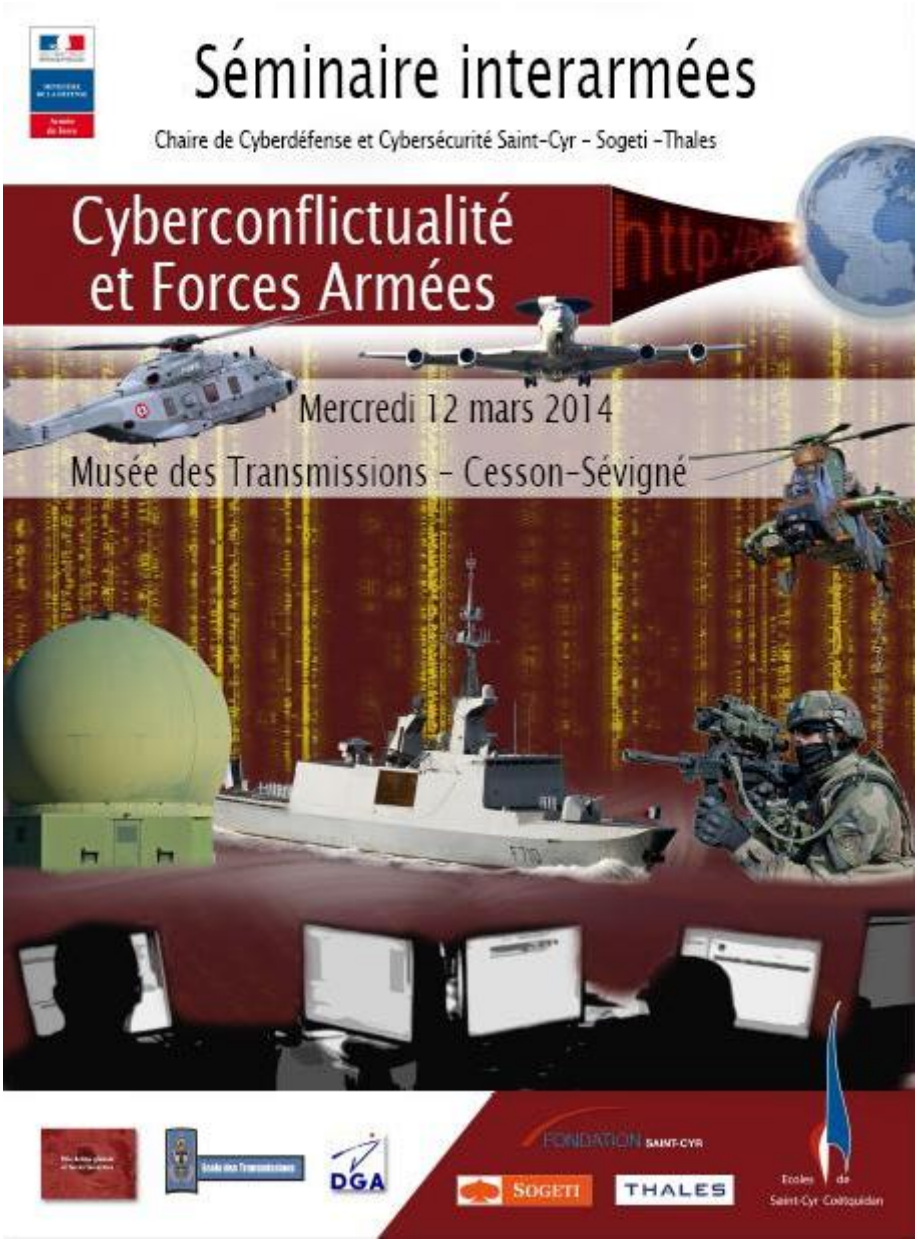
Compte rendu du séminaire du 12 mars 2014

« Cyberconflictualité et Forces Armées »

musée des Transmissions, Cesson Sévigné

dans le cadre des activités de la chaire Cyberdéfense et Cybersécurité

Saint-Cyr / Sogeti / Thales



Prolongement du séminaire du 12 février 2013 qui avait traité de la Cyberconflictualité pour les Forces Terrestres, ce séminaire organisé avec le soutien de l'Ecole des Transmissions et de la DGA-MI, a rassemblé un peu moins de 100 personnes, pour la plupart des militaires des trois Armées, et des personnels de la Défense.

