

REPUBLIQUE DU CAMEROUN  
Paix – Travail - Patrie

-----  
MINISTERE DES POSTES  
ET TELECOMMUNICATIONS



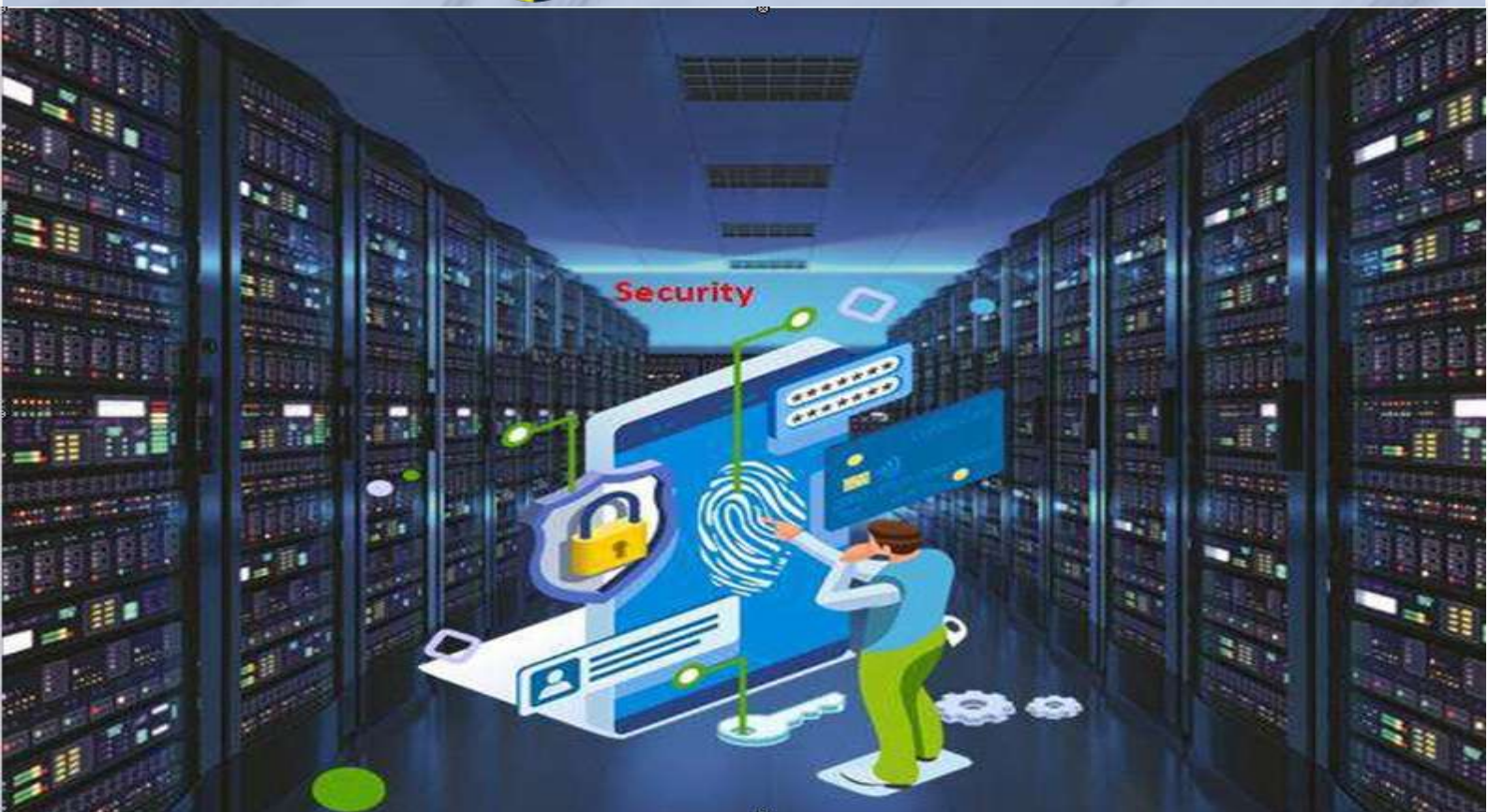
REPUBLIC OF CAMEROON  
Peace – Work – Fatherland

-----  
MINISTRY OF POSTS AND  
TELECOMMUNICATIONS

**PREMIER FORUM NATIONAL SUR LA CYBERSECURITE ET  
LA LUTTE CONTRE LA CYBERCRIMINALITE  
FIRST NATIONAL FORUM ON CYBERSECURITY AND THE  
FIGHT AGAINST CYBERCRIME**

THEME : CYBERESPACE NATIONAL ET DEFIS SECURITAIRE  
THEME : NATIONAL CYBERSPACE AND SECURITY CHALLENGE

# ACTES FINALS FINAL ACTS



Palais des Congrès de Yaoundé du 03 au 05 Novembre 2020  
Yaounde Conference Center, 03-05 november 2020



# Sommaire

GLOSSAIRE.....	4
CEREMONIE D'OUVERTURE.....	5
TRAVAUX EN PLENIERE.....	17
PANEL 1 : Aperçu global de la cybersécurité au Cameroun.....	18
PANEL 2: Cybersécurité dans les infrastructures de télécommunications.....	53
PANEL 3: Lutte contre la cybercriminalité au Cameroun.....	101
PANEL 4: Coopération internationale et renforcement des capacités.....	128
CEREMONIE DE CLÔTURE.....	137
ANNEXES.....	148

# GLOSSAIRE

<b>A</b>	
<b>ANTIC :</b>	Agence Nationale des Technologies de l'information et de la Communication
<b>ART :</b>	Agence de Régulation des Télécommunications
<b>C</b>	
<b>CAMSIS :</b>	Cameroun Télécommunications
<b>CAMTEL :</b>	Cameroun Télécommunications
<b>CEA :</b>	Commission Economique de l'Afrique
<b>CIRT :</b>	Cyber Incident Response Team
<b>CNC :</b>	Conseil National de la Communication
<b>COP :</b>	Child Online Protection
<b>D</b>	
<b>DGRE</b>	Direction Générale de la Recherche Extérieure
<b>DGSN</b>	Délégation Générale à la Sureté Nationale
<b>F</b>	
<b>FAI :</b>	Fournisseur d'Accès Internet
<b>FNCC :</b>	Forum National sur la Cybersécurité et la Lutte contre la Cybercriminalité
<b>G</b>	
<b>GCI</b>	Global Cybersecurity Index
<b>M</b>	
<b>MINPOSTEL :</b>	Ministère des Postes et Télécommunications
<b>P</b>	
<b>PKI :</b>	Public Key Infrastructure
<b>S</b>	
<b>SED</b>	Secrétariat d'Etat à la Défense
<b>SUP'PTIC :</b>	Ecole Nationale Supérieure des Postes, des Télécommunications et des Technologies de l'Information et de la Communication
<b>SWOT</b>	Strengths Weaknesses Opportunities Threats
<b>T</b>	
<b>TIC :</b>	Technologies de l'Information et de la Communication
<b>U</b>	
<b>UIT :</b>	Union Internationale des Télécommunications



# Security

**CEREMONIE D'OUVERTURE**



ALLOCUTION D'OUVERTURE DE MADAME LE  
MINISTRE DES POSTES ET TÉLÉCOMMUNICATIONS DU CAMEROUN



MADAME LIBOM LI LIKENG  
MINETTE.

Mesdames et Messieurs les Ministres ;  
Monsieur le Représentant du Bureau de zone de  
l'Union Internationale des Télécommunications  
pour l'Afrique Centrale et Madagascar;  
Monsieur le Représentant du Bureau sous-régional  
de l'Afrique Centrale de la Commission Economique  
des Nations Unies pour l'Afrique;  
Monsieur le Représentant Résident de l'Institut Afri-  
cain d'Informatique pour le Cameroun ;  
Monsieur le Secrétaire Général du Ministère des  
Postes et Télécommunications ;  
Mesdames et Messieurs les Directeurs Généraux ;  
Mesdames et Messieurs les experts et représentants  
des administrations partenaires; Distingués Invités  
Mesdames et Messieurs.

C'est pour moi un immense plaisir de prendre  
la parole à l'occasion de la cérémonie d'ouverture  
du Forum National sur la Cybersécurité et la lutte  
contre la Cybercriminalité qui se tient du 03 au 05  
novembre 2020 au Palais des Congrès de Yaoundé,  
sous le thème: **Cyberespace national et défis sécuri-  
taires.**

Mon plaisir est d'autant plus grand 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 Té-  
lécommunications il y'a quelques temps, une étape

supplémentaire de la mise en œuvre sur Très Hautes  
Prescriptions du Chef de l'Etat, de la politique natio-  
nale de cybersécurité.

En effet, véritable carrefour d'échanges entre  
experts en matière de cybersécurité, la rencontre qui  
s'ouvre ce jour constitue la phase importante de la  
réflexion devant accompagner ladite politique.

Qu'il me soit donc permis en début de mon  
propos, de souhaiter une chaleureuse bienvenue à  
vous tous qui avez accepté de prendre part à ce grand  
rendez-vous d'échanges sur ce sujet d'actualité qu'est  
la cybersécurité, en dépit d'un agenda fort chargé.

**Distingués invités Mesdames et Messieurs.**

Les réseaux de communications électro-  
niques et les Technologies de l'Information et de la  
Communication (TIC) sont devenus des outils indis-  
pensables pour les gouvernements, les entreprises,  
la société civile et les individus. Ces technologies  
ont augmenté la libre circulation des informations,  
contribué à des gains réels sur le plan du rendement,  
de l'efficacité, de la productivité et de la créativité à  
travers le monde et favorisé par conséquent, un dé-  
veloppement économique considérable. L'utilisation  
des TIC, internet en particulier, est aujourd'hui de-  
venue une question d'importance stratégique pour  
les pays.

Un internet ouvert et sécurisé représente un moteur de croissance économique et du développement social qui facilite la communication, l'innovation, la recherche scientifique et la transformation des administrations et des entreprises. Il convient ainsi de reconnaître que l'utilisation croissante de l'internet a conduit à de nouveaux défis pour les communautés nationale et internationale. En effet, plus nous sommes connectés, plus nous nous exposons aux menaces cybernétiques.

Par ailleurs, l'évolution rapide de l'internet a créé de nouvelles opportunités pour commettre des activités de cybercriminalité à grande échelle. C'est ainsi qu'aujourd'hui, les cybermenaces touchent toutes les catégories de la population et tous les types de plateformes et équipements numériques.

Il s'agit des sites web, des applications réseaux, des serveurs, des smartphones et bien d'autres en gros des systèmes d'informations. Ces cybermenaces deviennent souvent des « tueurs silencieux » car certaines prennent plusieurs années pour s'installer et en un seul jour lorsque le composant viral se déclenche, les dégâts s'avèrent parfois irréparables.

Et la reconstruction exige non seulement d'importants moyens financiers mais aussi une mobilisation en termes de ressources humaines compétentes. S'agissant de ces menaces, la plupart des agences de sécurité des systèmes d'information relèvent trois grands types auxquels peuvent être confrontés les Etats, les citoyens, les entreprises et les collectivités territoriales décentralisées : la cyber malveillance, le renseignement et le sabotage.

Ce phénomène de grande ampleur évolue de manière croissante au fil des années dans tous les pays du monde. C'est pour cela que tous les Etats ont adoptés depuis quelques années des politiques permettant de lutter contre toute forme de criminalité dans le cyber espace. Et le Cameroun n'est pas en reste. A titre d'illustration en ce qui concerne le Cameroun, les statistiques collectées auprès des services compétents démontrent l'ampleur du phénomène de cybercriminalité dans notre pays.

C'est ainsi que pour l'année 2018, 3 388 cas d'usurpation d'identités ont été constatés. En 2019, 2050 plaintes relatives au scamming et au phishing dont environ 5 milliards FCFA de perte financière, ainsi que près de 6 milliards de pertes relatives aux fraudes bancaires, et 11 617 vulnérabilités ont été détectés sur les sites webs des administrations publiques.

Le Cameroun dispose cependant d'une Politique Nationale de Sécurité des Réseaux et des Systèmes d'Information. Cette politique, véritable boussole de l'action du Gouvernement dans ce domaine fixe les orientations stratégiques et les initiatives prioritaires à mettre en œuvre pour opposer une réponse appropriée à l'utilisation malveillante du cyberspace camerounais.

Et dans ce cadre nous ne citerons que trois axes stratégiques majeurs, le renforcement du dispositif légal et réglementaire destiné à réprimer les déviations qui pourraient survenir d'une utilisation malsaine des technologies de l'information et de la communication. C'est dans cette optique que la loi N°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun a été promulguée par le Chef de l'Etat. Cette loi qui régit le cadre de la sécurité des réseaux de communications électroniques et des systèmes d'information, définit et réprime les infractions liées à l'utilisation des technologies de l'information et de la communication au Cameroun. Dans le cadre de sa mise en application et afin de garantir un environnement numérique sain, l'Etat dispose de plusieurs structures. A savoir :

- le Ministère des Postes et Télécommunications, chargé de l'élaboration et du suivi de la mise en œuvre de la politique nationale en matière de sécurité des communications électroniques et des systèmes d'information ;
- l'ANTIC qui assure pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des réseaux de communications électroniques ;
- le SED, la DGSN, la DGRE qui participent à la lutte contre la cybercriminalité, notamment en matière des investigations numériques ;
- la deuxième orientation majeure de cette politique est le développement des infrastructures de cybersécurité visant à mettre en place des outils technologiques qui permettent la prévention, la détection et la neutralisation des menaces qui pèsent sur les réseaux et les systèmes d'information.

A cet effet, l'Etat a mis sur pied un centre d'alerte et de réponse aux incidents cybernétiques (CIRT) ; une infrastructure à clé publique (PKI) ; les laboratoires d'investigation numérique à la Direction de la Police Judiciaire et à l'Ecole Nationale Polytechnique de Yaoundé.



Le troisième volet important porte sur la sensibilisation, le renforcement des capacités et la gestion du changement qui visent à accroître les aptitudes des usagers à une meilleure utilisation du cyberspace.

C'est dans ce cadre que se situe la campagne nationale pour la promotion de la culture de la cybersécurité et la sensibilisation à l'utilisation responsable des réseaux sociaux qui a démarré le 12 août 2020 sous le thème : « **Tous mobilisés pour la cybersécurité au Cameroun** » et dont l'objectif principal est de mobiliser toutes les couches sociétales dans la lutte contre la cybercriminalité. De manière à :

- Éveiller l'attention des citoyens camerounais sur les menaces en provenance du cyberspace mondial et susciter leur adhésion dans la mise en place de mesures de cybersécurité ;
- Attirer l'attention des décideurs et responsables des structures de l'Etat ainsi que des entreprises, en vue d'une prise de conscience et de l'implémentation des protocoles de sécurité des réseaux ;
- Sensibiliser toutes les couches sociétales sur l'usage responsable des réseaux sociaux qui sont utilisés de plus en plus à des fins malveillantes.
- Mettre en place une COALITION NATIONALE pour la promotion de l'utilisation citoyenne des réseaux sociaux.

