Discours d'ouverture de la 1ère session nationale

« Souveraineté numérique et Cybersécurité »

Madame Hélène Cazaux-Charles, directrice de l'INHESJ

4 octobre 2018

(Seul le prononcé fait foi)

Mesdames et messieurs,

Chères auditrices, chers auditeurs,

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

Le « notre » comme vous le constatez à travers cette intervention conjointe, celle du général Patrick Destremau, et maintenant la mienne, n'est pas un « notre » de majesté, mais bien le signe d'un pluriel. Celui d'une volonté commune d'aborder un tel sujet sous l'angle d'une pédagogie renouvelée mais aussi d'une conscience accrue de nos responsabilités, celle de directeurs d'instituts nationaux de hautes études de la défense, de la sécurité et de la justice.

1- Le choix résolu d'une approche interministérielle de la cybersécurité est en effet et tout d'abord la résultante d'une analyse désormais largement partagée, de l'état de notre monde et de sa reconfiguration prévisible.

➢ *De la déstabilisation des états émergents …*

Dire que nous vivons dans un environnement géopolitique instable relève d'un doux euphémisme : instabilité voire même implosion ou explosion de régions entières, à très forte teneur stratégique, à la suite de l'effondrement des Etats en Afghanistan, au levant ou en Afrique ; guerres civiles déclarées (en Syrie notamment), ou larvées à la suite des printemps arabes qui fragilisent les Etats en Afrique du Nord et 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.

- *… à la fragilisation des pays développés*

Les pays développés ne sont pas non plus épargnés par les risques de déstabilisation politiques, nous le savons bien : essoufflement – pour les plus optimistes – de l'Europe sonnée par le « Brexit », bousculée par la montée des populismes, fragilisée par sa démographie et « ses » économies ; désengagement des Etats-Unis de la scène internationale ; hyperréalisme, disons cela comme ça, de la Russie qui privilégie le rapport de force et la stratégie du fait accompli ; enfin ambition affirmée de la Chine, puissance incontournable promouvant un multilatéralisme alternatif, assurant fermement la protection de ses approvisionnements et poursuivant résolument sa montée en puissance militaire sur terre, en mer et dans les airs.

- *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*

- Au plan international d'abord

Comme le souligne justement le SGDSN dans la revue *Chocs futurs*, *« la technologie apparait à la fois enjeu, arbitre et perturbateur des équilibres stratégiques* », et j'ajoute en tout premier rang, la technologie numérique. 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.

- Ensuite et surtout dimension stratégique du numérique au plan de notre sécurité intérieure

Nous devons acquérir de toute urgence, au sein des Etats-Nations, d'une part des capacités défensives et offensives, d'autre part, une culture de la cybersécurité, dès le premier âge, et tout au long de la vie, puisque l'innovation est structurellement permanente. 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 à l'heure où le baromètre Ipsos pour PwC jette une lumière inquiétante sur l'attitude des entreprises françaises qui ne perçoivent pas la cybersécurité comme une priorité.

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. En outre, au plan national, le déploiement de stratégies cohérentes et de moyens

efficaces exigerait une connaissance approfondie de la géographie souterraine de cette menace « cyber » et de la délinquance corrélative, à ce jour largement sous-évaluée malgré quelques travaux engagés. En d'autre termes, recruter des agents de la DGSI, des OPJ, des magistrats, créer des services d'enquête et des parquets spécialisés, construire une politique pénale éclairée, réfléchir à la judiciarisation du renseignement, tout cela n'a de sens que si nous cernons précisément le périmètre, la nature, l'ampleur et la gravité de la menace cybernétique.

2- 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* ».

Il est temps d'agir, car nous faisons face – le Général Destremau nous l'a expliqué – 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)*, 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 vous le savez, 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 (vous êtes ainsi tous en voie d'habilitation confidentiel défense), 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. La question n'est pas celle-là. Elle est désormais de savoir quelles sont les conditions de survie de nos démocraties et du socle des valeurs qui les fondent, en revisitant sans doute les grands équilibres sur lesquels nous avons traversé le 20ème siècle : équilibres entre renseignement extérieur et renseignement intérieur, entre renseignement et justice, entre police administrative et police judicaire, entre enquête de police et enquête judiciaire ; je pense encore à la césure consciencieusement entretenue entre privé et public, entre l'Etat et l'Europe, etc.

