Discours d'ouverture de la 2e session nationale

« Souveraineté numérique et Cybersécurité »

Monsieur Frédéric DESAUNETTES, directeur par intérim de l'INHESJ

26 septembre 2018, École militaire

Seul le prononcé fait foi

Monsieur l'Ambassadeur,

Mesdames et messieurs,

Chères auditrices, chers auditeurs,

J'ai le plaisir de vous souhaiter la bienvenue à l'école militaire, en vous accueillant aujourd'hui au sein de *notre* deuxième session nationale « **souveraineté numérique et cybersécurité».**

Le « *notre* », comme vous le constatez à travers cette intervention conjointe, avec le général Patrick Destremau, est le signe d'un pluriel. Celui d'une volonté commune à nos deux instituts d'aborder un tel sujet sous l'angle d'une pédagogie renouvelée mais aussi d'une conscience accrue des responsabilités qui nous ont été confiées par le Premier ministre et le Secrétariat général de la défense et de la sécurité nationale (SGDSN).

Depuis la création de cette session commune en octobre 2018 de nombreux évènements en matière de sécurité informatique sont intervenus et notamment l'adoption de dispositifs législatifs.

Je ne les décrirais pas ici, mais, *« la mauvaise nouvelle* » est que la menace ne faiblit pas, qu'elle se diversifie avec notamment certains attaquants qui semblent préparer les conflits de demain en s'intéressant à des secteurs particulièrement critiques (défense, santé, recherche, etc.). Ceux-ci pénètrent nos système avec d'importantes ressources et restent discrets, patients jusqu'à ce que ce qu'un conflit éclate ou une opportunité se révèle.

La « *bonne nouvelle* », c'est que les décideurs publics et privés ne peuvent plus ignorer cette menace. Progressivement, on assiste au sein des organisations à une prise de conscience qui permet à la sécurité numérique de se hisser au même niveau de préoccupations que celui concernant les enjeux économiques, politiques et sociétaux.

Dire que nous vivons dans un environnement géopolitique instable est une évidence :

- instabilité voire même implosion ou explosion de régions entières à la suite de l'effondrement des Etats en Afghanistan, au levant ou le long de la bande sahélo-saharienne ;
- constitutions de « hub » terroristes sur les ruines de la Lybie ;

- rivalités exacerbées entre l'Iran et l'Arabie Saoudite sur fond d'affrontements immémoriaux entre chiites et sunnites ;

- accroissement massif des flux de réfugiés fuyant les guerres et bientôt les catastrophes climatiques. Bref, tout ceci place notre ordre mondial sous tension et signe le retour de rapports de forces brutaux dans les relations internationales.

Les pays développés ne sont pas non plus épargnés par les risques de déstabilisation politiques, nous le savons bien :

- essoufflement de l'Europe sonnée par le « *Brexit* », bousculée par la montée des populismes, fragilisée par sa démographie et « ses » économies ;

- brutalité des Etats-Unis sur la scène internationale ;

- hyperréalisme, disons cela comme ça, de la Russie qui privilégie la stratégie du fait accompli ;

- enfin ambition affirmée de la Chine, puissance incontournable assurant fermement la protection de ses approvisionnements et poursuivant résolument sa montée en puissance militaire sur terre, en mer, dans les airs et dans le milieu cyber.

Dans un tel contexte de reconfiguration annoncée des rapports de force, des stratégies, des territoires et des modes de confrontations,

il est évident que le cyberespace occupe et occupera une dimension stratégique majeure.

Le numérique est le futur juge départiteur des luttes de pouvoir et d'influence mondiales. Ce faisant, il met à l'épreuve le cadre de souveraineté des Etats et oblige au moins partiellement, à une redéfinition des *frontières* pour en maintenir pleinement la fonction, le sens et l'intelligence. Car sans frontière, il n'y a plus rencontre et diplomatie mais seulement confrontation et guerre.

Nous devons acquérir au sein des Etats-Nations, d'une part des capacités défensives et offensives, d'autre part, une culture de la cybersécurité.