**For the kick-off** of this campaign, several meetings were held with the aim of setting up a genuine national coalition for cybersecurity in Cameroon. These include:

- A National Workshop on the stakes and challenges of cybersecurity in Cameroon**, which brought together representatives of different ministerial departments and

other public institutions ;

- A Civil Society Forum on Cybersecurity issues**, with the different components of the civil society in Cameroon ;
- And the Business Awareness Seminar with representatives of all business groups and consular chambers.**

The purpose of these various meetings was to bring together around a table the different stakeholders to discuss the stakes and challenges related to cybersecurity, to define the role of each societal component in the fight against cybercrime, and to encourage the adherence as well as the commitment of all in the fight against cybercrime.

This national awareness-raising programme will be pursued in the coming weeks through training campaigns for some stakeholders and, above all, through a media campaign, an awareness-raising programme in the printing, online and audiovisual media in both the official and national languages.

#### **Ladies and Gentlemen.**

The national forum on cybersecurity and the fight against cybercrime which opens today is therefore a milestone in implementation of the government's cybersecurity strategy. This forum is designed to bring together experts from the public and private sectors, the civil society and international organisations, to carry out together an in-depth reflection, with the aim of defining operational guidelines. Specifically, it has to do with:

- Drawing up an inventory of Cameroon's achievements in terms of cybersecurity;
- Presenting cybersecurity

strategies, means and technical solutions, implemented for the protection of telecommunications networks and information systems in Cameroon ;

- Presenting international cooperation actions in the field of cybersecurity and the fight against cybercrime.

The presentations and debates on the theme of this forum, namely «national cyberspace and security challenges» as well as the recommendations that will result from it will undoubtedly enable us to strengthen the national cybersecurity mechanism and effectively fight against cybercrime, especially through awareness raising, strengthening of cooperation ties, developing technical and technological mechanism, without leaving out the legal framework.

This forum therefore has a twofold mission: to bring together experts and enable them to exchange views and make progress together, but also to act collectively as active and vigilant awareness-raisers throughout the country, especially among the youngest, the most vulnerable and the most exposed to these new practices.

The stakes of the national campaign to promote the culture of cybersecurity and raise awareness on the responsible use of social media, as presented above and this national forum, are of great importance: it is about mobilising the nation as a whole around cybersecurity, which we all know is an indispensable condition for the development of digital economy. It is needless recalling, the importance of this sector for the emergence of our country, which is so dear to President Paul BIYA, and the pressing need to promote digital governance, in order to achieve



the security and social peace objectives as well as economic development. Addressing young officers of the 37th batch of the combined Services Military Academy of Cameroon on 24 January 2020, the President gave an overview of this phenomenon when he declared: "You may have to face so-called asymmetric conflicts. You may also have to combat cybercrime which can, at the same time, undermine national security and destabilize the national economy."

**Mesdames et Messieurs les Ministres ;  
Monsieur le Représentant du Bureau de zone de l'Union Internationale des Télécommunications pour l'Afrique Centrale et Madagascar;  
Monsieur le Représentant du Bureau Sous-Régional de l'Afrique Centrale de la Commission Economique des Nations Unies pour l'Afrique;  
Monsieur le Représentant Résident de l'Institut Africain d'Informatique pour le Cameroun ;  
Monsieur le Secrétaire Général du Ministère des Postes et Télécommunications ;  
Distingués Invités ;  
Ladies and Gentlemen.**

Les actions menées par le Cameroun pour la lutte contre la cybercriminalité s'alignent sur les recommandations du forum sous-régional sur la cybersécurité et la lutte contre la cybercriminalité et le cyberterrorisme organisé à Yaoundé du 24 au 27 février 2015, et formulées à l'endroit de chaque Etat membre de la Communauté Economique des Etats de l'Afrique Centrale.

Le crime numérique a aujourd'hui changé de paradigme, il ne s'agit plus seulement de s'at-

taquer aux infrastructures physiques, mieux protégées qu'un coffre-fort, mais de pénétrer par des voies bien plus simplistes, telles que les espaces numériques extérieurs, communément appelés Cloud, où sont stockées les données et qui sont connectés aux systèmes et applications.

Il est donc impératif que les experts des Etats se réunissent régulièrement pour débattre des stratégies nouvelles sur ces questions de cybersécurité.

Je lance donc un appel à tous les participants ici présents, afin que nous nous penchions tous ensemble au plus vite sur les problématiques liées aux menaces cybernétiques de tous ordres et que d'ores et déjà, nous anticipions sur celles liées à l'avancée rapide du monde du numérique, avec ses avantages et aussi ses défis à relever. Au sortir de nos travaux, nous devons être à même d'identifier les leviers d'intervention essentiels qui devraient être activés, pour garantir un environnement qui favorise l'intégrité des activités menées au sein de notre cyberspace.

Au regard des compétences, de la disponibilité de tous les experts et participants ainsi que de notre volonté commune à impulser le développement de notre secteur, je reste convaincu que nous y parviendrons.

Aussi, j'invite tous les participants à s'impliquer pleinement dans les travaux, afin de tirer le meilleur parti de cette concertation. C'est sur cette exhortation, que je déclare ouvert le Forum national sur la cybersécurité et la lutte contre la cybercriminalité au Cameroun

**Pour que vive l'économie numérique Le Cameroun et son illustre chef, S.E. M. Paul BIYA  
Je vous remercie de votre bienveillante attention.**



## Allocution du Représentant de Zone de l'Union Internationale des Télécommunications (UIT) pour l'Afrique Centrale et Madagascar



Monsieur MASSIMA LANDJI  
Jean Jacques

- **Excellence Madame le Ministre des Postes et Télécommunications ;**
- **Excellences Mesdames et messieurs les membres du Gouvernement ;**
- **Excellences Mesdames et messieurs les chefs de Mission et représentants du corps diplomatique et des institutions internationales, ainsi que des organismes spécialisés des TIC , chers collègues ;**
- **Autorités Universitaires et académiques ;**
- **Monsieur le Secrétaire Général du MINPOSTEL ;**
- **Monsieur le Directeur Général de l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) ;**
- **Monsieur le Directeur général de l'ART ;**
- **Messieurs les Directeurs généraux et représentants des opérateurs des TIC au Cameroun ;**
- **Chers acteurs du secteur des TIC représentant la Société civile ;**
- **Mesdames et Messieurs , Distingués invités et chers participants , en vos grades et titres respectifs, tout protocole observé.**

A plusieurs occasions qui m'ont été offertes du haut de cette même tribune, en juillet 2013 et en février 2015 lors de précédents fora sur la Cybersecrurité, j'ai loué le dynamisme du Cameroun qui a pris la juste mesure des choses et qui travaille sans répit à protéger son cyberspace et celui de la sous-région notamment en régissant sous la haute et dynamique

impulsion du Ministère des Postes et Télécommunications et par le biais de ses bras séculiers que sont l'ANTIC et l'ART, deux entités sous tutelle essentielles à la mise en place continuelle des politiques réglementaires en matière de TIC, un secteur d'activité contraignant qui se veut concurrentiel et transparent, et notamment exacerbé par une forte densité et variabilité technologiques dont les incidences socio-économiques sont aujourd'hui bien mesurables. La pandémie du COVID -19 nous le rappelle sans équivoque !

En effet les TIC, sont perçus de plus en plus comme un véritable catalyseur de développement, un formidable outil de création de richesses et d'emplois décents mais surtout portent en elles l'espoir d'une égalité de chance pour tous, alliant l'innovation aux talents d'une jeunesse exigeante et méritante qui souhaite construire et bâtir elle-même son avenir, à travers les arcanes de sa société de l'information.

*Six (6) milliards de dollars américains sera le coût mondial du W cyber crime en 2021 selon CSO online. 58% des responsables de sécurité informatiques des entreprises reconnaissent que leurs systèmes sont définitivement ou probablement sous attaques sans qu'il ne puissent le déceler !*



Le Cameroun était classé 13ème régional et 91ème mondial selon l'édition de 2018 de l'indice mondial de la cyber sécurité, mesuré par l'UIT et plusieurs autres partenaires. Je reste persuadé que le score s'améliorera pour l'édition de l'index GCI en cours de finalisation.

Je voudrais donc me réjouir de la tenue de ce forum qui est sans aucun doute non seulement le lieu de refaire l'état de l'art, le lieu de mesurer sans aucune complaisance le chemin parcouru, mais qui est une rare opportunité de tester la solidité de notre chaîne de sécurisation. Comme vous le savez tous la solidité de toute chaîne se mesure par son maillon le plus faible... Il nous faut donc l'identifier, en analyser les faiblesses et le renforcer.

Et c'est le but ultime de cet exercice (SWOT Analysis) qui va vous permettre pendant 3 jours de confronter vos expériences par rapport aux meilleures pratiques mondiales. Des experts de haut niveau, des spécialistes de la cyber sécurité, des gestionnaires des ressources critiques et des spécialistes de la lutte contre le cyber-terrorisme sont tous là, convaincus de venir donner et recevoir, dans ce rendez-vous du palais des congrès.

### **Mesdames et Messieurs, chers participants,**

Le bureau régional de l'UIT pour l'Afrique vient d'organiser le forum régional de développement, en ligne, de manière à identifier les lacunes et les pistes d'amélioration de notre écosystème digital. Sans surprises certaines des lacunes relatives à la cyber sécurité, identifiées par les pays membres sont les suivantes :

- Manque de ressources pour mettre en place les structures nécessaires pour renforcer la résilience des réseaux ;
- Manque de ressources supplémentaires pour continuer à renforcer les capacités de toutes les parties prenantes, en adoptant des politiques / stratégies appropriées au niveau national ;
- Manque d'interconnexion des réseaux IXP des pays;
- Enfants en ligne qui pourraient être améliorées notamment par:
  - La recherche des synergies sur les travaux de la COP ;
  - Une approche régionale coordonnée ;
  - La mobilisation du Financement ;
  - Une recherche de plus de partenariats stratégiques ;

La recommandation principale du RDF2020 relative à la cyber sécurité est de placer la cyber sécu-

rité en tant qu'élément clé, pierre d'angle pour bâtir la sécurité et la confiance dans le cyberspace.

### **Mesdames et Messieurs, chers participants,**

L'UIT a publié en 2019 un nouveau guide de développement de stratégies nationale de cyber sécurité, je vous exhorte à le consulter de manière à évaluer la stratégie nationale de cybersécurité en cours et l'améliorer si nécessaire. Les technologies numériques ont ouvert de nombreuses nouvelles façons de communiquer, d'apprendre, de se divertir, de profiter de la musique et de participer à un vaste éventail d'activités culturelles, éducatives et de perfectionnement des compétences. L'Internet peut fournir un accès crucial aux services de santé et d'éducation ainsi qu'à des informations sur des sujets importants pour les jeunes mais qui peuvent être tabous ou délicats dans leurs sociétés ou dans leur environnement.

Cependant, tout comme les enfants et les jeunes sont souvent à l'avant-garde de l'adoption et de l'adaptation aux nouvelles technologies connectées ainsi que des opportunités et des avantages qu'elles apportent, ils sont également exposés à une gamme de contenus, de contacts et de menaces et préjudices en ligne. Il est important que les décideurs prennent conscience de ces menaces et préjudices potentiels lors de la formulation des réponses politiques. Le bureau Afrique de l'UIT, dans cette optique, a lancé fin octobre 2020, la protection des enfants en lignes. Je vous exhorte à utiliser cet outil et vous réitère que l'UIT se tient prête à vous accompagner à mettre en place une stratégie appropriée de protection de l'enfance en ligne au Cameroun.

### **Excellence Madame le ministre, Distingués invités, Mesdames et Messieurs, chers participants ;**

Pour clore mon propos, je voudrais appeler de tous mes vœux à plus d'initiatives en faveur d'une bonne coopération entre tous les acteurs et espérer une implication active de tous et à tous les niveaux de responsabilité, pour que vive au Cameroun, en Afrique et dans le monde entier une Société de l'Information véritablement ouverte, accessible, participative, juste et inclusive pour le bonheur de l'Humanité. Je vous remercie de votre très aimable attention.



# LEÇON INAUGURALE

## LEÇON INAUGURALE



MONSIEUR  
JACQUES BONJAWO  
FONDATEUR DU TECHNOPÔLE OCEAN INNOVATION  
CENTER

### 1. INTRODUCTION

#### 1. 1. La Problématique

#### 1. 2. Pourquoi devons-nous agir ?

#### 1. 2.2 Exemples de risques dont sont victimes les organisations

#### 1. 2.3 Risques d'attaque auxquels doit faire face l'Etat

#### 1. 3 Facteurs de succès de la lutte contre la cybercriminalité

#### 1. 4 La nécessité d'une volonté politique forte

### CONCLUSION





## 1. INTRODUCTION

### 1. 1. La Problématique

La dimension internationale d'Internet et de la cybercriminalité constituent de formidables défis pour le monde globalisé et interconnecté dans lequel nous vivons.

Ces défis deviennent de plus en plus complexes et globaux avec des effets parfois dévastateurs, loin de leur origine géographique.

Toutes ces raisons accroissent la nécessité de collaboration et de coopération tant au niveau national qu'international.

C'est tout le sens de ce premier Forum National.

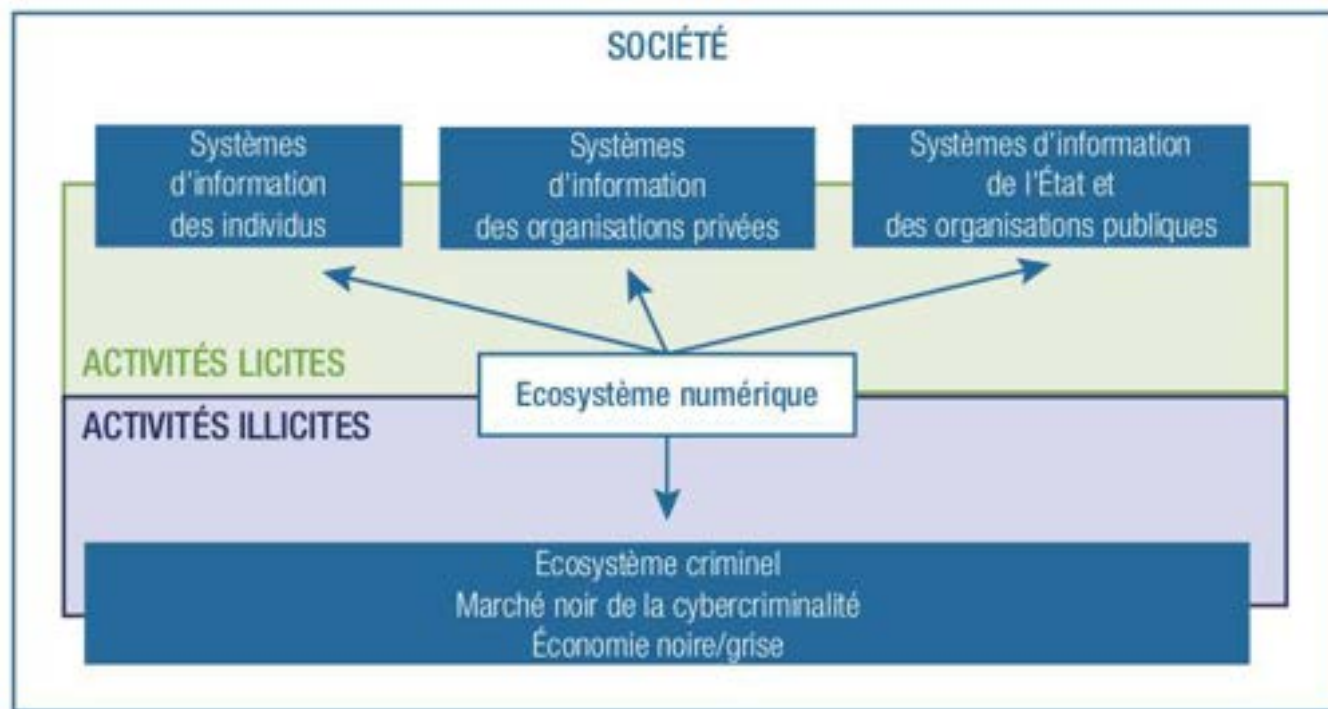


Figure 1 – L'écosystème numérique (adaptée du livre *Cyberpower, crime, conflict & security in cyberspace*, S. Ghemaouti, EPFL Press, 2013)

### 1. 2. Pourquoi devons-nous agir ?

- L'incroyable essor de l'Internet, et plus généralement de la technologie, est porteuse d'opportunités, mais aussi de risques, que cela soit pour les individus, les organisations publiques et privées ou l'État et la société;
- 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, à distance ou derrière une identité virtuelle, une fausse identité ou un pseudonyme;
- Nous ne disposons d'aucun mécanisme « de sécurité » permettant de garantir la bonne foi des internautes.

