Allocution de l'Ambassadeur Jean-Paul Laborde au séminaire interarmées sur « Le système d'armes Scorpion à l'épreuve de la cybersécurité » du 12 avril 2018 à l'Ecole des Transmissions

Mon général mesdames messieurs,

Nous voici de nouveau réunis ici à l'École des Transmissions pour, encore une fois réfléchir sur notre cyber défense. Le sujet qui nous intéresse aujourd'hui est particulièrement important. Notre système de communication Armée de Terre, le système Scorpion, indispensable à la coordination des différentes composantes de celle-ci sur le champ de bataille, est effectivement très performant et nous n'avons tous qu'à féliciter du travail accompli dans ce secteur, et en particulier l'Arme des Transmissions pour ce travail. Ce satisfecit hélas ne suffit pas. Il faut toujours réfléchir pour améliorer nos systèmes et les rendre de plus en plus résilients aux attaques cyber. Nos systèmes de transmission constituent, c'est certain des cibles privilégiées. Il nous est interdit de penser que les attaques cyber …c'est pour les autres, ce serait une grave erreur, ce serait notre ligne Maginot en quelque sorte, pour employer une expression militaire. Il nous faut aussi une cohérence globale entre nos différents services impliques, votre École bien entendu mais aussi le ComCyber, la DGA et tous les services, en complémentarité avec le secteur privé qui fournit les outils cyber ou informatiques.

Et je sais que nous prenons au sérieux ces menaces pour éviter ce qui est arriver voilà presqu'un an, à savoir l'offensive informatique massive survenue en mai 2017 qui a frappé le monde entier à un niveau sans précédent, paralysant des hôpitaux au Royaume-Uni ou des usines Renault en France. Les pirates ont profité d'une faille de Windows et ont bien entendu réclamé des rançons.

De plus, selon Europol, plus de 150 pays et 200 000 systèmes ont été touchés par des cyberattaques, sans distinction entre monde de l'entreprise et institutions publiques ; le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), décrivait cette attaque comme *« particulièrement virulente »*. *« Nous menons des opérations contre environ 200 cyberattaques par an mais nous n'avions encore jamais rien vu de tel »*, a appuyé le patron d'Europol. Un dernier exemple : selon une étude du cabinet de conseil PwC publié par le quotidien Ouest France, les entreprises françaises ont vu leurs pertes financières liées aux cyberattaques augmenter de 50 % en un an, à 2,25 millions d'euros en moyenne sur douze mois.

Quelles conclusions en tirer ? Que nous devons, travailler tous ensemble, secteur public, secteur privé et secteur recherche.

C'est pourquoi, j'ai la ferme conviction que la Chaire St-Cyr, Sogeti, Thalès a tout sa place ici dans la troisième composante recherche. La Chaire soutenu non seulement par le mécénat de ces deux entreprises mais aussi par son action directe à nos côtés quand cela est nécessaire tout en nous laissant toute notre indépendance sur le plan scientifique, a été établie en 2012. Elle assure le développement de la recherche en cyberdéfense et cybersécurité en lien étroit avec le Pôle Mutation des conflits mais aussi avec les autres pôles du Centre de recherche des Écoles de St-Cyr Coëtquidan, en particulier à travers des colloques et des publications. La Chaire permet, en outre, aux futurs officiers de l'Armée de Terre mais aussi aux stagiaires des trois armes et services du Ministère des Armées en scolarité aux Écoles de ST-Cyr Coëtquidan de participer au Mastère spécialisé Gestion de crise Cyber et d'être ainsi mieux préparés dans leurs fonctions futures à faire face à ces menaces. Ainsi, en 2018, elle organisera avec le CREC plusieurs colloques et participera à de nombreux évènements dont celui d'aujourd'hui.

C'est pourquoi, par exemple, sur le système Scorpion une réflexion du Centre de Recherche des Écoles de St-Cyr incline à réfléchir sur le rapport du système Scorpion à l'espace numérique qui est aujourd'hui principalement envisagé à travers le prisme technique et à une cyber sécurité comprise comme un ensemble de mesures techniques. Or, Scorpion peut aussi être envisagé comme un système sociotechnique, ce qui veut dire que sa résilience est aussi l'affaire de ceux qui seront appelés à le servir et de l'organisation qui le mettra en œuvre. Sur ces différents points, les travaux du CREC conduits avec l'appui de la chaire pourraient apporter un éclairage utile.

