***Internet : La Cyberguerre, concepts et rÃ©alitÃ©.***
**Internet**
PostÃ© par : JulieM
PubliÃ©e le : 19/2/2013 13:00:00

On parle de plus en plus de cyberguerre, mais que veut dire ce termeÂ rÃ©ellement? **Jarno LimnÃ©ll**, spÃ©cialiste des politiques de dÃ©fense chez Stonesoft, apporte des prÃ©cisions sur le sujet.

La Cyberguerre est une question tendance dans les fils d'actualitÃ©, et bien que le terme soit employÃ© Ã tort et Ã travers, le concept nâ□□est pas complÃ¨tement saisi. La Cyberguerre est une rÃ©alitÃ©, mais la rÃ©alitÃ© de la situation peut Ãªtre trÃ¨s diffÃ©rente de ce quâ□□on peut croire. Il faut admettre que, sans en Ãªtre pleinement conscients, nous vivons dÃ©jÃ dans une Ã¨re de Cyberguerre menÃ©e par les Ã©tats.

## La rÃ©alitÃ©

Il semblerait que les gouvernements prennent au sÃ©rieux les menaces potentielles, avec lâ□□Ã©laboration de programmes de cyber-guerre en cours chez au moins 12 des 15 puissances majeures. Ces programmes visent Ã Ã©valuer les tactiques et capacitÃ©s qui domineront dans une guerre future. Le taux dâ□□accusations au sujet des cyber-attaques est Ã©galement en augmentation dans le monde entier. L'Iran est devenu "une force avec laquelle il faut compter," a dÃ©clarÃ© le GÃ©nÃ©ral William Shelton du Â« US Air Force Â», division Espace, au cours de son discours en Janvier Ã Washington. Selon le site Allthingsd.com, l'Iran renforce ses capacitÃ©s de cyber-attaques suite Ã lâ□□action du logiciel malveillant Stuxnet, auquel on attribue l'explosion de plusieurs centrifugeuses nuclÃ©aires iraniennes.

## Les changements de stratÃ©gie

Tandis que le monde se dirige vers une plus grande utilisation stratÃ©gique des armes informatiques pour motiver les adversaires Ã  modifier leurs comportements, les cyber-opÃ©rations sont devenues une partie reconnue des combats stratÃ©giques. Il fallait dans les conflits passÃ©s des soldats physiquement et mentalement assez forts pour rÃ©ussir dans la bataille, mais ce nâ□□est plus le cas. La force physique ne rentre pas en ligne de compte dans la nouvelle race de soldats, qui doivent possÃ©der une connaissance approfondie de la sÃ©curitÃ© et les langages informatiques.

"*Les pirates sont maintenant soit des criminels motivÃ©s par le gain financier, soit des militants ou des gouvernements engagÃ©s dans lâ□□espionnage ou des cyber-attaques contre leurs propres citoyens ou d'autres gouvernements*,Â», explique **The Guardian.** Toutes les attaques malveillantes, cependant, ne tombent pas dans la catÃ©gorie de cyber-guerre, ce qui explique la paranoÃ¯a injustifiÃ©e et les idÃ©es fausses associÃ©es avec le terme.

## Les idÃ©es fallacieuses

Ce qui compte comme Â«cyber-guerreÂ» reste une question ouverte. Un malentendu courant est la notion que la cyber-guerre a lieu dans un domaine distinct, Ã  savoir le cinquiÃ¨me domaine, qui est totalement dissociÃ© de toutes les autres formes de guerre, quâ□□elles soient terrestres, maritimes, aÃ©riennes ou spatiales. Or, force est de constater que le Â«monde des octets" fait bel et bien partie de tous les autres domaines. Les combats qui se dÃ©roulent sur terre, sur mer, dans les airs ou dans l'espace ont leurs propres composantes Â« cyber Â», et le monde dit Â« des octets Â» est partout. Il intervient Ã  tous les niveaux et dimensions de la guerre, que ce soit en matiÃ¨re d'armement, de communication, dâ□□Ã©quipement ou d'autres questions liÃ©es au phÃ©nomÃ¨ne.

Toute crise future, mÃªme si elle n'est pas considÃ©rÃ©e comme une cyber-guerre en tant que telle, est susceptible de comporter un composant cyber. Il serait difficile de l'Ã©viter, en particulier dans les grandes guerres entre pays dÃ©veloppÃ©s. La dimension Cyber est la seule qui permet d'avoir un impact sur toutes les autres dimensions. Les cyber-composants peuvent faire dÃ©vier les sous-marins et les navires, entraver les fonctions de commande de vol et de prÃ©cision de largage, interfÃ©rer avec les satellites, couper la distribution d'Ã©lectricitÃ©, affecter les performances des Smartphones, des vÃ©hicules, des prisons, et engager une sÃ©rie de de manÅ□uvres supplÃ©mentaires pour dissuader ou dÃ©truire les ennemis.