Le fait de rassembler essentiellement des personnels du monde de la Défense, avec une ouverture interarmées, était souhaité pour plusieurs objectifs :

- Traiter des questions caractéristiques du Cyberespace et de ses spécificités entre l'armée de Terre, la Marine ou de l'armée de l'Air.
- Traiter des spécificités de la formation militaire pour chacune des écoles militaires de formation initiale des officiers des Armées.
- Répondre à la vocation du pôle d'excellence en Cyberdéfense de Bretagne, lequel s'appuie entre autres sur les organisateurs de ce séminaire (chaire Saint-Cyr / Sogeti / Thales, ETRS, DGA-MI), qui est d'effectuer des activités de recherche au profit du ministère de la défense et de la communauté nationale de Cyberdéfense, et ainsi de répondre à l'axe 4 des priorités du Pacte Défense Cyber exprimé par le ministre de la Défense Jean-Yves Le Drian le 7 février 2014, au même lieu.
- Répondre à la vocation du pôle Action Globale et Forces Terrestres du CREC Saint-Cyr d'analyser les mutations de la conflictualité, et de contribuer à irriguer par ses recherches l'enseignement supérieur à Saint-Cyr Coëtquidan.

Etaient représentés l'ensemble des Etats Majors des Armées (EMA, EMAT, EMM, EMAA) et l'ensemble des Ecoles de formation initiales d'officiers (Navale, Ecole de l'Air, Saint-Cyr, l'EOGN ainsi que l'Ecole des Transmissions). La DICOD était également présente pour un reportage Web TV sur la CyberDéfense.

Très dense de par les thématiques couvertes durant cette journée, le spectre couvert étant volontairement très large, ce séminaire a permis d'effectuer une première rencontre résolument interarmées, et de donner aux personnes concernées par le monde cyber de se rencontrer et d'échanger. A l'avenir, le but poursuivi est de sanctuariser une date en début d'année pour que le pôle d'excellence en CyberDéfense du Grand Ouest organise un temps de rencontre régulier entre les acteurs majeurs de la région, et poursuivre ses réflexions sur le caractère stratégique de la Cyberconflictualité, dimension structurante pour les Armées tant pour le rang que la France doit occuper parmi les puissances majeures, que pour son efficacité opérationnelle.

Introduction au séminaire :

Depuis les systèmes étanches protégés du début des années 2000 centrés la défense périmétriques des systèmes et des réseaux, les évènements Estoniens et Géorgiens font prendre conscience qu'il faut sortir de la simple sécurité passive, et qu'il faut protéger nos systèmes devenus incontournables. L'impulsion politique du livre blanc de 2008 ouvre le chemin à une stratégie de Défense active en profondeur, avec protection de nos systèmes, surveillance permanente et réaction rapide en cas d'attaques.

Dans ce prolongement, l'année 2013 fut structurante pour la CyberDéfense : outre le livre blanc publié en 2013, et la Loi de Programmation Militaire (LPM) de décembre 2013 qui sert de support juridique pour l'action spécialisée, le ministre de la Défense Jean-Yves Le Drian a lancé plusieurs travaux concrets, dont la création du pôle d'excellence en Cyberdéfense de Bretagne avec ses 6 axes d'effort et ses 50 actions concrètes. Afin d'appliquer cette politique de CyberDéfense voulue par le ministre et relayée par l'officier général Cyber l'amiral Coustillère, il apparait la nécessité de

développer un corpus doctrinal interarmées à jour, de la conception jusqu'à la mise en œuvre, avec des documents adaptés pour chacune des Armées. Il est prévu par exemple, à l'été 2014, un document de mise en œuvre de la CyberSécurité pour les Forces terrestres, s'appuyant sur le triptyque CyberDéfense, CyberProtection (anciennement SSI) et CyberRésilience (capacité à résister et se rétablir).

