L'innovation technologique est un domaine où le monde privé et le monde de la défense ont un intérêt commun à travailler en 'équipe France'.

Le Capitaine de frégate Nicolas Malbec est chef de la planification des opérations au Commandement de la Cyberdéfense et directeur du cursus Cyberdéfense de l'École Hexagone. Cet entretien a été publié le 4 février 2022.

1/ Quelle est votre fonction au sein du ComCyber et en quoi cela consiste-t-il ?

Au sein du commandement de la Cyberdéfense, je suis en charge de la planification des opérations. Il s'agit de préparer des options militaires dans le cyberespace pour accompagner les Armées dans leur manœuvre d'ensemble. Les Armées françaises agissent dans les trois domaines de lutte que sont la Lutte Informatique Défensive (LID), la Lutte Informatique d'Influence (L2I) et la Lutte Informatique Offensive (LIO). Dans le détail, ces opérations sont classifiées et je ne puis en dire plus.

2/ La cyberdéfense est garante de la souveraineté nationale. Qu'est-ce donc que cette souveraineté dont le monde va aujourd'hui jusqu'à contester le mot ? De quelle manière la cyberdéfense en est-elle garante ?

Fondamentalement, la souveraineté nationale, c'est le caractère d'un État qui n'est soumis à aucun autre État. L'article 3 de la Constitution souligne que cette souveraineté

appartient au peuple qui l'exerce par ses représentants et par la voie du référendum. Dans le domaine numérique la soumission peut arriver plus vite qu'on ne le croit : extraterritorialité du stockage des données des citoyens ou des entreprises stratégiques, dépendance de pays tiers pour la fourniture de matériels stratégiques (75% des semi-conducteurs sont produits à Taïwan, pays qui par ailleurs est le seul à atteindre la précision nanométrique pour la gravure des composants), dépossession de l'exclusivité de battre monnaie (émergence des cryptomonnaies), etc. À son niveau, dans son aspect défensif, la cyberdéfense va combattre pour préserver la confidentialité, l'intégrité et la disponibilité des données et des systèmes d'information des Armées. Cela passe par le choix des matériels et des architectures de sécurité et par la supervision de la cybersécurité des réseaux. La cyberdéfense va aussi rechercher une forte résilience en préparant le pire. En cas de crise cyber, des équipes de réponses à incident sont déployées pour analyser les attaques et restaurer les systèmes. Pour les systèmes critiques, des plans de continuité et de reprise d'activité sont mis en œuvre.

3/ Que pensez-vous des relations qui existent entre le monde privé (entreprises mais aussi banques et VC) et le monde de La Défense sur les sujets technologiques (en termes d'investissement, au sens large) ?

Ces relations sont organisées pour le ministère des Armées par la Direction Générale de l'Armement qui est responsable de la politique de soutien à la BITD (Base Industrielle et Technologique de Défense). La DGA s'appuie en partie sur l'Agence d'Innovation de la Défense qui met en œuvre la politique ministérielle en matière d'innovation et de recherche scientifique et technique. En novembre 2019, une convention a été signée entre le Ministère des armées et 8 grands maîtres d'œuvres industriels et principaux équipementiers. Ce partenariat s'articule autour de 4 piliers : le partage de l'information au sein d'un cercle de

confiance, l'évolution de l'organisation et l'établissement de gouvernance partagée, l'acculturation et la sensibilisation au cyber et la volonté commune de maîtriser les risques cyber sur l'ensemble de la chaîne de soutien de défense.

Ces relations avec les entreprises sont indispensables pour développer les outils dont les Armées ont besoin. Mais ça marche dans les deux sens : par exemple, dans le domaine des outils d'identification (de radars, d'images, de sous-marins, etc.) basés sur des intelligences artificielles, les entreprises ont besoin des données opérationnelles recueillies sur le terrain par les Armées pour alimenter correctement leurs algorithmes d'apprentissage profond. L'innovation technologique est un domaine où le monde privé et le monde de la Défense ont un intérêt commun à travailler en « équipe France », sans oublier, bien sûr, d'y associer le monde de l'éducation et de la recherche. Pour procéder à des échanges de données opérationnelles classifiées, il faut un tissu national d'entreprises de confiance.

