Le 14 juillet arrive, la loi de programmation militaire se construit, le cyber et « big brother » sont partout.

Ce 1er juillet 2013 se tenait donc aux Invalides le premier colloque de la chaire « cyberdéfense et cybersécurité » des écoles de saint-Cyr Coëtquidan. Je pense que cela a été une vraie réussite et arrivait à point nommé avec l'affaire Snowden.

Avez-vous remarqué que les « vilains » Américains (et les Britanniques, très discrets) espionnaient tout le monde… mais que nous n'espionnions personne ? Il en a outre été peu mis en avant l'alliance permanente du monde anglo-saxon à travers le « *five eyes only* » … que nous côtoyons sinon subissons même en opération, même entre alliés.

Américains, Canadiens, Néo-zélandais, Australiens et Britanniques ont tissé leur réseau de renseignement et d'influence à travers les différentes alliances existant dans le monde. L'information ne se partage qu'entre eux. Cette approche transverse et coordonnée face à nos divergences notamment européennes ne peut que se faire à notre détriment. Mais que faisons-nous ? Pas grand-chose semble-t-il.

Revenons à notre colloque. Consacré au thème *« Comprendre les stratégies et politiques de cybersécurité et cyberdéfense de la Chine »*, il se tenait loin des platitudes convenues sur le cyber et entendues depuis plus d'un an. Il était donc plutôt concret et faisait appel surtout à des intervenants moins connus et tout aussi intéressants.

Clin d'œil de l'actualité, le 25 juin, Louis Pouzin que personne ne connaît ou presqu'en France, recevait des mains mêmes de la reine d'Angleterre et devant le premier ministre britannique, le Prix de la reine Elizabeth pour l'ingénierie. Louis Pouzin, ingénieur français, polytechnicien, 82 ans, a inventé l'internet en concevant le datagramme.

Celui-ci permet d'envoyer des paquets de données ensemble et de les laisser voyager séparément avant qu'ils ne se regroupent en bout de ligne. Sa technique sera ensuite utilisée par deux Américains, Robert Kahn et Vinton Cerf, pour développer ce qui deviendra l'Internet. Ensuite, un Britannique, Tim Berners-Lee, crée le World Wide Web, et un autre Américain met au point un navigateur, Mosaic. L'invention devient alors accessible au grand public. (Cf. article du Monde du 1er juillet 2013). Je vous rassure. Son nom n'a pas été cité durant ce colloque.

Le contexte chinois

Le thème a donc été abordé d'une part par la présentation de la cybersécurité chinoise, d'autre part par l'impact des stratégies chinoises sur les relations internationales. Que peut-on retenir ? Comme partout, Internet devient la principale source d'information. La Chine contrôle de fait le web 1.0. Weibo (équivalent de Twitter) en revanche se constitue en contre-pouvoir, dénonçant les scandales, amplifiant les revendications et devenant en fait un facteur d'instabilité pour le gouvernement chinois.

La réponse est une nouvelle forme de nouvelle forme de propagande du gouvernement chinois avec l'aide de propagandistes recrutés depuis les années 2000 pour influencer l'internaute. Il faut rétablir la légitimité du parti et bien sûr soutenir le président de la République chinoise.

Internet devient un outil de communication gouvernemental. Il permet aussi d'évaluer, de prévenir depuis 2007 les mouvements sociaux et donc d'anticiper leurs attentes. Si des actions positives sont menées, au demeurant, pourquoi pas ?

Dans le domaine stratégique, il a été souligné que le contexte des guerres a changé. L'armée populaire chinoise (PLA) n'a plus la priorité d'accès aux ressources. L'économie prime. S'ajoutent une observation attentive des guerres menées par les autres Etats et une orientation vers des guerres limitées à fort environnement technologique (Cf. les rapports annuels du Pentagone au Congrès depuis 2000). Enfin, il ne faut pas oublier que l'armée populaire est une partie du parti communiste chinois. Chaque officier à compter du grade de sous-lieutenant en est membre.

