MINISTERE DES POSTES ET TELECOMMUNICATIONS
-CAMEROUN-

Deuxième Forum National sur la Cybersécurité et la Lutte contre la Cybercriminalité (FNCC) 2022

Thème: Cyberespace national et réponse à la menace sécuritaire

RAPPORT GENERAL

Palais des Congrès de Yaoundé, le 14 octobre 2022

SOMMAIRE

I. INTRODUCTION

Dans le cadre de la mise en œuvre de la politique gouvernementale en matière de sécurité des réseaux et des systèmes d'information, le Ministère des Postes et Télécommunications a organisé du 12 au 14 octobre 2022 au Palais des Congrès de Yaoundé, le deuxième Forum National sur la Cybersécurité et la Lutte contre la Cybercriminalité (FNCC 2022) sur le thème : « ***cyberespace national et réponse à la menace sécuritaire*** ». Le but de ce forum était de susciter des échanges entre experts nationaux sur les réponses aux menaces qui pèsent sur le cyberespace national et d'en dégager des recommandations qui permettront de consolider les politiques, les stratégies et les programmes de cybersécurité.

Ce forum a connu la participation des experts issus du secteur public, du secteur privé, des organisations internationales et de la société civile (liste des experts jointe en annexe).

Le présent rapport restitue le déroulement des travaux et en dégage les principales recommandations.

II. DEROULEMENT DU FORUM

Le Forum National sur la Cybersécurité et la lutte contre la Cybercriminalité s'est articulé autour des points suivants :

1. Cérémonie solennelle d'ouverture ;
2. Travaux en plénière ;
3. Salon d'exposition.

II.1 - Cérémonie solennelle d'ouverture

La cérémonie solennelle d'ouverture a été présidée par le Secrétaire Général du Ministère des Postes et Télécommunications, Monsieur Mohamadou SAOUDI, représentant personnel de Madame le Ministre des Postes et Télécommunications. Cette cérémonie était rehaussée par la présence d'un ensemble de personnalités tant nationales qu'internationales, parmi lesquelles, le Chef du Bureau de Zone de l'Union Internationale des Télécommunications pour l'Afrique Centrale et Madagascar et le Recteur de ICT UNIVERSITY. Elle a été ponctuée par la lecture du rapport du niveau de mise en œuvre des recommandations du premier forum, une leçon inaugurale et deux (02) allocutions.

II.1.1 Lecture du rapport du niveau de mise en œuvre des recommandations du FNCC-2020

La lecture du rapport du niveau de mise en œuvre des recommandations issues du premier Forum National sur la cybersécurité et la lutte contre la cybercriminalité a été faite par le Rapporteur Général du forum. Il ressort de cette présentation que sur les quarante-deux (42) recommandations formulées, vingt (20) ont été exécutées soit un pourcentage de 48% ; seize (16) sont en cours d'exécution, soit un taux de 38% et six (06) n'ont pas été exécutées, soit un taux de 14%.

La mise en œuvre de ces recommandations a rencontré quelques difficultés au rang desquelles :

- l'insuffisance des moyens alloués à cette activité;
- la résistance au changement ;
- la carence de l'expertise en la matière.

Il est à noter que ces difficultés ont été amplifiées en raison de l'absence d'une structure chargée du pilotage, de l'accompagnement et de l'évaluation de la mise en œuvre des recommandations formulées. A cet égard, la mise en place d'un Groupe de Travail y afférent a été proposé comme préconisé au cours du dernier forum.

II.1.2 Allocution du Représentant du Bureau de zone de l'UIT pour l'Afrique Centrale et Madagascar

