Table ronde

Guerre froide sur le net

Jeudi 25 novembre 2010 – Amphithéâtre Des Vallières

Ouverture

VAE Richard Laborde
Directeur de l'Institut des hautes études de défense nationale

Monsieur le Vice-Président du Sénat,
Messieurs les officiers généraux,
Mesdames et Messieurs,

Nous voici réunis pour une réflexion commune sur les enjeux stratégiques du cyberespace.

Le titre retenu n'est pas le seul fait du hasard : « Guerre froide sur le net ».

Permettez-moi de le commenter.

Un bon auteur chinois enseigne que « Pour conduire une guerre, il est préférable de sauvegarder un pays plutôt que de le détruire… Le mieux est de soumettre l'ennemi sans combattre ».

Après une période de 40 ans d'extrême tension, la chute du mur de Berlin montre que cette stratégie peut être payante.

Aujourd'hui, une nouvelle guerre froide fait rage. Pas de combattants, pas de champs de bataille, pas d'affrontement direct et pas d'ennemi identifié. Mais des ordinateurs et des réseaux, nouveaux moyens, nouveaux champs de conflictualité pour servir des fins commerciales ou plus stratégiques, comme autrefois les agents secrets ou les pays tiers.

Dans le domaine d'une technologie duale par nature, cette guerre froide de nouvelle sorte crée une course non plus aux armements, mais aux technologies. Les aspects industriels du domaine sont énormes ! Les seuls marchés gouvernementaux ont été évalués à 8,12 milliards de dollars pour 2009. Somme à démultiplier si l'on considère que les acteurs privés se sentent aussi menacés et donc prêts à assurer leur sécurité.

Nouvelle guerre froide, la cyberguerre n'est pas virtuelle comme le montre les attaques de grande ampleur menée en Estonie, en Géorgie, ou en République de Corée, pour les plus connues.

Nouveau risque, nouvelle menace, les opérateurs publics et privés se sont mis en ordre de marche pour survivre dans ce nouvel Etat de nature numérique.

Ainsi le Livre blanc sur la défense et la sécurité nationale publié en 2008 met-il en évidence l'ampleur de cette menace. J'y relève quelques phrases clé.

« Dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude. Certaines d'entre elles pourront être de grande ampleur.

S'agissant des attaques d'origine étatique, plusieurs pays ont déjà défini des stratégies de lutte informatique offensive et se dotent effectivement de capacités techniques relayées par des pirates informatiques ».

« Les intérêts européens et les intérêts nationaux sont étroitement corrélés dans le cyberespace. […] La France proposera aussi que la Commission impose aux opérateurs des règles de durcissement des réseaux et des procédures destinées à en accroître très fortement la résilience. »

« Le réseau Internet devra être considéré comme une infrastructure vitale et un effort important devra être mené pour améliorer sa résilience. »

« Il convient donc de disposer d'une capacité de neutralisation à l'intérieur même des centres d'opérations adverses, c'est l'objet même de la lutte informatique offensive. »

Voilà pour ce qui concerne notre stratégie de sécurité nationale. Face aux défis d'ordres technique, juridique, culturel et géopolitique associés au cyber espace, la réponse française repose, comme vous le savez, sur cinq grandes orientations portées par l'agence nationale de la sécurité des systèmes d'information, l'ANSSI, rattachée au SGDSN.

J'en retiendrais trois, se doter de capacités de détection et de réaction en temps réel à une cyberattaque massive, développer un réseau de partenaires fiables dans le monde et davantage sensibiliser la société dans son ensemble à la cybersécurité.

Sensibiliser aux nouvelles menaces, c'est construire de la résilience, c'est l'une des missions de l'IHEDN, c'est aussi l'objet de cette table ronde.

***

Mais revenons un instant à nos partenaires stratégiques. Ceux-ci partagent cette vision et se sont mis en mouvement.

Aux Etats-Unis, l'ensemble des sommes consacrées à la protection des systèmes d'information pour 2009 est de 7,2 milliards $, soit, en pleine crise, un effort supplémentaire de 600 millions $.

Le 23 juin 2009, le ministre de la défense Robert Gates a signé une directive créant un U.S. Cyber Command (U.S. CYBERCOM) dépendant de l'U.S. Strategic Command, dont l'objectif est d'assurer la défense nationale dans le cyberespace. U.S. Cyber Command a vu le jour le 21 Mai 2010. Son chef est un Général (4*), le général Keith Alexander. Il est responsable de la mise en commun et de la coordination des ressources.

Entre ces deux dates, le 2 mars 2010, la Maison blanche avait rendu public son Initiative nationale globale de cyber-sécurité, qui est en fait la décision de mettre en œuvre les recommandations de la Cyberspace Policy Review.

Tous ces éléments montrent que, pour nos amis américains, le cyberespace est un espace de bataille militaire.

