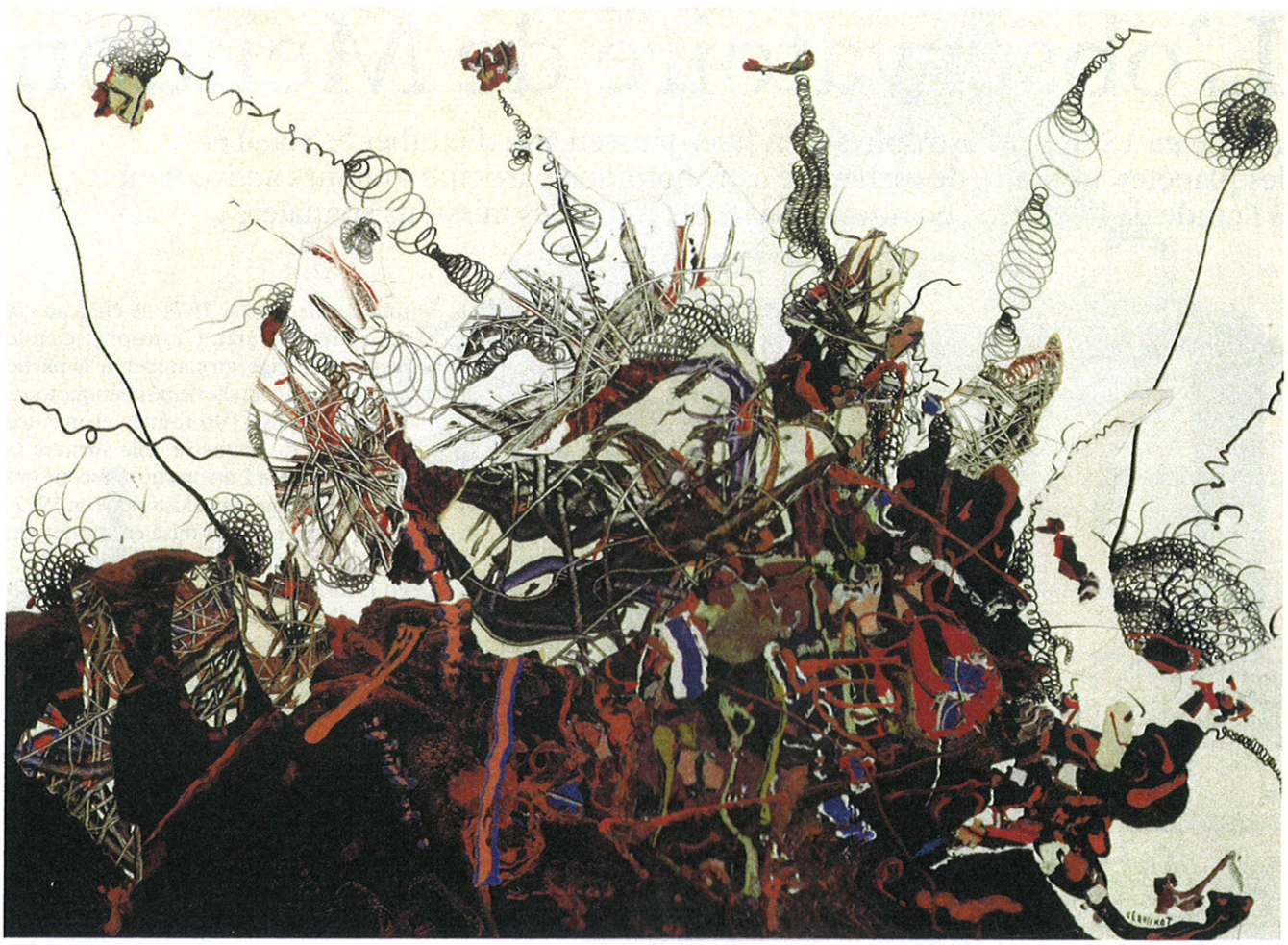
Avec le Livre blanc sur la défense et la sécurité nationale de juin 2008, Nicolas Sarkozy a parlé ouvertement du « risque d'attaques informatiques qui pourraient paralyser la nation », précisant même que la France et plusieurs pays européens en avaient été victimes récemment. Ce qui l'a conduit à annoncer une grande première : la France s'autorise désormais à mener des opérations offensives de cyberguerre. Et, avec la loi sur la sécurité intérieure, les services de police sont en mesure de procéder – sous le contrôle d'un juge – à « la captation de données numériques se trouvant dans un ordinateur ou transitant par lui ». En clair, d'y introduire des logiciels espions.

