Extrait du El Correo

http://www.elcorreo.eu.org/L-OTAN-accroit-sa-politique-de-cyberdefense-renforcee

L'OTAN accroît sa « politique de cyberdéfense » renforcée

- Empire et Résistance - OTAN -

Date de mise en ligne : lundi 29 septembre 2014

Selon un commandant des Etats-Unis, l'annexion de la Crimée de la part de la Russie et le conflit postérieur qui a éclaté en Ukraine a démontré que la Russie a su intégrer dans son dispositif militaire une stratégie cyberoffensive qui s'est avérée très efficace.

La confrontation en cours entre la Russie et l'Occident a relancé une discipline dont l'imaginaire a été nourri par l'informatique, le cinéma, la littérature, les rumeurs et une poignée de faits constatés : la *cyberguerre*. Le déplacement d'un conflit depuis un territoire au cyberespace a durant des années généré des spéculations et, dans quelques cas, des affrontements réels comme la cyberattaque massive dont a été objet l'Estonie en 2007, l'attaque contre les systèmes de fusées « air-terre » de la Syrie la même année, les opérations en Géorgie, le harcèlement digital permanent dans lequel la Chine et les États-Unis d'Amérique jouent le rôle principal, ou l'opération (2010) contre le programme nucléaire iranien ourdie par les US et Israël grâce au virus **Stuxnet**. Ce dispositif est le descendant de **l'Opération Olympic Games** développée par **l'Agence Nationale de Sécurité** (NSA) usamericana et « **l'Unité 8200** » d'Israël. La crise qui est apparue avec la Russie a accéléré le recours à la cyberguerre. Pendant le dernier sommet du 4 et 5 septembre - qui s'est tenu en pleine crise avec Moscou, l'OTAN a actualisé ses standards de défense en Europe au moyen d'un programme nommé « **politique de** *cyberdéfense* renforcée ». Selon le commandant us des forces alliées en Europe, l'annexion de la Crimée de la part de la Russie et le conflit postérieur qui a éclaté en Ukraine ont démontré que la Russie a su intégrer dans son dispositif militaire une stratégie *cyberoffensive* qui s'est avérée très efficace. Moscou aurait réussi à interrompre toutes les communications électroniques entre les troupes ukrainiennes basées dans la péninsule et les centres de commando répartis dans le reste d'Ukraine. C'est l'argument de l'Occident pour développer dans le cyberespace un front de conflit.

Le document élaboré par l'OTAN sur la cyber*guerre* est de facto une attitude menaçante. *L'Alliance Atlantique* (OTAN) a étendu au cyberespace toutes les garanties du Traité. Cela veut dire que toute attaque contre les réseaux informatiques d'un pays membre sera considérée comme une attaque contre tous, c'est à dire, équivalente à une agression classique. L'occident crée avec ce texte un cyberespace « indivisible ». La conséquence est évidente : si l'État extérieur à l'Alliance Atlantique apparaît comme responsable d'une cyberattaque, il sera l'objet de représailles qui peuvent inclure y compris les moyens classiques. Avec son le cynisme récurrent, en mal de confrontations, *l'Alliance Atlantique* joue le rôle de future victime comme si l'OTAN ou ses membres les plus puissants, les États-Unis n'avaient par exemple, jamais lancé de cyberattaques contre un de leurs adversaires, ou espionné l'intimité de chaque être humain de la planète grâce au dispositif « **Prism** » monté par la NSA, avec la collaboration de serviles entreprises privées - google, Yahoo, Facebook, Microsoft, etc.-. Sorin Ducaru, adjoint au secrétaire général de l'OTAN et responsable des « défis émergents » a précisé que l'organisme se limitera à se défendre. Selon Ducaru, il est « exclu de lancer des opérations cyberoffensive. C'est le domaine de chaque pays membre ».

La cyberguerre devient ainsi, et maintenant à un niveau collectif, le nouveau *El Dorado* des armées. *L'Alliance Atlantique* dispose déjà d'une infrastructure, le « **Ccdcoe** » (Voir : **Cooperative Cyber Defence Centre of Excellence**), située en Estonie et en pleine phase de développement et d' exercices de « piratage » de serveurs civils, surveillance des réseaux et attaques réelles. Tout semble être prêt pour une grande confrontation délocalisée vers le cyberespace. La rhétorique occidentale est amplement dominée par l'idée que c'est l'unique solution pour se défendre du grand ennemi russe. Le général Keith Alexander - ex-directeur de la NSA - a accusé à Moscou d'avoir piraté il y a quelques mois la banque JP Morgan pour voler des données sensibles en forme de représailles, après les sanctions financières adoptées par Washington contre la Russie à la suite du conflit en Ukraine. Le premier spoliateur mondial de données privées planétaires se présente maintenant avec le profil d'un *petit chat innocent*, victime d'une cyberattaque organisée par une puissance subitement ennemie.

