Matinale mensuelle du CyberCercle

Mardi 6 juillet 2021

Allocution d'ouverture de Mme Françoise DUMAS

Présidente de la Commission de la Défense nationale et des Forces armées de l'Assemblée nationale, ancienne présidente de la DPR

Général,
Madame la Présidente, chère Bénédicte PILLIET,
Mesdames et Messieurs, chers amis,

Permettez-moi tout d'abord de vous remercier de votre invitation à participer aujourd'hui à cette matinale du cyber-cercle qui, depuis bientôt dix ans, vous réunit autour des questions de sécurité numérique. Vous avez très tôt mis en évidence les enjeux stratégiques liés au développement du cyber, à ses opportunités mais aussi à ses dangers pour nos intérêts économiques, la défense nationale et aussi notre vie démocratique.

La Délégation parlementaire au renseignement, que j'ai eu l'honneur de présider jusqu'à la semaine dernière, a consacré d'importants travaux aux questions de cyberdéfense, pour souligner la contribution majeure des services de renseignement au sujet qui nous intéresse ce matin.
Je suis aussi très heureuse de m'exprimer aux côtés du Général Bucquet, Directeur du renseignement et de la sécurité de la Défense (DRSD) avec qui j'ai le plaisir d'échanger régulièrement dans le cadre de mes fonctions, tant à la DPR qu'à la Commission de la Défense de l'Assemblée nationale.

Je voudrais ce matin insister sur trois grands enjeux qui me semblent importants :

- D'abord, la montée en puissance de la menace cyber ;
- Ensuite, le rôle des services de renseignement pour détecter, entraver et attribuer les attaques cyber ;
- Enfin, et ce sera ma conclusion, la nécessité de bâtir une filière industrielle souveraine dans le domaine cyber.

1. La montée en puissance de la menace cyber

La stratégie nationale du renseignement publiée il y a deux ans, en juillet 2019, souligne la **prégnance de la menace cyber**, qui est de plusieurs natures : vol de données, sabotage au préjudice d'entreprises comme des administrations, intrusion dans les systèmes informatiques à des fins d'espionnage, chantage en vue d'obtenir une rançon…
Certaines de ces opérations de prédation relèvent de ce qu'on peut qualifier de nouvelle forme de **cybercriminalité organisée**.
Notre stratégie nationale du renseignement rappelle également que, par le biais d'internet et des réseaux sociaux, l'espace cyber est aussi un vecteur de **diffusion de messages haineux et de manipulation de l'information**.

Le Plan national d'orientation du renseignement (PNOR) prend la pleine mesure de l'évolution et de l'intensification de cette menace cyber, et de l'exposition accrue de nos sociétés, de plus en plus numérisées et interconnectées.

Les auteurs d'attaques informatiques poursuivent des objectifs multiples tels que l'espionnage, les trafics illicites, la déstabilisation et le sabotage. Ils peuvent conduire aussi bien des **opérations très ciblées que massives et indifférenciées.**
Par ailleurs, la montée en puissance de la menace cyber se nourrit de la multiplication des acteurs, de l'accroissement des capacités offensives de certaines puissances étrangères, de ce qu'il convient d'appeler la **prolifération des armes informatiques et la banalisation des techniques d'attaques**.

On observe également une **imbrication de plus en plus forte des enjeux de cybercriminalité et de sécurité nationale**.

En quelques années, **le cyberespace est donc devenu un lieu de confrontation, de conflictualité, à part entière**. Il possède une dynamique qui lui est propre et qui repose sur l'instantanéité des échanges, la diffusion en réseau, la massivité de données accessibles à tous et bien sûr, l'effacement des frontières.

L'essor du « darkweb » rend accessible à moindre coût et donc au plus grand nombre ces armes de destruction informatique qui ne sont plus l'apanage des plus expérimentés. Les modes opératoires évoluent constamment et l'ANSSI, notre agence nationale de la sécurité des systèmes d'information, doit se mettre en capacité de toujours garder un temps d'avance.

Nos armées ne sont pas à l'abri de la cyber-menace. Des virus informatiques ont pu être découverts sur des systèmes d'arme, généralement à l'occasion d'opérations de maintenance par des industriels.
Les opérations militaires font également régulièrement l'objet d'attaques informationnelles sur les réseaux sociaux, parfois massives et coordonnées.

Ainsi, **l'anticipation et la maîtrise du risque cyber sont les deux paramètres clés d'une lutte informatique défensive devenue indispensable pour préserver le fonctionnement quotidien de nos intérêts nationaux**, qu'ils s'agisse des administrations et services de l'Etat (y compris nos armées), des opérateurs d'importance vitale ou de services essentiels, mais aussi de toutes autres formes d'activités ou d'organisations : des collectivités territoriales ou des entreprises, en passant par les organes de presse ou des associations.

