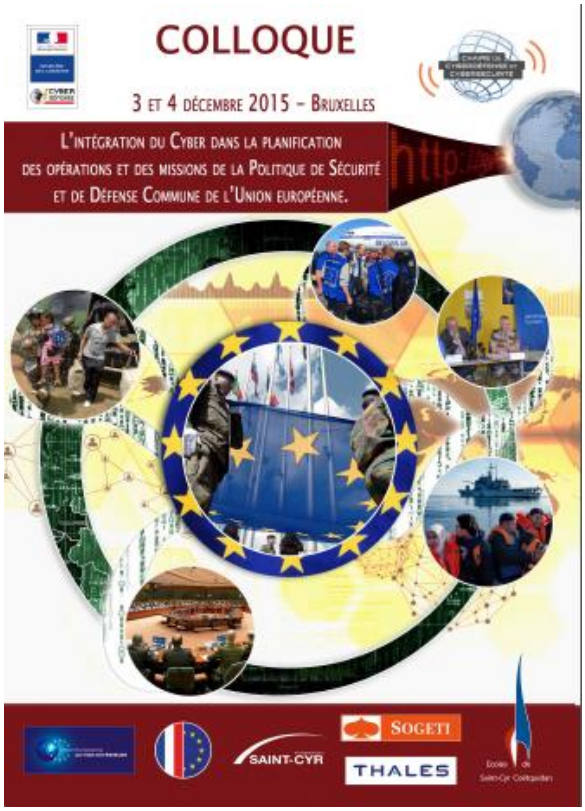
L'intégration du Cyber dans la planification des opérations et des missions de la Politique de Sécurité et de Défense Commune de l'Union européenne.

Compte rendu du colloque des 3 et 4 décembre 2015 à Bruxelles,

organisé par la chaire cyberdéfense et cybersécurité Saint-Cyr / Sogeti / Thales

dans les locaux de la Représentation Militaire Française.



L'idée d'une politique de sécurité et de défense n'est pas nouvelle pour l'Union Européenne. La volonté de défense commune est introduite par le traité de Maastricht des 1992 dans son article 17 du TUE (traité de l'union européenne).

L'omniprésence des systèmes automatisés de traitement de l'information et la généralisation de leur interaction a pour conséquence un renforcement de la politique de défense de l'union européenne. Cette dernière est présente dans les activités nationales quotidiennes et lors des opérations extérieures. L'action de défense européenne se base sur une action commune (PSDC : politique de sécurité et de défense commune).

La PSDC de l'UE doit affronter les menaces liées à l'expansion de l'espace numérique, comme celles de la cyberattaque ou de la cybercriminalité. Elle doit s'adapter et développer de nouveaux outils contre ces menaces. Le conseil européen s'est ainsi doté les 17 et 18 Novembre 2014 du document « EU Cyber Defence Policy Framework », détaillant les priorités pour intégrer au mieux la dimension cyber dans les mécanismes de coopération, de formation et de gestion de crise de l'Union européenne.

Le colloque du 3 et 4 décembre 2015 a eu pour finalité de retracer les expériences des armées nationales en matière de planification et de conduites des opérations ainsi que des raisonnements des partenaires civils et industriels pour les solutions technologiques et organisationnelles.

Dans cette optique, fut élaboré et présenté un scénario prospectif de planification d'une intervention de l'UE en dehors de ses frontières, à proprement parler le scénario pose le problème d'une réaction de défense vis-à-vis d'une probable cyberattaque en représailles de son action sécuritaire dans le pays fictif de SURINIA en conflit avec les forces rebelles extrémistes de CELEGO. Ce scénario, qui fut précédé d'une introduction au colloque présentant la stratégie et l'intégration du cyberespace dans la politique de cyberdéfense européenne par Mr Philippe Setton, ambassadeur et représentant permanent de la France au Comité politique et de sécurité de l'UE (COPS) puis par Mr Francois Rivasseau chargé de l'espace et de la sécurité du numérique SEAE (Service Européen pour l'Action Extérieure), ce dernier rappelant que la volonté de l'Europe est de ne pas être en dessous des Etats membres pour les questions de cybersécurité et de cyberdéfense.