Alors oui, 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. Tous ces débats ont été ceux des lois anti-terroristes, renseignement, des lois pour une République numérique, ou encore sur le secret des sources des journalistes.

- *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. Elle 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.

3- 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 trois.

- *Un enjeu de souveraineté*

Je l'ai dit, la menace cyber est mal connue à l'exception d'un petit cercle d'initiés comme celui réuni cette matinée… et je soupçonne même certains d'entre vous d'en savoir plus long que la plupart de nos intervenants sur les coulisses de cette menace !!

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 2008, et surtout de 2013. La loi de programmation militaire qui a suivi porte ainsi création du commandement Cyber. Quelques entreprises françaises travaillent aussi sur les vulnérabilités et se spécialisent dans le 0day !

Ce sont ensuite les Etats. 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 se dotait en 2008 d'une agence, l'ANSSI, originellement dirigée par Patrick Pailloux, prédécesseur de Guillaume Poupard que j'ai le plaisir de saluer ici. 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.

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 fiduciaire : celui du devenir 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, objet d'un intense lobbying après des gouvernements et des organisations internationales.

Cette pratique est à ce jour très strictement encadrée et n'est pas laissée à discrétion des particuliers, personnes privées ou morales. Et c'est tant mieux ! Car 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 légiférants et militaires que s'attribueraient quelques grands duchés (les GAFAM et BATX), voire aussi quelques baronnies (de très grands groupes privés), vassalisant toute une série de comtés et rétribuant généreusement mercenaires, corsaires et pirates dans le cadre d'un marché lucratif de failles de sécurité identifiées (0day). Dans une telle configuration, pas sûr que les Etats aient même le rang de marquis !

Comment alors garantir à nos concitoyens la protection de leurs données personnelles, l'application de la directive NIS, du RGPD et autres instruments de régulation internationale de cet espace numérique ? Nous sommes au pied du mur : celui du choix de modèle. Tel est le sens de l'initiative prise par l'ANSSI en 2017, qui organisait la première conférence internationale sur les rôles et responsabilités des acteurs publics et privés de cette société numérique.

- *Dernier enjeu, n'ayons pas peur des mots : un enjeu anthropologique*

Je n'en dirai que quelques mots, terminant mon propos par un sujet que nous ne devons pas occulter quand on réfléchit à la « cybernétisation » des enjeux de défense, de sécurité et de justice : celui de l'évolution de l'espèce humaine. Nos sociétés voient-elles encore dans l'humain, l'animal mystérieusement parlant que la philosophie aristotélicienne a porté jusqu'à ce jour ? Ou bien, considère-t-on désormais l'humain comme un agrégat de comportements prédictibles par analyse algorithmique de données personnelles ? Ou encore, comme simple supplétif d'équations mathématiques qui en sauront plus sur l'homme que l'homme lui-même ?

Ces évolutions, conjuguées à l'essor des neurosciences, nous laissent entrevoir ce que peut être cette humanité augmentée promise, (d'ailleurs seulement pour certains), ou cette humanité plagiée par des machines auto-apprenantes, aux performances sans commune mesure avec celles dont nous sommes capables. Selon notre réponse, ce ne seront pas le même soldat, le même policier, le même juge, ce ne seront pas non plus les mêmes institutions et les mêmes hiérarchies qui adviendront au 21ème siècle.

Il nous faut très vite décider si nous voulons faire de la donnée numérique seulement un marché ou essentiellement un sujet politique, un sujet de civilisation qui convoque les plus grands experts, les plus grands intellectuels, qui, sans doute, oblige de toute urgence à repenser la fabrique de nos élites et l'articulation des sciences humaines et sociales avec les sciences de l'ingénieur.

En tout état de cause, reprenant une expression entendue dans votre bouche, général Watin-Agouard, 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 et habitable par l'homme.