#ANSSI10+

Synthèse de l'atelier « Futurs imaginaires, imaginaires futurs »

Le 3 décembre 2019 s'est tenu à l'ANSSI l'**atelier collaboratif ouvert « Futurs imaginaires, imaginaires futurs »** – dernier de la séquence ANSSI10+ – avec le double objectif

- **de réfléchir aux contours d'un imaginaire cyber maîtrisé et mobilisateur** ;
- **d'identifier les angles morts de la cybersécurité d'aujourd'hui et de la stratégie de l'ANSSI,** grâce à une projection libre dans des futurs dystopiques.

Autour de ces thèmes atypiques, qu'une réunion classique et exclusivement interne n'aurait sans doute pas permis de traiter en un temps si court, **cet atelier a réuni une cinquantaine de personnes issues de l'ANSSI, du secteur privé mais également des étudiant(e)s**, grâce au forum de Sciences Po pour la cybersécurité.

1. Imaginaires futurs

Au départ, **des constats partagés** :

- L'imaginaire cyber est aujourd'hui *subi* plutôt que construit. Il découle principalement des mots et de l'iconographie véhiculés dans les médias, les films et séries télé, et non d'une stratégie conscientisée, porteuse d'objectifs en termes de perceptions souhaitées du sujet.
- Il véhicule de nombreux *clichés négatifs*, centrés principalement autour de la menace, au travers de la figure de l'attaquant, seul, la nuit, sous sa capuche ; mais aussi des dommages que peuvent causer les cyberattaques aux particuliers.
- L'imaginaire cyber est, pour finir, *spécialisé*, s'adressant – au travers de l'empreinte historique d'une certaine culture geek, tech, du jeu, etc. – à un certain public, principalement masculin et technophile.

Face à ce constat, **une hypothèse** : l'imaginaire, d'autres domaines technologiques, comme celui de l'exploration spatiale, ont fait l'objet – d'abord aux États-Unis puis en Europe – d'un effort de définition d'un imaginaire mobilisateur, incarnant désormais dans l'inconscient collectif des valeurs positives : l'exploration plutôt que la guerre, la science et les technologies au service d'un intérêt supérieur humain, la conquête et l'espoir. Ne fut-il pas défini, cet imaginaire aurait pu se concentrer prioritairement sur les rapports de puissance interétatiques liés à l'espace, les risques considérables associés aux technologies spatiales, ou encore les obstacles insurmontables face à l'ampleur de la tâche. Tel ne fut pas le cas, par le choix

d'institutions comme la NASA et aujourd'hui de l'agence spatiale européenne, grâce à des *role models* ou des récits cinématographiques inspirants. Ceci a permis de maintenir le domaine spatial haut dans les priorités des gouvernements, en dépit d'une moindre priorisation du sujet à la suite de l'effondrement de la confrontation entre les blocs de l'est et de l'ouest.

De la même manière, un imaginaire cyber maîtrisé et mobilisateur devrait parvenir à concilier la nécessité de mobiliser

- **s'une part, le grand public**, en l'amenant à se forger une représentation positive de la cybersécurité au travers de la plus-value que celle-ci apporte, s'agissant notamment de la « confiance » et de « l'harmonie » dans les usages numériques qu'elle autorise, des conquêtes scientifiques qu'elle a permises, d'une représentation d'un « autre » protecteur plutôt que d'un « autre » menaçant, etc. *« Lorsque l'on évoque le métier du jardinier, on parle du jardin harmonieux qu'il a fait pousser et non pas des coups de sécateur qu'il a dû donner afin de parvenir à ce résultat* » indiquait un participant. De la même manière, la sécurité numérique devrait être associée à la « confiance numérique », permise par la sécurité et la défense des systèmes d'information, plutôt qu'à sa dimension opérationnelle et encore moins aux menaces évitées ;
- **d'autre part, les spécialistes** en parvenant à s'adresser à une plus grande diversité de profils, tant en termes d'âge – des jeunes aux personnes en cours de carrière – que de parcours académiques – scientifiques, techniques, ingénierie, droit, sciences sociales – que, bien entendu, de genre.. Ce faisant, il s'agit de valoriser l'accessibilité de la cybersécurité au-delà des seuls spécialistes à l'état-de-l'art, par exemple aux « hackers/makers ».

Pour véhiculer ces imaginaires construits, **des leviers** : besoin de *role models* – notamment féminins – et à l'image de la diversité des spécialistes souhaitée pour le secteur ; besoin de récits de fiction (films, séries) ; besoins de rituels visibles (les jeux olympiques de la cybersécurité) ; besoin d'embarquer dès le plus jeune âge (primaire, collège, lycée), par le jeu notamment ; besoin de valoriser davantage les métiers et les opportunités associées, etc.

2. Futurs imaginaires

Deux points d'entrée en 2030 ont été proposés aux groupes de travail :

- **Un monde en crise : réchauffement climatique et tensions géopolitiques**.
- **Tout numérique : hyperconnexion des activités humaines et du vivant**.

Ces projections ont permis de faire l'hypothèse de plusieurs évolutions à prendre en compte dès aujourd'hui :

- **L'accroissement de la menace :** face à l'accroissement de la surface d'attaque due à l'hyperconnexion du réel (Internet des Objets, 5G et demain 6G) et à

l'intrication croissante des systèmes d'information ; face à l'accroissement des tensions géopolitiques entre États Nations, dans un contexte fragilisation de la légitimité du cadre institutionnel européen mais également de renforcement des tensions entre États face aux conséquences grandissantes du réchauffement climatique.

- **Le risque de perte croissante de confiance des utilisateurs, susceptibles de faire le choix de la déconnexion** : perte de confiance au regard de l'omnipotence des géants du numérique ; volonté de se reconnecter au monde physique.
- **L'impact sur le réchauffement climatique et ses conséquences, des développements du numérique** – dont la cybersécurité – premier secteur en devenir en termes d'émissions de gaz à effets de serre.

Cette dernière évolution, pour la première fois formellement évoquée au sein de l'ANSSI, ouvre la voie à des questions tout aussi importantes que complexes : quelle est l'empreinte carbone des produits et services de cybersécurité ? Prévenir et contrer les attaques informatiques participe-t-il à diminuer l'impact environnemental susceptible d'être généré par ces dernières ? De futurs développements, notamment autour de la donnée au profit des métiers et missions de la cybersécurité (création de bases ou lacs de données, leur valorisation, etc.), constituent-elles une orientation contraire à un objectif de sobriété énergétique ou, en renforçant la capacité d'action des acteurs de la cybersécurité, en diminuent-elles l'empreinte globale ?

N.B. Cette synthèse a été élaborée sur la base des restitutions orales et écrites effectuées lors de cet atelier collaboratif, dans le cadre d'une démarche expérimentale.

Bien qu'un effort particulier ait été fait pour capter et retranscrire l'essence des travaux, ce document ne saurait être parfaitement exhaustif.

Conçu pour recueillir et documenter les idées issues de l'atelier, il ne saurait par ailleurs être considéré comme un document engageant pour l'ANSSI.