Sur le plan de la formation globale, la prise en compte de la spécificité du domaine de la CyberDéfense impose de faire migrer le profil de spécialiste SSI vers un profil de spécialiste en CyberSécurité, lequel inclut des compétences supplémentaires telles que la cryptographie par exemple. Les compétences techniques supplémentaires requises pour la formation des militaires s'appuient sur des expertises développées dans le civil, et imposent donc une encore plus grande ouverture vers les formations qu'il dispense.

Pour des formations militaires plus spécialisées, l'ETRS propose de nouvelles formations qui intègrent le traitement des incidents Cyber, parfois en lien avec le CALID. Cette formation se veut aussi appliquée, ce qui passe par des exercices d'entrainement opérationnels pour nos Forces, avec des incidents Cyber concrets pris en compte dans la manœuvre.

Pour ce qui concerne la ressource humaine, des créations de postes sont planifiées, postes modélisés et redéfinis avec une orientation interarmées. Hors du personnel militaire, et pour appuyer l'action des Forces, la Réserve citoyenne CyberDéfense, composée de bénévoles se lance en 2013 sous 5 régions, dont la Bretagne, pour des missions de sensibilisation. La réserve opérationnelle Cyber est quant à elle moins avancée, et devraient faire l'objet de travaux en 2014.

Sur le plan doctrinal, le CICDE avait émis un document de concept de Cyberdéfense en 2011, et la doctrine DIA 6.3 en 2012, rattachée au domaine 6 des SIC, définissant les moyens, l'organisation et les responsabilités pour traiter du volet défensif de la CyberDéfense.

Face à l'impulsion ministérielle, le CICDE a produit un nouveau document de doctrine, la DIA 3-40 pour les opérations (3) dans le Cyberespace (sous domaine propre = 40). Il décrit les caractéristiques du Cyberespace comme étant certes un 5eme milieu, mais un substrat qui servant de support aux 4 autres milieux que sont l'air, la terre, la mer et l'espace.

Selon la DIA 3-40, la CyberDéfense comprend 3 types d'action que sont la LID, l'exploitation des réseaux à des fins de renseignement, et l'exploitation offensive (LIO), ce qui est cohérent avec la doctrine de l'OTAN. Elle a pour mission de servir aux opérations militaires (préparation et conduite), au fonctionnement des ministères, et au ministère de la Défense pour son appui en cas de crise Cybernétique.

Les 5 grands principes qui la sous-tendent sont:

- Une chaine de commandement unique qui assure une cohérence, centralisée et spécialisée.
- Un appui sur les compétences civiles, au travers de coopération et d'échange avec les industriels et les universitaires.
- Une permanence du dispositif.
- Le respect du cadre juridique de la loi française et du droit international.

- La mobilisation et l'implication constante des utilisateurs des SI.

La conduite opérationnelle de la LID comporte deux volets : un volet spécialisé avec le CALID, en lien avec les opérateurs, et un volet opérationnel avec effet sur les réseaux qui est en contact avec les commandements opérationnels. Le volet offensif opération cybernétique y est lui mentionné, très centralisé et sous contrôle du plus haut niveau stratégique.

On y trouve également la notion de Renseignement d'Intérêt CyberDéfense, le RIC, qui permet d'extraire les informations utiles du milieu du cyberespace (ex : nouveau virus, la forme du réseau ennemi etc).

D'une façon globale, cette doctrine pose les principes des opérations dans le cyberespace, mais avec une mise en oeuvre propre à chaque armée. C'est l'officier général Cyber qui en final donne les directives, on peut citer par exemple les Groupes d'Intervention Rapides (les GIR) gérés par le CALID, mais aux ordres de l'OG Cyber.

Les logiques de milieux :

Les différents Etats Majors ont présenté leur vision des spécificités de leur Armée dans le cyberespace. Le cyberespace est un milieu propre, avec une stratégie qui en découle pour le contrôle des autres milieux. Le contrôle du Cyberespace consiste à maîtriser son exploitation pour garantir la continuité opérationnelle, en vue de priver l'adversaire de cette possibilité. Ainsi, dans le Cyberespace, la logique du milieu est un préalable à la logique du soutien, et qui implique une unicité du contrôle et du commandement.

