La cyberguerre n'aura pas lieu

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 octobre 2012

https://www.bortzmeyer.org/cyberguerre.html

Un concept est très à la mode depuis deux ou trois ans, celui de cyberguerre. Les consultants en sécurité le citent à tout bout de champ, les journalistes le mettent dans leurs titres (moi aussi, vous avez remarqué ?), les politiques le brandissent en classant le risque de cyberguerre dans « l'une des principales menaces auxquelles nous devons faire face ». Y a-t-il une réalité derrière ce concept ?

Il est facile d'ironiser sur cette soi-disant « cyberguerre » en faisant remarquer qu'elle ne fait pas de cybermorts et que personne n'a encore signé de traité de cyberpaix. Il est clair que la cyberguerre n'a pas les caractéristiques habituellement associées à la guerre. La guerre, ce n'est pas seulement la violence physique, directe et organisée, contre l'autre camp (à ce compte-là, criminels et patrons voyous pourraient être qualifiés de guerriers). La guerre, c'est surtout l'engagement massif de moyens, la mobilisation (pas forcément sous l'uniforme) de tas de gens dont ce n'était pas le métier. C'est le risque, en cas de défaite, de changements radicaux (et en général négatifs) dans la vie de millions de gens. On ne parle pas de guerre pour quelques coups de feu de temps en temps, sauf quand on est un politicien malhonnête cherchant à faire parler de lui à la télé en exagérant les problèmes.

Ainsi, l'exemple souvent cité de « première cyberguerre de l'Histoire », l'attaque russe contre l'Estonie ne peut être qualifiée de guerre que par des gens qui n'ont jamais vécu une vraie guerre ! Si la Russie avait envahi l'Estonie, il y aurait eu pour les Estoniens des conséquences autrement plus graves que celui de ne pas pouvoir retirer d'argent à la banque pendant quelques jours ! Le terme de cyberguerre est ici une insulte aux victimes des vraies guerres menées par le pouvoir russe, comme celles contre la Tchétchénie ou contre la Géorgie.

Et les actions ayant des conséquences physiques, comme Stuxnet ? Ce qui fait que Stuxnet ne mérite pas d'être appelé « cyberguerre », ce n'est pas seulement le fait qu'il n'y ait pas eu de morts. C'est surtout le fait que toute action hostile d'un État voyou contre un autre (ici, le sabotage des installations nucléaires iraniennes) n'est pas forcément une guerre ou alors le terme ne veut plus rien dire. À l'extrême rigueur, on pourrait parler de « cyberguérilla » ou de « cybersabotage ». Imaginons que les services secrets israéliens ou états-uniens aient procédé à un sabotage classique, avec dépôt et mise à feu d'explosifs. Parlerait-on de guerre ? Le résultat aurait pourtant été le même.

Et c'est encore plus net pour des opérations comme Duqu ou Flame, où il n'y avait pas d'action, juste de l'espionnage. Certes, l'exploitation de failles de sécurité de MS-Windows change des méthodes de Mata Hari mais c'est simplement le progrès technique. Et ce n'est pas la « cyberguerre » pour autant, ou alors les États sont en guerre en permanence ! (Puisqu'ils s'espionnent en permanence.)

Mais, alors, pourquoi tant de gens utilisent-ils ce terme erroné de « cyberguerre » ? Dans le numéro de novembre 2010 de la revue « Réalités industrielles », on trouve un article de Nicolas Arpagian avec cet aveu touchant : « on peut reconnaître néanmoins l'efficacité [pour toucher un large public] du mot cyberguerre ». Tout est dit : « cyberguerre » est simplement un moyen, pour les consultants, d'obtenir davantage de budget et de missions, pour les journalistes, d'avoir plus de lecteurs et pour les politiques, de faire voter ce qu'ils voudraient.

C'est ainsi que le documentaire « La guerre invisible <http://seenthis.net/messages/90692> » fait défiler une longue cohorte d'ex-généraux ou ex-ministres âgés, tous reconvertis dans la cyberpeur, et tous annonçant qu'on peut faire dérailler un train ou empoisonner l'eau via l'Internet. L'un des pires de ces cyberpaniqueurs, Richard Clarke, brandit pendant toute l'émission son livre, pour qu'on n'oublie pas de l'acheter. Il est clairement dans une démarche commerciale et pas dans une tentative de sensibiliser les citoyens à un problème réel.