#### 1. 2.1 Exemples de risques dont peut être victime un individu

- Harcèlement, intimidation, chantage, incivilités, etc.;

- Diffamation, mise à mal de la réputation;
- Exposition à des contenus malveillants, offensifs ou non désirés (virus, spam, pornographie dure, scène de violence, incitation à la haine raciale et à la xénophobie, propagande, etc.), à des publicités intrusives, canulars, escroqueries, chantages, fraudes ou abus en tout genre;
- Objet de surveillance, de traçabilité, de profilage excessif, d'écoutes environnementales (atteinte à la vie privée et à l'intimité numérique, espionnage);
- Vol de données (données personnelles, informations confidentielles, propriété intellectuelle, etc.);
- Vol d'équipements (ordinateur, clé USB, CD-ROM, etc.);



- Destruction de valeurs;
- Usurpation d'identité;
- Désinformation, manipulation d'opinion, influence;
- Usage détourné des capacités informatiques;
- Prise de contrôle des systèmes par des entités tierces.

### 1. 2.2 Exemples de risques dont sont victimes les organisations

- Atteintes à l'image, à la réputation, à la fiabilité, etc;
- Incapacité à produire, à fonctionner (dysfonctionnements, indisponibilité des services, perte de qualité, altération des processus décisionnels, etc.);
- Falsification, défiguration de sites web;
- Infection des ressources informatiques, détournement des capacités informatiques;
- Prise de contrôle des ressources informatiques à des fins de chantages;
- Criminalité financière et économique.. ;
- Espionnage industriel et économique (vol/perte de secrets des affaires, de valeurs immatérielles, de savoir-faire, etc.);
- Attaques concurrentielles (vol de fichiers clients, de prix, de fournisseurs, de plan de fusion-acquisition, etc.);
- Atteintes à la propriété intellectuelle, au droit des marques, etc.;
- Attaques sémantiques (rumeurs, fausses informations, manipulation d'information, désinformation, etc.);

### 1. 2.3 Risques d'attaque auxquels doit faire face l'Etat

- Des systèmes informatiques contrôlant les infrastructures critiques;
- Des systèmes informatiques relatifs à la prise de décisions dans le secteur de la défense militaire et sur des systèmes d'armement (contrôle de missiles, drones, aviation militaire, équipement du soldat...);
- L'information (manipulation de) constituant des stratégies d'influence et de guerre psychologique.

## 1. 3 La mise en place d'un Plan d'Action

- Il va sans dire qu'il est très difficile d'agir sur un phénomène comme la cybercriminalité qui continue de se développer aussi rapidement, mais il est important pour chaque pays de pouvoir établir un état des lieux afin d'être en mesure d'identifier et de dégager les moyens nécessaires à sa transformation numérique.
- Cela peut être envisagé sous la forme de la réalisation du diagnostic de la situation nationale, d'une analyse des vulnérabilités, des menaces et des risques afin de

piloter, développer, mettre en œuvre, optimiser les plans d'action stratégique et opérationnelle.

### 1. 3.1 Un Plan d'Action adéquat

- conduire le diagnostic de l'état de cybersécurité et de cyberdéfense dans leur écosystème ;
- identifier leurs infrastructures critiques et de garder un œil vigilant sur tous les opérateurs d'importance vitale ;
- mettre en œuvre une structure de réponse d'urgence aux incidents de sécurité de l'information ;
- définir des mécanismes appropriés de protection des données à caractère personnel;
- définir des mécanismes appropriés de protection des enfants, de la jeunesse, des plus faibles, dans le cyberspace ;
- développer le capital humain pour assurer la cybersécurité et la cyberdéfense;
- déployer les structures organisationnelles de la cybersécurité et de la cyberdéfense;
- développer les mesures législatives devant réguler la cybersécurité et la cyberdéfense;
- assurer coopération et coordination nationale, régionale et internationale dans le cadre de la cybersécurité et de la cyberdéfense ;
- élaborer une stratégie nationale de cybersécurité et cyberdéfense et d'en assurer la mise en œuvre effective, le contrôle, l'évaluation et l'optimisation;
- Définir un cadre législatif approprié pour faire face aux menaces.

### 1.3.2 Facteurs de succès de la lutte contre la cybercriminalité

- la réduction du nombre de vulnérabilités techniques, organisationnelles, juridiques et humaines des environnements connectés à Internet ;
- le renforcement de la robustesse et de la résilience des infrastructures informatiques par des mesures de sécurité technologiques, procédurales et managériales cohérentes et complémentaires ;
- une réelle capacité d'adaptation des moyens de cybersécurité et de cyberdéfense à une situation en constante évolution ;
- l'allocation de moyens pour gérer les crises « cyber » afin de retourner à un fonctionnement normal.

#### 1. 4 La nécessité d'une volonté politique forte

- faire de la lutte contre la cybercriminalité et du renforcement des capacités de cybersécurité et de cyberdéfense une priorité ;
- renforcer la coordination entre les différents États et gouvernements ;
- mettre en œuvre des mesures appropriées et proportionnées aux menaces ;
- mobiliser, fédérer et engager les différents acteurs privés du numérique et de la société civile ;
- respecter les droits fondamentaux des personnes ;

#### CONCLUSION

Au regard de ces effets dévastateurs sur l'individu, le climat des affaires, la crédibilité des entreprises et la qualité des institutions, il s'impose plus que jamais la nécessité de:

- Construire ou d'adapter un dispositif juridique moderne de contrôle et de régulation de la cybernétique au Cameroun.
- Renforcer les mesures de lutte contre la cybercriminalité ;
- Améliorer la fiabilité et la qualité du matériel de veille;
- Sensibiliser les profanes sur les bonnes pratiques sur internet;
- Renforcer les compétences des ressources humaines.
- Etablir une véritable plateforme d'échange de compétences et de partage d'expériences;
- Mutualiser les efforts des secteurs privé et public.





919.03

# TRAVAUX EN PLENIERE

551.58

764.72

327.35



# PANEL 1

## APERÇU GLOBAL DE LA CYBERSÉCURITÉ AU CAMEROUN



### MODERATEUR



#### **NGAE Denis**

Titulaire d'un Doctorat/PhD in Communications and Business Management, Madison International Institute & Business School (USA).

Ses recherches ont été centrées sur l'appropriation des TIC et performance hospitalière au Cameroun.

Chef de Division des Projets, des Etudes et de la Prospective, au Ministère des Postes et Télécommunications, il totalise vingt cinq (25) années d'expérience professionnelle dans le domaine des télécommunications et TIC au Cameroun.

# PANEL 1

## OVERVIEW OF CYBERSECURITY IN CAMEROON

# Presentation 1

### CYBERSECURITY/CYBERCRIME CONCEPTS, ISSUES AND CHALLENGES



Presented by: **Thierry MINKA, Ing.**

RCMP Expert,

- Computer Engineer;
- Expert in Governance Risk and Compliance (GRC);
- Approved Judicial Expert. 15 years of experience.

#### AGENDA

- About the speaker;
- History;
- What are cybersecurity & cyber criminality about?
- Cybersecurity landscape;
- Cybersecurity as a game-changer;
- Some recommendations for the State.

#### ABOUT THE SPEAKER

- IT Governance: holder of Certified in the Governance of Enterprise IT (CGEIT), and Control Objectives for Information and related Technology Foundation Certificate (COBIT-F);
  - Cybersecurity: holder of the Cybersecurity Foundation Certificate (CSX-F);
  - IT Risk & control: holder of Certified in Risk and Information Systems Control (CRISC);
  - Data Rights, Protection and Privacy: holder of Certified Data Privacy Solutions Engineer (CDPSE);
  - Audit: holder of Certified Information Systems Auditor (CISA), Public Finances' Auditor (CONSUPE);
  - Information Security Management: holder of Certified Information Security Manager (CISM);
  - Teaching: University Lecturer; holder of IDI certificate of completion for the online training for Learning Management Systems;
  - Network Security: holder of Fortinet Network Security Expert 1&2;
  - Management: holder of SCRUM Foundation Professional Certificate;
- Member of: NOEE, ISACA, ISC<sup>2</sup>, IIA, ACM, EAI, MyData, ...

#### History

**computer security - network security - information security - cybersecurity**

Cybersecurity plays a significant role in today's ever-evolving cyberlandscape. New trends in mobility and connectivity present a broader range of challenges than ever before as new attacks continue to develop along with emerging technologies. Cybersecurity professionals must be informed and flexible to identify and manage potential new threats, such as advanced persistent threats (APTs), effectively

#### What are Cyber Security & Cyber Criminality about?

#### Definitions

##### • Cybersecurity

According to Information Systems Audit and Control Association (ISACA), Cybersecurity is the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems

##### • Cyber criminality

It is an activity that consists of using computer systems, and/or networks to perpetrate actions prohibited by law. Simply said, it's a crime committed in the cyberspace, or using digital devices.

##### • Risk

The combination of the probability of an event and its consequence (International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 73). Risk is mitigated through the use of controls or safeguards.  $R=P \times C$ , R: risk; P: probability; C: consequence



- **Threat**

Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. ISO/IEC 13335 defines a threat broadly as a potential cause of an unwanted incident. Some organizations make a further distinction between a threat source and a threat event, classifying a threat source as the actual process or agent attempting to cause harm, and a threat event as the result or outcome of a threat agent's malicious activity.

- **Asset**

Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation

- **Vulnerability**

A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

- **Residual risk**

Even after safeguards are in place, there will always be residual risk, defined as the remaining risk after management has implemented a risk response.

- **Inherent risk**

The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls) Cybersecurity addresses both internal and external threats to an organization's digital information assets by focusing on critical electronic data processes, signal processing, risk analytics and information system security engineering.

### Concepts

- **Confidentiality**

Confidentiality is the protection of information from unauthorized access or disclosure. Different types of information require different levels of confidentiality, and the need for confidentiality can change over time.

- **Integrity**

Integrity means protection from unauthorized modification. Any violation of integrity is significant because it may be the first step in a successful attack against system availability or confidentiality

- **Availability**

ensures the timely and reliable access to and use of information and systems. This would include safeguards to make sure data are not accidentally or maliciously deleted. This is particularly important with a mission-critical system, because any interruptions in its availability can result in a loss of productivity and revenue.

- **Non-repudiation**

In a digital context, nonrepudiation refers to the concept that a message or other piece of information is genuine. It assures that the data's integrity has been protected and that the party sending or receiving it cannot deny or repudiate that they sent or received it. Nonrepudiation is important in transactions that require trust, such as financial transactions and legal matters. Nonrepudiation is implemented through transactional logs and digital signatures.

### Protecting Digital Assets

In their cybersecurity frameworks, both the National Institute of Standards and Technology (NIST) and the European Union Agency for Network and Information Security (ENISA) have identified five key functions necessary for the protection of digital assets. These functions coincide with incident management methodologies and include the following activities:

- **Identify:** Use organizational understanding to minimize risk to systems, assets, data and capabilities;
- **Protect:** Design safeguards to limit the impact of potential events on critical services and infrastructure;
- **Detect:** Implement activities to identify the occurrence of a cybersecurity event;
- **Respond:** Take appropriate action after learning of a security event;
- **Recover:** Plan for resilience and the timely repair of compromised capabilities and services.

**Cybersecurity Roles**

The structure and governance of every organization is different and varies based on the type of organization. Each organization has its own mission (business), size, industry, culture and legal regulations. However, all organizations have a responsibility and duty to protect their assets and operations, including their IT infrastructure and information. At the highest level, this is generally referred to as governance, risk management and compliance (GRC). Governance is the responsibility of the board of directors and senior management of the organization. A governance program has several goals:

- Provide strategic direction;
- Ensure that objectives are achieved;
- Ascertain whether risk is being managed appropriately;
- Verify that the organization’s resources are being used responsibly.

Risk management is the process by which an organization manages risk to acceptable levels. Risk management requires the development and implementation of internal controls to manage and mitigate risk throughout the organization, including financial and investment risk, physical risk and cyber risk.

Compliance is the act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations. It also includes voluntary requirements resulting from contractual obligations and internal policies.

Cybersecurity is the responsibility of the entire organization at every level

**Different cybersecurity approaches**

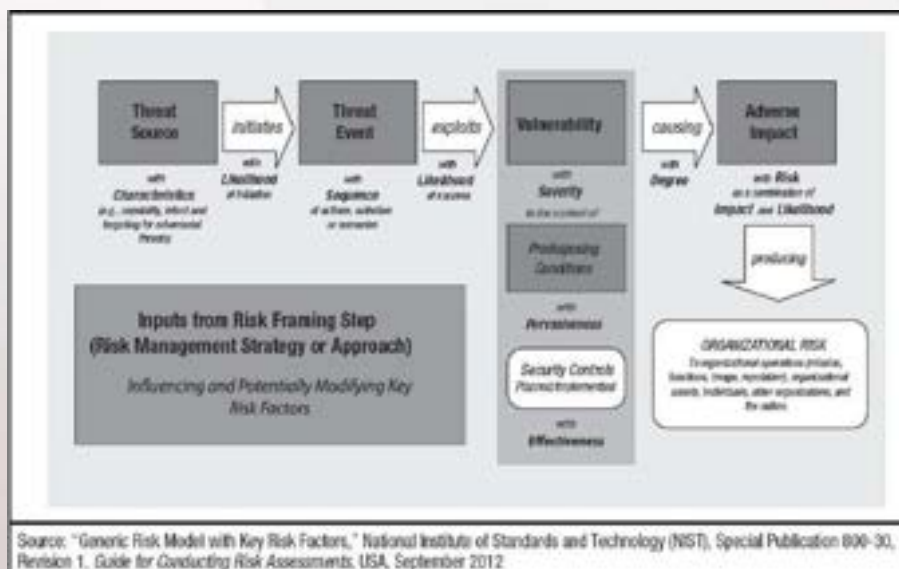
Generally, there are three different approaches to implementing cybersecurity.

