INTERVIEW

Enzo ALLAIN

Consultant en cybersécurité

WERRA

Février 2021

Bonjour Enzo, tout d'abord nous tenions à vous remercier pour votre temps et notamment pour nous permettre de réaliser cette interview ! Pour nos lecteurs qui ne vous connaissent pas encore, pourriez-vous vous présenter brièvement ?

EA : Merci à vous pour votre proposition d'entretien ! J'ai commencé mes études avec une Licence d'Histoire à la Sorbonne. Après ces trois années j'ai décidé de me réorienter vers des études plus axées sur l'actualité. J'ai réussi à intégrer l'Institut Français de Géopolitique (IFG) pour ma première année de Master puis l'Institut Catholique de Paris en Master 2 Géopolitique et Sécurité Internationale. C'est durant cette dernière année que je me suis spécialisé sur les enjeux du cyberespace à travers mon mémoire qui traitait de la cybersécurité en Afrique de l'Ouest.

Vous êtes donc actuellement consultant en cyber sécurité pour un cabinet de conseil mais vous avez également écrit un livre intitulé « ***La cybersécurité en Afrique de l'Ouest : Entre cyberinfluences étrangères et cybercriminalité endogènes*** » paru le 1er avril 2020 aux éditions du Cygne. Quelles sont les raisons qui vous ont poussé à vous intéresser particulièrement à la cyber sécurité en Afrique de l'Ouest ?

EA : Comme j'ai pu vous l'indiquer lors de votre précédente question je n'avais pas du tout orienté mes premières années d'étude supérieures vers ce domaine. C'est lorsque je suis arrivé à la fin de ces trois années de Licence que j'ai d'abord décidé de m'orienter vers la thématique du cyberespace, qui est un domaine de recherche important à l'IFG. Ensuite, j'ai souhaité traiter une aire géographique qui n'avait pas encore été beaucoup étudiée dans ce domaine, c'est pour cela que je me suis orienté naturellement vers l'Afrique, et plus particulièrement l'Afrique de l'Ouest. J'avais quelques informations sur ce sujet mais c'est vraiment lorsque je m'y suis penché que j'ai découvert toute la richesse de ce domaine dans une région du monde qui peut paraître délaissée par les enjeux du cyberespace.

Dans votre ouvrage, vous réfutez l'idée que le continent africain est délaissé par la cybersécurité, la cybercriminalité et toutes les thématiques qui en découlent. Pensez-vous que l'Afrique, dont une croissance exponentielle est attendue dans les prochaines décennies, devienne un terreau important de cyberattaques ?

EA : Selon moi, l'Afrique est déjà un terreau important de cyberattaques, il suffit d'ailleurs de voir le vaste panorama d'attaques cyber qui existe sur ce continent. Effectivement, les pays ouest-africains n'ont pas encore la force de frappe de pays comme les États-Unis, Israël, la Russie ou l'Iran mais il existe de nombreuses cyberattaques à l'échelle individuelle, réalisées par des cyberdélinquants ou cyberescrocs.

Certaines escroqueries africaines sont bien connues comme l'attaque nigériane ou fraude 4-1-9 - il s'agit d'une escroquerie où la victime reçoit un e-mail lui indiquant qu'une personne X bénéficie d'une grande entrée d'argent (le plus souvent d'un héritage). Par la suite l'attaquant demande l'aide de la victime pour percevoir cet argent hypothétique en lui indiquant que l'héritage est bloqué sur un compte et que les démarches coûtent quelques centaines ou milliers d'euros. La victime, crédule, avance de l'argent afin de toucher une portion de l'héritage en contrepartie - ou le broutage ivoirien - durant cette arnaque, l'escroc tente de créer une relation sentimentale avec la victime pour mieux lui soutirer de l'argent pendant une longue période.Mais au-delà de ces cyberarnaques à échelle « humaine », l'Afrique de l'Ouest apparaît comme un territoire particulier au sein du cyberespace, en raison de l'absence d'hygiène informatique dans la région, le développement d'infrastructures importantes durant les dernières années (notamment les câbles sous-marins) ou encore le développement de partenariats internationaux entre les pays de la région et les pays extérieurs dans le domaine de la cybersécurité.

