Sensibiliser les lycéens à la cyberdéfense

D'abord spécialiste dans le soutien technique d'aéronefs, le Colonel Thierry KESSLER-RACHEL s'est par la suite orienté dans le domaine de la cyberdéfense (1). Après une formation dans la sécurité des systèmes informatiques qui lui ouvrit de nouvelles responsabilités, il exerça comme chef du centre des opérations cyber au sein du tout nouveau COMCYBER (2) avant de devenir l'actuel commandant de la base aérienne 709.

C'est en tant que spécialiste en cyberdéfense qu'il vint à la rencontre des élèves de la Terminale G4 du Lycée Jean Monnet ce jeudi 19 janvier 2023. Avec le double objectif d'éclairer les jeunes esprits sur les enjeux cruciaux que pose l'omniprésence du cyberespace dans nos vies individuelles comme professionnelles, et celui de présenter les différents parcours pouvant mener aux nombreux métiers de la cyberdéfense, l'officier fit un exposé mêlant à la fois perspective historique, enjeux contemporains et données techniques. Son propos fut d'autant plus intéressant qu'il fut accessible pour un public de lycéens nonobstant sa technicité.

Ces derniers furent d'abord introduits dans le sujet par l'Histoire de la cryptographie (le fait de rendre incompréhensible un message afin d'en protéger les informations) dont l'usage remonte à l'Antiquité. Plus proche de nous, la guerre cryptographique menée par les Alliés durant la Deuxième Guerre mondiale avec les exemples de la bataille de Midway en 1942 et la capture des livres de code de la machine allemande Enigma.

Une chronologie simple permit ainsi de tracer une problématique de protection des informations et des chaînes de décision de l'Antiquité à nos jours que vint remettre en cause la première grande cyberattaque de l'Histoire. En 2007, l'Estonie alors pays le plus numérisé au monde subit une attaque cybernétique d'une ampleur inédite paralysant ses institutions et son économie. Cette attaque – que beaucoup attribuaient à la Russie – est restée à la fois un marqueur et une rupture faisant émerger de véritables doctrines nationales de cyberdéfense. D'autres attaques mettant en œuvre des virus particulièrement dangereux ont eu lieu depuis (STUXNET, Snowden, Wannacry, Solarwinds…), et l'évolution technologique permet désormais de mettre en œuvre des processus de dissimulation autrement plus sophistiqués dépassant la cryptographie classique. Ainsi, le pixel d'un fichier jpeg, qui en contient des centaines de milliers, peut de nos jours cacher une information codée voire un virus. L'exemple permit d'introduire la notion de stéganographie (technique de dissimulation de l'information).

Partant d'une définition du cyberespace à travers ses trois couches (physique, logique, cognitive), le Colonel KESSLER-RACHEL s'employa à mettre en place les grands principes de la guerre informatique sur ses trois volets essentiels : défensif, offensif et lutte d'influence. La guerre informatique a pour objectif d'atteindre ou d'assurer en permanence la disponibilité, l'intégrité et la confidentialité des informations : un triptyque fondamental et incontournable. La posture de cyberdéfense posera d'abord la question de savoir ce que nous voulons protéger et contre qui/quoi. Elle cherchera ensuite à empêcher l'extension d'une attaque à l'ensemble d'un système pour finir par l'identification de la source de la menace et de l'attaque.

Ce dernier point est ce que l'on appelle l' « attribution ». L'officier souligne son extrême difficulté eu égard au trop grand nombre d'acteurs (individus, organisations plus ou moins clandestines, mafias…) pouvant entrer en jeu, voire son impossibilité lorsqu'il s'agit d'un État… Quant aux cyberattaques que nous pourrions mener, elles sont frappées du sceau de

l'ultra confidentialité afin de ne pas révéler à la fois les failles et les cibles visées. La lutte contre l'État islamique a, par exemple, fait l'objet de mesures de cyberdéfense et de cyberattaques.

La cyberguerre est d'autant plus complexe qu'elle peut faire aussi intervenir des actions qui ne viennent pas directement du cyberespace. La bataille peut revêtir une dimension matérielle à travers des dommages infligés aux infrastructures : couper des câbles sous-marins, élever la température dans les data centers, « abandonner » des clés USB infectées… Face à ces menaces dont les implications ne sont pas toutes connues, la France s'est donnée en 2017 un commandement interarmées entièrement dédié à la cyberguerre le Commandement Cyber (COMCYBER). L'année suivante, une doctrine officielle de lutte informatique offensive a vu le jour pour la première fois ; les publications de la politique de lutte informatique défensive et de la lutte informatique d'influence ont suivi.

La cyberguerre a, en fait, déjà commencé et elle est permanente. Elle fait partie de ces nouveaux déséquilibres contemporains qui contournent désormais l'alternance classique du cycle paix-guerres. En 2010, les Etats-Unis annonçaient déjà qu'ils considéreraient les cyberattaques comme des actes de guerre pouvant être militairement traités en retour. À partir de 2013, émergeait aussi Outre-Atlantique la notion de « Pearl Harbor cybernétique ». En France, le MINARM mais aussi les hôpitaux ou les mairies subissent très régulièrement des attaques majeures.

Tout en menant son exposé, le Colonel KESSLER-RACHEL développa - à partir d'exemples concrets du quotidien - un véritable questionnement sur la nécessité d'adopter une hygiène informatique. La posture de défense est d'abord individuelle tant les failles dans les systèmes sont avant tout… humaines. Projetant les lycéens dans un avenir professionnel proche, il les encouragea à porter cette sensibilisation au plus haut niveau de leur future entreprise en obtenant, par exemple, l'adhésion de leurs responsables de services et de direction sur la question de la cybersécurité. L'enjeu peut sembler évident mais achoppe trop souvent sur les efforts budgétaires réclamés par une véritable traduction opérationnelle de la cyberdéfense sur le terrain… Il faut donc convaincre de l'intérêt de celle-ci pour le service, l'entreprise, voire pour la stratégie globale de cette dernière.

Article écrit le 22 janvier 2023
Nghia NGUYEN
180e promotion Cardinal de Richelieu
Professeur au Lycée Jean Monnet (Cognac)

---

(1) Cf. Il est l'auteur de plusieurs articles sur le sujet avec entre autres BUSSER (Marion) et KESSLER-RACHEL (Thierry), « La culture du choc. Fluctuat nec mergiteur », in *DSI*, 148, juillet-août 2020, pp. 84-87. BUSSER (Marion) et KESSLER-RACHEL (Thierry), « Y a-t-il un pilote dans la donnée ? », in *Revue Défense Nationale*, 847, 2022/2, pp. 93-98. BUSSER (Marion) et KESSLER-RACHEL (Thierry), « La donnée et la guerre : vers la guerre « donnée-centrée » ? », in *Revue Défense Nationale*, 854, 2022/9, pp. 18-23.

(2) Cf. Le *JDEF* du 27 juin 2022 « Cyber, un combat virtuel bien réel » pour approfondir.