L'autre grand accusé est la Chine

Pekin apparaît régulièrement cité comme responsable de contaminer le cyberespace par les attaques destinées à dérober les secrets de l'Europe et des États-Unis. Cependant, comme, le démontrent, les documents révélés par l'ex-analyste de la *NSA* et de la *CIA*, Edward Snowden, les US ont des yeux et des oreilles branchées dans chaque maison, même chez leurs alliés comme la France et l'Allemagne. Washington a espionné des dizaines de responsables allemands et est parvenu à mettre sur écoute le téléphone cellulaire d'Angela Merkel. Comme représailles, vers la mi juillet, le chef des services secrets US en Allemagne a été invité par la chancelière allemande à quitter le territoire. Dans un entretien publié par la revue Wired, Edward Snowden a raconté que la *NSA* avait parmi son arsenal une arme orientée vers les cyberconflits. Il s'agit du programme **« MasterMind »**. Selon Snowden, ce dispositif est totalement consacré à la cyberguerre. *MasterMind* a été construit pour analyser le trafic dans le réseau, pour détecter et arrêter les cyberattaques contre les US. Cependant, l'ex-analyste de la *CIA* et de la *NSA*, aujourd'hui exilé en Russie, a révélé que *MasterMind* est aussi doté « d'une interface de réponse offensive automatique, sans intervention humaine ».

Les analystes militaires ne sont toujours pas d'accord sur ce que comprend le concept de cyberguerre. Par exemple, **Maxime Pinard**, directeur de Cyberstratégie à l'**Institut de Relations Internationales et Stratégiques** (IRIS), note avec pertinence que le terme de cyberguerre n'est soutenu par aucune réalité concrète. Pinard souligne que « *certainement il y a des cyberattaques, mais non une cyberguerre dans le sens d'un conflit entre, au moins, deux protagonistes identifiés qui causent des dommages humains et économiques l'un contre l'autre* ». Le chercheur français met aussi en relief une autre incohérence dans l'usage excessif du terme cyberguerre : « *Les cyberattaques semblent nouvelles, quand en réalité elles correspondent seulement à des techniques classiques de sabotage et de perturbation des communications de l'ennemi* ». En résumé, un simple espionnage numérique ou la contamination simple mais coûteuse de serveurs avec un virus. Cela n'enlève pas sa pertinence à une autre idée très répandue en ces temps de nouvelles guerres : la course aux armements numériques. Jusqu'à présent, ses acteurs principaux étaient les États-Unis d'Amérique et la Chine.

Cependant, l'inclusion de l'OTAN et sa « **politique de cyber*défense* renforcée** » ajoute un protagoniste supplémentaire et augmente le risque qu'effectivement se concrétise une cyberguerre généralisée, beaucoup plus pointue que les cyberstratégies nationales de défense et de contre-attaque courante. Le contre-amiral Arnaud Coustillière, responsable de la cyberdéfense au Ministère de la Défense français, assure avec réalisme : « *Si nous pouvons neutraliser les radars avec l'arme informatique avant que ce soit avec un missile, c'est beaucoup mieux* ». Le contre-amiral français ne croit pas qu'un jour puisse survenir une sorte d'Hiroshima informatique : « *Nous sommes si globalisés que je ne le crois pas. Cependant, une attaque catastrophique contre les infrastructures vitales, oui cela peut se produire* ». Pour Maxime Pinard, le résultat de ces nouvelles politiques manque de secrets : « *Nous nous dirigeons vers une militarisation renforcée du cyberespace avec un risque certain d'engrenage où les internautes* (simples utilisateurs) *seront les principales victimes* ».

Eduardo Febbro pour Página 12

Titre original : « **Rusia y Occidente aceleran su ciberguerra** »

Página 12. Depuis Paris, le 28 septembre 2014.

Traduit de l'espagnol pour *El Correo* par : Estelle et Carlos Debiasi

El Correo. Paris, le 28 septembre 2014.