- **Compliance-based**  
Also known as standards-based security, this approach relies on regulations or standards to determine security implementations. Controls are implemented regardless of their applicability or necessity, which often leads to a “checklist” attitude toward security.
- **Risk-based**  
Risk-based security relies on identifying the unique risk a particular organization faces and designing and implementing security controls to address that risk above and beyond the entity’s risk tolerance and business needs.
- **Ad hoc**

An ad hoc approach simply implements security with no particular rationale or criteria. Ad hoc implementations may be driven by vendor marketing, or they may reflect insufficient subject matter expertise, knowledge or training when designing and implementing safeguards.

Most organizations with mature security programs use a combination of risk-based and compliance-based approaches. In fact, most standards or regulations require risk assessments to drive the particular implementation of the required controls.

**Framing risk management**



Source: "Generic Risk Model with Key Risk Factors," National Institute of Standards and Technology (NIST), Special Publication 800-30, Revision 1. Guide for Conducting Risk Assessments, USA, September 2012



## Cybersecurity landscape

### Threat agents

**Corporations:** Corporations have been known to breach security boundaries and perform malicious acts to gain a competitive advantage.

**Nation States:** Nation states often target government and private entities with a high level of sophistication to obtain intelligence or carry out other destructive activities.

**Hacktivists:** Although they often act independently, politically motivated hackers may target specific individuals or organizations to achieve various ideological ends.

**Cyberterrorists:** Characterized by their willingness to use violence to achieve their goals, cyberterrorists frequently target critical infrastructures and government groups.

**Cybercriminals:** Motivated by the desire for profit, these individuals are involved in fraudulent financial transactions.

**Cyberwarriors:** Often likened to hacktivists, cyberwarriors, also referred to as cyberfighters, are nationally motivated citizens who may act on behalf of a political party or against another political party that threatens them.

**Script Kiddies:** Script kiddies are young individuals who are learning to hack; they may work alone or with others and are primarily involved in code injections and distributed denial-of-service (DDoS) attacks.

**Online Social Hackers:** Skilled in social engineering, these attackers are frequently involved in cyberbullying, identity theft and collection of other confidential information or credentials.

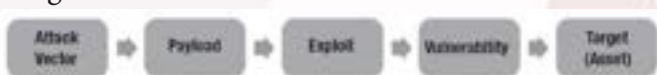
**Employees:** Although they typically have fairly low-

tech methods and tools, dissatisfied current or former employees represent a clear cybersecurity risk. All of these attacks are adversarial, but some are not related to APT cyberattacks.

### Attacks attributes

An attack is the actual occurrence of a threat. More specifically, an attack is an activity by a threat agent (or adversary) against an asset. From an attacker's point of view, the asset is a target, and the path or route used to gain access to the target (asset) is known as an attack vector. There are two types of attack vectors: ingress and egress (also known as data exfiltration). While most attack analysis concentrates on ingress, or intrusion, into systems, some attacks are designed to remove data from systems and networks.

Therefore, it is important to consider both types of attack vectors. The attacker must defeat any controls in place and/or use an exploit to take advantage of a vulnerability. Another attribute of an attack is the attack mechanism, or the method used to deliver the exploit. Unless the attacker is personally performing the attack, the attack mechanism may involve a payload, or container, that delivers the exploit to the target.



Attacks can be analyzed and categorized based on their type and patterns of use. From these characteristics, it is possible to make generalizations that facilitate better design and controls. There are two broad categories for threat events: adversarial and nonadversarial. An adversarial threat event is made by a human threat agent (or adversary), while a nonadversarial threat event is usually the result of an error, malfunction or mishap of some sort.

### Generalized Attack Process

While each attack is different, most adversarial threat events follow a common process, as shown in the picture below



- Perform reconnaissance: The adversary gathers information using a variety of techniques ;
- Create attack tools: The adversary crafts the tools needed to carry out a future attack ;
- Deliver malicious capabilities: The adversary inserts or installs whatever is needed to carry out the attack;
- Exploit and compromise: The adversary takes advantage of information and systems in order to compromise them;
- Conduct an attack: The adversary coordinates attack tools or performs activities that interfere with organizational functions;
- Achieve results: The adversary causes an adverse impact;
- Maintain a presence or set of capabilities: The adversary continues to exploit and compromise the system;
- Coordinate a campaign: The adversary coordinates a campaign against the organization.

## Malware and Attack Types

- Malware, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations. There are several types of malware, the most important being computer viruses, network worms and Trojan horses, which are differentiated by the way in which they operate or spread.
- Viruses: A computer virus is a piece of code that can replicate itself and spread from one computer to another. It requires intervention or execution to replicate and/or cause damage.
- Network worm: A variant of the computer virus, which is essentially a piece of self-replicating code designed to spread itself across computer networks. It does not require intervention or execution to replicate.
- Trojan horses: A further category of malware is the Trojan horse, which is a piece of malware that gains access to a targeted system by hiding within a genuine application. Trojan horses are often broken down into categories reflecting their purposes.
- Botnets: A botnet (a term derived from “robot network”) is a large, automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as denial-of-service (DoS).
- Spyware: A class of malware that gathers information about a person or organization without the knowledge of that person or organization.
- Adware: Designed to present advertisements (generally unwanted) to users.
- Ransomware: A class of extortive malware that locks or encrypts data or functions and demands a payment to unlock them.

### Malware and Attack Types (cont.)

- Keylogger: A class of malware that secretly records user keystrokes and, in some cases, screen content.
- Rootkit: A class of malware that hides the existence of other malware by modifying the underlying operating system.
- Advanced persistent threats: Complex and coordinated attacks directed at a specific entity or organization. They require an enormous amount of research and time, often taking months or even years to fully execute.
- Backdoor: A means of regaining access to a com-

promised system by installing software or configuring existing software to enable remote access under attacker-defined conditions.

- Brute force attack: An attack made by trying all possible combinations of passwords or encryption keys until the correct one is found.
- Buffer overflow: Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes type of security attack on data integrity.
- Cross-site scripting (XSS): A type of injection in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.
- Denial-of-service (DoS) attack: An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.
- Man-in-the-middle attack: An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system and then replaces the traffic between the two components with the intruder’s own, eventually assuming control of the communication.
- Social engineering: Any attempt to exploit social vulnerabilities to gain access to information and/or systems. It involves a “con game” that tricks others into divulging information or opening malicious software or programs.
- Phishing: A type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering.



### Malware and Attack Types

- Spear phishing: An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim.
- Spoofing: Faking the sending address of a transmission in order to gain illegal entry into a secure system.
- Structure Query Language (SQL) injection: According to MITRE, SQL injection results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design.
- Zero-day exploit: A vulnerability that is exploited before the software creator/vendor is even aware of its existence

Some statistics

National statistics are unreachable. So here are some USA's one.

### **Attacks**

- Hackers attack every 39 seconds, on average of 2,244 times a day;
- Data breaches exposed 4.1 billion records in the first half of 2019;
- Average cybersecurity spending per employee is \$1,178.

### **Sources**

- 48% of malicious email attachments are office files;
- 34% of data breaches involves internal actors;
- 65% of groups used spear-phishing as the primary infection vector;
- 94% of malware are delivered by email.

### **Other statistics**

- Only 5% of folders were properly protected ;

- The average cost for a stolen record is \$150
- 88% of companies spent over \$1 million in GDPR preparation

Les statistiques nationales sont inaccessibles. Alors en voici quelques une des Etats Unis d'Amérique.

### Cameroon's nowadays Challenges

Cybersecurity is a field that demands skilled professionals who possess the foundational knowledge, education and thought leadership necessary to confront the difficulties that accompany constant technological change. Advanced threat vectors, emerging technologies and myriad regulations require cybersecurity professionals to be skilled in technology as well as business and communications. These are some challenges for our country:

- Having the right person et the right place, and at the right time
- Having reliable and accurate information about cybersecurity incidents occurred ;
- Addressing Internet and particularly social media issue (hate speech, people and country bashing, phishing , ...);
- Promoting the emergence of a cybersecurity culture at the nation wide level;
- Non-repudiation of acts committed on the internet.

## Cybersecurity as a game-changer

### Education & Awareness

The cyber criminality reality imposes

- The creation of new education cursus, related to information technology and cyber security;
- The democratization of awareness training related to cyber security;
- The recurrence of security audits by the ANTIC;
- The democratization of cyber security related certifications;
- The funding of some related training by the MINPOSTEL.

### Law and rules

- The 2010's law
  - Law N°2010/012 of the 21 December 2010, about Cybersecurity & Cyber criminality;
  - Law N° 2010/021 of the 21 December 2010, about electronic commerce;
  - Law N° 2010/013 of the 21 December 2010, about electronic communications;
- Other law
  - Law 2015/006 of the 21 April 2015, about electronic communications
- International standard and guidelines;
  - Convention on cybercrime of 23 november 2001 (Budapest convention);
  - African declaration on data, diversity, privacy, freedom and security on internet;
  - Declaraion on fundamental digital rights ;
  - African convention on cybersecurity and privacy of 27 june 2014;
  - General reglementation on data privacy;

### Needs for new skills and organization charts' updates

#### - Skill gap

- a survey late last year from ISC<sup>2</sup> estimate the amount of additional trained staff needed to close the skills gap is 4.07 mil lion professionals worldwide;
- there is no such kind of statistics for our country up to now. but if we consider as mandatory that there is a need for at least 3, skilled cybersecurity professional per organization, we can then easily calculate the gap;

- the MINPOSTEL recently via the FSE, funded some cybersecurity training for civil servants. But we are still far from the goal;

•The necessity of a personalized training program for closing the skill shortage is mandatory for all organization, and it starts with the skill matrix ;

#### - Organization charts

- the organization charts of public administrations do not have a position dedicated to cybersecurity, risk based and information security. certain private enterprises do have;
  - in some public enterprises and administrations, there is no adequation between the position and skill. When it comes to cybersecurity this is very critical;
  - organizations should update their charts to comply with the actual needs.

### Some recommendations for the State

- Special status of informatics and tele-informatics civil servants
  - incorporate the Security and/or Cybersecurity Engineer role;
  - take into account obtaining a certification in the criteria for advancement in career step.
- Organigram
  - incorporate the Information Risk related position in computer unit;
  - incorporate the Information Security related position in computer unit;
  - incorporate the Cybersecurity related position in computer unit;
  - incorporate the Information Systems Auditor related position in audit and control unit ;
- Exchange platform
  - create and maintain the national cybersecurity experts' file;
  - create and maintain an exchange platform for cyber security professionals from the public and private sectors under the aegis of ANTIC;
  - set periodic meeting for the cybersecurity national experts;
  - set up a monthly newspaper dedicated to cybersecurity, under the supervision of MINPOSTEL ;



- Academics and research
  - set up a national cybersecurity laboratory of research under the supervision of MINESUP, MINPOSTEL and MINRESI;
  - harmonized the different programs of cybersecurity taught in the country, by education level;
  - promote a cybersecurity awareness culture;
  - set a dedicated cursus for cybersecurity training in university;
  - write the first national cybersecurity white book.
- Law and rules
  - update different local law in cyberspace, e-commerce and telecommunication field, taking into account latest worldwide trends in privacy and personal data protection issues;
  - under the supervision of ANTIC select or develop a national mandatory framework for cybersecurity's and related audits;
  - update the national cybersecurity policy and set it mandatory;
- Information security deals with information, regardless of its format. it encompasses paper documents, digital and intellectual property in people's

minds, and verbal or visual communications. Cybersecurity, on the other hand, is concerned with protecting digital assets everything from networks to hardware and information that is processed, stored or transported by internetworked information systems. It is helpful to think of cybersecurity as a component of information security.

- Cyber criminality is the criminality over the cyberspace;
- Because technologies breakdown boundaries, we are all (individual, corporations, states, ...) concerned by cybersecurity;
- The skill gap in cybersecurity field is a serious worldwide concern, corporations and states should hold it as main priority and promote cybersecurity champions;
- As game-changer cybersecurity and cyber criminality impose updating certain behaviors, laws, and rules.

As the new world is cyber, we won't do without it, so let's make the needed changes to well start the race.

**Hoping that we will all be engaged in the cybersecurity race,**



# PANEL 1

## APERÇU GLOBAL DE LA CYBERSÉCURITÉ AU CAMEROUN

### Exposé 2

# LE CADRE INSTITUTIONNEL LÉGAL ET STRATÉGIQUE



Présenté par : **Emmanuel POKOSSY BELLE**  
Chef de la Division des Affaires  
Juridiques au MINPOSTEL

Titulaire d'un diplôme de l'Ecole Nationale d'Administration et de la Magistrature. Il est Magistrat hors échelle, Chef de Division des Affaires Juridiques au Ministère des Postes et Télécommunications. Il totalise plus de 25 ans d'expérience en matière d'élaboration des textes de loi du secteur des postes, télécommunications et technologies de l'information et de la communication.

#### PLAN DE L'EXPOSE

##### INTRODUCTION (la problématique)

##### I. LA PROBLEMATIQUE DE LA CYBERSECURITE ET DE LA CYBERCRIMINALITE AU CAMEROUN

##### II. LE CADRE LÉGAL

##### III. LE CADRE INSTITUTIONNEL

##### IV. LES PERSPECTIVES





## INTRODUCTION

Les Technologies de l'Information et de la Communication (TIC) s'appréhendent comme étant un ensemble des technologies issues de la convergence de l'informatique et des techniques évoluées du multimédia et des télécommunications. Ces technologies ont permis l'émergence de moyens de communication plus efficaces, en améliorant le traitement, la mise en mémoire, la diffusion et l'échange de l'information.

Cette définition reflète davantage le point de vue des institutions internationales qui considèrent les TIC comme étant l'intégration des techniques des télécommunications, de l'informatique, des multimédias et de l'audiovisuel.

Ainsi présentées, les TIC s'agrègent autour de l'Internet qui met en relation une communauté virtuelle d'utilisateurs dans le cyberspace.

Cependant, l'usage incontrôlé des TIC peut entraîner des abus aux conséquences dommageables et incommensurables à telle enseigne qu'il y a lieu de se demander si l'espace cybernétique est un « no man's land », où tout est permis sous le couvert d'une prétendue « liberté »?

Jean Jacques Rousseau disait et à juste titre dans son célèbre ouvrage Du Contrat Social que, « Sitôt qu'on peut désobéir impunément, on le peut légitimement ».

La réponse à ce questionnement ne pourrait être que négative même dans un contexte de mondialisation. Ainsi, conviendrait-il à priori de ressortir la problématique de la sécurisation du cyberspace Camerounais (I), avant le cadre normatif mis en place par le législateur Camerounais (II), suivi des institutions mises sur pied pour l'implémentation de ce cadre (III), enfin nous terminerons par les perspectives envisageables (IV).

