FUTURA

Cyber Humanum Est : la cyberguerre selon l’armée française

Podcast écrit par et lu par Emma Hollen

[*Générique d’intro, une musique énergique et vitaminée.*]

Un exercice de cyberdéfense géant pour se former aux combats en ligne, c’est l’actu de la semaine, dans Vitamine Tech.

[*Fin du générique.*]

C'est une guerre silencieuse qui s'est déroulée la semaine dernière à Nancy. Pas d'explosions ni de balles qui sifflent, bien heureusement, mais des batailles de grande ampleur qui ont eu lieu sur les réseaux. À dire vrai, il ne s’agissait même pas d’un vrai combat, mais plutôt d'un exercice géant de cyberguerre mené par le Commandement de la Cyberdéfense (ou COMCYBER) et l'université de Lorraine.

[*Une musique électronique calme.*]

Baptisé Cyber Humanum Est – ou peut être Kyber ou Tchiber Humanum Est, qui sait comment les Romains l’auraient prononcé –, cet exercice de cyberdéfense a nécessité plus d’un an de travail, la collaboration de 50 organisateurs, enseignants-chercheurs, réservistes opérationnels, industriels, et réuni plus de 130 participants, dont une bonne centaine d’étudiants, du 6 au 10 février dernier. Le scénario : à cause du réchauffement climatique, l'île fictive des Riverchelles, située dans l'archipel des Maladives, assiste à l’effondrement complet de son économie, basée sur le tourisme. La découverte récente de ressources minières sur son sol pourrait sauver l’île de la banqueroute, amenant ses deux pays voisins, le tout aussi fictif Cryptanga et l’Anumeric, à se livrer un combat sans merci pour accéder le premier au précieux permis d’exploitation. Au programme : une véritable guerre d’information en ligne entre le Cryptanga et l'Anumeric, chacun doté de ses ambassades, de ses infrastructures vitales et tactiques, de ses médias… bref, d’une portion du cyberespace qu’il lui faudra défendre âprement tout en attaquant celle de la nation adverse. Ce type d’exercice, c’est ce que l’on appelle un « Wargame » ou CTF, pour « Capture The Flag ». Chaque équipe est dotée d’un réseau de sites et d’infrastructures à défendre. Elle dispose généralement d’un temps de préparation pour identifier les failles potentielles et mettre en place des mesures de protection. Puis les deux réseaux sont connectés entre eux et le combat commence. Et vous allez voir que ce genre de conflit est finalement loin d’être nouveau. Il se situe après tout dans la droite lignée de l’espionnage - contre-espionnage, et de la propagande, qu’elle soit médiatique ou étatique. La stratégie se divise en trois volets : se renseigner pour identifier l’environnement informationnel de son adversaire, ses intentions et ses dispositifs militaires ; se défendre en contrant les attaques informationnelles de l’ennemi, que ce soit en les discréditant ou en empêchant leur propagation ; et, bien

entendu, attaquer, ou agir comme le dit la présentation du ministère des armées. Cela peut passer par promouvoir l'action de ses propres troupes, convaincre les acteurs d'une crise d'agir dans le sens souhaité, dénoncer les incohérences ou les mensonges de l'adversaire, ou encore l'induire en erreur en lui donnant accès à des informations incorrectes ou incomplètes. Évidemment, aujourd'hui, la plupart de ces combats ont lieu en ligne, où l'information est stockée, dissimulée, ou diffusée. On parle alors de lutte informatique d'influence ou lutte d'influence informationnelle, aussi baptisée L2I, un ensemble d'opérations militaires dont la supervision est généralement confiée au Commandement de la Cyberdéfense, le COMCYBER. COMCYBER qui se trouve justement être l'organisateur de cette 3e édition de l'événement, en collaboration avec l'université de Lorraine. L'exercice s'est joué en simultané sur trois sites distincts : la caserne Verneau Blandan de Nancy, Polytech Nancy et Télécom… Nancy. Durant 48 heures, les équipes rouge et bleue ont dû tout mettre en place pour infiltrer les réseaux de l'opposant, attaquer ses médias pour y diffuser leur propagande, promouvoir leurs actions militaires sur les réseaux et, bien sûr, contrer les attaques réalisées sur leur propre terrain virtuel. Si vous croyez que l'exercice se cantonne à des batailles de tweets avec l'ennemi, détrompez-vous. Durant l'exercice, les participants ont dû gérer, protéger ou attaquer plus de 200 équipements virtuels, un drone militaire et son pilote, ainsi que des robots. Parmi les menaces, outre la conception de malwares dédiés, on trouvait également des attaques par ondes radio et même un groupe de hackers baptisés APT54, faisant une apparition surprise en plein milieu de l'opération. Après ces 48 heures non-stop de bataille, les meilleurs cybercombattants (qui, oui, étaient principalement masculins) ont reçu des prix selon le type d'opérations réalisées.

[*Virgule sonore, une cassette que l'on accélère puis rembobine.*]
[*Une musique de hip-hop expérimental calme.*]

L'objectif du COMCYBER, au-delà de la sensibilisation aux nouveaux enjeux des espaces virtuels, c'est bien entendu d'identifier de potentielles recrues. La compétition s'étendant sur 48 heures, du 6 au 9 février, la dernière journée du 10 février était consacrée au forum des métiers organisé par la Base de défense de Nancy au palais du gouvernement. Sur place, les partenaires de l'événement et les différents services et armées du ministère des Armées ont présenté leurs emplois dits « cyber ». Comme le dit le colonel Koessler, Commandant de la base de défense de Nancy et correspondant zonal de cyberdéfense pour l'Est, sur le site du ministère de la Défense, l'exercice et le forum ont pour but de : « faire prendre conscience [aux participants] que l'on peut s'engager au service de la défense du pays sous différentes formes ». Et ça marche, puisqu'au terme de ces wargames, plusieurs étudiants affirment avoir rejoint les rangs de la Défense. Alors que cet exercice venait de s'achever, le chef d'état-major de l'armée de terre annonçait une nouvelle organisation dans ses régiments. Celle-ci réduira l'utilisation des chars et de l'infanterie, au profit de cybercombattants et de drones. La guerre du futur est donc bel et bien en marche. Espérons qu'elle se révèle beaucoup moins meurtrière que nos anciennes formes de combat.

[*Virgule sonore, un grésillement électronique.*]

C'est tout pour cet épisode de Vitamine Tech. Si ce podcast vous plaît, je compte sur vous, pensez à vous abonner pour nous retrouver deux fois par semaine, et si vous le pouvez, parlez de ce podcast à vos proches pour le leur faire découvrir. Ça n'a l'air de rien, mais ça nous aide grandement à faire vivre Vitamine Tech et à lui garantir un bel avenir. Sur ce, je

vous souhaite une excellente journée ou une très bonne soirée, et je vous dis à la semaine prochaine, dans Vitamine Tech.

[*Un glitch électronique ferme l'épisode*.]