En Afrique de l'Ouest la France est très bien implantée, notamment à travers ses diverses entreprises comme Total par exemple. Avec la course aux investissements chinois, russes et américains sur le continent africain, faut-il craindre pour les investissements français en Afrique ? Quels seraient les principaux risques en matière de cybersécurité pour des institutions gouvernementales ou privées françaises ?

EA :L'enjeu n'est pas uniquement présent en Afrique de l'Ouest. Le cyberespace est international et l'attaque d'un système d'information d'une PME française peut avoir des répercussions sur des grandes entreprises du monde entier. Tout est interconnecté actuellement, ça n'a donc plus réellement de sens de ne protéger qu'une partie d'un système d'information d'une entreprise sous prétexte qu'elle se situe dans telle ou telle partie du monde. La cybersécurité doit être globale et internationale et cela les grands groupes le savent très bien et s'en prémunissent.

L'Afrique, notamment dans le Sahel, voit une recrudescence de la menace terroriste ces dernières décennies. Pourtant les menaces en matière de cybersécurité semblent être ignorées lorsque l'on fait allusion au terrorisme en Afrique. Connaissez-vous des groupes terroristes usant de failles dans le domaine cyber pour perpétrer des attaques en Afrique de l'Ouest notamment ? Si oui, quels types d'attaques mènent-ils et quelles sont les principales menaces planant sur les entreprises présentes sur zone ?

EA : L'Afrique de l'Ouest, notamment la région du lac Tchad, apparaît comme une zone fertile pour les mouvements terroristes mais on ne peut pas dire qu'actuellement ces derniers mouvements terroristes de la région procèdent à des actions de cyberattaques, comme pourraient le faire certaines Advanced Persistent Threat[1], cela est sans doute dû à la fracture numérique qui est réelle dans la région puisqu'il est difficile d'apporter Internet sur tout le territoire et notamment jusqu'aux villages les plus reculés (la 2G représente encore plus de la moitié des connexions en Afrique de l'Ouest).

Cependant, les groupes terroristes s'adaptent et notamment dans leur communication, Internet est une véritable arme pour eux. La communication de Boko Haram, par exemple, a beaucoup évolué en quelques années. Jusqu'en 2015 leur propagande est assez classique. Il s'agit de revendications anti-occidentales, de divulgations d'informations ou de revendications faites par le biais de vidéos. Cependant, depuis 2015, et l'allégeance du groupe terroriste à l'État islamique, sa propagande s'est perfectionnée. Les vidéos sont maintenant directement traduites en français et en anglais et présentent les actions réalisées par les terroristes : jugement, égorgement, présentation des armes et matériels militaires... Enfin, à partir de juillet 2016, les vidéos de Boko Haram reprennent véritablement les codes visuels de l'État islamique (avec effets sonores, musiques grandiloquentes, chants religieux etc.). Il n'y a donc pas d'attaque cyber comme on pourrait l'entendre mais ces groupes terroristes utilisent fortement le cyberespace comme moyen de communication. L'application de messagerie cryptée Telegram est très utilisée par les djihadistes pour communiquer entre eux par exemple. Cela leur permet de partager les vidéos et les communiqués qui vont par la suite être relayés sur Twitter ou Facebook.