Monsieur Jean Jacques MASSIMA LANDJI, Représentant du Bureau de zone de l'Union Internationale des Télécommunications pour l'Afrique Centrale et Madagascar a pris la parole pour saluer l'initiative entreprise par le Cameroun en vue de combattre la cybercriminalité à travers l'organisation des fora. Il a relevé les bienfaits des Technologies de l'Information et de la Communication qui sont un catalyseur de développement et un véritable outil de création de richesses. Cependant, il a déploré les pertes annuelles engendrées par les cybercrimes qui sont de l'ordre de 4 milliards de dollars en Afrique d'après l'organisation Techcabal. C'est ainsi qu'il a encouragé le Cameroun à mettre en place des mesures visant à sécuriser son cyberespace et a réaffirmé la disponibilité de l'Union Internationale des Télécommunications, qui élabore des outils visant à promouvoir la cybersécurité à l'instar des lignes directrices pour la protection des

enfants en ligne, à assister les pays dans la lutte contre la cybercriminalité. Il a clos son intervention en invitant le Cameroun et toutes les forces vives du numérique à contribuer à la cinquième édition de l'Indice Mondiale de la Cybersécurité de l'UIT connue sous son appellation anglaise « Global Cybersecurity Index (GCI) ».

II.1.3 Leçon inaugurale

La leçon inaugurale a été faite par le Professeur Emmanuel PONDI, Recteur de « ICT UNIVERSITY » qui a axé sa présentation en trois (03) points à savoir la perception de la cybercriminalité et de la cybersécurité à travers les âges et les communautés, les éléments de vulnérabilités du Cyberespace national et continental et, les propositions de stratégies pour la sécurisation des échanges dans le cyberespace africain et camerounais. Poursuivant son propos, il a défini la notion de cybercriminalité et a indiqué que sa perception était étroitement liée à l'aire géographique. Par la suite, il a présenté les facteurs de vulnérabilité du cyberespace national et continental comme des facteurs sociologiques, réglementaires et économiques. Il a enfin fait état des suggestions de stratégies pour la sécurisation des échanges dans le cyberespace africain et camerounais en insistant sur la zone de libre échange continentale.

I.1.4 Allocution de Madame le Ministre des Postes et Télécommunications

Le Secrétaire Général du Ministère des Postes et Télécommunications, Monsieur Mohamadou SAOUDI, qui représentait Madame le Ministre des Postes et Télécommunications, a prononcé le discours d'ouverture.

Dans son allocution le Secrétaire Général du Ministère des Postes et Télécommunications a commencé par souhaiter la bienvenue aux experts participants au forum.

Il a poursuivi son propos en indiquant que ce forum constitue avec la campagne nationale pour la promotion de la culture de la cybersécurité et la sensibilisation à l'utilisation responsable des réseaux sociaux engagée par le Ministère des Postes et Télécommunications il y a quelques années, une étape supplémentaire de la mise en œuvre, sur Très Haute Instructions du Chef de l'Etat, de la politique nationale de cybersécurité. En effet, a-t-il ajouté, ce regroupement d'experts en matière de cybersécurité, constitue une phase importante de la réflexion devant conduire ladite politique.

Ensuite il a présenté les avantages des Technologies de l'Information et de la Communication en général et de l'Internet en particulier, dans le développement économique, social, scientifique et administratif. Au-delà de ces avantages, il a indiqué les menaces auxquelles sont confrontés les usagers et les organisations dans le cyberespace et la nécessité de les endiguer en vue de garantir une confiance totale dans l'utilisation du numérique. Enfin, au regard des menaces en constante évolution, il a exhorté les experts à trouver des solutions appropriées pour assurer la sécurisation du cyberespace camerounais.

II.2 Travaux en plénière

Quatre (04) panels, composés de vingt-et-un (21) exposés, ont meublé les travaux en plénière. Les présentations et les échanges ont globalement porté sur : la protection des infrastructures et des données de l'Etat ; la sécurisation des réseaux de télécommunications ; les procédures de répression des infractions et de défense du cyberespace national ; le développement du capital humain et de la coopération internationale en matière de cybersécurité.

