GOUVERNEUR
MILITAIRE DE
LYON

Discours de Monsieur le général de corps d'armée Philippe Loiacono
Cybersécurité

SEUL LE PRONONCE FAIT FOI

Madame la député,

Monsieur le Président du Conseil Départemental du Rhône,

Madame la Vice-présidente de la Région Auvergne Rhône Alpes, en charge du numérique,

Monsieur le général de corps d'armée commandant la région de gendarmerie Auvergne-Rhône-Alpes,

Madame la présidente du CyberCercle,

Mesdames et Messieurs en vos appellations, grades, et qualités respectives,

**

Sachez qu'avant de me présenter devant vous ce matin, j'ai consulté plus d'une dizaine de fois mon smartphone connecté, ouvert mon ordinateur, traité des mails, répondu à des appels, lu des articles de presse sur internet, mis en œuvre le GPS de mon véhicule… Mon quotidien, mais je n'en doute pas aussi le vôtre, est rythmé par l'utilisation incessante de ce que l'on nomme désormais : l'espace Cyber.

Cet espace, qui à ses prémisses était imaginé comme celui qui devait reconnecter le monde, favoriser les échanges entre les nations, les peuples, les cultures, permettre d'accéder au savoir universel, d'améliorer la productivité pour faciliter le travail quotidien, de commercer et de discuter en temps réel et tant d'autres choses encore… Cet espace est bien aujourd'hui tout cela. Mais il est aussi plus.

Il est aussi cet espace où chaque jour des actions de sabotage, de vol de données, de subversion, d'intoxication informationnel, de déstabilisation, sont commises, presque dans l'impunité et l'anonymat. Il est cet espace qui, utilisé à des fins malveillantes, peut permettre de mettre à bas des institutions (comme le système bancaire international), de paralyser des nations comme ce fut le cas en Estonie en 2007, de neutraliser une centrifugeuse nucléaire, ou encore de s'attaquer aux

intérêts vitaux de notre pays en violant notre souveraineté. Et tout cela à portée de « clic ».

Dans ce cadre, il convient de facto de réfléchir, ensemble, aux moyens de tirer pleinement parti des potentialités incroyables qu'offre le domaine Cyber, mais aussi de se prémunir des risques qui y sont liés. Ne soyons pas dupe, ni naïf, ni aveugle, Mesdames et Messieurs, la guerre cyber a déjà commencé.

**

C'est pourquoi le Ministère des Armées s'engage pleinement dans la montée en puissance de ses capacités cyber afin de se donner les moyens de construire une cyberdéfense à la hauteur des ambitions opérationnelles de la France. Ainsi, la Ministre des Armées, Florence Parly, a inauguré début octobre à Rennes la Cyberdéfense Factory pour travailler en synergie avec le monde industriel et celui de la recherche, sous l'impulsion de deux principaux acteurs : le Commandement de la cyberdéfense et la Direction générale de l'armement. La loi de programmation militaire 2019-2025 prévoit l'investissement de 1,6 milliards d'euro dans ce domaine, avec des fonds d'investissement pour aider les start-up, les PME et les grandes entreprises, mais aussi le recrutement de 1000 cyber combattants supplémentaires. Chaque année les Armées réalisent un grand exercice de cyber sécurité baptisé DEFNET, le cyber est au cœur de tous les grands programmes d'armement, et nos doctrines d'actions investissent désormais pleinement ce nouvel espace, en défensif comme en offensif, sur le territoire national comme sur les théâtres d'opérations extérieures ! Ce qui est en jeu, c'est aussi la capacité de nos systèmes à continuer d'opérer, de fonctionner quand toute l'architecture de nos réseaux s'effondre. Il nous faut pouvoir maitriser ce nouvel espace, mais aussi savoir travailler sans lui : c'est cela la résilience. Vous l'aurez compris, la cyberdéfense est une priorité absolue du ministère des Armées, car elle est garante de notre souveraineté nationale.

Mais comme le soulignait madame la Ministre : « le cyber est un sport collectif », et c'est bien chaque entreprise, je pense notamment aux sous-traitant défense, chaque ministère, chaque personnel qui doit aujourd'hui cultiver une hygiène cyber irréprochable. Dans ce combat, il faut agir ensemble, pour sécuriser nos réseaux, pour être capable de parer aux attaques, de remonter aux sources, et de contre-attaquer si nécessaire. N'oublions pas qu'une cyberattaque sur des structures civiles peut très facilement avoir des répercussions nationales, tant le cyberespace est systémique. Il nous faut aussi échanger nos bonnes pratiques, développer nos moyens d'actions, recruter et former notre jeunesse à ce nouveau

domaine, tant sur le plan technique que sur le plan éthique ! A ce titre, le ministère des Armées a lancé une campagne de recrutement cet hiver, et il y aura plus de 200 postes à pourvoir en 2020.

En somme, ce qu'il nous faut : c'est créer une véritable chaine de confiance cyber et mettre cette technologie au service de l'humain.

Nous en avons les moyens et les capacités, n'en doutons pas. Il est désormais temps de faire preuve d'ambition, de pragmatisme et détermination pour relever, ensemble, ce défi majeur du XXIe siècle.

Je vous remercie de votre attention.