



La « cyberguerre » échauffe les esprits au salon informatique Cebit

Par [AFP](#)

Thème: [Histoire, société et culture](#)

Mondialisation.ca, 03 mars 2011

[france24.com](#) 3 mars 2011



Entre ceux qui voient son heure arrivée depuis l'attaque du virus Stuxnet contre l'Iran et ceux qui dénoncent un fantasme médiatique, la « cyberguerre » divise les professionnels de l'informatique réunis à Hanovre (ouest).



« La cyberguerre a quitté les livres de science-fiction pour la réalité », affirme à l'AFP Wilhelm-August Scheer, président de la fédération allemande des hautes technologies, en marge du salon Cebit qui se déroule jusqu'à samedi en Allemagne.

AFP - Entre ceux qui voient son heure arrivée depuis l'attaque du virus Stuxnet contre l'Iran et ceux qui dénoncent un fantasme médiatique, la « cyberguerre » divise les professionnels de l'informatique réunis à Hanovre (ouest).

« La cyberguerre a quitté les livres de science-fiction pour la réalité », affirme à l'AFP Wilhelm-August Scheer, président de la fédération allemande des hautes technologies, en marge du salon Cebit qui se déroule jusqu'à samedi en Allemagne.

Sandro Gaycken, chercheur à la Freie Universität de Berlin, utilise lui aussi le terme de « cyberguerre » dans un article récent: « Les attaques ne viennent plus des adolescents fous d'informatique ou de petits délinquants mais des Etats, des armées et des services secrets ».

« Bien sûr que le temps de la cyberguerre est venu. Une guerre physique, c'est très cher, il est bien moins coûteux d'attaquer par internet », assure à l'AFP Natalya Kaspersky, présidente de la société russe de sécurité informatique du même nom.

Le « think tank » américain EastWest en est lui déjà à réfléchir à un « droit de la cyberguerre » inspiré des conventions de Genève de 1949, qui ont créé la Croix-Rouge, afin d'épargner les civils en cas de conflit via le web.

Mais d'autres professionnels rejettent le terme, comme Michael Hange, président de l'Agence gouvernementale allemande de sécurité informatique (BSI).

« La cyberguerre, c'est un mot fort qui plaît aux médias mais pour ma part je suis plus mesuré », a-t-il déclaré lors d'une conférence de presse à Hanovre.

« Dans les cyberattaques, on ne trouve pas de carte de visite d'un Etat. Le modèle classique

de la guerre ne s'applique pas », poursuit M. Hange.

Une analyse partagée par l'experte internationale de cyberdéfense Katharina Ziolkowski, qui déclarait récemment au quotidien *Süddeutsche Zeitung*: « Sous le terme de cyberguerre sont évoqués des phénomènes qui n'ont rien à voir avec des conflits militaires, à savoir l'espionnage, la cybercriminalité ou le détournement d'internet à des fins terroristes ».

« Nous pourrions avoir des phénomènes qui se déroulent sur internet avec des conséquences réelles si graves que l'on pourrait parler de conflit armé. Mais je crois que nous sommes à l'abri pour encore cent ans », estimait-elle.

L'Allemagne n'en a pas moins annoncé la semaine dernière la création d'un centre national de cyberdéfense, afin de mieux se protéger en cas d'attaque informatique visant par exemple les centrales nucléaires.

Aux Etats-Unis, un projet de loi a été rédigé pour donner au président un « interrupteur » qui permettrait de déconnecter le pays d'internet en cas d'attaque majeure.

Le terme de « cyberguerre » avait surgi en 2007 après une attaque en règle de sites internet de l'Estonie, alors en plein conflit diplomatique avec la Russie.

Mais le concept a gagné en popularité depuis l'apparition l'an dernier du virus Stuxnet, qui a endommagé des installations nucléaires iraniennes.

« Stuxnet va entrer dans l'histoire comme la première cyberarme de destruction massive. Il n'a pas attaqué des cibles virtuelles mais causé des dégâts matériels à des objectifs militaires, en se substituant à un bombardement », affirme à l'AFP Ralph Langner, spécialiste allemand de cybersécurité et l'un des premiers à avoir analysé le virus.

La presse américaine a depuis révélé que Stuxnet aurait été élaboré en collaboration par les Etats-Unis et Israël.

La source originale de cet article est france24.com

Copyright © AFP, france24.com, 2011

Articles Par : AFP

Avis de non-responsabilité : Les opinions exprimées dans cet article n'engagent que le ou les auteurs. Le Centre de recherche sur la mondialisation se dégage de toute responsabilité concernant le contenu de cet article et ne sera pas tenu responsable pour des erreurs ou informations incorrectes ou inexacts.

Le Centre de recherche sur la mondialisation (CRM) accorde la permission de reproduire la version intégrale ou des extraits d'articles du site Mondialisation.ca sur des sites de médias alternatifs. La source de l'article, l'adresse url ainsi qu'un hyperlien vers l'article original du CRM doivent être indiqués. Une note de droit d'auteur (copyright) doit également être indiquée.

Pour publier des articles de Mondialisation.ca en format papier ou autre, y compris les sites Internet commerciaux, contactez: media@globalresearch.ca

Mondialisation.ca contient du matériel protégé par le droit d'auteur, dont le détenteur n'a pas toujours autorisé l'utilisation. Nous mettons ce matériel à la disposition de nos lecteurs en vertu du principe "d'utilisation équitable", dans le but d'améliorer la compréhension des enjeux politiques, économiques et sociaux. Tout le matériel mis en ligne sur ce site est à but non lucratif.

Il est mis à la disposition de tous ceux qui s'y intéressent dans le but de faire de la recherche ainsi qu'à des fins éducatives. Si vous désirez utiliser du matériel protégé par le droit d'auteur pour des raisons autres que "l'utilisation équitable", vous devez demander la permission au détenteur du droit d'auteur.

Contact média: media@globalresearch.ca