II.2.1 Protection des infrastructures et des données de l'Etat

Les échanges qui ont été abordés dans ce panel ont porté sur cinq (05) communications. A l'entame de ce panel, le cadre légal, réglementaire et institutionnel de la cybersécurité et de la lutte contre la cybercriminalité a été présenté. Il en ressort qu'il existe non seulement plusieurs institutions qui collaborent dans le cadre de la gestion de cette question mais également plusieurs textes nationaux et internationaux qui s'y rapportent. Par la suite, le mécanisme de protection des infrastructures critiques a été abordé. Il s'agit des infrastructures dont la mise hors service a un impact significatif sur le fonctionnement de l'Etat. Les menaces y relatives ont été identifiées et un projet visant à les protéger a été annoncé. Les échanges se sont poursuivis sur les solutions aux menaces des infrastructures bancaires qui font l'objet d'une transformation digitale avancée, ouvrant la voie aux multiples cyberattaques dont les modes opératoires et les réponses associées ont été présentés. Par ailleurs, la technologie blockchain a été discutée et il ressort qu'elle constitue une solution idoine pour la protection des services gouvernementaux. Enfin, la discussion sur la souveraineté des données a

permis de prendre conscience du fait que la perte de contrôle des données peut altérer l'autorité de l'Etat.

A l'issue de ces échanges, les difficultés suivantes ont été soulevées :

- la méconnaissance par certains acteurs de la législation en vigueur en matière de cybersécurité et de cybercriminalité ;
- l'obsolescence de la législation en vigueur du fait du caractère essentiellement dynamique des TIC ;
- la non mise en œuvre des recommandations issues des audits de sécurité ;
- la résistance au changement ;
- l'inexistence d'une autorité de protection des données à caractère personnel ;
- la gestion anarchique des données étatiques ;
- la non existence d'un Data center étatique dédié.

II.2.2 Sécurisation des réseaux des télécommunications

Les débats qui ont meublé ce sous thème ont été animés par les opérateurs de télécommunications, les fournisseurs de service Internet et le Régulateur des Télécommunications. Ces échanges ont essentiellement porté sur les mécanismes mis en œuvre par ces différents acteurs pour la protection des points critiques et des abonnés. Il en est globalement ressorti que les points critiques sont protégés à travers les procédures et outils techniques spécifiques. Les abonnés quant à eux sont protégés à travers le processus d'identification et de sensibilisation à l'adoption d'une culture de cybersécurité. S'agissant du phénomène des SIMBOX, des mesures particulières sont prises par les opérateurs en relation avec les partenaires spécialisés pour les atténuer.

Au titre des problèmes soulevés, l'on note :

- l'absence d'un cadre légal sanctionnant l'activité des SIMBOX ;
- l'absence d'un cadre de collaboration entre les opérateurs ;
- la non fiabilité des données issues du processus d'identification des abonnés.

II.2.3 Procédures de répression des infractions et de défense du cyberespace national

Dans le cadre de ce panel, une approche de recueil des preuves numériques faisant recours à un expert en la matière, afin d'établir les responsabilités en cas d'infraction cybernétique, a été présentée. Ensuite, les méthodes d'investigations numériques ayant recours aux organes d'appuis tels que les opérateurs de téléphonie mobile et les agences de régulation du numérique comme l'ANTIC et l'ART ont été relevées. Il a également été fait état des méthodes de conduite des opérations de cyberdéfense de même que les mécanismes de réponse disproportionnée à une crise insurrectionnelle.

Les problèmes soulevés dans ce cadre ont porté sur :

- l'inexistence d'un cadre spécifique lié à l'activité d'investigation numérique ;
- l'absence d'une structure de veille en matière de cybersécurité ;
- la difficulté de réponse aux réquisitions ;
- l'absence d'un tribunal spécialisé dans les affaires du numérique ;
- le cloisonnement des structures opérant dans le domaine de la cybersécurité ;
- la non prise en compte de la composante cyberespace dans les corps de défense.

II.2.4. Développement du capital humain et de la coopération internationale en matière de cybersécurité

Les discussions abordées dans ce panel ont traité de quatre (04) sujets. Les institutions qui offrent des formations dans le domaine de la cybersécurité au Cameroun ont été présentées, de même que les problèmes liés à la cyber-expertise. Par la suite, les enjeux de l'utilisation inappropriée des réseaux populaires ont été évoqués. Enfin, les mécanismes de maîtrise des réseaux sociaux par les Etats ont été traités.