***

Pour sa part, le Royaume-Uni a publié une Cyber Security Strategy en 2009 détaillant la protection de ses infrastructures contre une attaque. Un « Cyber-security operation » center a été ouvert en septembre 2009 au quartier général des communications gouvernementales. Ce dispositif est complété d'un bureau de la cyber-sécurité intégré au Cabinet pour coordonner les politiques au sein du gouvernement.

Il y a très peu de temps, David Cameron a plaidé pour une augmentation de 500 millions de £ du budget alloué à la cyber-sécurité, ce qui porte le total des sommes consacrées à ce domaine à un peu moins de 2 milliards £.

***

Un mot sur l'Alliance quelque jours après le sommet de Lisbonne et avant que ce sujet ne soit abordé dans le détail.

La cyberdéfense est une des priorités de l'OTAN depuis 2002. L'OTAN s'est naturellement d'abord préoccupée de la protection de ses propres installations avant de s'interroger sur son rôle en tant qu'Alliance défensive, suite aux événements survenus en Estonie, au printemps 2007.

Un concept de cyberdéfense a été adopté en 2008 et un centre d'excellence créé à Tallin. Le très récent concept stratégique adopté à Lisbonne précise que
« Les cyberattaques augmentent en fréquence, sont mieux organisées et causent des dommages plus coûteux aux administrations, aux entreprises, aux économies, voire aux réseaux de transport et d'approvisionnement ou autres infrastructures critiques ; elles risquent d'atteindre un seuil pouvant menacer la prospérité, la sécurité et la stabilité des États et de la zone euro-atlantique ».

***

L'approche de l'Union européenne, quant à elle, semble plus timide. La protection des systèmes d'information fait l'objet de documents nombreux, mais qui semblent peu opératoires. Enfin, l'agence européenne chargée de la sécurité des réseaux et de l'information, l'ENISA, a fait l'objet d'un regard critique que relaye d'ailleurs le Livre blanc en notant que l'efficacité de cette agence doit être notablement accrue.

***

Que conclure de ce rapide tour d'horizon ?

D'abord, que la cyberguerre n'est pas virtuelle et que les moyens utilisés dans ce nouveau champ de conflictualité peuvent permettre l'atteinte de but stratégique.

Ensuite que la plupart de nos grands alliés et partenaires se sont mis en mouvement pour se doter de capacités de cyberdéfense afin, je cite un extrait du rapport du Sénateur Roger Romani, ici

présent, « de répondre aux « atteintes portées aux systèmes d'information susceptibles de mettre en cause la sécurité et la défense du pays » et de se doter des « moyens de s'en protéger »

Enfin, qu'il importe de définir ce concept de cyber-défense et le distinguer des autres cyber-risques, ou des traductions hasardeuses de l'Anglais cyber-security.

Etant dans le domaine des enjeux stratégiques, nous avons donc fait appel pour éclairer le débat sémantique à la Délégation aux affaires stratégiques, et plus précisément au Général Emmanuel de Romémont.

Comme rien ne remplace une séance de travaux pratiques, surtout lorsque le sujet est complexe, nous avons pensé qu'une démonstration était le meilleur moyen de vous faire découvrir la vulnérabilité d'un système d'information.

Venant tout spécialement de Rennes pour nous, Christophe Rault du centre Maitrise de l'Information (ex CELAr) de la Direction Générale de l'Armement vous empêchera désormais de vous sentir en sécurité derrière un pare feu et un antivirus.

Ensuite, notre table ronde "Cybercapacités, cyberrésilience, cyberwarfare : quelles réalités ?" réunira :

- Le Sénateur Roger Romani, vice président du Sénat mais surtout auteur du rapport « CYBERDÉFENSE : UN NOUVEL ENJEU DE SÉCURITÉ NATIONALE » que vous avez trouvé à l'entrée ;
- Guillaume Tissier, directeur du pôle "Risques opérationnels", de la Compagnie Européenne d'Intelligence Stratégique ;

Cette table ronde a pour parrains deux entreprises leaders sur leur secteur d'activités : Capgemini-Sogeti et THALES et je les remercie tout de suite pour leur participation à cette manifestation.

Viendront donc se joindre à nos orateurs :

- Monsieur Edouard Jeanson, directeur de l'European Security Expertise Center, pour Capgemini-Sogeti ;
- Monsieur Stanislas de Maupeou, chef de la cyber-défense pour THALES.

Enfin, la conclusion de cette journée sera faite par notre invité venant spécialement de Bruxelles, et je l'en remercie vivement, le Major-Général Glynne Hines de l'armée de l'air canadienne, mais surtout directeur de l'état-major des C3 au sein du Quartier Général de l'OTAN.

Ce discours, par le directeur de la branche de l'Alliance en charge de la cyber-défense, cinq jours après le sommet de Lisbonne, retiendra, j'en suis sur, toute notre attention.

Mesdames et messieurs,

La cyber défense, de quoi s'agit-il ? La réponse appartient à la DAS, à qui je cède sans plus tarder la parole.