



La "cyberguerre" : concept virtuel ou réalité?

Gras Gaëtan (st)

Mis en ligne le 22/10/2010

"Ce qui est certain, c'est que les nouvelles formes de conflictualité ne peuvent ignorer l'aspect cybernétique". L'utilisation de l'informatique dans les conflits armés est désormais une réalité. L'évolution des technologies a, en effet, abouti au concept de « cyberguerre ». Redéfinissant entièrement le champ de bataille réel, on peut déjà se demander s'il existe une escalade vers une prochaine « cyberguerre » dans le sens où on voit une course à l'armement électronique et numérique dans plusieurs Etats, comme l'Allemagne, les Etats-Unis et bien d'autres. Ce qui est certain, c'est que les nouvelles formes de conflictualité ne peuvent ignorer l'aspect cybernétique. Et que l'utilisation offensive des technologies de l'information va se développer. Soit avec des actions strictement numériques, soit en complément d'attaques physiques (attentats, engagements de troupes armées sur le terrain...). Nicolas Arpagian, rédacteur en chef de la revue « Prospective stratégique » et directeur scientifique du cycle « Sécurité Numérique » à l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ) à Paris, a accepté de nous éclairer quelque peu sur cette nouvelle forme d'attaques qui soulève déjà tant de questions.

1) Que recouvre exactement la désignation de « cyberguerre » ? Quelles sont les principales caractéristiques des « cyberattaques » ? Comment s'opèrent-elles ?

Le terme « cyberguerre » désigne les usages offensifs des technologies de l'information en général, et d'Internet en particulier. Ces attaques peuvent porter tant sur les réseaux informatiques, avec la capacité de les espionner, de les altérer, de les suspendre ou des les interrompre. Ou sur les informations numérisées. Qu'il s'agisse de données bancaires, personnelles, industrielles, étatiques ou militaires. Il va s'agir de capter, de modifier ou de supprimer de telles informations. Sans oublier de possibles campagnes de dénigrement ou de désinformation visant à cacher ou à diffuser des messages néfastes pour sa cible.

De telles attaques ne nécessitent pas forcément des moyens financiers importants. Mais bien une connaissance des failles ou faiblesses informatiques de son adversaire. Les assaillants peuvent être de natures juridiques variées (gouvernement, sociétés commerciales, lobbies, associations, militants, simples citoyens...) et de tailles disparates. Seule compte in fine la maîtrise de l'outil informatique. Parmi les autres particularités de ces cyberagressions, il faut noter que l'attaquant n'a pas toujours intérêt à faire savoir à sa victime qu'elle a été visitée. A l'inverse, pour marquer les esprits, certaines pénétrations cybernétiques gagnent à être très médiatisées. Il est souvent difficile en outre d'évaluer le préjudice subi. Et encore plus aléatoire de vouloir imputer avec certitude une responsabilité juridique à l'auteur de tels actes, s'il a pris des précautions élémentaires de discrétion technologique. Comme par exemple le fait de faire circuler ses commandes informatiques à travers plusieurs pays.

2) Quels avantages offrent une guerre cybernétique par rapport une « simple » guerre?

Les avantages sont les conséquences des particularismes évoqués précédemment. C'est en effet un « confort » pour l'attaquant que chacun soit persuadé qu'il était à la manœuvre mais que personne ne soit effectivement capable de le prouver. Il en tirera un mérite politique sans risquer de voir sa responsabilité engagée.

De telles cyberattaques peuvent, comme c'est par exemple le cas avec des escroqueries fondées sur la naïveté des internautes, devenir des sources de revenus conséquentes pour des organisations terroristes ou maffieuses (mafieuses). La faible coopération judiciaire internationale sur ces dossiers de cyberattaques offre de facto une certaine impunité à leurs auteurs. Pour lesquels il est possible de déminager des données compromettantes d'un serveur à l'autre, placé chacun sur deux continents différents, d'un simple clic de souris. Tandis que les règles juridiques imposeront des délais interminables aux enquêteurs chargés de les débusquer.



3) Quels nouveaux enjeux législatifs, techniques, économiques, politiques, moraux, ... peuvent être attribués à ce nouveau concept, à cette nouvelle réalité ?

Toutes les grandes organisations internationales (OTAN, Interpol, G7/G20, OCDE, Union européenne, Organisation des Nations Unies...) ont souhaité un moment ou à un autre s'approprier la thématique d'Internet et de sa sécurité. Mais dans les faits, le seul texte de dimension internationale reste une Convention du Conseil de l'Europe de novembre 2001. Et il n'existe pas à proprement parler de consensus politique, ni même économique avec le débat sur la Neutralité du Net qui pose la question de la hiérarchisation des contenus pour éventuellement organiser leur circulation sur la Toile, pour réguler le réseau. Les Etats ne tiennent finalement pas à renoncer à leur souveraineté sur le Net. Malgré l'idée de globalisation volontiers popularisée par l'avènement de l'ère de la société de l'information. Les Chinois, les Etats-Unis, les Russes... chacune des grandes puissances veut conserver ses prérogatives sur ces territoires numériques. Fait nouveau, des acteurs économiques participent désormais à cette géopolitique renouvelée. A l'instar d'un Google, qui malgré ses douze ans d'âge, fait quasiment jeu égal dans une négociation internationale avec un pays comme la Chine.

4) Comment les politiques de défense prennent en compte cette problématique ? Existe-t-il une coopération transnationale ? Quels moyens peuvent être mis en œuvre, nationalement et internationalement, pour se protéger d'une « cyberattaque » (ainsi que pour contre-attaquer) ?

Les Etats intègrent désormais systématiquement un volet cybernétique dans leur défense. La France a publié un Livre Blanc sur la Défense et la sécurité nationale en juin 2008 explicite à ce propos. Idem pour les Etats-Unis avec la Quadriennal Defense Review de février 2010 ou la National Security Strategy émise par la Grande-Bretagne en octobre 2010. Une des formes les plus abouties de coopération en matière de cyberattaque est certainement le point de contact 24/7 du G-20 qui permet aux Etats membres de s'avertir rapidement d'une agression informatique qui aurait frappé leurs infrastructures. Afin que les autres pays se préparent à leur tour. C'est basique mais au moins cela fonctionne. Hors cas spécifiques, la coopération internationale ne va guère au-delà.

5) Est-il possible d'harmoniser une législation mondiale concernant le problème ?

Lors de la dernière édition du Forum de Davos, le secrétaire général de l'Union Internationale des Télécommunications (UIT), l'agence des Nations-Unies en charge des télécoms avait plaidé pour un traité bannissant les cyberattaques. Il est à craindre que cela relève pour l'instant de l'utopie. Etant donné que de nombreux Etats semblent aujourd'hui davantage apprécier de disposer avec Internet d'une arme supplémentaire dans leurs arsenaux respectifs. Tant pour porter des coups aux systèmes économiques, administratifs ou militaires de leurs adversaires que pour agir en sous-main sans risque réel de voir leur responsabilité mise en cause. Encore plus que dans le monde physique stricto sensu les Etats ne jouent pas encore franc jeu en ce qui concerne les cyberattaques.