Sur le domaine aérien, face à la globalité de la problématique, il a été rappelé que les maillons faibles des systèmes d'armes sont les systèmes industriels qu'il convient de maitriser, et les systèmes de commandement, et que le soutien et la protection aux systèmes de combat doivent s'opérer quelques soient les élongations. La nécessité d'intégrer des briques technologiques issues du civil obligent à intégrer la sécurité dans les systèmes d'armes ou d'information, dès en amont dans leur conception, en impliquant tous les acteurs étatiques et industriels. L'Armée de l'Air doit également pouvoir conduire des activités pour intervenir militairement dans le cyberespace, afin de garantir l'action des Forces aériennes, et s'assurer de l'état de Cybersécurité de ses missions essentielles, ce qu'elle met en œuvre dès à présent.

Sur le domaine maritime, on constate une impossibilité d'embarquer de nombreux experts SIC sur un bateau ou un sous marin. Ils doivent donc rester en soutien en base arrière, accentuant la dépendance envers les liens de transmissions mer/terre, les données des attaques Cyber devant être collectées et transmises à terre pour une étude plus approfondie, ce qui pose un problème pour les sous-marins nucléaires. On observe une prise en compte de la dépendance et de la vulnérabilité aujourd'hui avec les SCADA embarqués qui conditionnent la navigabilité des navires (sur des fonctions parfois annexes comme la ventilation). La formation des personnels reste donc une priorité, et doit s'effectuer entre autres au travers d'exercices Cyber.

Enfin sur le domaine terrestre, on observe des caractéristiques communes avec les autres Armées aux niveaux stratégiques et opératifs, mais avec une limite apparente à partir du niveau des GTIA et

au dessous, où les spécificités du milieu deviennent plus marquées. Notamment avec la numérisation du fantassin (FELIN), au sein d'une multitude d'acteurs interconnectés, où les barrières des réseaux sont retirées progressivement pour une meilleure efficacité. L'infovalorisation du champ de bataille s'appuie en effet sur les échanges de communication entre systèmes, parfois automatisés, pour décider et agir plus rapidement, les anciens systèmes étant progressivement intégrés dans le futur Système d'Information des Armées (SIA), qui reliera en temps réel tous les systèmes d'information à chaque niveau, et interarmées. La formation de l'homme est également mise en avant, afin que les bons réflexes en cas de problèmes cyber soient appliqués, et qu'une habitude de non dépendance à l'égard de systèmes techniques non opérationnels (Facebook, mails privés etc) soit cultivée, en gardant toujours l'homme au cœur de l'action.

Les menaces et les seuils de déclenchement :

Une menace des sécurités des systèmes d'information qui peut être protéiforme, permanente et évolutive, est une composante du risque, ce dernier se mesurant par une menace, une vulnérabilité et un impact. Mais la menace est biaisée par la perception que l'être humain en a, et l'imprévisibilité de l'homme notamment en cas de gestion de crise. Les vendeurs de solutions de sécurité orientent leur discours en fonction de certaines menaces, en fonction de leurs intérêts. En effet, selon ces acteurs, il y aurait eu 20 millions de codes malveillants en 2013, mais cela contient des déclinaisons d'une même souche de virus, il faut regarder ce qui est sous jacent et ce que recouvre vraiment la réalité. Il convient donc d'être prudent face au discours anxiogène courant actuellement, porté par les entreprises de sécurité. Les attaques, si elles ne sont pas nouvelles, sont de plus en plus élaborées et amplifiées, leur typologie n'ayant pas changé radicalement en 2013. Et il reste l'homme, qui peut toujours être le maillon faible. Pour un système d'information donné, la menace sera toujours composite, incluse dans une chaine d'attaques adaptée à son environnement. Elle exploitera toujours majoritairement les vulnérabilités classiques, contournables par une hygiène comportementale simple. Seules 5% des attaques sortent de ce cadre et sont précisément ciblées, ayant nécessité des moyens de développement importants par des équipes spécialisées.