Il faut donc une mobilisation de nos institutions régaliennes, au premier rang desquelles l'éducation nationale et la recherche bien sûr,

mais aussi, outre les armées, les forces de sécurité intérieures et la magistrature, soit les deux ministères de référence de l'INHESJ.

Mobilisation aussi de l'entreprise car la cybersécurité est l'affaire de tous et l'entreprise est souvent la première victime de chantage, d'espionnage ou de sabotage.

Nous le savons, l'accroissement du niveau général de la menace n'est pas encore aujourd'hui compensé par l'amélioration du niveau de sécurité des systèmes, confrontés à la numérisation massive des données et à l'inter-connectivité croissante des réseaux.

Ainsi, relever le défi jeté à notre pays par cette menace cyber nécessite de construire une communauté d'experts de haut niveau, dans un cadre garant d'une confiance mutuelle. C'est notre ambition.

Il nous faut d'abord promouvoir des connaissances de haut niveau pour agir juste

En février 2018, la revue stratégique de cyberdéfense du SGDSN affirmait que « *la maîtrise de la culture de sécurité numérique doit être érigée en priorité des programmes de formation*

initiale et de formation continue […] dans les écoles de la fonction publique nationale et territoriale » et demandait *« le développement des formations cyber à l'institut des hautes études de la défense nationale et à l'institut des hautes études de sécurité et de justice apparaissent ainsi indispensables*».

Nous faisons face à une menace polymorphe et hybride, en évolution constante et rapide, dont la connaissance réelle nous échappe en garde partie, une menace inédite par son ampleur

(en 2013, 1 à 3 milliards de boites mail Yahoo ! piratées ; après les attentats de janviers 2015 des milliers de collectivités locales ou d'institutions ont vu la page d'accueil de leur site défigurée par un appel au Jihad ; en mai 2017 WanaCry a frappé 200 000 entreprises et 150 pays, etc…),

inédite aussi par sa géographie transnationale et sa mise à exécution quasi instantanée.

Nous devons mettre en formes ce cyberespace qui avantage l'attaquant (hacker, activiste, délinquant isolé ou organisation criminelle, terroriste mais aussi membre des services de renseignement ou soldat en opération) car les techniques d'attaque utilisées préservent l'anonymat ou rendent l'identification longue, couteuse et aléatoire.

L'attribution d'une attaque ne peut résulter que d'une décision judiciaire ou politique, aboutissement d'une analyse complexe.

Il nous faut aussi créer une communauté d'experts fondée sur des relations de confiance

Cette confiance est nécessaire d'abord pour échanger loyalement des informations classifiées, mais aussi pour nous autoriser à penser autrement, hors des sentiers battus et du prêt-à-penser.

Nous souhaitons participer avec vous à l'élaboration d'une culture commune dans laquelle il est vain d'opposer sécurité et liberté.

Sans doute au terme de cette formation, il est possible,

il est souhaitable,

que se dessine une façon spécifique de penser les rapports

- entre secret et transparence,

- neutralité du net et exigence de civilisation d'un espace numérique que nous ne pouvons abandonner à la naïveté de libertariens ou au cynisme de prédateurs, légaux ou délinquants.

Il nous faut enfin contribuer à la construction d'une politique de sécurité numérique, vecteur d'une reconfiguration des métiers de responsables de sécurité dans le secteur privé comme dans le secteur public

Tel est le sens du recrutement opéré à travers vos profils, mesdames et messieurs les auditeurs.

Vous occupez tous des fonctions de responsabilités importantes au sein des structures privées et publiques que vous représentez.

Nous pensons, avec bien d'autres, que le déploiement d'une politique de sécurité numérique relève du plus haut niveau de responsabilité car elle participe de la stratégie de déploiement de l'entreprise privée, des conditions de sa survie au même titre qu'elle participe de la protection des libertés, de la protection des intérêts fondamentaux de la Nation, des secrets d'Etat et du secret des affaires sans lesquels nous ne pourrons résister dans un monde dont j'ai décrit plus haut l'extrême tension.

Cette politique de sécurité sera sans aucun doute le levier d'une redéfinition du périmètre des missions des directeurs de sécurité dans les grandes entreprises comme de leur place auprès des plus hauts décideurs.