4/ Pierre Bellanger a beaucoup théorisé sur l'analogie entre les eaux territoriales et extra-territoriales et les mers numériques. L'actualité vous incite-t-elle à filer la métaphore ?

La haute mer, c'est la res nullius par excellence, la promesse d'une liberté de naviguer et d'agir à sa guise. Cette liberté de mouvement irrigue l'âme et les mœurs du marin : « Homme libre, toujours tu chériras la mer ! » et partant des grandes nations maritimes. Pourtant cette extra-territorialité est de plus en plus limitée par les traités (notion de zone économique exclusive de la convention de Montego Bay qui éloigne à 200 nautiques des côtes la haute mer et même jusqu'à 350 nautiques en prenant en compte le plateau continental !) ou par les contestations du droit international (revendications chinoises sur la mer de Chine). Les flots numériques constituent un vaste océan mondial appelé l'Internet. Historiquement sous contrôle organisationnel,

physique et logique des États-Unis, il pouvait toutefois jusqu'à récemment faire penser à un vaste espace de liberté sans frontière. Cependant, les États ou les grandes entreprises mondiales du numérique ont tendance à mettre sous contrôle des pans entiers de ce vaste océan numérique, créant des mers intérieures ou des lieux de passage obligés. Ainsi la Russie élabore son RuNet en tissant un réseau dédié de routeurs et de datacenters à ses frontières, la Chine est prête à s'abriter derrière son great fire wall, et les géants américains du numérique représentent plus de 50% des investissements dans les câbles sous-marins. On le voit, la liberté de navigation doit être défendue avec force aussi bien en mer que dans le cyberespace !

5/ Comprenez-vous que l'on puisse communiquer publiquement sur nos vulnérabilités ? ***(Ex : quand la présidente de la Commission européenne déclare que nous serons toujours dépendants de puissances étrangères en matière de semi-conducteurs).***

Les affaires de dépendance en matière de semi-conducteurs ne sont pas secrètes et ne concernent pas que les Européens. Il suffit de regarder le poids de Taïwan dans la manufacture des semi-conducteurs de précision. Dans un régime démocratique, il est important que les citoyens aient conscience de l'état de sa Défense. À ce titre, les autorités militaires sont régulièrement entendues par les députés et les sénateurs pour rendre compte des succès rencontrés mais aussi des difficultés, y compris matérielles, pour remplir les missions confiées. Ce discours de vérité permet d'orienter les politiques publiques et l'effort de Défense.

6/ Un bon cybercombattant, est-ce un bon militaire qui maîtrise l'environnement technologique et ses menaces, ou un bon ingénieur qui saurait tenir un fusil ?

On m'a déjà posé la question à propos de l'officier de marine ! La réponse est similaire : le cybercombattant est avant tout

un militaire qui a le culte de la mission et qui est prêt à tous les sacrifices pour l'accomplir. Il doit néanmoins être compétent dans son domaine de lutte et dans le cas qui nous intéresse il doit avoir une maîtrise approfondie de l'environnement cyber et de l'arsenal numérique qu'il y déploie. Cela dit, tous les cybercombattants ne sont pas des ingénieurs : nous avons aussi des juristes, des linguistes, des experts en marketing digital ou en géopolitique, etc.

7/ Que vous inspire le développement fulgurant des drones et la perspective d'un monde peuplé d'objets connectés produits dans des pays potentiellement ennemis ?

Les drones armés sont aujourd'hui, notamment suite au conflit dans le Haut-Karabagh, des armes incontournables des champs de bataille. Utilisés en essaims, éventuellement pilotés par une intelligence artificielle capable d'exploiter leurs capteurs (camera, radio, …) ils sont caractéristiques d'une transformation numérique du champ de bataille qui peut conduire à des tactiques de rupture et à un rééquilibrage des forces en faveur non plus du belligérant le plus riche en matériel mais du plus innovant.

