Entre 2016-2017, l´Etat camerounais a injecté plus de 14 milliards de francs CFA pour sécuriser son cyberespace. Mise à la disposition de l´Agence nationale des TIC, cette enveloppe provient du Fonds spécial des télécommunications (FST), renfloué chaque année par les opérateurs de télécommunications en activité au Cameroun.

Le gouvernement camerounais se veut mobilisé contre la cybercriminalité. Tant le fléau fait des ravages dans le pays. Entre 2016-2017, les autorités camerounaises ont injecté pas moins de 14 milliards de francs CFA dans la sécurisation du cyberespace du pays. Selon le ministère camerounais des postes et télécommunications, il s´agit d´une enveloppe qui provient d´un Fonds spécial des télécommunications (FST), lequel est dépendant des cotisations des opérateurs de télécommunications en activité du pays.

Les sources officielles indiquent que cette enveloppe a été mise à la disposition de l´Agence nationale des TIC (ANTIC) pour financer la réalisation des travaux et à l´achat d´équipements divers, dans le cadre d´un programme de sécurisation du cyberespace camerounais. « Internet permet de communiquer avec potentiellement tout le monde et donc n´importe qui. Il est difficile, voire impossible, de vérifier qui se cache derrière un écran ou une identité virtuelle. Les esprits malveillants utilisent l´Internet et les réseaux sociaux à des fins de propagande, d´escroquerie ou de terrorisme », a rappelé la ministre camerounaise des postes et télécommunications, Minette Libom Li Likeng, très au fait de la menace. Ces dernières années,

en raison de la prolifération rapide de la technologie, le pays est de plus en plus exposé à la cybercriminalité qui occasionne d´importantes pertes financières aux particuliers, aux entreprises et même à l´administration publique camerounaise et qui prend de l´ampleur dans le pays, estime la responsable gouvernementale.

A en croire l´ANTIC, une variété d´activités de cybercriminalité est répandue actuellement au Cameroun. L´agence a déjà répertorié le ´´scamming´´ (escroquerie financière sur Internet), le ´´skimming´´ (fraude à la carte bancaire), la fraude à la Simbox (boîtier électronique utilisé pour se faire facturer le trafic téléphonique international aux prix du tarif national), le ´´Web defacement´´ (modifications non autorisées de la page d´accueil d´un site web), ou encore le ´´spoofing´´ (usurpation d´identité), etc.

Près de 8 milliards perdus à cause du "scamming" et du "skimming" Fin publicité dans 89 s

L´engagement de l´ANTIC est compréhensible vu les dégâts que cause la cybercriminalité. L´agence a indiqué que le Cameroun a perdu ces dernières années près de 4 milliards francs CFA dues au scamming. Aussi, l´Etat camerounais a perdu environ 3,7 milliards de Francs CFA à cause du skimming. En ce qui concerne l´usurpation de profiles Facebook et le cyberchantage, c´est plus de 200 cas qui ont été enregistrés. Madame Li Likeng a annoncé que 51% du volume de trafic Internet national est lié aux téléchargements illicites. « Dans le cadre des cyberguerres vécues de nos jours, des Etats attaquent les systèmes d´informations d´autres Etats dans le but de les paralyser. Le piratage des moyens de télécommunication, des infrastructures sensibles comme les aéroports, les gares et les métros, est devenu monnaie courante. Le cyberterrorisme est une menace réelle. Depuis 2013, le Cameroun a connu 12 800 cyberattaques », a indiqué la ministre face aux gouverneurs des 10 régions du pays, au cours d´une conférence à Yaoundé, en août dernier.

Vu l´ampleur du phénomène, l´Etat camerounais a mis en place plusieurs dispositifs. « Sur le plan réglementaire, on peut citer l´adoption de trois (3) lois importantes visant à réglementer, à contrôler et à sanctionner les dérives liées à l´usage du cyberespace national. Il s´agit de la loi n° 2010/012 régissant la cybersécurité et la cybercriminalité, la loi n° 2010/013 régissant les Communications électroniques au Cameroun et la loi n° 2010/021 régissant le Commerce électronique au Cameroun, ainsi que de leurs textes d´application », précise la ministre. Elle a ajouté qu´en plus du cadre réglementaire et institutionnel mis sur pied, des actions précises ont été menées. « L´ANTIC dispose en son sein d´un Centre d´alerte et de réponse aux incidents cybernétiques (en abrégé le CIRT), dont la mission est d´assurer la veille sécuritaire sur le cyberespace national en collaboration avec d´autres Etats », a argué la ministre des postes et télécommunications.

Source:latribune.fr