Au titre des problèmes soulevés, l'on note :

- la non adhésion du Cameroun au Forum GFCE c'est-à-dire au « Global Forum on Cyber Expertise » ;

- l'absence du droit du numérique dans les programmes de formation universitaire ;
- l'absence de collaboration entre les administrations, les entreprises et les universités pour la recherche des solutions aux nouvelles attaques ;
- l'inexistence d'un ordre national des experts en cybersécurité ;
- l'absence d'une politique de reconversion des hackers ;
- la prolifération des abonnements non désirés effectués par les opérateurs de télécommunications.

II.3 Salon d'exposition

En marge des travaux en plénière, un salon d'exposition s'est tenu sur le hall attenant à la salle des travaux. Ce salon, qui a été ouvert par le Secrétaire Général du Ministère des Postes et Télécommunications représentant le Ministre des Postes et Télécommunications, a connu la participation des structures publiques et privées suivantes : MINPOSTEL, ANTIC, MTN, ESOKA CYBERSECURITY DIVISION, ICT UNIVERSITY, DELOITTE, SANCFIS, IMPROVE MANAGEMENT.

Ces structures ont présenté aux visiteurs les activités qu'elles mènent dans le domaine de la sécurité des réseaux et des systèmes d'information.

III. RECOMMANDATIONS

Au terme des débats qui ont alimenté le forum, les recommandations ont été formulées dans les domaines :

- de la protection des infrastructures et des données de l'Etat ;
- de la sécurisation des réseaux de télécommunications ;
- des procédures de répression des infractions et de défense du cyberespace national ;
- du développement du capital humain et de la coopération internationale en matière de cybersécurité.

Pour ce qui est de la protection des infrastructures et des données de l'Etat, il a été suggéré :

- d'intensifier les campagnes de sensibilisation des acteurs du cyberespace national sur la législation en vigueur en matière de cybersécurité et de cybercriminalité ;
- de mettre à jour la législation en vigueur afin de prendre en compte les avancées technologiques et les nouvelles infractions ;
- de mettre en place un mécanisme juridique contraignant les administrations publiques et privées à mettre en œuvre les recommandations issues des audits de sécurité ;
- de mettre en place une autorité de protection des données à caractère personnel ;
- de mettre en place un Data center gouvernemental dédié et redondé.

S'agissant de la sécurisation des réseaux de télécommunications, il a été préconisé :

- de mettre en place un cadre réglementaire sanctionnant l'activité des SIMBOX ;
- de favoriser un cadre de collaboration entre les opérateurs ;
- de mettre en place la plateforme commune d'identification des abonnés.

Concernant les procédures de répression des infractions et de défense du cyberespace national. Il a été demandé de mettre en place :

- un cadre réglementaire lié à l'activité d'investigation numérique ;
- une structure dédiée à la veille en matière de cybersécurité ;
- des points d'accès aux bases de données des opérateurs aux fins du traitement des réquisitions dans les unités de police et de gendarmerie ;
- un tribunal spécialisé dans les cybercrimes ;
- une plateforme d'échange entre les structures opérant dans le domaine de la cybersécurité ;
- un commandement de la composante cyberespace dans les corps de défense nationale.

S'agissant du développement du capital humain et de la coopération internationale en matière de cybersécurité, il a été proposé :

- de procéder à l'adhésion du Cameroun au Forum GFCE c'est-à-dire au « Global Forum on Cyber Expertise » ;
- d'introduire le droit du numérique dans les programmes de formation universitaire ;
- de créer des synergies entre les administrations, les entreprises et les universités pour la recherche des solutions à de nouvelles attaques ;
- de mettre en place un ordre national des experts en cybersécurité ;
- de mettre en place une politique de reconversion des hackers ;
- de mettre en place à l'ART des mesures destinées à combattre les abonnements non désirés effectués par les opérateurs de télécommunications.

Au vu des recommandations formulées au cours du précédent et de l'actuel forum et, de l'importance de leur mise en œuvre pour l'émergence d'un cyberespace camerounais plus sûr, il a été suggéré, pour plus d'efficacité, de mettre en place un Groupe de Travail coordonné par le MINPOSTEL et comprenant l'ensemble des parties concernées et chargé du pilotage, de l'accompagnement, de l'évaluation et de l'implémentation desdites recommandations. /-