Reportage exclusif au sein d'une réunion TIDE Sprint de l'OTAN à Saint-Malo

Sur les terrasses bondées de vacanciers cette première semaine de vacances de Pâques, les hommes en costume sombre discutant en anglais faisaient tache sous le soleil brillant de Saint-Malo. Seuls des avertis qui tendaient l'oreille vers leurs conversations où il était souvent question de « Norfolk » auraient pu s'imaginer que se tenait non loin de la ville intra-muros, la 29e réunion d'un *Think-tank for Information Decision and Execution Superiority* (TIDE) de l'OTAN.

© Christina Mackenzie

Un cyberespace plus stable pourrait améliorer la capacité de l'OTAN à conduire des opérations dans ses domaines traditionnels.

Retour en arrière : en juin 2016, l'OTAN décida, lors du sommet de Varsovie, que le cyberespace devait être « *un domaine d'opérations dans lequel l'OTAN doit se défendre aussi efficacement qu'elle le fait sur la terre, dans les airs et sur la mer* ». L'Alliance atlantique est donc en train de revoir non seulement ses doctrines mais aussi la façon dont ses 28 nations membres interagissent ensemble dans ce domaine. Alors, même si la cyberdéfense est loin d'être le seul sujet abordé lors des sessions de travail TIDE Sprint (« *le début du voyage technologique* ») organisées par l'OTAN deux fois par an, au printemps en Europe et en automne aux États-Unis (la 30e réunion a eu lieu entre le 23-27 octobre dernier à Virginia Beach... mais nous n'y étions pas invitée !), c'était clairement le sujet phare de la réunion qui a eu lieu pour la 1re fois en France entre le 3 et le 7 avril 2017.

« *Nous devons développer des normes et prendre des mesures de confiance pour favoriser un cyberespace plus stable pour la communauté internationale* », déclara l'Amiral allemand Manfred Nielson, adjoint au commandant allié Transformation de l'OTAN, lors de la séance plénière du 4 avril. « *Ceci améliorera notre capacité à conduire des opérations dans nos domaines traditionnels* », dit-il. Mais, comme prévenait la veille le Général Dominique-Marie Pinel, adjoint spécialisé Transformation-Interopérabilité, à la direction de la stratégie de la Direction générale de l'armement, « *il faut que les solutions soient faciles à utiliser car les situations sur le champ de bataille ne sont pas les mêmes que dans un laboratoire* ».

L'Amiral Nielson expliqua à son auditoire d'environ 300 experts, que le 6 décembre 2016, l'OTAN et l'Union européenne avaient adopté une dizaine de mesures pour encadrer la lutte contre les menaces hybrides et s'étaient mises d'accord pour participer ensemble à des exercices, tandis qu'en février les ministres de la défense avaient approuvé une feuille de route pour 36 mois découpés en périodes de 12 mois. « *Mais les processus sont lents* », reconnut-il « *et nous sommes limités par des considérations financières* ». Et le fait est, comme le souligna le colonel François-Régis Boulvert, Section Head NNEC & Plan chez NATO ACT, que « *chaque nation est maître et se débrouille, mais quand on est en exercice, ça ne marche pas* ».

D'après l'amiral Nielson, l'Alliance avait deux gros défis à relever : d'abord trouver le bon équilibre entre les efforts cyber faits par les nations – sachant que ces dernières ne voudront peut-être pas dévoiler leurs portfolios cyber – et ceux fait par l'Alliance. Et puis il faudra travailler dans l'application de l'État de droit, dans des cadres législatifs qui n'ont pas été conçus pour prendre en compte les spécificités cyber.

Il ajouta qu'il y avait 3 questions urgentes à traiter, dont la 1re est de savoir « *si l'OTAN est vraiment le bon endroit pour [traiter cette problématique cyber] car ses processus sont lents et peu agiles ?* ». La 2e est de décider si « *nous sommes prêts à embrasser l'incertitude ?* » Et la 3e de savoir si « *on anticipe correctement la menace ?* »

Hors des sessions plénières quotidiennes, il y avait un grand choix de tables-rondes dont celle qui débattait de ces questions cyber fut prise d'assaut. Tamsin Moye, scientifique du cyber au sein de la NATO Communications and Information (NCI) Agency à La Haye, souligna la complexité des questions que se posait l'OTAN : « *si l'effet* [d'une cyber-attaque] *est dans le monde physique* [prenant le contrôle, par exemple, de voitures] *est-ce que cela est une cyberattaque ou une attaque hybride ?* ». Ou : « *quelle est une réponse proportionnée ?* » Ou encore : « *est-ce qu'une cyber-attaque peut-être lancée par des acteurs des autres domaines* [terre/air/mer] *et si oui, est-ce que chacun a besoin de cyber spécialistes ?* » Ce sont ce genre de questions qui ont occupé les experts pendant toute la semaine.

Pour l'Amiral français Arnaud Coustillière, l'officier général cyber pour la France (« *et être interarmées est un élément clé pour le succès* » précisa-t-il) il ne faut jamais oublier « *qu'on ne peut pas gagner une guerre avec le cyber mais qu'on peut en perdre une avec le cyber* ». Il expliqua d'ailleurs que dans l'organisation OTAN celui-ci était placé sous J3, c'est à dire *Conduite des opérations* et non pas sous J6 *Systèmes d'opérations* (solutions/services). L'Amiral Coustillière indiqua que dans le Livre Blanc sur la défense et la sécurité nationale 2013, la France s'engageait non seulement à tripler son investissement dans le cyber pour atteindre 1Md€ mais aussi à recruter 2 000 spécialistes du domaine.

Pour Philip Lark, directeur du programme des études cyber-sécurité au George Marshall European Centre for Security Studies à Garmisch-Partenkirchen en Allemagne, « *le secteur privé a un rôle vital à jouer* ». Pour lui les réponses actuelles aux menaces cyber « *n'incluent pas suffisamment le secteur privé, en-dehors des partenariats public/privé. Les citoyens et le secteur privé sont centraux* », plaida-t-il, en rappelant que « *d'ici 2020 il y aura 5 milliards de personnes connectées, 4 trillions de dollars de revenus, plus de 25 millions d'applications, 50 trillions de gigabytes de données, et des risques de fraudes, de vols, de violations de la vie privée, et de dangers pour la chaîne logistique* ».

Ph. Lark souligna que « *même si nous trouvions les bonnes réponses au sein de l'OTAN et de l'UE, le reste du monde ne bénéficierait pas de nos réglementations* ». Il ajouta que chaque pays devait avoir dans le domaine cyber une stratégie, une politique, des règlements, des droits, des normes et des pratiques exemplaires. « *Le problème* », regretta-t-il « *c'est que tout cela est d'une lenteur glaciale* ».

Christina Mackenzie SN42 CHEAr*

A Saint-Malo, le fort du Petit Bé voit monter les grandes marées d'équinoxe. TIDE 2017 a conclu au besoin de faire face au développement rapide et inexorable du cyberespace.