Nicolas Arpagian, expert en cyberdéfense

"La Côte d'Ivoire doit renforcer la formation des policiers et des magistrats"

Le thème annoncé pour la 3e édition de Shield Africa est la cyberguerre. Ne pensez-vous pas qu'il est prématuré pour l'Afrique de se pencher sur de telles préoccupations?

Dès lors qu'un particulier, une entreprise, une administration ou un état-major est connecté à Internet et s'appuie sur un système informatique pour exercer son activité, la cybersécurité doit être un sujet de préoccupation. Qu'il s'agisse de détournement d'argent, d'usurpation d'identité ou de prise de contrôle à distance des systèmes informatiques, les menaces sont multiples. Sans oublier la possible contamination d'un ordinateur dont la puissance de calcul serait utilisée, par exemple, à l'insu de son légitime propriétaire pour mener des opérations d'attaques informatiques. Avec Internet, la notion de frontière physique doit être reconsidérée. Il suffit d'un clic pour accéder à un site ivoirien ou européen. Et le transfert de fichiers d'un continent à l'autre s'effectue en quelques minutes à peine. Dès lors que l'informatisation des organisations (sociétés commerciales ou services étatiques) africaines se renforce, il est indispensable d'intégrer la logique de cybersécurité. Tant pour les particuliers que pour les professionnels, civils ou militaires.

L'Afrique est-elle réellement exposée à beaucoup d'attaques ?

A partir du moment où l'on peut récupérer des coordonnées bancaires, le détail de vos correspondances commerciales pour connaître vos secrets d'affaires ou espionner vos négociations politiques ou diplomatiques, l'Afrique n'a pas de raison d'être épargnée par de telles attaques. D'autant plus que quelques euros suffisent, par exemple, pour louer ponctuellement un réseau d'ordinateurs contaminés (on parle de *botnets*) pour mener une opération de blocage à distance d'un site Internet par déni de service. En clair, une multitude d'ordinateurs vont recevoir l'ordre de se connecter simultanément à un même site Internet, comme celui d'un cybermarchand, pour empêcher l'accès des clients légitimes ou faire s'écrouler son infrastructure informatique.

Quelles seraient les mesures que la Côte d'Ivoire pourraient prendre pour intégrer les standards internationaux en matière d'internet?

Pour formaliser sa démarche, la Côte d'Ivoire pourrait s'inspirer de la Convention du Conseil de l'Europe de novembre 2001 sur la cybercriminalité qui est le texte international de référence sur le sujet. Dans cet esprit, elle pourrait renforcer la formation de policiers et magistrats afin qu'ils soient davantage familiarisés avec les techniques de cyberattaque. De manière à comprendre cette nouvelle forme de criminalité dont les Ivoiriens peuvent également être les victimes. Et si des cybercriminels agissent à partir du territoire ivoirien, cette connaissance facilitera les poursuites à leur encontre et la coopération avec les services policiers ou judiciaires à l'étranger. Il est important que les pays qui sollicitent la coopération de la Côte d'Ivoire puissent identifier aisément des interlocuteurs spécialisés au sein des administrations. Et que par leur réactivité, ils contribuent à la poursuite des

cybercriminels. Cela demande une adaptation constante, mais cela est nécessaire en raison de l'évolution permanente des modes opératoires.

La France a-t-elle une réponse en matière de cyberdéfense et de développement d'armes informatiques offensives ?

Désormais, les principaux pays du monde publient des doctrines de cyberdéfense. Ce sont, en général, des documents que l'on trouve sur les sites Internet de leurs ministères de la Défense. En France, depuis 2008, les autorités reconnaissent que l'on peut mener des ripostes informatiques offensives. Et le Livre blanc sur la défense et la sécurité nationale de 2013 explique clairement que la France est dotée « *de capacités défensives et offensives, qui concernent aussi bien toutes les administrations que les services spécialisés et les armées* ». Tout le monde s'accorde désormais sur le fait que les cyberattaques font désormais pleinement partie des arsenaux des Etats. Qu'il s'agisse de capter des informations chez des adversaires ou des compétiteurs ou de mettre hors d'état de fonctionner normalement les systèmes d'information de sa cible. Cela peut atteindre des infrastructures civiles ou militaires.