Enfin, je voudrai attirer ce matin votre attention sur les questions liées à la responsabilité et à l'impunité de ceux qui procède à ces attaques.

Or, il m'apparaît très important en ma qualité de Conseiller honoraire à la Cour de Cassation mais aussi d'ambassadeur d'une organisation multilatérale, que cette impunité soit combattue avec la dernière énergie. Certes, une fois éliminé le problème de la compétence juridictionnelle, il reste à s'attaquer à cette question pour l'instant quasi insurmontable de l'attribution de l'attaque à une personne, à des personnes précises ou à des organisations particulières. Car parce que c'est difficile, il ne peut pas être question de dire que c'est insurmontable. A cet effet, la recherche a toute sa place à jouer et la Chaire est prête à s'associer à toute initiative dans ce sens.

A cet égard, je voudrai vous entretenir pour finir d'un sujet qui me tiens particulièrement à cœur, celui de la coopération internationale en matière pénale pour soutenir la Cyberdéfense et de son corollaire la e-evidence ou preuve électronique.

Certes, devant ce parterre d'entrepreneurs de hauts représentants de l'État spécialisés dans la Cyberdéfense, vous pourriez penser que j'arrive de la Lune ou de Mars... ah ces juristes de droit pénal!
Il est évident que développer la Cyberdéfense et proposer une stratégie et une coopération pour protéger l'État et les entreprises contre les cyber-attaques veut d'abord dire que l'on

doit s'attacher aux questions scientifiques qui le sous-tendent. Ces éléments constituent le socle fondamental permettant effectivement de mettre en place des mesures efficaces de protection des systèmes d'armes et des éléments au cœur de l'indépendance stratégique nationale. Les entreprises telles que Thales ou Sogeti qui font œuvre de mécénat à la Chaire Cybersécurité/Cyberdéfense de St-Cyr Thales Sogeti y participent pleinement. Mais, au-delà des questions éthiques, sociologiques ou juridiques qui œuvrent pour cette protection, il faut aller plus loin, voir plus loin. Comme je le rappelais au Forum International Cybersécurité de Lille, il faut toujours garder à l'esprit que 75% des cyber attaques proviennent de groupes criminels organisés. Or, ces derniers agissent en toute impunité. Pourquoi? Si nos systèmes juridiques commencent à s'organiser au niveau national et européen, on est loin d'un consensus au niveau international. Et pourtant, première question, croyez-vous que les attaques majeures proviennent de la France et de l'Europe? Sûrement pas! Et ensuite, seconde question, croyez-vous que les uns et les autres, Communauté internationale et entreprises nous ne pourrions pas nous unir pour lutter contre le cyber crime et l'impunité qui l'entoure? Pas de condamnation des criminels, pas de progrès sur la Cybersécurité et la Cyberdéfense.
La question fondamentale est donc qu'il faut aller pour les Etats et les entreprises, au-delà des règles françaises et européennes, utiliser la coopération internationale en matière pénale et en particulier, travailler en se fondant sur la Convention de Budapest et la Convention des Nations unies contre la criminalité transnationale organisée appelée plus couramment Convention de Palerme. Il faut en outre et c'est essentiel sur le plan procédural sensibiliser tous les acteurs du secteur et en particulier ceux des secteurs juridique et judiciaire à la question fondamentale de la e-evidence. Certes, il existe sur ce point quelques règles de recueil des preuves mais il faut aller beaucoup plus loin et travailler de concert entre la Justice, tous les acteurs chargés de la police judiciaire et entreprises voire société civile sur cette question si importante de la preuve électronique. Je reviens ce matin de New-York où, à l'ONU, j'ai représenté St Cyr et sa Chaire pour une réunion sur cette question et nous avançons. Car, si nous ne nous attelons pas tous ensemble à cette tâche, les criminels resterons impunis, ferons des profits considérables à notre détriment, les profits de la cybercriminalité il faut le rappeler sont plus importants que le budget de la France et la Cyberdéfense ne marchera que sur un pied, et encore!

Mesdames messieurs je vous remercie de votre attention.