Quelle est la dimension économique de cette « guerre » ?

Les entreprises sont particulièrement visées, par leurs concurrents ou par des puissances étrangères. Ainsi, en 2008, selon les services de renseignements allemands, plus de 750 000 ordinateurs appartenant à des sociétés allemandes auraient été contaminés par des logiciels espions. Les Etats-Unis ont créé un concept très intéressant : les Bens *(Business Executives for National Security)*. En postulant chez les Bens, tout citoyen américain peut offrir ses services et partager ses connaissances pour contribuer à la sécurité des Etats-Unis. Ces experts bénévoles aident l'administration à définir les technologies stratégiques, par exemple.

Le Web 2.0 modifie-t-il les stratégies ?

Le principe de l'interactivité joue un rôle essentiel dans les guerres de l'information. Le Web 2.0 est un amplificateur considérable pour les acteurs de la



CNAC/MNAM/RMN

« Episode de la guerre des nerfs », Bernard Réquichot (1957). Selon Nicolas Arpagian, « le Web 2.0 est un amplificateur considérable pour les acteurs de la désinformation. Il est de plus en plus compliqué de savoir d'où viennent les messages et quel est leur degré de véracité. »

désinformation. Il est ainsi de plus en plus compliqué de savoir d'où viennent les messages et quel est leur degré de véracité. N'importe qui peut devenir audible sur la Toile s'il est assez habile. L'impact de la désinformation est de plus en plus fort quand diminue la consommation des médias « traditionnels », ceux qui doivent vérifier leurs informations et leurs sources. Quand un moteur de recherche est la porte d'entrée sur le Net, les guerres de l'information, à l'encontre d'un pays ou simplement d'une entreprise, deviennent dangereusement efficaces.

Dans le cadre des réseaux sociaux, de type Facebook ou Myspace, les internautes livrent tant d'informations personnelles, voire intimes, qu'il est aisé d'établir une cartographie des liens qui unissent des individus, avec leurs centres d'intérêt respectifs. Cela facilite l'élaboration de stratégies pour approcher ou influencer tel décideur ou tel cadre d'entreprise.

Les batailles idéologiques passent aussi par la censure, on le voit en Chine...

Bien sûr. En disant leur intention d'installer des logiciels espions dans tous les ordinateurs commercialisés à partir du 1er janvier 2010, au nom de la lutte contre la pornographie, les responsables chinois annoncent la couleur. C'est la première légitimation de logiciels de censure intégrés dès la fabrication des ordinateurs. Un contrôle initial des contenus qu'il suffira ensuite de paramétrer à bon escient... Dès 2006, le magazine étatsunien *Salon* racontait comment les censeurs de Pékin réunissaient chaque mois les représentants des principaux sites Internet (Google, Yahoo!, MSN...) pour leur faire connaître la liste des informations autorisées.

Quelle est l'attitude des Etats-Unis?

Barack Obama est un gros consommateur de technologies. Dès son accession à la présidence, il a commandé un audit sur la sécurité des systèmes d'information des Etats-Unis, qui a abouti à la création d'un poste de coordinateur de la cybersécurité à ses côtés juste avant l'été. Dans son discours du 29 mai dernier, il a clairement indiqué que les entreprises états-uniennes du secteur high-tech devront se mettre au service des intérêts de leur nation. On l'a vérifié lorsqu'il a demandé à Twitter de maintenir ses réseaux ouverts pendant les manifestations en Iran. Concernant la définition des domaines stratégiques, les Etats-Unis ont opté pour une règle simple : est stratégique tout ce que le président sera amené à considérer comme tel. La France a préféré établir une liste limitative, ce qui n'est peut-être pas la décision la plus pertinente dans le domaine des nouvelles technologies, car on ne sait pas toujours ce qui peut devenir stratégique demain.