Concernant les seuils de déclenchement d'une riposte, le pouvoir politique au travers du député M. Rihan Cypel, invité à préciser la position politique française le 8 octobre 2013 lors du colloque « le droit et l'éthique face aux défis de la Cyberconflictualité », avait sollicité les organisateurs du CREC pour proposer des éléments de réponse.

Selon S.A Baker, le droit serait une machine à bloquer les militaires, l'encadrement normatif toujours plus dense entravant leur action. Toutefois, selon Didier Danet, il est en fait un levier pour l'action à partir du moment où il lui sert d'appui, et légitime le recours aux cyberattaques. Ainsi Harold Koh, conseiller juridique du ministère des affaires étrangères U.S, a défini clairement la position des Etats-Unis sur cette question à Fort Meade le 15 septembre 2012, en indiquant que le droit international s'applique au Cyberespace qui de fait n'est pas un espace de non droit, que la technologie permet maintenant d'identifier les auteurs des attaques et qu'ainsi ils seront poursuivis, que les Etats hébergeurs d'actions menées sur leurs instructions, sous leur direction ou sous leur contrôle « par procuration » sont tenus pour responsables. Il va même plus loin en indiquant qu'une cyber-attaque est une agression armée si elle produit des effets comparables à ceux d'une arme classique (dommages aux personnes ou aux biens), que la riposte peut être préventive en cas de menace

imminente, et que la notion de seuil doit rester floue, la seule question importante étant de savoir si la riposte est nécessaire et proportionnée. Léon Panetta quant à lui postule que si une attaque paralysante (crippling attack) est lancée, le peuple américain sera protégé selon les directives données par le Président, ce qui offre une marge de manœuvre politique plutôt large.

Il apparait dès lors que la position des Etats-Unis sur cette question, au travers de leurs déclarations et postulats juridiques, montre clairement une volonté de vouloir agir à leur guise, sans définir précisément les seuils de riposte et déclenchement pour garder toute opportunité pour l'action, par interprétation de façon extensive des conditions de légitime défense à la suite des attentats du 11 septembre 2011, et ainsi mener des opérations militaires dans des conditions où l'emploi de la force armée ne va pas forcément de soi au regard de la Charte des Nations Unies. Se pose alors la question de la volonté politique de la France sur ces mêmes questions, et sur la politique industrielle qui vient en support, et plus précisément sur les intérêts souverains que notre pays souhaite sanctuariser.

Les menaces au travers de cas concrets :

Les menaces sont aujourd'hui réelles : de la prise de contrôle d'une voiture, du tracking system d'un bateau, ou d'un avion au travers des protocoles de contrôle non sécurisés, elles sont multiples sur les systèmes et les flux logistiques. Les attaques peuvent être opérées au travers de l'informatisation des systèmes, de leur interconnexion, ou par la réutilisation des technologies civiles par les militaires sans adaptation préalable. S'y rajoute une complexité croissante des logiciels, les lignes de code explosant en nombre dans les systèmes en réponse au besoin de disposer de logiciels plus fiables et plus performants. Il faut noter cependant que la prise d'un contrôle d'un système nécessite d'accéder à un médium intégré au réseau, autrement dit qu'il faut une connexion « on air » légitime et autorisée pour accéder au cœur d'un système. De ce fait la croyance en la prise de contrôle d'un système par le simple envoi de signaux est, dans l'état de nos connaissances techniques, fausse, ne permettant que de brouiller un système et non pas d'en prendre le contrôle.

De plus, les attaques sont pour la plupart non intentionnelles, les ¾ étant favorisées par des négligences humaines. S'y rajoute le fait que 80% des fuites de données trouvent leur origine dans l'action d'un individu disposant d'un accès légitime et autorisé à ces dernières, montrant dans les deux cas que c'est l'humain la première faiblesse d'un système. La dissuasion, le contrôle et la pédagogie sont donc des solutions à mettre en œuvre, intégrées dans une approche globale de la sécurité. Malgré tout, l'externalisation géographique du stockage des données (délocalisation) augmente la non maîtrise des environnements critiques, laquelle est difficilement évitable pour de nombreuses structures de taille petites ou modérées, pour des raisons évidentes de coût.