### I- La problématique du cyberspace Camerounais

Dans son principe, l'Internet au moyen des Technologies de l'Information et de la Communication (TIC) constitue par essence un espace de liberté dans le cyberspace.

Cependant, l'on constate la recrudescence des infractions cybernétiques au nom du principe de la liberté alors que l'usage du cyberspace est suffisamment encadré par la législation et la réglementation

du secteur des Télécommunications et TIC

## II- Le cadre légal

### A- La législation

On peut citer :

- **la loi 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun**

Cette loi régit le cadre de sécurité de communications électroniques et des systèmes d'information, définit et réprime les infractions liées à l'utilisation des TIC. A ce titre, elle fixe le cadre d'exercice de la cybersécurité notamment les activités de certification électronique, les activités de sécurité des réseaux de communications électroniques et des systèmes d'information (Titre II). Par ailleurs, elle définit et réprime les infractions relatives à la cybercriminalité (Titre III).

### 1- De la Cybersécurité

Les activités de certification électronique relèvent de la cybersécurité. Ainsi, elles sont soumises à une autorisation préalable et exercées par des autorités de certification (article 10).

Pour ce qui est des activités de sécurité des réseaux de communications électroniques et des systèmes d'information, elles sont soumises à un audit de sécurité obligatoire (article 13).

De même, la protection des réseaux de communications électroniques et des systèmes d'information est respectivement consacrée par les articles 24 et 26.

En outre, la loi pose l'obligation d'information aux personnes dont l'activité est d'offrir un accès à des services de communications électroniques à leurs abonnés (article 33).

Elle consacre également un droit de réponse à toute personne victime d'une diffamation au moyen d'un service de communications électroniques en précisant que celle-ci peut en exiger la rectification. (article 39).

Par ailleurs, dans le cadre de la cybersécurité, la protection de la vie privée des personnes est garantie, notamment le droit au respect de la vie privée (article 41), la confidentialité des communications électroniques (article 42), l'atteinte à la dignité humaine et à l'honneur (article 43),

l'interception frauduleuse et illicite des communications électroniques (article 44), l'obligation par les fournisseurs de communications électroniques de conserver le contenu des données stockées dans leurs installations pendant 10 ans (article 46), l'interdiction de l'émission des messages électroniques à des fins de prospection en dissimulant l'identité de l'émetteur au nom duquel la communications est faite (article 48).

## 2- De la Cybercriminalité

Pour ce qui concerne la cybercriminalité, elle procède du caractère transnational des infractions commises dans le cyberspace. Ainsi, la loi sus visée consacre les dispositions relevant du droit processuel (articles 54 à 59), avant de fixer les sanctions prévues aux infractions cybernétiques notamment l'interception ou la violation des communications électroniques par des moyens techniques, la perturbation ou l'interruption du fonctionnement d'un réseau de communications électroniques (articles 65, 66), l'atteinte à l'intégrité d'un réseau des communications électroniques ou d'un système d'information, ainsi que l'accès ou le maintien frauduleux (articles 67, 68), la saturation ou l'attaque d'une ressource de réseau de communications électroniques ou d'un système d'information (article 70), la contrefaçon, la falsification d'une carte de paiement de crédit par la voie d'un système d'information (article 73), l'atteinte à l'intimité de la vie privée, la diffusion à but lucratif par voie de communications électroniques ou d'un système d'informations des images portant atteinte à l'intégrité corporelle (articles 74, 75), la propagation de fausses nouvelles « fake news » (article 78) etc.

• **la loi n°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun modifiée et complétée par la loi n°2015/006 du 20 avril 2015 ;**

Elle régit les communications électroniques au Cameroun. De même qu'elle encadre la fourniture de service des communications électroniques à l'instar de l'identification des abonnés et des terminaux (articles 55 et 56).

De plus, cette loi réprime la violation du secret de la correspondance par toute personne admise à participer à l'exécution d'un service de communications électroniques (article 80 et suivant).

Pour la mise en œuvre de ce cadre légal, le Gouvernement a prévu un cadre institutionnel.

## III- le cadre institutionnel mis en place

Sur le plan institutionnel, l'Etat a mis en place les entités ci-après pour la régulation des communications électroniques et des Technologies de l'Information et de la Communication .

Il s'agit de :

### A- le Ministère des Postes et Télécommunications (MINPOSTEL)

Au terme des dispositions de l'article 6 de la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité « l'Administration chargée des Télécommunications élabore et met en œuvre la politique de sécurité des communications électroniques en tenant compte de l'évolution technologique et des priorités du Gouvernement».

De même, l'article 35 de la loi n°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun dispose que « l'Administration des Télécommunications veille à l'élaboration et à la mise en œuvre de la politique sectorielle des Télécommunications et des Technologies de l'Information et de la Communication»

Par ailleurs, l'article 1er alinéa 2 du décret n°2012/512 du 12 novembre 2012 portant organisation du Ministère des postes et Télécommunications dispose que « le Ministère des Postes et Télécommunications est responsable de l'élaboration et de la mise en œuvre de la politique du Gouvernement en matière des Postes, des Télécommunications et des Technologies de l'Information et de la Communication [...]». Et le sixième tiret de cet alinéa précise bien que le MINPOSTEL suit les questions de cybersécurité et de cybercriminalité.

### B- le Ministère de la Justice (MINJUSTICE)

A travers ses juridictions de l'ordre administratif et de l'ordre judiciaire, est chargé de la poursuite et du jugement des auteurs des infractions et éventuellement de leur répression.

### C- L'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC)

Dans la perspective de mettre en place la cybersécurité et de lutter contre la cybercriminalité



L'ANTIC a été instituée par la loi n°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun en son article 96.

Par ailleurs, au terme de l'article 3 du décret n°2019/150 du 22 mars 2019 portant organisation et fonctionnement de l'ANTIC, elle assure pour le compte de l'Etat deux principales missions, à savoir:

- la promotion et le suivi de l'action des pouvoirs publics en matière des Technologies de l'Information et de la Communication;
- la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques, ainsi qu'à la certification électronique en collaboration avec l'Agence de Régulation des Télécommunications (ART).

S'agissant de la promotion et du suivi de l'action des pouvoirs publics en matière des Technologies de l'Information et de la Communication, l'ANTIC est notamment chargée de veiller, dans l'usage des TIC au respect de l'éthique ainsi qu'à la protection de la propriété intellectuelle, des consommateurs, des bonnes mœurs et de la vie privée.

Pour ce qui est de la régulation, du contrôle et du suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques, l'ANTIC a entre autres missions:

- d'assurer la sécurisation du cyberspace national notamment les transactions en lignes, des systèmes d'information et des réseaux de communications électroniques.

#### D- L'Agence de Régulation des Télécommunications (ART)

Au terme de l'article 7 de la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun, l'Agence de Régulation des Télécommunications (ART) collabore avec l'ANTIC dans le cadre de la régulation des activités liées à la sécurité des réseaux de communication électroniques et des systèmes d'information.

Cette disposition est reprise dans le texte organique de l'ART en l'occurrence le décret n°2012/203 du 20 avril 2012 portant organisation et fonctionnement en son article 4 alinéa 6.

A l'observation, il apparaît donc clairement que dans le domaine de la sécurité des réseaux de communications électroniques, le cadre législatif et réglementaire prévoit une co-régulation entre les

deux agences pour plus d'efficacité.

Cependant, bien que le législateur ait prévu un cadre législatif et mis en place des institutions sus évoquées, il y a lieu tout de même de relever quelques difficultés auxquelles nous suggérerons quelques propositions de solutions.

#### E- Les difficultés rencontrées

Au chapitre des difficultés rencontrées, on peut citer :

- le caractère dynamique de la technologie qui exige une révision permanente de la législation et de la réglementation;
- le défaut d'obligation pour les Administrations publiques de faire sécuriser leurs applications ;
- réticence des fournisseurs d'accès à internet (FAI) et des opérateurs à faire passer leur trafic par l'IXP ;
- la non mise en œuvre des recommandations issues des audits de sécurité réalisés et des bulletins de sécurité émis par l'ANTIC ;

#### IV- Perspectives

Au terme de cet exposé, il apparaît que l'accès et l'usage du cyberspace Camerounais sont encadrés. Toute chose qui en appelle à n'en point douter à la responsabilité des usagers du cyberspace.

Toutefois, malgré cet important dispositif institutionnel et législatif, on constate tout de même au regard du caractère dynamique de la technologie, la recrudescence des infractions cybernétiques.

Cependant, à défaut de les éradiquer complètement, il y a lieu d'envisager des perspectives visant à les réduire considérablement.

A ce titre nous pouvons citer :

- la ratification et l'internalisation des instruments juridiques internationaux notamment la convention de l'Union Africaine sur la cybercriminalité (Malabo, 27 juin 2014), et la convention de Budapest sur la cybercriminalité;
- l'appropriation des textes spécifiques du secteur par les acteurs institutionnels (magistrats, Officiers de Police Judiciaire) ;
- la formation notamment des OPJ aux techniques d'investigation dans le cyberspace ;

- l'acquisition et le déploiement des outils techniques de pointe afin de protéger les infrastructures critiques du cyberspace Camerounais ;
- le renforcement de la coopération internationale sur la cybersécurité notamment par la mise en conformité aux normes internationales de nos infrastructures de protection ;
- la refonte du cadre légal en vigueur : révision de la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité.

A cet effet, il y a lieu de préciser qu'une nouvelle mouture a été élaborée et transmise à la Haute Hiérarchie pour suite de la procédure.

Ce texte apporte plusieurs innovations notamment : le ren-

forcement du régime des sanctions tant administratives que pénales, la précision sur la qualification des infractions, l'aggravation des peines des infractions commises dans le cyberspace, l'introduction des nouveaux concepts « cyberchantage pornographique, données à caractère personnel, phishing, ou hameçonnage, scamming webdefacement ».

A titre d'exemple, on peut citer :

- les atteintes au fonctionnement des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux ;
- les atteintes aux moyens de paiement ;
- le vol d'information ;
  - les atteintes aux données ;

- l'exploitation sexuelle des mineurs;
- les atteintes aux biens.
- la poursuite et le renforcement de la sensibilisation des populations et le développement de l'expertise locale sur la cybersécurité (à titre d'exemple, le MINPOSTEL a organisé plusieurs activités à savoir : le séminaire à l'intention des journalistes de la section camerounaise de la francophonie sur l'usage responsable des réseaux sociaux, la campagne nationale pour la promotion de la culture de la cybersécurité et sensibilisation à l'utilisation responsable des réseaux sociaux);

**Je vous remercie de votre aimable attention**





# PANEL 1

## OVERVIEW OF CYBERSECURITY IN CAMEROON

### Presentation 3

# INFRASTRUCTURE AND TECHNICAL CYBERSECURITY MEASURES: CIRT AND SOC



**Presented by: MBUH Godlove MBUH**  
**IT Engineer, Master Pro. InfoSec**

- IT Engineer, Information Systems Security Expert.

He has already carried out more than 200 hours of information systems security audit in Public and Private Structures, currently, Deputy Director in charge of Preventive Security at ANTIC

- PRESENTATION OF NATIONAL CIRT ;
- ON CYBERCRIMINALITY AND CYBERSECURITY (FROM JANUARY 2020);
- DIFFICULTIES ENCOUNTERED BY CIRT ;
- SECURITY OPERATIONS CENTER (SOC) ;
- CONCLUSION AND RECOMMENDATIONS.

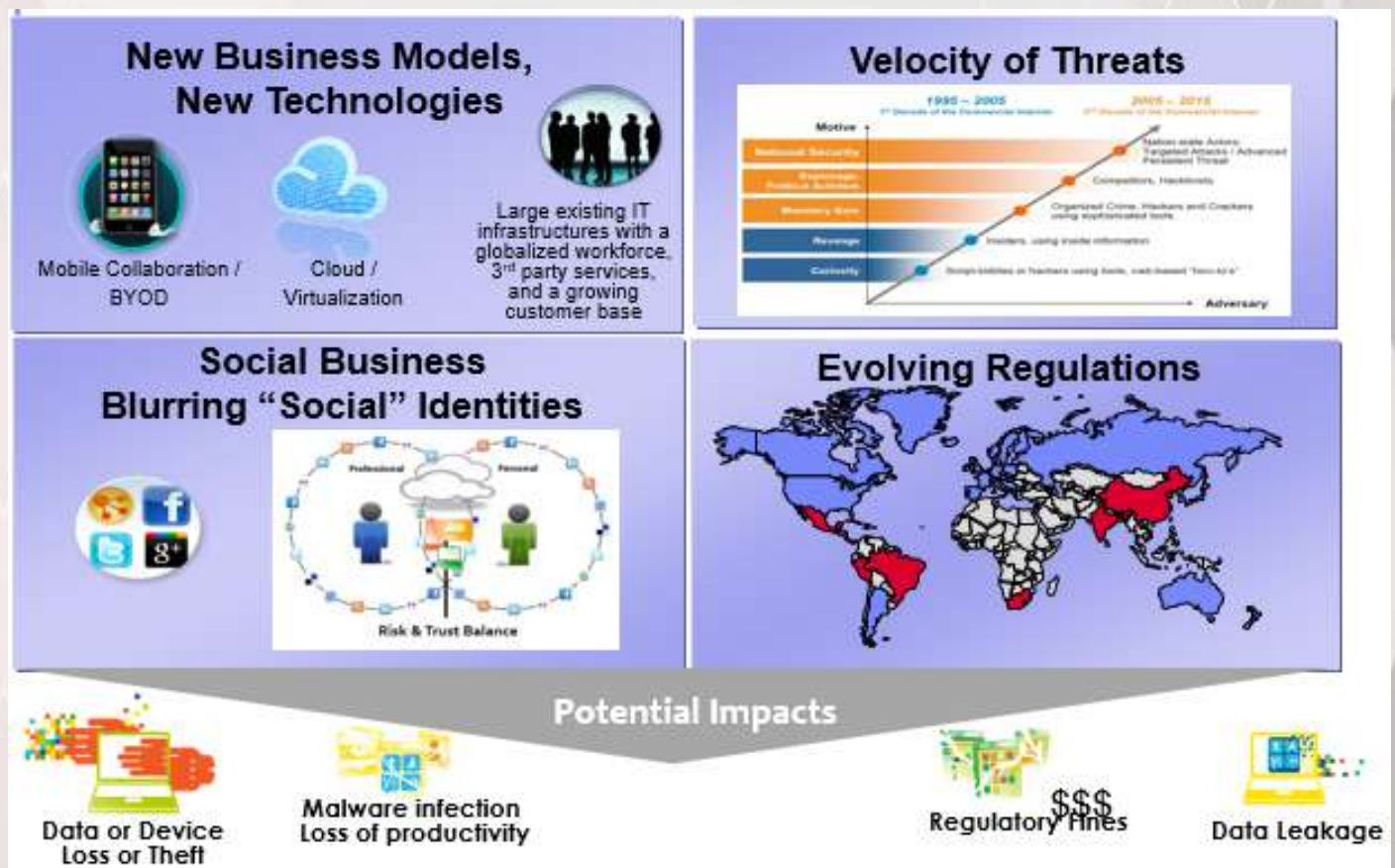
**INTRODUCTION**

- Information systems nowadays have become an indispensable cornerstone in the functioning of Enterprises and States as they provide managements and State officials excellent decision making tools.
- The development and evolution of these information and communication technologies has brought about new forms of risks to both Enterprises and to the Cameroonian cyberspace.