Cyberstratégie militaire chinoise

En terme de stratégie militaire chinoise, la guerre est conçue en interarmées (terre, air, mer). Elle nécessite une connaissance partagée de la situation opérationnelle, à l'occidental, et donc une information mise au cœur des opérations (technologies de l'information, réseau de réseaux, influence), aussi bien en temps de paix qu'en temps de guerre. Le processus est donc permanent et global, y compris par les actions d'influence et la communication avec la recherche de l'affaiblissement de la résilience de l'adversaire par exemple en l'inhibant juridiquement.

Dans ce contexte, j'ai bien sûr été intéressé par l'approche américaine « *information dominance : PLA views of information warfare and cyberwarfare* » par Dean Cheng, chercheur à la *Heritage Fondation*. Il a présenté l'approche chinoise de la guerre de l'information qui paraît fortement ressembler à la doctrine occidentale des opérations sur l'information avec deux différences majeures qui valident pour la seconde la doctrine française.

La première est le développement depuis les années 90 de la résilience des infrastructures chinoises. Cette forte capacité limiterait les vulnérabilités cyber chinoises. La seconde est la prédominance doctrinale de la prise en compte du facteur humain. Il s'agit d'attaquer la volonté de l'autre. Le cyber devient le porteur du message et vise à influencer les perceptions (Cf. les actions sur les perceptions et l'environnement opérationnel de la stratégie militaire d'influence en France).

Formation française des hackers et montée en puissance des capacités

La réflexion sur ce colloque peut se poursuivre dans le Monde Magazine du 29 juin avec l'article *« A l'école des Hackers »*. Ainsi on apprend que le ministère de l'enseignement supérieur a ouvert en 2008 une formation de « *hackers* » sous le terme prudent *« CDAISI pour Collaborateurs pour la défense et l'anti-intrusion des systèmes informatiques »*.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) pourrait compter 500 salariés en 2015, contre 190 en 2009. « *Le ministère de la défense ouvre également des postes « cyber » au sein de la Direction générale de l'armement (DGA), de la sécurité extérieure (DGSE) et de l'administration centrale. Les entreprises comme Google, Microsoft ou EADS sont aussi des employeurs potentiels ».*

Il faut lire aussi cette audition du contre-amiral Coustillière par la commission de la défense de l'Assemblée nationale le 12 juin (Audition du contre-amiral Arnaud Coustillière, officier général en charge de la cyberdéfense à l'état-major des armées). Très informative, elle fait le point au titre de la défense nationale de la capacité cyber française. Ayant pris ses fonctions en 2011, le contre-amiral occupe une double fonction.

Il est en charge de la montée en puissance des capacités de cyberdéfense des armées françaises et il est le chef cyber du centre de planification et de conduite des opérations (CPCO) avec la mission d'assurer la défense de l'ensemble des systèmes d'information du ministère de la Défense et la synchronisation des actions informatiques d'accompagnement des actions militaires.

Le ministère compte actuellement 1 600 personnels investis dans cette question, dont 1 200 relevant de l'état-major des armées, avec 300 personnels en charge des équipements de chiffrement et 900 du seul périmètre cyber. La LPM à venir devrait confirmer le plan d'augmentation des effectifs à hauteur de 350 personnels, notamment pour assurer des missions de prévention et de défense.

Il faut noter que le centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI emménagera bientôt dans des locaux situés en bord de Seine et accueillera le centre opérationnel du ministère de la Défense. Une vraie collaboration civilo-militaire ! Sur les crédits de R&D, cette audition évoque enfin une progression des crédits qui devraient tripler pour atteindre un montant total de 30 millions d'euros.

Cette période est donc favorable à la cyberstratégie dès lors qu'elle saura associer à l'innovation de défense et à la haute technologie, une stratégie d'influence créative et anticipatrice.