Table ronde

Guerre froide sur le net

Jeudi 25 novembre 2010 – Amphithéâtre Des Vallières

Cybercapacités, cyberrésilience, cyberwarfare : quelles réalités ?

Stanislas de MAUPEOU
Chef de projet cyberdéfense, Thales

Le livre blanc sur la défense et la sécurité nationale est très clair sur la question en plaçant les cyber menaces en seconde position dans la hiérarchie des menaces pesant sur la France dans les 15 prochaines années. De plus, les attaques informatiques sont considérées comme fortement probables avec des impacts majeurs.

Fortement probable parce que cela est déjà arrivé ! Nous ne sommes pas dans l'ordre du scénario mais d'une réalité.

Impact majeur parce que les systèmes d'information irriguent nos sociétés en particulier dans les systèmes de gestion de processus industriels comme dans les systèmes d'armes.

Dans le même temps le rapport Albright (OTAN 2020) place les cyber-menaces en troisième position et le nouveau concept stratégique de l'OTAN affirme : « *nous continuerons de développer notre capacité à prévenir et à détecter les cyber-attaques, à nous en défendre et à nous en relever*».

Dans ce contexte, la question de la réalité des menaces se pose-t-elle encore ? Lors des premiers pas de l'aéronautique, le 13 mars 1912 le commandant de Rose le père de l'aviation française s'interrogeait : « *Les aéroplanes détruiront-ils les autres aéroplanes ? Cette question n'est pas encore au point* »[1]

Les ordinateurs détruiront-ils un jour d'autres ordinateurs ? Cette question n'est pas encore au point mais les menaces informatiques sont une réalité opérationnelle ![2]

Puisque la menace fait doute tentons de mieux l'identifier pour mieux l'apprécier.

De façon classique, la menace peut se construire autour de trois facteurs :

- un élément ayant la volonté et la capacité de nuire ;
- une vulnérabilité ou une faille dans le système de défense ;
- l'impact de l'attaque sur le système.

---

[1] Source : http://rha.revues.org/#ftn16
[2] "World War Web 3.0" Revue de la défense nationale mars 2010 (www.rdn.fr)

L'origine des menaces

Des Etats et des organisations non étatiques ont opté pour des postures agressives, offensives sur les réseaux informatiques. Les chiffres de la cybercriminalité parlent d'eux mêmes.

L'exemple récent du code stuxnet[3] ou les attaques subies par l'Estonie ou la Géorgie témoignent de cette réalité.

Les vulnérabilités

Il y publié tous les ans environ 8000 vulnérabilités ! Cela signifie que les failles pour pénétrer ou perturber un système sont nombreuses. Ne perdons pas de vue que les logiciels sont des constructions humaines qui ont des défauts de conception ou de réalisation. C'est pourquoi il est vital pour des enjeux de sécurité nationale de disposer de moyens agréés par les services de l'Etat. Mais cela à un coût !

L'impact

Les Etats comme les entreprises sont de plus en plus dépendant des systèmes informatiques pour leur bon fonctionnement. De ce fait, une attaque majeure provoquant des dysfonctionnements pourraient avoir des répercutions économiques considérables. Les systèmes d'information sont devenus les systèmes nerveux de nos sociétés et nous savons les conséquences pour le corps entier lorsque le système nerveux est atteint.[4]

Si nous attendons une attaque pour en apprécier la réalité, nous resterions dans une posture dangereuse sur le plan stratégique (la rupture technologique) et irresponsable sur le plan de la défense du pays.

Pour une défense active

Je souhaiterais enfin indiquer que la détection des attaques autrement que par leurs effets, c'est à dire de façon préventive est aujourd'hui encore embryonnaire. Non pas sur le plan technique car les solutions et les services existent mais sur le plan de la décision de s'équiper et d'investir dans de tels services de sécurité.

Dans le domaine de la cyber défense, à l'instar d'autres domaines de la défense et de la sécurité, pour détecter les attaques avant que les conséquences ne nous surprennent, il est impératif de mettre en place des solutions de détection, d'analyse et de réaction faces aux attaques informatiques.

En pleine réforme budgétaire, la Grande Bretagne vient pourtant d'annoncer un plan de 650M€ pour la cyber défense. Quelle est la situation de la France dans ce domaine ? « La survie de l'instrument de riposte et de défense impose son adaptation permanente aux diverses formes de la menace et des mesures conservatoires prises en temps de paix »5. Au risque d'affecter les capacités de nos forces en opérations, la menace informatique ne peut-être traité légèrement en diminuant les investissements.

La guerre n'a probablement pas changé fondamentalement de nature par l'arrivée de moyens sophistiqués de surveillance, de transmission ou de précision des armes. Si certains ont pu penser dans les années 90 que l'information lèverait l'incertitude, la réalité des opérations est que le chef garde son libre arbitre. Mais il serait cependant bien imprudent de sous estimer les impacts que

[3] Source : http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-009/
[4] Source : Cahier de la sécurité (INHES), octobre-décembre 2008.
[5] Général Pierre Galois, Revue de la Défense Nationale, mai 1995.

pourrait engendrer une attaque informatique sur la mission des forces en opération. Les cyber-attaques constituent une réalité quotidienne qui doit entrer dans le champ de la réflexion stratégique.[6]

Un risque systémique

Il existe un risque systémique lié à l'exploitation massive de l'informatique : conduisons des analyses de risques sans écarter d'emblé les cas non conformes ; mettons en œuvre des capacités de défense active par la détection d'attaques informatiques afin d'en limiter les impacts ; entraînons les militaires à ce nouveau champs d'affrontement.

Les attaques informatiques visant les systèmes des forces en opération ne sont pas nécessairement complexes à mettre en œuvre. Contrairement aux technologies nucléaire ou spatiale, le coût d'entrée est faible et des Etats comme les organisations non-étatiques ont déjà opté pour des postures d'attaque sur les réseaux. Dans un monde incertain et ouvert dans lequel l'information est vitale, il est impératif de développer des systèmes résilients détectant et s'adaptant en permanence aux nouvelles menaces.

Il n'y aura pas de crise informatique au sens d'une crise limitée à ses seuls effets techniques ; le fait technique débouchera inévitablement sur une crise sociétale car les systèmes d'information irriguent la société.[7]

[6] « Internet, infrastructure vitale ! » Revue de la défense nationale, mars 2009 (www.rdn.fr)
[7] « Crise financière et crise informatique » Revue de la défense nationale, janvier 2009 (www.rdn.fr)