- The law No 2010/012 gave ANTIC the responsibility to carry out Security Intelligence of Information Systems and electronic communication networks in Cameroon amongst other missions.
- To fulfill its security intelligence mission, ANTIC since 2013 established a Computer Incident Response Team (CIRT), having among other responsibilities, the Investigation of cyber related crimes and Incident Response.

The current environment is putting new demands on security operations

1. Presentation of National CIRT



**Definitions**

- Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy ;
- CIRT: is responsible for responding to security breaches, viruses and other potentially catastrophic incidents in enterprises that face significant security risks, as well as in the National cyberspace;
- CERT collects and disseminates security information, typically for the benefit of a country or industry;
- A SOC is where a country or organization monitors and defends its network, servers, applications, and endpoint computers. Can be compared to a NOC.



**National CIRT AND ITS ROLE**

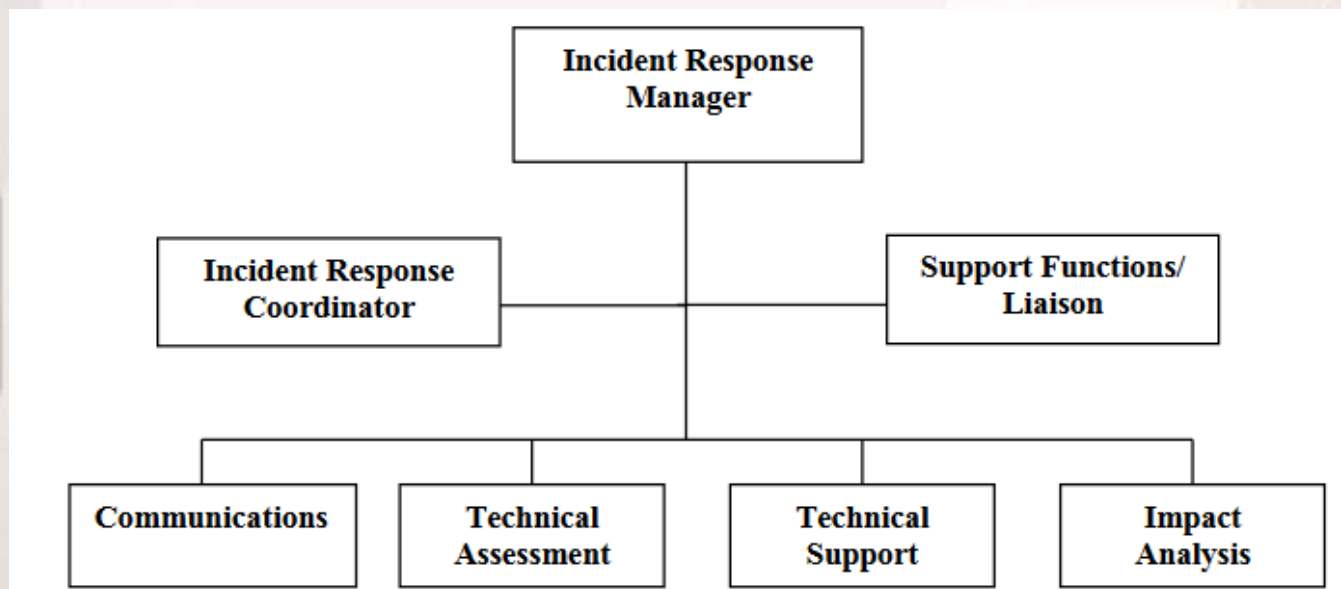
- The COMPUTER INCIDENT RESPONSE TEAM (CIRT) is a center put in place by the State through ANTIC to guarantee the security of the Cameroonian cyberspace;
- The law N°2010/012 of December 21, 2010, in its article 7, stipulates that ANTIC is responsible for ensuring Security intelligence, issuing alerts and recommendations on the security of electronic communications networks;
- Security monitoring is a continuous process that consists, on one hand, of ensuring that the critical infrastructure has the latest security patches and, on the other hand, monitoring the infrastructure in a bid to detect in real time attempted attacks, intrusions and to react quickly and effectively;
- The roles of CIRT are divided into two (02) major groups;
- Preventive: taking appropriate measures to prevent cyber attacks, through the dissemination of security information and bulletins amongst other aspects ;
- Proactive: CIRT must react promptly in order

to counter the attack on one hand, and to detect, contain and eradicate cyber incidents as well as the restauration of the affected IT systems.

**MISSIONS OF THE NATIONAL CIRT**

- National Cyberspace’s sensitive infrastructure monitoring and real-time response to incidents ;
- Investigations related to cybercrime in the National cyberspace (Section 52 of law N ° 2010/012 of 21 December 2010) ;
- Carrying out Awareness campaigns on cybersecurity and cyber-criminality ;
- Issuing security bulletins, newsletters and security alerts ;
- Providing assistance to users and companies in the handling of security incidents ;
- Development of information system security standards ;
- Collaboration with other CIRTs (CIRT also collaborate with organizations such as IMPACT, INTERPOL and AFRICACERT.

**ORGANIZATIONAL STRUCTURE OF AN INCIDENT RESPONSE TEAM**



## 2. STATISTICS ON CYBERCRIMINALITY AND CYBERSECURITY (2020)

From January 2020,

- ANTIC has received and processed 135 complaints relating to scams or attempted financial scams, of which 95 are through Mobile Money;
  - Investigated Two (02) cases of ransomware attacks ;
  - Processed Thirty-two (32) complaints related to Facebook account hijacking;
  - Resolved Twenty-two (22) complaints from users who were victims of cyber blackmail;
  - Processed Sixteen (16) cases of harassment via social networks ;
  - Received Twelve (12) calls relating to theft of telephone and laptop computers;
  - CIRT has assisted the Forces of Law and Order with over 5000 digital investigations;
- Statistics on cybersecurity are as follows:
- more than 5,000 vulnerabilities have been discovered in eighty-five (85) sensitive government and private enterprise web sites/applications;
  - twenty-four (24) security bulletins have been issued by the ANTIC;
  - CIRT conducts a routine monitoring of 175 websites of Ministries and Public Administrative Establishments (EPA). It emerges from this monitoring

that :

- 23 websites have an availability rate below 50%;
- 35 have an availability rate between 50% and 100%;
- 117 have an availability rate at 100%
- Thirty-five (35) Facebook pages/accounts of ministries and State Officials have been VERIFIED by Facebook with the assistance of ANTIC
- CIRT organized several awareness campaigns through various channels including 14 radio broadcasts, 03 seminars and 05 training workshops.

## 3. DIFFICULTIES ENCOUNTERED BY CIRT

- Budget constraints with security incidents becoming more costly;
- Collaboration with international institutions and foreign service providers, Facebook, Google, Yahoo, within the framework of user assistance and digital investigations remains a challenge;
- The regulatory framework in the field of cybersecurity and cybercriminality has certain shortcomings, as it fails to take into account specific measures to protect personal identifiable data;
- Also, most of the recommendations issued by CIRT, in the form of security bulletins, alerts, vulnerability scan reports, etc., are not regularly implemented by the Companies/Administrations.

## THE SECURITY OPERATIONS CENTER (SOC)

Primary Objective	Organization Type	Rationale
Collect and Disseminate Security Information	CERT	A CERT is equipped to collect and curate security information from several sources but not to defend a network or respond to individual incidents.
Monitor and Defend an Organization's Infrastructure	SOC	A SOC is an organization that invests in technology and staff skilled at monitoring and defending networks, endpoints, servers, and other infrastructure.
Respond to Security Incidents	CIRT	A <b>CIRT</b> is a cross-functional organization that is chartered with responding to security incidents. Some team members may not be full time but are called in as needed.

- A Security Operation Center (SOC), just like a NOC is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity issues.
- ...but the types of issues and impact they have are considerably different. The SOC focuses on "intelligent adversaries" while the NOC deals with naturally occurring system events.



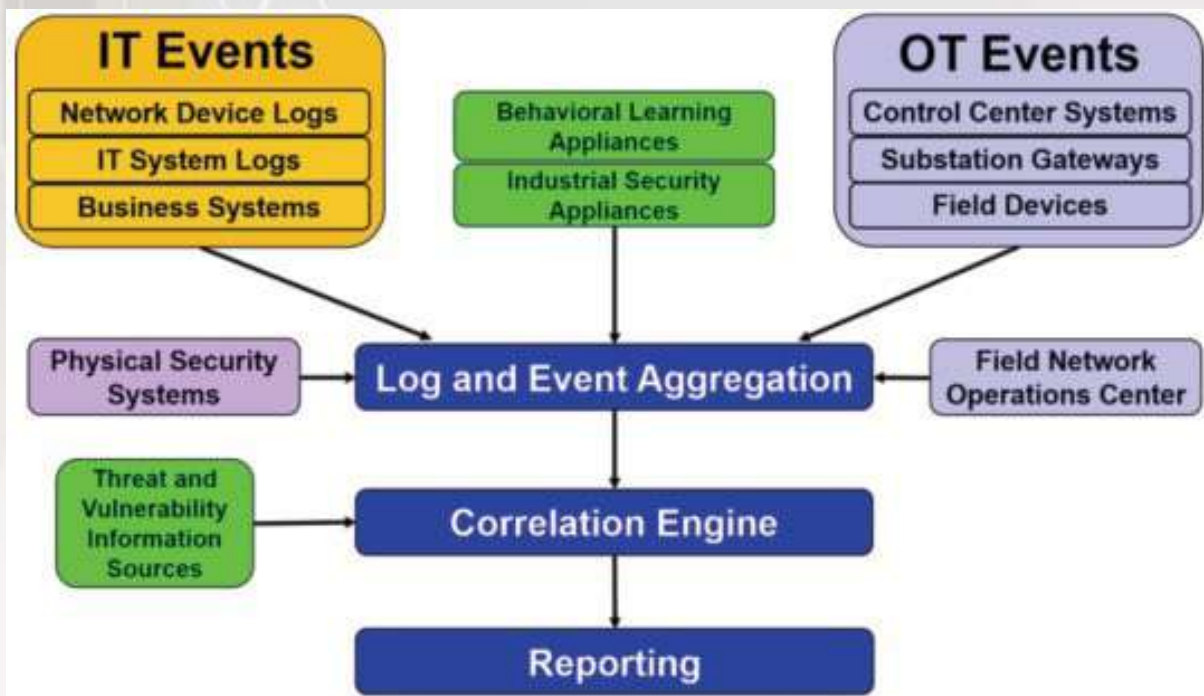
**Why do we build operational security controls & capabilities?**

- Reduce enterprise/National risk. Protect the business;
- Move from reactive response to proactive mitigation;
- Increase visibility over the environment;
- Meet compliance/regulatory requirements.

**...how to build a SOC:**

- Develop your security operations center strategy;
- Design your SOC solution (SIEM solutions);
- Create processes, procedures, and training;
- Prepare your environment;
- Implement your solution;
- Deploy end-to-end use cases;
- Maintain and evolve your solution.

**SOC ARCHITECTURE**



**4. CONCLUSION AND RECOMMENDATIONS**

**CONCLUSION**

- The fight against cybercriminality is a global problem and therefore require a global response;
- The National CIRT alone may not be able to completely eradicate cybercrimes;
- There is need to reinforce the National and International collaborative platforms (consisting of all the actors) in order to block the road for those criminals endangering the lives of Cameroonians;
- Each company/administration could deploy their SOC in order to appropriately monitor the security of their critical assets.

**RECOMMENDATIONS**

- The Government should allocate more Budget for cybersecurity projects;
- The State should engage international institutions and foreign service providers, such as Facebook, Google, Yahoo, within the framework fighting cybercriminality and reinforcing cybersecurity;
- The regulatory framework in the field of cybersecurity and cybercriminality should be updated to take into account the protection of personal data, amongst other aspects;
- There is need to create information systems security Units in the different Ministerial Departments ;
- There is also, need to reinforce the infrastructural capacity of CIRT, as well as the sensitization of the population.

Contact Information

https://www.cirt.cm

Anglais Français

**ANTIC**  
CENTRE D'ALERTE ET DE REPONSE AUX INCIDENTS CYBERNETIQUES  
COMPUTER INCIDENT RESPONSE TEAM

Search

ACCUEIL PRÉSENTATION BULLETINS ALERTES CONTACTER L'ÉQUIPE A SAVOIR ARCHIVES

**LATEST ALERT**

- Microsoft Releases Security Updates to Address Remote Code Execution Vulnerabilities
- NCSC Releases Alert on Microsoft SharePoint Vulnerability
- Adobe Releases Security Updates for Magento
- Juniper Networks Releases Security Updates for Multiple Products
- Microsoft Addresses Windows TCP/IP RCE/DoS Vulnerability
- Adobe Releases Security Updates for Flash Player
- Apache Releases Security Updates for Apache Tomcat
- Microsoft Releases October 2020 Security Updates

**TOP 10**  
Most popular attack in national cyberspace 2018

- Web defacement (unauthorized modification of the homepage of a site)
- Skimming (Fraud on the bank card)
- Scamming (money scam through the Internet or social network)
- Fraudulent use of identification element of natural or legal person
- Falsification of administrative documents on the Internet
- Attacks on the Image (threat, insults, harassment, defamation, slanderous denunciation on social networks)
- Illegal registration of private communication
- Spoilation of mail account
- Publication of personal data

**REPORT AN INCIDENT**

We encourage you to report activities that you believe meet the criteria for an incident

[Report an Incident](#)

**NOTIFIER UN INCIDENT**

Nous vous encourageons à signaler les activités qui selon vous répondent à un incident informatique

https://cirt.cm

Services are available 24h/24, 7d/7

You could also contact CIRT via the toll free number **8202** or through the email address **alerts@cirt.cm**



## PANEL 1

### APERÇU GLOBAL DE LA CYBERSÉCURITÉ AU CAMEROUN

## Exposé 4

# INFRASTRUCTURES ET MESURES TECHNIQUES DE CYBERSÉCURITÉ: E-GOV ET PKI NATIONALE



Presenté par : **GBITHICKI NDANGA Brice**  
**Chef Service de la Régulation**  
**des Activités de Certification Electronique**

Titulaire d'un diplôme d'ingénieur de conception en informatique, il a 10 ans d'expérience dans le secteur informatique travaillant dans les organisations publiques et privées, son domaine d'intérêt est la certification électronique, la cybersécurité, la criminalistique numérique et le cloud computing.

Depuis 2016, il occupe le poste d'Ingénieur Sécurité en charge de la Régulation des Activités de Certification Electronique à l'ANTIC.