Peut-on savoir le principal défi de la cyberguerre offensive ?

Il n'y a pas, a priori, de «bonne» cyberarme. Il y a celle qui permet d'atteindre l'objectif que l'on s'est fixé. Cela peut être d'espionner des secrets diplomatiques ou industriels sans se faire repérer ou de détruire par un dérèglement technique des centrifugeuses nucléaires iraniennes. En Estonie en 2007, ce furent des sites Internet d'administrations gouvernementales, de médias et de sociétés privées qui furent bloqués. En 2008, les pages d'accueil de sites officiels géorgiens furent modifiées de manière à faire comprendre à leurs propriétaires qu'ils n'en avaient plus le contrôle : le portrait d'Hitler remplaçait celui du Premier ministre en place. En matière d'attaque informatique, l'imagination est sans limite. Car des failles techniques peuvent toujours être identifiées. Et si la technologie était consolidée, il existe toujours l'option humaine. Que ce soit Bradley Manning dans le cas de *Wikileaks* ou *Snowden*, plus récemment, ce sont bien des individus qui ont permis de passer outre l'outillage informatique.

Quels devraient être les points principaux d'une doctrine d'emploi des armes informatiques offensives ?

Au-delà des déclarations politiques incantatoires, les Etats semblent finalement assez réticents à faire la lumière sur les techniques de cyberattaque. Car les gouvernements apprécient de disposer d'outils qui rendent difficile l'attribution de la responsabilité du vol de données ou de la destruction d'équipement d'un pays tiers. Surtout que des Etats peuvent être des alliés politiques, mais des concurrents économiques. Et dans ce cas, on peut avoir intérêt à espionner un allié pour lui dérober son savoir-faire économique, mais sans pour autant aller à l'affrontement avec lui. Et si on ne peut pas prouver que vous êtes à la manœuvre, les relations restent cordiales. Mme Clinton avait annoncé, il y a quelques années, que les Etats-Unis s'autorisaient à riposter à une cyberattaque par des moyens conventionnels (tirs, bombardements...).

Pensez-vous que l'on arrivera un jour à une dissuasion cyber ?

Le principe de la dissuasion nucléaire est fondé sur la crainte d'être soi-même anéanti dès lors qu'on attaquerait un pays doté de l'arme atomique. La transposition de cette dissuasion à la matière informatique ne peut être envisagée qu'à partir du moment où cette technologie permettrait de commettre des dégâts assimilables par leur ampleur, leur durée et leur caractère irrémédiable à une bombe nucléaire. Dans ce domaine du pire, l'Homme sait, hélas, faire preuve de créativité.

PROPOS RECUEILLIS PAR **ALAKAGNI HALA**

Un expert en cyberdéfense

Nicolas Arpagian est directeur scientifique du cycle " Sécurité numérique à l'Institut national des hautes études de la sécurité et de la justice (Inhesj). Il enseigne aussi à l'Ecole nationale supérieure de la police (Ensp) et à l'université de Strasbourg sur le sujet. Il est rédacteur en chef de la revue Prospective stratégique du Centre d'étude et de prospective stratégique (Ceps). Il a son actif plusieurs ouvrages publiés sur le sujet. Parmi lesquels « *La cyberguerre* – La guerre numérique a commencé» (Editions Vuibert). Ou «*La Cybersécurité*» aux Presses universitaires de France (Puf).

Il convient de noter que l'Institut national des hautes études de la sécurité et de la justice est un établissement public. Il est placé sous l'autorité du Premier ministre français.

A. H