On retiendra de ce colloque la volonté assumée d'organiser, de perfectionner et de financer la cybersécurité européenne tant du point de vue des entreprises privées, publiques, de l'armée que des représentants politiques européens.

Pour autant que cela peut paraître difficile dans une UE où 28 Etats aux capacités techniques et technologiques bien inégales doivent coopérer, et en effet il en est ressorti que la cybersécurité ne doit jamais se faire au prix de l'efficacité économique (François Rivasseau), but pour lequel est né et s'est élargi l'UE. Mais bien que les opinions puissent diverger à l'exemple historique d'une idée de défense commune (depuis le rejet de la CED (communauté européenne de défense) en 1949) et bien qu' « il faudrait une défense européenne avant d'avoir une cyberdéfense européenne » (Amiral Arnaud Coustillère) il ne faut pas pour autant enterrer cette idée qui est prise de plus en plus au sérieux comme l'a montré le colloque.

Mr Philippe Setton introduit bien la séance quand il notifie que l'UE en est à ses débuts en matière de coopération opérationnelle cyber, il rappelle en effet que c'est de novembre 2014 que date la décision communautaire d'intégrer l'outil cyber dans les travaux de défense européenne, « un phénomène récent qui va encore se développer », puis il fait référence à la responsabilité qui incombe aux Etats » qui définissent leur stratégie, leur capacité d'action pour ainsi définir plus justement celles de l'UE en matière de cybersécurité.

Phase 0

Une première phase de compréhension va développer le cas d'une intervention militaire d'un pays européen : l'exemple français, notamment l'intégration du cyber dans la planification des opérations militaires où le lieutenant-colonel Victor Le Bihan, officier anticipation, état-major des armées,

cellule CYBER, présente les différents échelons impliqués, indiquant que la planification des opérations Cyber suit le même cycle que celui des opérations cinétiques.

Phase 1

C'est au tour de la place du cyber dans la planification des opérations militaires de l'UE d'être développé, avec pour commencer la prise en compte des questions de cyber défense dans la planification des opérations de la PSDC, c'est-à-dire selon le lieutenant-colonel Gernot Schwierz l'élaboration d'une architecture, d'une structure adaptée aux défis militaires, techniques, technologiques et juridiques. Importance est donnée à l'évaluation des menaces avec l'évaluation des risques et la sensibilisation cyber (cyberawareness) qui permettrait à travers les renseignements (intelligence) la protection, les règlements et procédures : la prévention, les formations techniques : la détection, et la coopération politique et militaire : la réaction. La planification est donc ce qui permet de concevoir une réponse adaptée en amont de la crise en développant des outils de réaction. Le colonel Heinrich Krispler avait auparavant rappelé que la cyberdéfense n'est pas que protection et réaction, mais aussi anticipation et préparation, avec un spectre qui couvre un champ plus large que la simple sécurité physique des réseaux : organisation, entrainement etc.

Sur le plan juridique, la capitaine Pascal Brangetto précise que la défense préemptive est autorisée en droit international, autrement appelée « last window opportunity », qui permet d'attaquer juste avant que l'autre ne le fasse. La notion de défense préventive restant quant à elle plus difficile à codifier en cyberdéfense.

Phase 2

La place du cyber dans la planification des missions civiles de l'UE.

Un représentant du CERT UE monsieur Emilien Le Jamtel, explique quant à lui ce que sont les CERTs divisés en 65 organisations pour 13 secteurs de recherche (aspect finances, administration, sécurité etc.), des groupes d'experts dont la mission est de maîtriser les techniques cybernétiques afin de les fournir à l'UE pour combattre les menaces (spear phishing, infection de sites etc.), et contrer les attaques de groupes tels que APT28, 29, ou SNAKE. C'est donc un partage de l'information pour évaluer l'origine, la gravité de la menace et les réponses possible à apporter.