8/ Le haut lieu de la cybersécurité, c'est Paris ou Rennes ? (joke)

Avec le TGV, et un temps de transport de moins d'une heure trente on peut dire que Rennes fait désormais partie de la banlieue parisienne (joke). Sans compter les visioconférences qui permettent de garder le lien en toutes circonstances. Les dispositifs rennais comme le Pôle d'Excellence Cyber et parisiens comme le campus Cyber se complètent harmonieusement. On pourrait ajouter que la cybersécurité n'est pas cantonnée à ces territoires. Je pense par exemple à Toulon qui comprend le centre support cyber de la Marine ou une bonne partie des effectifs cyber de Naval Group.

9/ Quels sont les outils ou logiciels français que vous

utilisez à titre professionnel ou personnel ?

La direction interministérielle du numérique (DINUM) met à la disposition des agents de l'État des systèmes numériques collaboratifs souverains comme Tchap (une messagerie type Whatsapp), Osmose (un portail collaboratif) ou la webconférence de l'État (un portail de visioconférence). Je suis utilisateur de ces solutions. Je pense qu'il est indispensable d'employer ce type de solutions souveraines plutôt que leurs concurrentes étrangères, et lorsqu'elles ne donnent pas complètement satisfaction, il existe des équipes de développement à l'écoute et capables de faire évoluer les produits.

10/ Si vous deviez résumer en quelques lignes la pensée qui gouverne votre enseignement à l'École Hexagone ?

L'école Hexagone m'a demandé de diriger le cursus cyberdéfense qui ouvrira au mois d'octobre 2022 à Versailles. L'idée est de répondre à la pénurie de talents cyber dont la France a besoin en s'appuyant, lorsque c'est possible, sur des enseignants issus soit du monde de la cyberdéfense, soit d'entreprises proposant des solutions de sécurité souveraine. C'est le cas par exemple de Stormshield ou d'HarfangLab. Non seulement les étudiants recevront les enseignements techniques des meilleurs spécialistes du domaine, mais en plus ils seront sensibilisés aux enjeux géopolitiques du cyberespace et à la guerre économique que se livrent les États et les entreprises. Ils seront aussi formés à travailler dans un environnement de crise cyber grâce à des wargames réalistes.

11/ Vous êtes nommé DSI de la France, quelle est la première mesure que vous défendez ?

Je pense que de nombreuses initiatives portées par la DINUM vont déjà dans le bon sens (Création du socle interministériel de logiciels libres, sites data.gouv.fr et api.gouv.fr, généralisation de FranceConnect, …). Après, il me semble

important de disposer d'un plan stratégique pour garantir la souveraineté dans tous ses aspects : enseignement, recherche, tissu industriel, approvisionnements stratégiques, hébergement, capacités de calcul, services cloud, arsenal juridique (à doser avec précaution car il ne doit pas être un frein à l'entreprenariat français), etc.

12/ Face à l'omniprésente menace virale (informatique), de quelle nature est selon vous la meilleure réponse à apporter ?

Il faut continuer à investir sur les moyens organisationnels et techniques pour éviter les attaques. Mais il faut aussi et surtout miser sur la résilience de nos systèmes. Qu'est-ce que je fais si je suis attaqué ? Suis-je capable d'évaluer les dégâts ? Suis-je capable de restaurer mes données et mes systèmes ? Ai-je des modes de fonctionnement dégradés ou de secours ? Comment vais-je gérer ma communication de crise (externe et interne) ? Si j'en ai les moyens je m'entraîne régulièrement à faire face au pire.

13/ Que vous inspire le fait que de très nombreux OIV aient choisi / eu la liberté d'héberger leurs données sur des clouds américains ?

Il faudrait regarder au cas par cas. En cybersécurité, la base est de conduire une analyse de risque. Les risques identifiés ont-ils été supprimés, couverts ou formellement acceptés ? Le tout est bien d'avoir conscience de ce que l'on fait et d'être en mesure d'assumer ses choix.