En vue de contenir ces risques au sein de l'environnement de Défense, la DIRISI gère le plus grand réseau Français, avec des dizaines de milliers de serveurs et des centaines de milliers d'ordinateurs, et avec une interconnexion croissante des systèmes. Le cloisonnement physique et logique des différents niveaux de confidentialité reste obligatoire, mais complexifie la gestion, la pression pour une simplicité plus grande obligeant à des choix parfois générateurs de risques (ex : Intradef et Internet sur le même poste de travail). De surcroît ces réseaux traditionnellement cloisonnés doivent de plus en plus communiquer, à l'instar des procédures en matière d'exportation de systèmes

d'armement, où l'échelon supérieur de classification doit pouvoir communiquer avec un échelon inférieur dans un souci d'efficacité.

La doctrine de la DIRISI repose sur une analogie entre la guerre urbaine et le monde de la Cyberconflictualité : l'ennemi est là, présent, mais invisible ou fondu dans la masse, pouvant surgir à tout moment. Il ne s'agit plus de se réfugier derrière un mur et de se défendre contre l'adversaire au dehors, mais bien d'employer des procédures de défense en profondeur associées à une action réactive, cette dernière étant mise en œuvre par le CALID.

Un grand oublié de la réflexion en CyberDéfense est le Renseignement, lequel revient en force depuis que l'on glisse vers une Défense active, laquelle se substitue à la doctrine ancienne de la protection. Il est en effet nécessaire d'identifier l'origine des attaques, et d'évaluer les capacités de l'adversaire, ces deux actions étant les missions par excellence du renseignement. Ce qui revient à intégrer les RIC, renseignements d'intérêt Cyber et le ROC, renseignement d'origine Cyber, les deux étant complémentaires tout en étant de nature différente. Le RIC à l'instar du renseignement d'intérêt Défense, vise à user de tout type de capteurs en vue d'identifier les menaces d'origine cyber, intégrant les moyens classiques de la collecte d'informations ouvertes et fermées. Le ROC en revanche se concentre sur les sources ouvertes du monde cyber, à l'instar de la collecte de la NSA (PRISM), et est confronté au problème inverse, c'est à dire la surabondance d'informations (information overload) associée parfois à la désinformation, et qui nécessite un important travail de traitement. Cette prise en compte de ces deux types ne bouleverse pas le métier de l'analyste qui verra seulement ses sources et ses outils augmentés. De ce fait le cycle du renseignement en tant que processus d'orientation, de recherche, de traitement, d'exploitation et de diffusion demeure inchangé, la CyberDéfense se trouvant en effet intégrée à la méthode de travail classique de l'analyste. Ainsi, le RIC n'est pas issu du ROC, mais tous deux sont exploités dans l'évaluation des menaces.

La formation Cyber au sein des forces :

La formation des cadres des Armées étant au cœur des préoccupations de la Défense, les expertises demandées en Cyber au sein des forces sont nombreuses et complexes. Il devient donc nécessaire d'adapter la formation militaire, ou bien recruter des profils techniques pour des carrières courtes afin de disposer d'un personnel continuellement formé aux dernières innovations en la matière. Mais cette dernière solution ne convient pas pour assurer une résilience en temps de crise, un historique au sein des forces étant le gage d'une bonne résilience. Un modèle de carrière Cyber trouve donc toute sa place au sein du dispositif de Cyberdéfense, dans le sens où la capacité de raisonner sur un temps long est primordiale pour l'encadrement, qui ainsi connaîtra ses subalternes, du soldat à l'officier, et saura de fait être plus réactif en particulier en matière de gestion de crise. A cette nécessaire fidélisation des personnels formés en matière cyber s'ajoute l'impératif d'éviter le syndrome « désert des tartares », aucune attaque cyber militaire n'ayant pas encore eu lieu, tout en assurant régulièrement une formation continue sur les nouveaux risques, à l'image d'autres professions confrontées à ces évolutions.