Le point de vue juridique est aussi exposé, avec pour départ une présentation globale de l'encadrement juridique des missions extérieures civiles présentée par monsieur Eric CHABOUREAU, lequel précise dans son exposé que des personnels contractuels pourraient être détachés pour la protection cyber des missions civiles.

S'ensuit l'intervention de maître Cécile Doutriaux (cabinet DOUTRIAUX-VILAR et Associés) qui témoigne de la lutte contre la cybercriminalité, notamment des attaques contre les infrastructures critiques tant au niveau national qu'international, nécessitant de fait la coopération entre juristes et experts informatiques, entre policiers et gendarmes et de même entre Etats dans le cadre de perquisitions de données qui supposent elles-mêmes des accords « de courtoisie ». Cette coopération se révèle complexe, les échanges d'informations pouvant être refusés entre Etats membres qui parfois s'agressent entre eux. Pour rappel, Europol (police européenne) et Eurojust (justice européenne) travaillent -bien que limités- à la croissance de ces coopérations. La France par ailleurs est en avance en termes de responsabilisation des géants de l'internet ou des opérateurs, pour les uns empêcher l'expansion de la propagande du cyber-califat et pour les autres l'obligation de rendre comptes des problèmes techniques majeurs. La cybersécurité se construit donc de même juridiquement, car faute d'être des directives contraignantes, les résolutions européennes devant satisfaire le plus grand nombre « portent atteinte à la crédibilité de l'UE ».

Les acteurs du cyberespace

Le colloque aborde ensuite la question de la place des acteurs du cyberespace dans les opérations et missions extérieures de l'UE. Mr Michael Sieber (chef de l'unité de la supériorité de l'information au sein de l'Agence Européenne de Défense (AED)) rappelle le rôle de l'AED : collecte de renseignement militaire, protection des forces sur les théâtres d'opération grâce entre autre à sa cyber-sensibilisation.

Au tour de Mr Grégoire Germain de préciser l'action de THALES, dans l'écoute des réseaux qui met à contribution des équipes de réparations face aux intrusions et des solutions de détection notamment par l'étude comportementale des attaquants qui passe aussi par de la recherche en open source et permet d'analyser, d'identifier le type d'agresseur, ses techniques usuelles pour mieux pour améliorer la cyber-résilience (capacité à remettre en disponibilité un réseau).

Mr Andrus Padar (commandant de l'unité de cyberdéfense, League estonienne de défense) rappelle quant à lui la possibilité d'utiliser des volontaires expérimentés, jusqu'à parler d'une cyber-réserve) dans l'usage de l'espace numérique pour une aide supplémentaire en termes de sécurité (objectifs

de réaction, soutien et de prévention). Pour autant il en précise les limites car tous ne peuvent être impliqués dans le cas par exemple des Anonymous (impératif de confiance exigé).

C'est à Mr Stéphane Taillat et à l'Amiral Coustillère qu'il appartient d'achever cette première journée. Le premier détaille le principe de la défense active en cyber où il est possible de se référer à des doctrines anciennes comme celle de Clausewitz qui démontre que toute stratégie demeure possible malgré la diversité et la rapidité croissante des attaques par le biais d'un continuum de postures stratégiques (possibilité de dissuader, bloquer, d'user de la « déception » ou tromperie etc.), et que somme toute la Défense n'est qu'une série de coups habiles portés à l'attaque de l'adversaire. Néanmoins il est également possible en cyberdéfense d'attirer l'ennemi dans ses filets afin de le cerner puis de le détruire. Le second rappelle en sa qualité d'officier général cyber que l'espace numérique est bel et bien un espace de confrontation et de combat, au cœur des autres espaces, et qu'il nécessite une approche globale, nécessitant d'intégrer des personnes formées dans les opérations complexes au cœur de cet espace.