Il est titulaire de plusieurs certifications, notamment : le E-Concil, la KICA certification, le MicroTik et Linus Professional Institute.

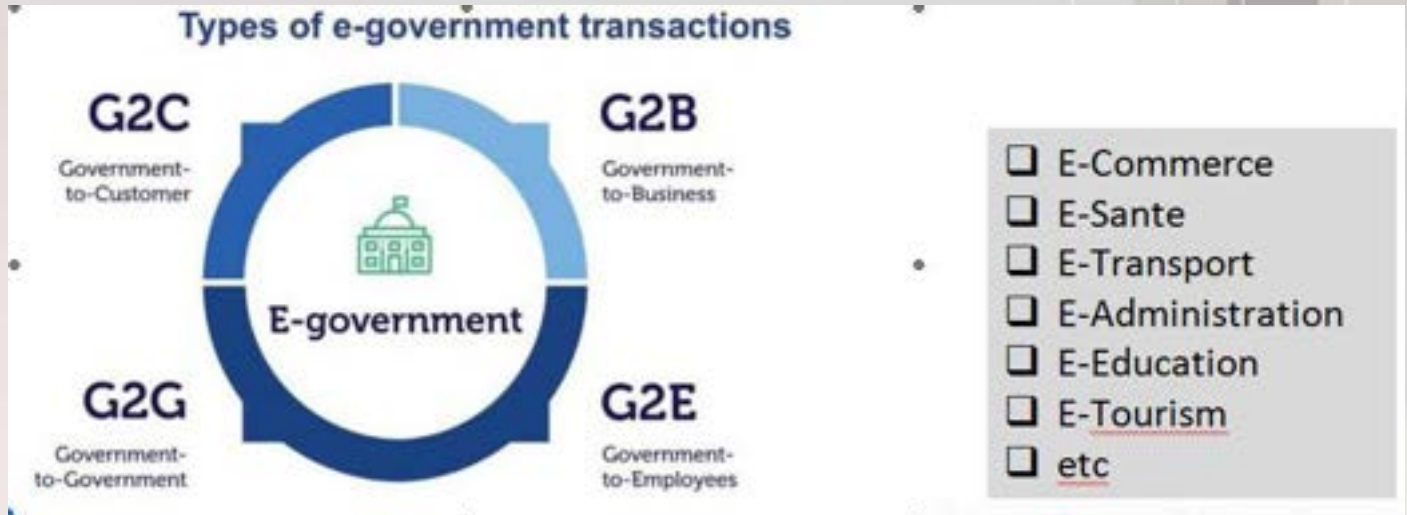
### PLAN DE L'EXPOSE

**I. Les initiatives du e-GOV et les risques de sécurités;**

**II. L'implication de la PKI dans la sécurisation des transactions du e-GOV et la lutte contre la cybercriminalité.**

**e-GOV : Définition**

L' e-Gouvernement (ou gouvernement électronique ou encore administration en ligne) décrit l'utilisation des Technologies de l'Information et de la Communication (TIC) par les administrations publiques afin de rendre les services publics plus accessibles aux citoyens et aux entreprises et afin d'améliorer le fonctionnement interne de l'État.

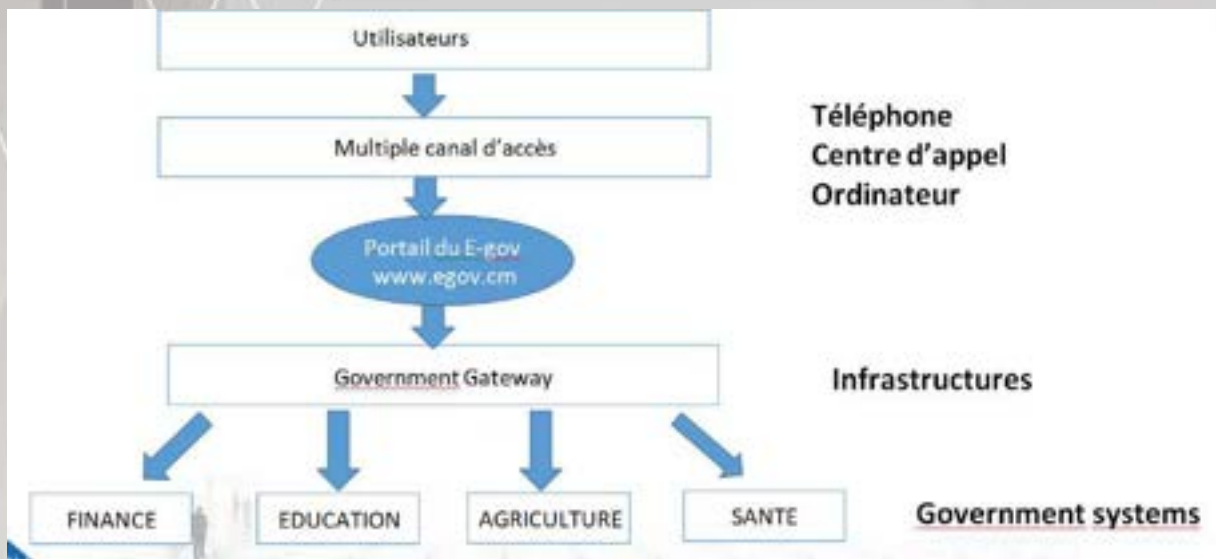


**e-GOV HISTORIQUE AU CAMEROUN**





e-GOV ARCHITECTURE



e-Government Interoperability Framework(e-GIF)  
Interopérabilité technique, organisationnelle et sémantique lors de la fourniture de services entre les différents systèmes.

Il se concentre sur 4 aspects à savoir :

- Interconnectivité;
- Intégration de données;
- Accès;
- Gestion de contenu.

se conformer à l'e-GIF signifie par exemple de :

- Fournir une interface de navigateur pour l'accès;
- Utiliser XML comme principal moyen d'intégration des données;
- Utiliser les images graphiques de qualité de base présentées au format .jpg ou .gif;
- Utiliser d'Internet et du World Wide Web (www);
- Utiliser des métadonnées pour la gestion de contenu.

e-GOV : Quelques initiatives dans le domaine des applications et services en ligne

**E-Santé :** Près de 04 centres hospitaliers interconnectés, les applications GiftMon, Cardiopad

**E-Agriculture**  
Portail de l'information phytosanitaire, Homologation des pesticides et vérification de l'authenticité du certificat phytosanitaire en ligne

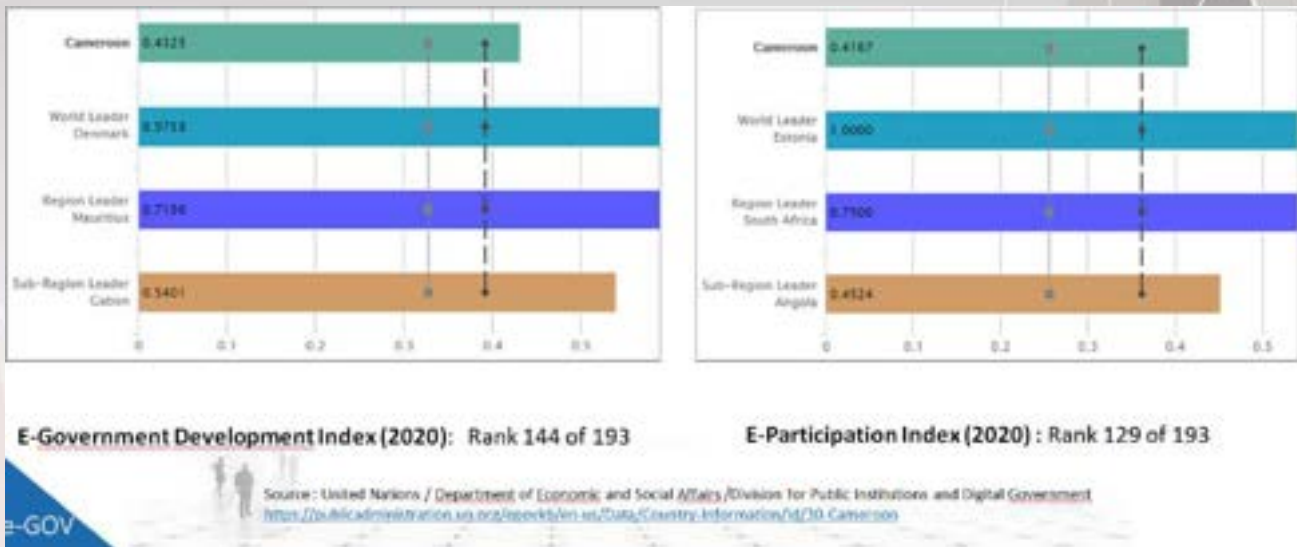
**E-Education**  
Paiements dématérialisés des frais de scolarité, Consultation des résultats des examens par SMS, Universités et lycées connectés à internet

**E-Transport**  
Achat de billet de transport en ligne (Camrail, Camaico), délivrance des titres de transport (carte grise, permit de conduire)

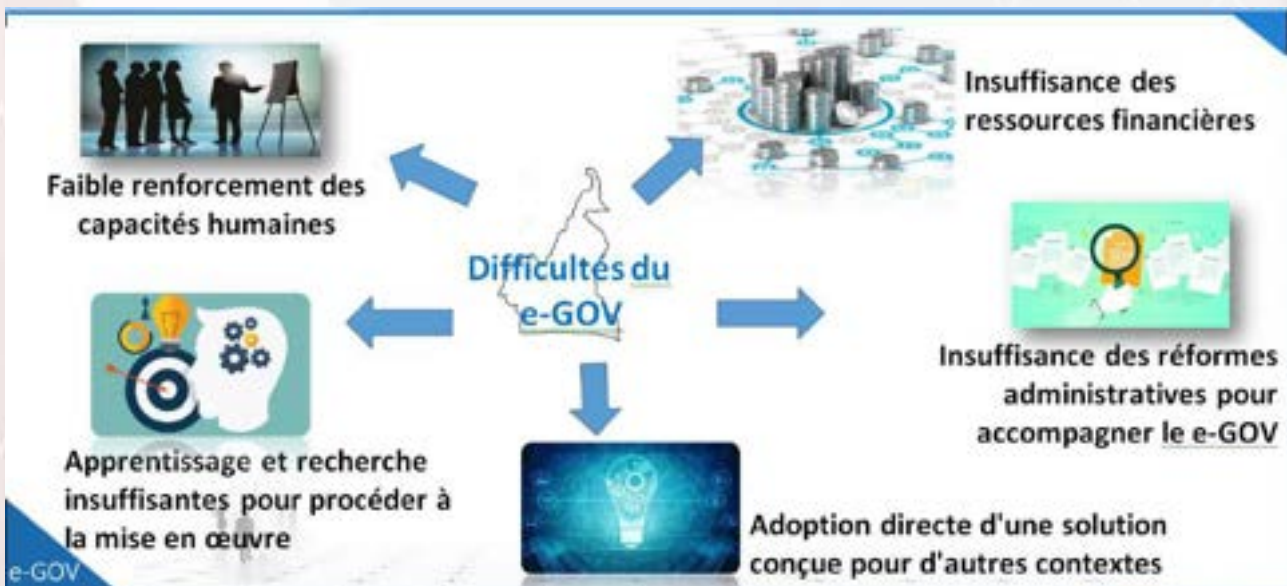
**E-Administration**  
Inscription en ligne au concours de la fonction publique en ligne, l'accès aux bulletins de soldes, immatriculation en ligne des contribuables, passation de marché en ligne

EXPOSÉ 4 : INFRASTRUCTURES ET MESURES TECHNIQUES DE CYBERSÉCURITÉ  
E-GOV ET PKI NATIONALE

Indice de développement de l'e-gouvernement (EGDI) et E-participation



DIFFICULTES DE MISE EN OEUVRE





RISQUES DE SECURITE



Comment impliquer la PKI dans la sécurisation des transactions du e-GOV et la lutte contre la cybercriminalité

II. L'IMPLICATION DE LE PKI DANS LA SECURISATION DES TRANSACTIONS DU e-GOV ET LA LUTTE CONTRE LA CYBERCRIMINALITE

PKI : c'est quoi (Public Key Infrastructure) ?



Différence entre la signature manuscrite et la signature numérique

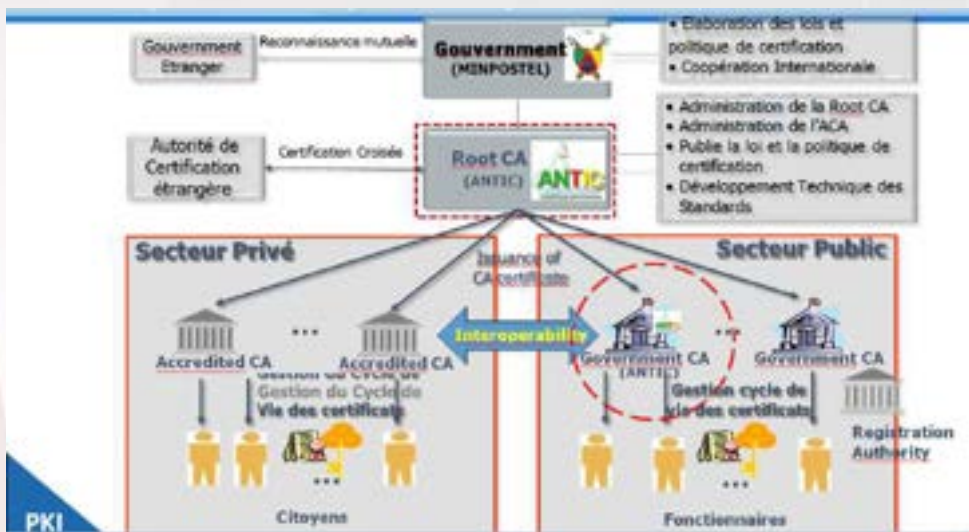
Signature manuscrite	signataire	Signature numérique
	Document à signer	
	Outil de signature	
Signature manuscrite	Document signé	
Falsification facile		Infaisifiable Authentique Irévocable

**ATTENTION** : une signature manuscrite scannée et apposée en bas du document n'est pas une signature numérique

Les types de certificats délivrés



PKI : ARCHITECTURE



PKI : ROLES

- Assurer cumulativement les fonctions de l'Autorité de Certification Racine et l'Autorité de Certification Gouvernementale;
- Sécuriser les contenus des systèmes d'informations et des réseaux de communications électroniques de manière générale;
- Réguler les activités de certification des organismes publics et privés;
- Jouer le rôle de tiers de confiance.