Le même mouvement touchera le secteur public au travers des hauts fonctionnaires de défense et des secrétariats généraux.

Relever le défi de la cybermenace, c'est aussi faire de cette session nationale un outil pédagogique au service d'une vision prospective, aidant les décideurs publics et privés à anticiper les enjeux de moyen et long terme.

J'en aborderai deux.

Un enjeu de souveraineté

La menace cyber est mal connue à l'exception d'un petit cercle d'initiés dont certains d'entre vous font partie.

Qui la connaît donc ? Ce sont d'abord les attaquants.

Il n'est pas inutile de rappeler ici que la France a reconnu disposer de capacités offensives depuis le livre blanc de la défense et de la sécurité nationale de 2008, et surtout de 2013. Concluant, à la suite de l'attaque en déni de service subie par l'Estonie, à la nécessité d'engager une politique publique visant à protéger l'Etat et les infrastructures critiques, la France s'est doté en 2008 d'une agence, l'ANSSI, dirigée par Guillaume Poupard que nous aurons le plaisir d'accueillir très prochainement.

Nous disposons avec l'ANSSI d'un formidable outil de connaissance de la menace, de protection contre les attaques et de reconstruction lorsque les défenses ont été insuffisantes (comme après l'attaque subie par TV5 Monde).

Tous les Etats ne disposent pas d'une telle agence qui est passée d'une centaine d'agents en 2009 à plus de 550 experts en 2018.

Le ministère des armées est aussi doté de capacités et a élaboré en 2019 une doctrine de lutte informatique offensive.

Enfin la France dispose d'entreprises performantes dont certaines travaillent sur les vulnérabilités et se spécialisent dans le « jour zéro » (Zero-day) !

Mais – et c'est une des caractéristiques du monde numérique – la connaissance des menaces et la maîtrise des contre-mesures pour les combattre (c'est-à-dire des armes) sont

entre les mains d'un petit nombre d'entreprises privées et en particulier celles qui éditent les anti-virus.

Ces anti-virus sont au cœur de toutes les entreprises, dans les foyers de tout détenteur d'ordinateur, ont accès aux stocks de données et aux flux ; ils en analysent les métadonnées.

Ils ont pour fonction de combler les failles et de s'adapter aux menaces.

Aucun grand éditeur d'anti-virus n'est français.

Les principaux sont américains, russes, chinois, israéliens et japonais. Un seul éditeur important est européen, localisé à Bratislava. Cela pose une première question de souveraineté pour la France et l'Europe.

Un enjeu majeur est celui de la confiance dans nos institutions

Vous avez tous immédiatement à l'esprit le sujet du « hack back », pratique qui consiste à se faire justice soi-même en répondant à une attaque informatique par une autre attaque.

Cette pratique n'est à ce jour pas laissée à discrétion des particuliers, personnes privées ou morales.

Derrière l'hyper modernité du numérique demeurent à l'œuvre des enjeux aussi vieux que le monde, et notamment celui, toujours vivace, de la résurgence de la vengeance privée, de la contestation du monopole de l'usage de la violence légitime par l'état.

Accepter de telles pratiques reviendrait assurément à transformer l'espace numérique en terrain d'affrontements généralisés, participant ainsi non seulement du discrédit des institutions et de la parole publique

mais aussi et surtout d'une reféodalisation, au plan mondial, des rapports politiques et sociaux.

Nous assisterions à la consolidation de tendances déjà à l'œuvre, c'est à dire à la structuration de pouvoirs que s'attribueraient quelques grands duchés (les GAFAM et B.A.T.X.), voire aussi quelques baronnies (de très grands groupes privés), vassalisant toute une série de comtés et rétribuant généreusement mercenaires, corsaires et pirates.

Reprenant une expression entendue dans votre bouche, général Watin-Augouard, ce qui est sûr, c'est que le « bataille du sens est engagée », et sans doute depuis bien plus longtemps que nous ne le pensons.

Alors, mesdames et messieurs, dans la mesure de nos responsabilités, modestement mais résolument, tentons de contribuer à comprendre, prévoir et organiser le monde qui s'annonce pour le conserver vivable pour l'Homme.