Ce 12 février 2015, le cercle de cybersécurité de Défense et Stratégie organisait les Premières Rencontres Parlementaires sur la cybersécurité et le milieu maritime. Ce colloque s'inscrit bien dans les autres billets de la semaine.

Ainsi, la formation des militaires (Cf. Rapport du 4 février 2015 et mon billet du 15 février 2015 sur la formation) évoque la montée en puissance de cette « quatrième armée ». La bataille dans le champ des perceptions a été rappelée par le CEMA (Cf. Audition du CEMA, 3 février 2015 et mon billet du 15 février 2015 sur les missions intérieures).

Retour sur la stratégie d'influence et la contre-propagande

Concernant la contre propagande (Cf. Article de La Croix du 10 février 2015 et mon billet du 8 février 2015), des éléments complémentaires à mon billet du 1er février peuvent être apportés.

En me référant aux attentats de Copenhague, il est bon de savoir que le collège militaire royal danois étudiait concrètement depuis 2006 la lutte contre la propagande djihadiste. Il a eu l'occasion de présenter régulièrement ses travaux aux groupes de travail de l'OTAN sur les opérations militaires d'influence, les opérations sur l'information et la communication stratégique, groupes où je représentais la France. Ils ont fait l'objet de comptes rendus détaillés en France restés sans beaucoup d'effets. Combien d'études concrètes, à vocation opérationnelle, ont été conduites en France durant la même période alors que nous combattions Al Qaida et les Talibans ?

Pour rendre plus précis et corriger mon billet de la semaine dernière (Cf. Mon billet du 8 févier 2015), un officier général a été depuis peu chargé de cette fonction « Influence » qui a été pleinement intégrée dans la planification des opérations. Le processus de l'influence en soutien aux opérations est (heureusement) désormais pris en compte.

Le CIAE monte en puissance pour analyser et comprendre les phénomènes de rumeur et de propagande. La capacité à concevoir une stratégie d'influence devient peu à peu une réalité pour contrer la propagande notamment djihadiste avec des militaires experts dans ces domaines.

De la cyberguerre en milieu naval

La menace cyber était considérée comme essentiellement terrestre. Pour l'OGX « cyber », le vice-amiral Coustillières, il y a de grandes similitudes entre l'espace maritime et le cyberespace. Les « Livre blanc » depuis 2008 ont largement engagé le débat sur la cybersécurité. Un milliard d'euros lui sont dédiés mais sont en cours de réévaluation.

Dans le secteur naval, militaire et civil, quatre types de risques peuvent être distingués : déviation des navires sinon détournement, propulsion, gestion de la cargaison, communication et liaison à bord. Les menaces sont d'abord crapuleuses, avec de fortes implications financières, sans exclure le risque terroriste. Pour le coût de 2 000 dollars, un virus russe a été la cause de 180 millions de dollars de réparation pour une société américaine en 2013.

Les navires se croyaient jusqu'à présent à l'abri en haute mer sauf dans le cas d'agressions

extérieures, plutôt rares. Or, aujourd'hui, les bâtiments civils et militaires sont pratiquement entièrement pilotés par logiciels. Dès lors qu'ils se connectent à internet, la vulnérabilité s'installe. En outre, la connexion des ordinateurs portables se reliant aux systèmes à bord font des hommes des chevaux de Troie. Les attaques sont désormais internes.

De la préparation opérationnelle de la Royale

La marine s'est préparée à cette guerre cybernétique. Il lui faut apprendre à combattre ce nouvel ennemi. Les menaces sont accrues par les connections de plus en plus grandes. La présence de plus en plus de composantes civiles dans les systèmes militaires, pour des raisons souvent budgétaires, créent des vulnérabilités qui permettent aux attaquants de préparer longtemps à l'avance leurs attaques contre des bâtiments militaires.

L'informatique est devenue le système de navigation des navires. Un bâtiment de la Royale ne part à la mer que s'il est « cyberqualifié » après une préparation dans un centre d'entraînement cyber. S'ajoute un audit régulier des systèmes pour identifier les attaques qui n'auraient pas été décelées.

La formation à la cyberguerre

Dans le cadre général de la préparation des armées à la cyberguerre, l'Ecole navale a créé sa chaire « cyberdéfense », avec l'amiral Hébrard. Elle fait suite à la création de la chaire de cyberstratégie des Ecoles de saint-Cyr-Coëtquidan (Cf. Rapport sur la formation du 4 février 2015). En septembre 2015, un master en opérations cybernétiques et gestion de crise y sera créé. L'Ecole de l'air créera sa chaire en 2015.

Enfin, le pôle d'excellence Cyber créé en 2014 met l'excellence militaire et cyber au service des entreprises (Cf. Le pôle d'excellence Cyber). 13 conventions ont été signées avec des entreprises.

Les armées sont en pointe et le domaine cyber apporte de nouvelles perspectives. Une réelle stratégie d'influence devra cependant être élaborée pour donner du sens à la contre-propagande, y compris à travers le cyberespace qui ne peut être dissociée de cette stratégie.