Les formations initiales des écoles militaires prennent en compte la dimension cyber dans la formation des élèves officiers. Du tronc commun, aux options plus spécialisées, on constate que le

domaine cyber devient une opportunité pédagogique pour l'enseignement de l'informatique, avec la pratique d'exercices de conflits cyber, intégrant les dimensions lutte Défensive (LID), mais aussi Offensive (LIO).

Cette dynamique est profondément interarmées et, conformément aux recommandations du livre blanc, aucune composante des armées françaises n'est dépourvue de programme en la matière, tant en matière de recherche que de formation de ses personnels. Ainsi par exemple, la Gendarmerie a déjà pris en compte la formation de ses élèves officiers en Cybercriminalité, domaine profondément imbriqué avec la Cyberdéfense. C'est une nécessité, pressée par le fait que la plupart des objets communicants de demain seront traçables et donc sanctuarisés. Le gendarme de demain devra donc pouvoir tracer ces objets dans l'espace immatériel, dans le Big Data ou bien directement, ce qui nécessitera une métamorphose ou une adaptation rapide de la formation dispensée.

Pour les carrières de demain, il devient donc nécessaire d'attirer des compétences Cyber vers le monde militaire, et de rendre les métiers attractifs avec une progressivité dans le temps. Il convient dès lors de réfléchir à un plan de carrière Cyber, et à une formation adaptée, souple, intégrant les dimensions techniques, éthiques et juridiques avec une certaine structuration des types de formations possibles, de la simple hygiène cyber à la gestion de crise. Les emplois sont encore à préciser, mais devront couvrir tout le spectre des missions militaires, sur les théâtres d'opération (officier LID, protection des SIC déployées localement, renseignement et accompagnement LIO de l'action militaire). L'enjeu principal au final étant de disposer continuellement de personnels formés et de haut niveau, personnels qui seront capables de comprendre une menace et de la restituer en des termes simples aux décideurs, et s'appuyant sur un modèle plutôt centralisé favorable aux synergies,. Maintenir la qualité des formateurs est aussi primordial, et conditionnera à moyen et long terme la capacité des institutions à former des professionnels adaptés à ces nouvelles menaces.

<u>Quelques éléments de synthèse complémentaires à ce séminaire:</u>

A. Il apparait que l'interconnexion des réseaux est un élément de faiblesse dans les réseaux numériques utilisés. Si l'interconnexion des réseaux militaires vers le monde civil (Internet notamment) est connu, reste plus problématique l'interconnexion avec les réseaux interalliés où les capacités de contrôle se heurtent à la question de confiance et de maîtrise technologique.
B. Une volonté politique de protection des intérêts nationaux dans le cyberespace se doit d'être clairement et rapidement précisée par le pouvoir politique, afin tout d'abord de définir le cadre de notre Cyberdéfense, et les seuils et graduation de la riposte nécessaire en représailles aux agressions sur nos intérêts, mais aussi de déterminer la politique industrielle qui vient en support (souveraineté sur des composants critiques (OS), sur des logiciels ou des réseaux).
C. Sur la réserve citoyenne et opérationnelle, aujourd'hui l'effort porte sur la sensibilisation des entreprises françaises à la menace Cyber, sensibilisation pour laquelle la réserve citoyenne est en appui. Si les GIR sont le fer de lance du CALID, il reste que les experts opérationnels sont rares et difficiles à trouver. Il semble donc nécessaire de développer une réserve opérationnelle se basant sur un vivier d'experts techniques en entreprises, et les former à des interventions possibles au profit de la Défense.

D. La plupart du temps, la faute (ou la faiblesse) humaine est la cause de nombre de malveillances. Dans le domaine de la CyberSécurité, les banques et les assurances ont développé un code de formation et de gestion des risques à la mesure des enjeux pour elles. Il pourrait être envisagé une journée d'étude sur cet aspect au bénéfice des Armées, avec le soutien de ces métiers, sur la question de la formation humaine à la CyberSécurité.

Gérard de Boisboissel

CREC Saint-Cyr