Compte rendu de la conférence du Sénateur Jean-Marie BOCKEL du 11 avril 2012
Cyberdéfense : Etat des Lieux stratégique, politique et technologique

Le Sénateur BOCKEL (ancien Ministre) et Daniel VENTRE, ingénieur de recherche au CNRS, sont intervenus devant un large auditoire d'auditeurs de l'Association IHEDN Paris Région Ile-de-France et d'Associations Associées (AA, CHEAr, ESSEC Défense, …) sur le sujet brulant de la Cyberdéfense.

Après une introduction de la Présidente Caroline GORSE-COMBALAT, le Sénateur prend la parole pour présenter son rapport parlementaire en insistant sur le fait que son point de vue est celui du politique et qu'il laissait à Daniel VENTRE le soin d'assurer le volet technique.

La cyberdéfense revêt une importance stratégique : de nombreux pays ont été attaqués, le centre d'excellence de l'OTAN est situé à TALINE et Jean-Marie BOCKEL a déjà rencontré pour avoir une vision comparative LONDRES, ROME et l'OTAN ; il rencontrera avant la remise de son rapport BONN, l'Union Européenne et WASHINGTON.
Après une incidente sur le concept attaque-défense (« la meilleure défense c'est l'attaque ») il constate que la politique à mettre en place par un état est avant tout un système de protection pour empêcher l'intrusion dans les réseaux en particulier ceux concernant les SAIV. On se souviendra ici de l'attaque massive subie par l'ESTONIE en 2007, du fait que les réseaux CHINOIS ont été attaqués et que, en France, le MINEFI a été victime d'une cyber attaque en 2011.
Pour lutter contre cette menace, dans ce nouveau Champ de Bataille la France, considérant qu'un conflit ne se produira pas sans cyber guerre, a mis en œuvre l'ANSI dont la mission est de lutter le plus possible dans la zone grise destinée à effectuer des chantages pour en limiter les effets d'une telle attaque et renforcer les mesures de défense possibles.
Aux Etats-Unis la cyber sécurité est un objectif stratégique (le cyber command US a un budget de 50 Milliard de $) au Royaume Uni le Sécurité Informatique est assurée par le Command Electronic Security Group (550 agents et 650 Millions de £) ; en Allemagne cette fonction est assurée par le Ministère Fédéral de l'Intérieur (80 Millions d'€ et 500 agents) ; l'OTAN a désigné une autorité de gestion de la cyber défense mais malgré le centre d'excellence de TALIN reste encore mal armée contre cette menace pour laquelle se pose la question fondamentale de l'utilisation de l'Article 5 du traité ; quant à l'UE son rôle est différent elle veut régir les réseaux et devenir un interlocuteur majeur sur le sujet. La France quant à elle n'est à ce jour ni bien préparée ni bien organisée : le réseau interministériel ISIS est d'un usage compliqué et n'a pas empêché les attaques sur le MINEFI et la centralisation au niveau de l'Etat est insuffisante ; la politique définie par le LIVRE BLANC a amené la création de l'ANSI qui a défini une stratégie d'action qui a provoqué la création de l'Autorité Nationale de Défense des Systèmes d'Information (directement rattachée au chef de l'Etat). Il reste beaucoup à faire :

- en 2012 - 50 fonctionnaires et un objectif de 360 en 2013
- les SAIV sont peu sensibilisées : les objectifs prioritaires sont les systèmes bancaires et la fonction distribution d'énergie

Et il faut pour cela mettre en place des parades, renforcer la coopération internationale, éviter de trop normer en Europe pour ne pas multiplier les parades, renforcer le contrôle des réseaux sociaux.
Tout cela c'est la réponse du Politique qui peut provoquer une aggravation des sanctions et faire effort sur la coordination.

En répondant aux questions de la salle modérées par Emmanuel DUPUY, Président IPSE, le Ministre et Daniel VENTRE :
. Insistent sur la difficulté qu'il y a à définir une frontière entre la cybercriminalité et la cyberdéfense ainsi que sur le fait qu'il y a un déplacement des limites paix-crise-guerre.
. Constatent que l'Europe n'est pas assez agressive et qu'il subsiste une question de droit international en rapport avec le concept de souveraineté.

La capacité de maîtrise de la technique est très difficile quand on sait que 80% des FAI (Fournisseurs d'Accès Internet) sont aujourd'hui aux Etats Unis et que l'on connait la prégnance actuelle de la CHINE tant en matière de HardWare que de SoftWare. La cyberdéfense se joue sur les trois plans : matériel, logiciel et cognitif ; techniquement on peut en particulier couper internet de l'extérieur les chinois l'ont prouvé sur une province.
Pour ce qui est du bilatéral et du multilatéral le Ministre précise que la souveraineté ne se délègue pas mais il constate et approuve que les initiatives multilatérales de l'OTAN qui sont bénéfiques ; il n'y a pas de réponse binaire à cette dualité et il faut construire la cyberdéfense sur le fond géopolitique du moment.
Au plan de la compatibilité et de la transparence ce qui change et marque la rupture c'est d'une part la mise en place de moyens par l'Etat (ANSI) et la prise en compte au plus haut niveau du fait de la prise de conscience et de la sensibilisation bien qu'il existe encore de nombreuses failles et que la sensibilisation des acteurs semble encore insuffisante

En guise de conclusion, Jean-Philippe BRAULT remercie le Sénateur et Daniel VENTRE pour avoir d'une façon si pertinente répondu aux attentes des auditeurs et d'avoir répondu si clairement aux questions. Il remercie également Emmanuel DUPUY et l'ambassadeur DENIAUD pour leurs actions de facilitateur de la rencontre.
Il reste maintenant à intégrer tout cela dans le LIVRE BLANC sur la défense et la sécurité en cours de révision.
Nous avons bien noté que cette menace était crédible et pernicieuse bien que son origine soit souvent non identifiée
Il me semble à l'instar de l'Ordonnance de 59 que nous devrions ajouter aux trois piliers de la Défense Globale qui mettent en œuvre la résilience : Militaire, Civile et Economique, le pilier CYBER puisqu'il touche tous les domaines :

- une menace aux militaires par l'intrusion dans les systèmes de défense
- une menace civile sans doute par l'endoctrinement des terroristes
- une menace économique par la désorganisation des systèmes et des flux

Le rapport touche à sa fin il est maintenant du devoir des auditeurs de vous aider dans la mesure de leurs moyens à le porter et pour faire inclure les conclusions dans le LIVRE BLANC afin que cette menace qui pèse sur chacun d'entre nous (personnes physiques et entreprises) soit prise en compte de le façon la plus pertinente possible et que les moyens pour s'en protéger soient mis en œuvre.

En guise de clin d'œil militaire et hors conférence voici ce qui pourrait être la conclusion du rapport parlementaire :
En vue de gagner la Cyber Guerre, je veux :

- Mettre en place des parades,
- Renforcer la coopération internationale,
- Eviter de mettre en place des normes trop contraignantes,
- Renforcer le contrôle des communications,
- Sensibiliser les entreprises à la cybermenace,
- Faire en sorte que les incidents dont sont victimes les entreprises soient déclarés à l'Etat,
- Former des ingénieurs et favoriser la recherche et le développement,
- Développer des capacités offensives.

En adoptant comme doctrine d'emploi la maxime « dissuader pour protéger »