## La dÃ©finition

Alors que Kaspersky limite sa dÃ©finition de la cyber-guerre Ã  l'activitÃ© qui utilise des cyber-armes pour provoquer des dommages physiques, Stuxnet est le seul outil qui rÃ©pond Ã  cette dÃ©finition Ã  ce jour. Les cyber-armes peuvent aussi Ãªtre dÃ©ployÃ©es pour perturber le commandement et le contrÃ´le sans destruction physique. Un pays appauvri par des relevÃ©s bancaires effacÃ©s, par exemple, serait victime d'une cyber-guerre mÃªme si aucun dommage physique nâ□□est constatÃ©. Cependant, une attaque qui se qualifie de cyber-guerre doit se produire dans le contexte politique et stratÃ©gique de la guerre.

Â«La guerre est donc un acte de force calculÃ© pour contraindre l'ennemi Ã  se plier Ã  notre volontÃ©Â», dit la cÃ©lÃ¨bre formule du stratÃ¨ge militaire prussien Carl von Clausewitz. Le GÃ©nÃ©ral Sun Tzu de Chine aspirait Ã  Â«maÃ®triser l'ennemi sans combat." Dans les deux cas la destruction physique nâ□□est pas obligatoire, bien que des buts politiques soient visÃ©s. La mÃªme notion sâ□□applique Ã  la cyber-guerre. L'instrument cyber peut avoir sa propre grammaire, mais sa logique est celle de la guerre dans son ensemble.

Le conflit en ligne sophistiquÃ© qui se dÃ©roule en Syrie, rapportÃ© par DefenseNews.com, fournit un excellent exemple de la cyber-guerre. Bien que les efforts Ã  la fois du cÃ´tÃ© du gouvernement syrien et du cÃ´tÃ© de ses adversaires entendent Â«saboter, perturber et

dÃ©truireÂ», tous nâ□□impliquent pas la destruction physique. Une des cyber-armes Ã©tait un cheval de Troie destructeur connu sous le nom de DarkComet. Le groupement autour des droits numÃ©riques, Electronic Frontier Foundation, lâ□□a dÃ©crit comme Â« un outil d'administration Ã distance qui permet Ã un attaquant de capturer l'activitÃ© dâ□□un Webcam, dÃ©sactiver le paramÃ¨tre de notification pour certains programmes antivirus, enregistrer les frappes clavier, voler les mots de passe - et envoyer des informations sensibles Ã une adresse IP de l'espace syrien ".

## Guerre vs paix

S'il est malheureusement clair que la Syrie est engagÃ©e dans une guerre civile, de nombreux autres pays sont plutÃ´t dans une zone grise ne valant ni un Ã©tat de guerre, ni un Ã©tat de paix. La cyber-rÃ©alitÃ© brouille davantage les frontiÃ¨res entre la guerre et la paix, ajoutant une dimension nouvelle et dangereuse d'instabilitÃ©. Au lieu d'Ãªtre une forme Ã©vidente de la guerre, les conflits futurs impliquant des cyber-guerres peuvent devenir des Ã©vÃ©nements flous sans dÃ©but ni fin. Il est Ã©galement important de noter que le concept de guerre risque d'Ãªtre volontairement floutÃ© en faisant rÃ©fÃ©rence Ã diffÃ©rentes cyber-actions.

Les victimes peuvent mÃªme ignorer lâ□□existence dâ□□un conflit, et entretenir une idÃ©e dâ□□incidents dÃ©sagrÃ©ables, tangibles, perÃ§us comme "le fruit du hasard." Ces Ã©vÃ©nements peuvent Ãªtre rÃ©guliers ou survenir Ã des intervalles alÃ©atoires et peu frÃ©quents. MalgrÃ© leur aspect informel, ils pourraient en effet faire partie d'une stratÃ©gie plus large dans le jeu de cyber-guerre.

La cyber-guerre est certes une rÃ©alitÃ©, mais il faut Ã©viter de sâ□□en servir comme Â« expression fourre-tout Â» pour toute activitÃ© informatique malveillante. Les attaques DDOS sans impact physique ou des activitÃ©s dâ□□espionnage ne devraient pas dâ□□office Ãªtre vues comme des pendants de cyber-guerre. Si chaque attaque malveillante Ã©tait classifiÃ©e dans une catÃ©gorie de cyber-guerre, nous vivrions dans un monde dÃ©chirÃ© par la guerreâ□¦

En outre, il n'y aurait plus de terme adaptÃ© pour dÃ©crire une cyber-guerre dÃ©vastatrice et dÃ©bilitante grave quand il se produit de maniÃ¨re ouverte entre les nations. DÃ©finir ce quâ□□on peut qualifier de cyber-guerre est un vrai dÃ©fi. Sâ□□il sâ□□agit officiellement de Â«guerreÂ», le terme doit Ãªtre mis dans le bon contexte et dans le cadre de prise de dÃ©cisions stratÃ©gique et politique. Nous pouvons aussi prendre pour rÃ©fÃ©rence une autre rÃ©plique de Clausewitz pour qui la guerre est Â«la continuation de la politique par d'autres moyens." Pour Ãªtre considÃ©rÃ© comme cyber-guerre, les moyens peuvent Ãªtre virtuels - mais l'impact devrait Ãªtre rÃ©el.