⇨ C'est dans ce contexte que nos services de renseignement ont vu leurs missions précisées. Ce qui m'amène au deuxième enjeu que je souhaitais évoquer ce matin : le rôle de nos services de renseignement face à la menace cyber.

2. Le rôle des services de renseignement face à la menace cyber

Nos services de renseignement contribuent activement à la politique publique de cyber défense, pilotée par l'ANSSI et le COMCYBER. Ils jouent un rôle essentiel pour **détecter, entraver et le cas échéant attribuer les attaques cyber dont notre pays, nos entreprises et nos infrastructures sont les victimes.**

Les différentes missions pour lesquelles les services de renseignement sont appelés à concourir concernent ainsi :

- **L'anticipation**, en contribuant au recueil des informations sur les groupes d'attaquants susceptibles de porter atteinte à des intérêts relevant de la sécurité nationale ;
- **La détection**, avec des moyens complémentaires à ceux de l'ANSSI :
- **L'attribution**, qui n'est pas nécessairement rendue publique, mais qui permet de remonter à l'instigateur d'une attaque.

Pour exercer leurs missions dans le domaine cyber, les services de renseignement peuvent bien sûr avoir recours aux techniques de renseignement autorisées par la loi.

Sur le périmètre cyber, en raison de la nature même de la matière, qui est à la fois mondiale et très mouvante, les techniques utilisées plus particulièrement, mais non exclusivement, sont le **dispositif technique de surveillance internationale ainsi que le recueil de données informatiques.**

Les services de renseignement disposent également de moyens d'entrave. L'article L.2321-2 du code la défense prévoit que en effet que :
« *Pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'État peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque* ».

Les services disposent ainsi, dans un cadre légal, des moyens juridiques indispensables pour permettre de défendre les infrastructures d'importance vitale contre une cyberattaque.

La montée en puissance des services de renseignement dans le domaine cyber exige des **investissements importants**, une adaptation de leur organisation, des **personnels spécialisés dans les technologies de la sécurité informatique**, dans le développement de nouveaux outils et de l'exploitation de ceux-ci, et enfin des **moyens financiers pour concevoir, développer, acquérir et exploiter les nouveaux outils.**

⇨ Cet effort suppose, en outre, le développement parallèle d'une filière industrielle souveraine, dernier enjeu sur lequel il me semble fondamental d'insister.

3. <u>La nécessité de bâtir une filière industrielle souveraine dans le domaine cyber</u>

C'est absolument nécessaire, si la France veut conserver les attributs de sa souveraineté.

Si l'on s'en tient à la communauté du renseignement, cela nécessite de **poursuivre et d'amplifier les efforts consentis ces dernières années en matière de recrutement et d'investissement des services consacré au domaine cyber.**

Cela suppose aussi **l'intensification et la consolidation capacitaire des grands programmes interministériels et de la cyberdéfense**, avec notamment l'acquisition et le développement de matériels permettant de tenir compte des évolutions technologiques et de l'augmentation du volume et de la qualité des données à traiter.
Dans un monde où la collecte des données, notamment en source ouverte, est massive, la performance d'un service de renseignement se mesure en effet davantage par ses capacités à exploiter intelligemment et rapidement l'information utile.

La loi de programmation militaire 2019-2025 prend en compte ces exigences ; par exemple, pour la DRSD, cela se traduit, et le Général va vous l'exposer en détails dans quelques instants, par une remontée en puissance significative des effectifs de votre direction, qui concerne au premier chef le domaine cyber.

Mesdames et Messieurs,

La sécurité dans l'espace cyber face à la multiplicité et l'intensité des menaces, repose sur la **pleine autonomie dans la mise en œuvre des outils de cyberdéfense et donc la maîtrise de capacités critiques souveraines.**

C'est d'autant plus vrai lorsqu'il s'agit de protéger les services de l'État et les activités d'importance vitale ou de soutenir l'action des armées ou des services de renseignement.

Dans nombre de technologies-clés, **l'excellence scientifique française est reconnu**e grâce au niveau de formation de ses mathématiciens et ingénieurs et à la qualité de ses organismes de recherche. Il nous faut mettre à profit cet avantage au service de la **constitution d'une industrie française de logiciels de cyber-sécurité, capable de rivaliser avec les entreprises américaines ou israéliennes.**

Les efforts déployés ces dernières années doivent être poursuivis, consolidés et renforcés à l'heure où l'ensemble des services de renseignement étrangers et des forces armées se dotent d'importantes capacités cyber.

Il n'est pas encore trop tard, mais la menace cyber, qui fait désormais partie intégrante de notre politique de défense et de sécurité, rebat les cartes et challenge notre statut de grande puissance.

Je vous remercie.