Pourtant, le problème n'est pas imaginaire. Il y a aura certainement dans les guerres futures, du piratage de drones, des attaques informatiques pour couper les communications de l'ennemi, etc. Mais ce n'est pas de la « cyberguerre », c'est simplement l'utilisation de moyens « cyber » pour la guerre. Si on définit la cyberguerre comme « l'utilisation du cyberespace par des groupes militaires dans le cadre de conflits armés » (Julie Horn <http://juliehorn.ca/>), alors on n'a pas avancé dans la terminologie : la guerre utilise forcément les moyens techniques existants. On n'a pas parlé d'« airguerre » avec le développement des avions de combat, ou de « guerre chevaline » lorsque la cavalerie a fait ses débuts...

Est-ce un simple problème de terminologie erronée ? Non, car le terme de cyberguerre n'est pas innocent. Il ne sert pas seulement à justifier le business de quelques consultants incompétents et powerpointeurs. Il vise surtout à conditionner les esprits, à faire croire que nous sommes en guerre, et à habituer les citoyens aux habituelles restrictions, matérielles et surtout de libertés, qui sont la conséquence habituelle de la guerre. Comme le fait remarquer Peter Sommer, interrogé dans le rapport OCDE de janvier 2011 <http://www.bbc.co.uk/news/technology-12205169>, « "*We don't help ourselves using 'cyberwar' to describe espionage or hacktivist blockading or defacing of websites, as recently seen in reaction to WikiLeaks*" ». Non, en effet, cette confusion n'aide pas. Mais elle n'est pas due à la paresse intellectuelle ou au manque de sang-froid. Elle est délibérée, cherchant aussi à criminaliser toute opposition en mettant dans le même sac des opérations d'un État puissant et surarmé avec des actions plus ou moins efficaces de groupes informels. Le même Sommer ajoute à juste titre « "*Nor is it helpful to group trivially avoidable incidents like routine viruses and frauds with determined attempts to disrupt critical national infrastructure,*". Mais une telle réserve dans l'analyse ne lui vaudra certainement pas de passer à la télévision...

Quelques bonnes lectures sur ce sujet :

— L'article d'Olivier Tesquet « Les va-t-en-cyberguerre débarquent <http://owni.fr/2010/10/06/les-va-t-en-cyberguerre-debarquent/index.html> », assez confus mais qui a le mérite d'analyser les raisons économiques du marketing de la cyberguerre,
— Parmi les experts qui refusent le terme, Arnaud Garrigues explique que « La cyberguerre n'est pas car : pas de victime, une violence inexistante ou limitée, pas toujours des objectifs politiques etc etc.... <http://cidris-news.blogspot.ca/2010/12/petit-lexique-lusage-des-lecteurs.html> », et il fait un tour d'horizon des opinions sur ce terme <http://cidris-news.blogspot.ca/2010/07/cyber-quelque-chose-war-maybe.html>,
— Une très bonne analyse <http://securid.novaclic.com/cyber-securite-industrielle/cyberloup.html> de plusieurs cas médiatiques, les dégonflant sérieusement,

— Les déclarations de Bruce Schneier <http://www.bbc.co.uk/news/technology-12473809> contre l'exagération,
— Sur son blog, Félix Aimé fait un grand tour d'horizon, très raisonnable, du sujet dans « De la cyberguerre, présentation <http://blog.felix-aime.fr/securite-des-systemes-dinformation/cyberguerre-guerre-cybernetique/> »,
— Un bon article de John Horgan, « "*Don't Believe Scare Stories about Cyber War*" <http://www.scientificamerican.com/blog/post.cfm?id=dont-believe-scare-stories-about-cy-2011-06- remet ce terme de cyberguerre dans la longue liste des exagérations de la propagande militariste,
— L'expert en sécurité bien connu Marcus Ranum ne prend pas de gants pour dire clairement que « "*Cyberwar is Bullshit*" <http://conference.hitb.org/hitbsecconf2008kl/materials/KEYNOTE%202%20-%20Marcus%20Ranum%20-%20Cyberwar%20is%20Bullshit.pdf> » (et il argumente très bien),
— Je n'ai pas eu le temps de lire la thèse de Karin Kosina <http://kyrah.net/da/wargames.pdf> (thèse en politique internationale, pas en informatique ou en sécurité) sur la cyberguerre mais elle m'a été recommandée par des gens très bien,
— Un autre article qui explique en détail l'utilisation du terme de cyberguerre pour obtenir des budgets, dans la grande tradition du complexe militaro-industriel : « "*The Cybersecurity-Industrial Complex*" <http://reason.com/archives/2011/07/25/the-cybersecurity-industrial-c> »,
— Un article d'OWNI <http://owni.fr/2012/11/29/dans-cyberguerre-il-y-a-guerre/index.html> a exploré le concept de cyberguerre,
— Et, bien sûr, Jean-March Manach s'y est mis aussi avec « C'est la cyberguerrrrrrrrrre! <http://owni.fr/revue-du-web/cest-la-cyberguerrrrrrrrrre/> ».