Les formations

La journée du 4 décembre s'inscrit, elle, dans la problématique de la formation, de ses besoins et de ses offres. En effet les experts cybers se révèlent être une ressource rare et l'interopérabilité des réseaux d'experts demeurent encore imparfaite.

Le colonel Nurenberg (président de l'EUMCWG/HTF) soumet l'importance de l'excellence opérationnelle par le biais de l'organisation d'un grand marché européen de la formation d'experts cyber, ceci ayant pour terme l'affirmation d'une cyber-souveraineté (idéal de fiabilité et de crédibilité).

Le Commandant Jeff Vandromme (du département stratégie du ministère de la défense belge développe quant à lui la planification d'une stratégie cyber belge qui comprend d'ores et déjà les partenariats d'acteurs européens cybers (AED, CERTs UE, CSED etc.) une stratégie de cybersécurité composée de trois pôles : cyberdéfense, « cyber intelligence », et contre-offensive cyber. Il prévoit la possibilité d'une organisation cyber mixte entre militaires et civils.

Mr Symeon Zambas (du collège européen de sécurité et de défense (CESD)) montre que la formation au sein du CESD est reconnu par tous les Etats de l'UE et en détaille les partenariats (AED, ENISA, etc.), ses composantes, dont notamment l'échange d'étudiants ou cadets militaires dans le cadre d'un « Erasmus militaire ».

Le LCL Pierre-Arnaud Borrelly conclut cette première phase dédiée aux besoins en formation cyber par une intervention montrant comment la France est passée du concept à la capacité opérationnelle, et montre que le J5 déjà intégré par la France dans les mécanismes de planification, devra prochainement l'être au niveau européen.

S'en suit une session dédiée aux offres de formation Cyber proposées ou proposables en Europe : la présentation de Mr Olivier Bartheye (enseignant chercheur au CREC Saint-Cyr) qui évoque l'adaptation croissantes des modèles à des types plus ou moins graves et élaborés d'attaques (partie plus technique).

Monsieur Hannes Möllits a de son côté présenté le programme de formation que propose le Baltic Defence College en Cyberdefense en langue anglaise, et notamment les différents niveaux de formation ouverts aux civils et aux militaires, et la nécessité de créer une synergie entre les experts du monde Cyber, et les opérationnels mettant en oeuvre la planification.

Le Lieutenant-colonel Paulo Nunes (MNCDE&T Project Manager) développe un véritable curriculum dans la formation cyber par la compréhension, l'étude des utilisateurs cyber (individus), du droit cyber (juristes cyber), du leader cyber (opérationnel), de la cybersécurité (spécialistes) et de la cyberdéfense (guerriers cybers).

Revient à Mr Didier DANET de conclure le séminaire par le questionnement de la valeur des diplômes, formations, stratégies et stratégies de formation des actuels et futurs acteurs cyber. Il soulève ainsi le fossé croissant entre les experts et les militaires où apparaît des incompréhensions de langage à mesure que les missions deviennent de plus en plus techniques, d'où la recherche nécessaire d'une plus grande complémentarité dans la formation. Mr DANET questionne enfin les stratégies face à des choix de préparation à la gestion de crise qui se veut actuellement conventionnelle alors que la crise est par définition non-conventionnelle. S'ouvre ainsi des possibilités vastes de stratégies, de planification d'actions dans le cyber espace (choix de l'intrusion acceptée si contrôlée, action dans un milieu contaminé) que les futures promotions d'experts en opérations devront nécessairement prendre à leur compte.

Les élèves officiers Barthélemy CANAL, Rémi DEYDIER, Nicky DORVAL, Gautier GRIALOU,

du 2ème bataillon de l'Ecole Spéciale Militaire de Saint-Cyr,

le 9 décembre 2015.


CHAIRE DE
CYBERDÉFENSE ET
CYBERSECURITÉ