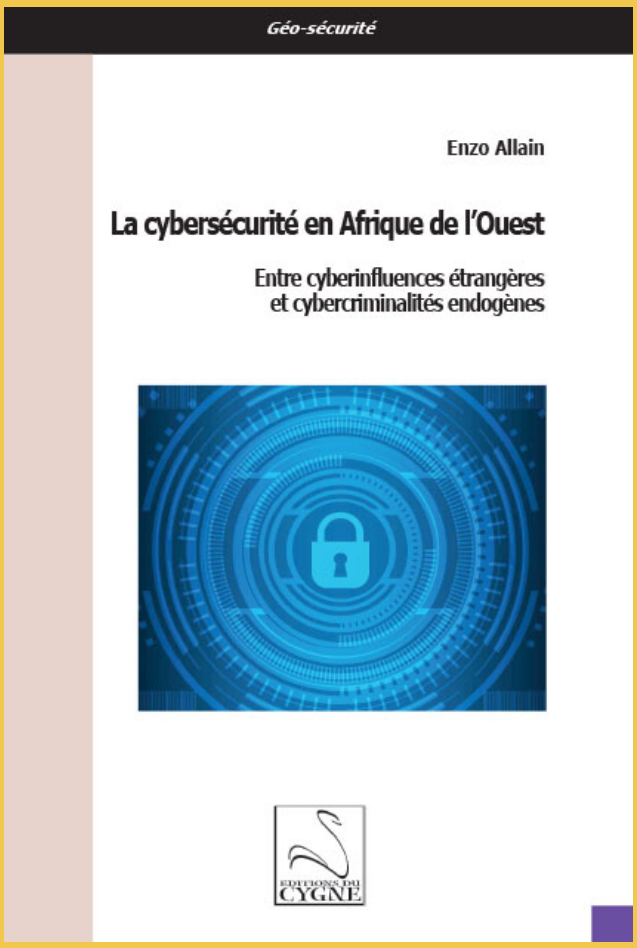
Quelles sont les stratégies sécuritaires mises en place par les Etats pour justement faire face à ces menaces et aux potentielles attaques dont ils peuvent-être les cibles ?

EA : Pour reprendre votre dernière question sur les groupes terroristes, les États peuvent mettre en place des actions pour contrôler leur espace cyber, même si cela peut flirter avec la cybercensure. Au-delà de cela, il existe de nombreux partenariats internationaux qui voient le jour, entre les pays de la région et les pays étrangers. La France, par exemple, permet depuis 2013 à des officiers et sous-officiers de disposer de formations à la sécurité informatique au Sénégal. C'est également le cas au Niger où la France, à la demande du pays, a envoyé un détachement d'instruction technique « cybersécurité » entre janvier et février 2018. Autre élément, la création en novembre 2018, de la première école nationale de cybersécurité à vocation régionale de Dakar. Cette école vise à former les cadres africains aux enjeux de la cybersécurité. Enfin, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) travaille avec l'AfricaCERT pour mettre en place des CERT (Computer Emergency Response Team) dans la région. Elle est également partenaire des SecurityDays qui ont lieu à Dakar chaque année[1] et elle met en place des protocoles de coopération bilatérale, comme avec l'ADIE (Agence de l'informatique de l'Etat du Sénégal) en 2016.

Au niveau plus national, les pays de la région prennent également en compte ces enjeux. On voit durant cette décennie la promulgation de loi portant sur la cybersécurité (Sénégal, Côte d'Ivoire, Nigéria…), la création d'une stratégie nationale de cybersécurité (Sénégal, Bénin, Nigéria…) et enfin, la création d'une agence de nationale sur la cybersécurité - équivalente à l'ANSSI en France - (Bénin, Burkina Faso, Sénégal…)

Les menaces cyber se sont-elles accrues avec la crise sanitaire actuelle ou bien sont-elles les mêmes qu'avant ? Ne risque-t-on pas de voir une augmentation drastique des cyberattaques contre des laboratoires, des hôpitaux, des entreprises par exemple ?

La cyberdéfense et la cybersécurité est un perpétuel jeu d'adaptation. Les attaquants s'adaptent aux nouvelles technologies et/ou aux évènements planétaires (COVID-19) afin de trouver sans cesse de nouvelles failles et les défenseurs s'adaptent aux nouvelles stratégies trouvées. En plus de cela, s'ajoute la sensibilité des données de santé. Cette association d'enjeux fait de la crise sanitaire actuelle un parfait exemple de potentielle crise cyber. On l'a vu en décembre dernier avec l'attaque à l'encontre de l'Agence européenne du médicament. Il n'y a pas de limite aux cyberattaques. Afin de mettre à mal la stratégie vaccinale de la France les attaquants peuvent très bien attaquer les hôpitaux, les cliniques, ou encore la chaîne logistique des vaccins pour déstabiliser la chaîne du froid qui est une question épineuse pour le transport des vaccins.



Retrouvez l'ouvrage d'Enzo Allain "***La cybersécurité en Afrique de l'Ouest : Entre cyberinfluences étrangères et cybercrimanlités endogènes***", sur les diverses plateformes de vente en ligne