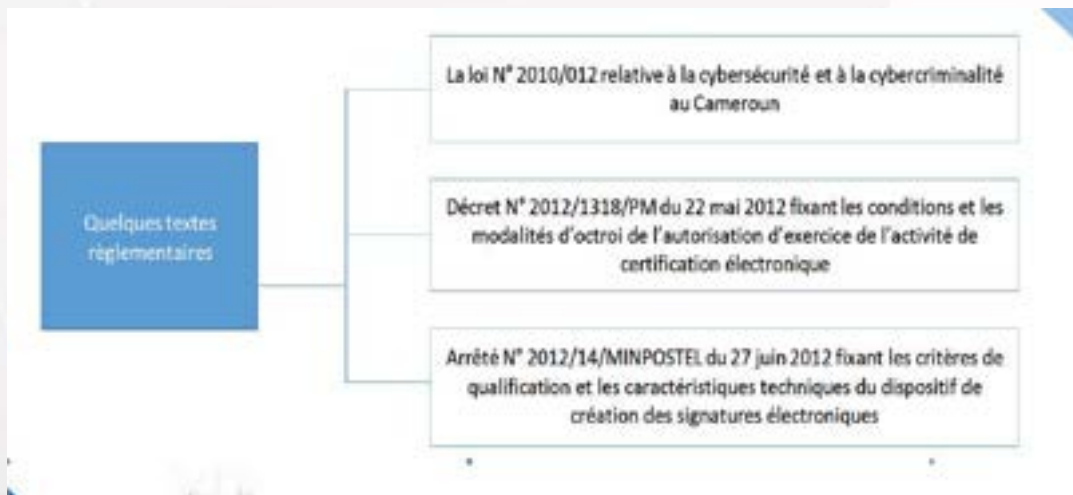
PKI : LES SERVICES DE LA PKI



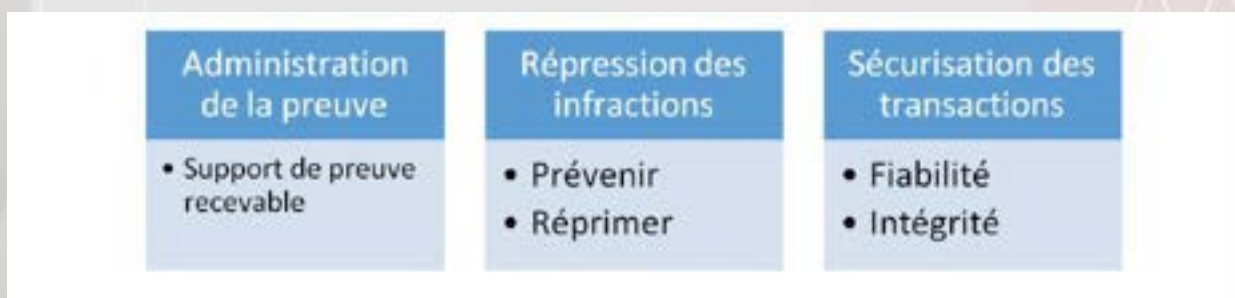
Les applications sécurisées et en cours de sécurisation



PKI : CADRE LEGAL

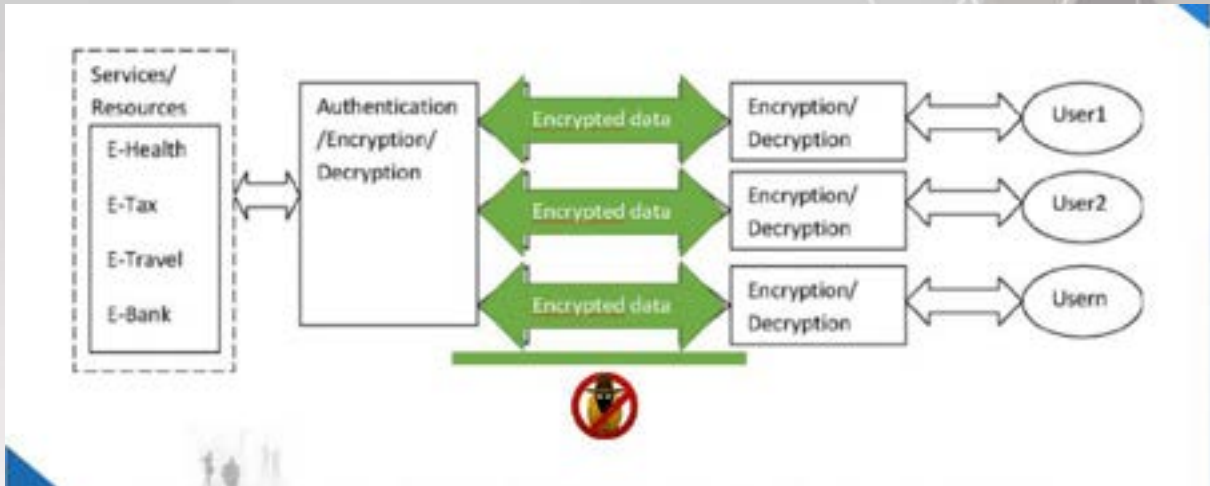


PKI : Rôles dans la lutte contre la cybercriminalité



EXPOSÉ 4 : INFRASTRUCTURES ET MESURES TECHNIQUES DE CYBERSÉCURITÉ  
E-GOV ET PKI NATIONALE

PKI : Architecture sécurisé PKI et e-GOV



PKI : l'importance dans la sécurisation des transactions du e-GOV



PKI : Difficultés rencontrées dans la réalisation des activités

- Non respect des critères techniques de sécurisation des applications à l'aide de la PKI
- Absence des experts PKI dans le processus d'acquisition ou de conception des applications
- Non reconnaissance automatique des certificats TLS/SSL
- Faible application des recommandations des audits de sécurité de l'ANTIC par les Administrations
- Inadéquation du cadre légal aux évolutions technologiques

PKI : PERSPECTIVES

- L'extension de la PKI vers le module PKI mobile
- Reconnaissance des certificats TLS\SSL
- Renforcement du cadre juridique et réglementaire et les mécanismes de financement
- Renforcement de la sensibilisation et de la formation des Administrations sur la PKI



## PANEL 1

### APERÇU GLOBAL DE LA CYBERSÉCURITÉ AU CAMEROUN

## Exposé 5

# INFRASTRUCTURES ET MESURES TECHNIQUES DE CYBERSÉCURITÉ: AUDITS DE SÉCURITÉ



Presenté par : **Cyrille A. MOLEMB BEAL**

**Ing. CEH 10 & 9, ISO 27005 RM, COBIT5...**

**Chef service de la Gestion des Audits, DAS,ANTIC**

- Ingénieur des télécommunications et réseaux ;
- Expert en cybersécurité et sécurité des systèmes d'information.
- Expert auditeur en sécurité des systèmes d'information disposant de 10 années d'expérience dans le domaine ;
- Chef service de la gestion des audits de sécurité au sein de la Direction de l'audit de Sécurité à l'antic.

Cyrille Augustin Molemb Beal est détenteur de plusieurs certifications professionnelles dans le domaine de la cybersécurité et la sécurité des SI dont le CEH9, le CEH10, Iso 27005 Risk Manager et le COBIT.

Il est également auteur de plusieurs articles dans le domaine.

### AGENDA

1. Généralités ;
2. Objectifs ;
3. Cadre réglementaire ;
4. Différents acteurs;
5. Méthodologie d'audit;
6. Statistiques;
7. Difficultés rencontrées;
8. Recommandations.

**GENERALITES**

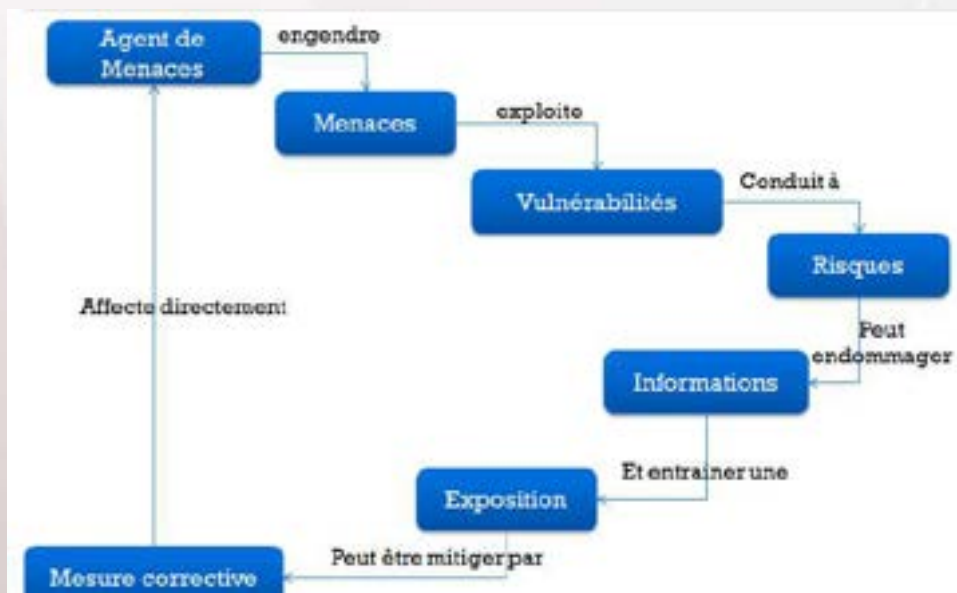
**Système d'information:** Ensemble de ressources organisées (logiciels, matériels, réseaux, documents, ressources humaines...) permettant l'élaboration, l'analyse, le traitement, le stockage, la diffusion et la destruction d'informations.



**Vulnérabilité:** Caractéristique d'une entité qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.

**Menace:** Cause potentielle d'incident, qui peut résulter en un dommage sur le système d'information.

**Risque:** Résultante de l'exploitation d'une ou plusieurs vulnérabilités par une menace.



**Eléments de sécurité**

Préserver ou tenir les restrictions autorisées sur l'accès aux informations et leur divulgation, y compris les moyens de protéger la vie privée et les informations propriétaires.



Protéger contre toute modification ou destruction inappropriée des informations et garantir la non-répudiation et l'authenticité des informations

Garantir un accès et une utilisation rapides et fiables des informations par les utilisateurs autorisés.

**OBJECTIFS**

**GLOBAUX**

- Prévenir les actes cybercriminels ;
- Améliorer la gouvernance des SI & RCE;
- Sécuriser le cyberspace Camerounais.

**SPECIFIQUES**

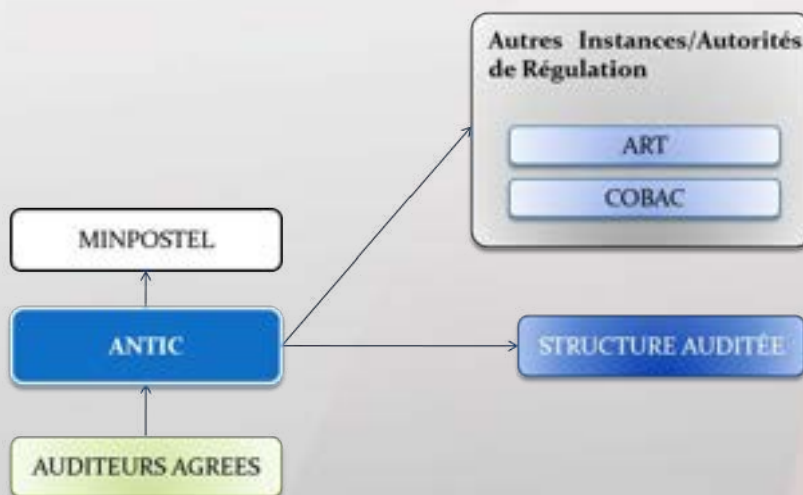
- Établir un état des lieux du système d'information audité vis-à-vis des risques ;
- Déterminer les failles de sécurité sur les plans organisationnel, physique et technique ;
- Apprécier le niveau de la mise en œuvre des recommandations issues des précédents audits s'il y a lieu ;
- Analyser et évaluer les risques de sécurité identifiés et les classer suivant leur niveau de criticité ;
- Proposer des contre-mesures adaptées et proportionnées aux problèmes identifiés;
- Accompagner éventuellement la structure à la mise en œuvre des actions recommandées.

**CADRE REGLEMENTAIRE**

- La Loi N° 2010 /012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun ;
- Le décret N° 2012/1643/PM du 14 juin 2012 fixant les conditions et les modalités d'audit de sécurité obligatoire des réseaux de communications électroniques et des systèmes d'information.

**APPORT DE L'AUDIT**

- Un conseil en management de la sécurité de l'information fourni par des spécialistes externes;
- Sécurisation et pérennisation du patrimoine informationnel ;
- Arrimage du niveau de sécurité du SI aux standards et normes, ceci en adéquation avec les objectifs stratégiques de l'entreprise ;
- Moyen pour impulser et orienter l'acquisition de nouveaux dispositifs ou tout autre changement majeur au niveau organisationnel visant à mitiger les risques identifiés.





**Méthodologie D'audit**

• L'audit de sécurité réalisé par l'ANTIC est essentiellement basé sur la Norme ISO 27001 à laquelle se greffent des mesures issues du NIST CSF, du cadre légal en vigueur, des politiques et procédures internes des entreprises et secteurs d'activité et aussi les méthodes d'analyse des risques MEHARI et EBIOS.

Les étapes de l'audit :

- L'état des lieux;
- L'audit organisationnel & physique;
- L'audit technique;
- L'évaluation du niveau de maturité;
- L'analyse des risques.

**ETAT DES LIEUX**

- Revue du système d'information existant ;
- Identification des processus métier ;
- Vision et stratégie de développement du SI ;
- Bilan des ressources matérielles et logicielles ;
- Architecture des réseaux et télécommunications;
- Structure technique en charge du Système d'Information.
- Evaluation de la mise en œuvre des recommandations issues des précédents audits.

**AUDIT ORGANISATIONNEL**

- Interviews des acteurs clés du SI ;
- Analyse documentaire ;
- Tests de corroboration ;
- Identification des forces et des faiblesses

(vulnérabilités) organisationnelles ;

- Formulation des recommandations de sécurité organisationnelle;
- Évaluation de la maturité organisationnelle de la sécurité de SI avec les méthodes CMM et ISM3.

**AUDIT PHYSIQUE**

- Observation physique des locaux contenant l'infrastructure technique (salles serveurs, Data Centers...);
- Evaluation de la sécurité environnementale;
- Gestion des accès physiques;
- Formulation des recommandations de sécurité physique;
- Évaluation de la maturité de sécurité physique.

**AUDIT TECHNIQUE**

- Audit de l'architecture du système d'information (reconnaissance, sondage...);
- Audit de l'infrastructure matérielle ( tests intrusifs de vulnérabilité,...) ;
- Audit de l'infrastructure logicielle (web et non web);
- Audit des bases de données;
- Évaluation de la maturité de sécurité technique.

**EVALUATION DE LA MATURETE DE LA SECURITE DU SI**

**NIVEAUX DE SECURITE DU SI SUIVANT LES TROIS AXES D'INTERVENTION**

Désignation de l'Axe	Maturité réelle	Maturité requise	Maturité parfaite
SECURITE ORGANISATIONNELLE	x%	60%	100%
SECURITE PHYSIQUE	y%	60%	100%
SECURITE TECHNIQUE	z%	60%	100%



EVALUATION DE LA MATURITE DE LA SECURITE DU SI



SYNTHESE DE L'ANALYSE DES RISQUES

$$Risque = (Potentialité * Impact) \quad R=P*I$$

Impact

4	2	3	4	4
3	2	3	3	4
2	1	2	2	3
1	1	1	1	2
	1	2	3	4
	Potentialité			

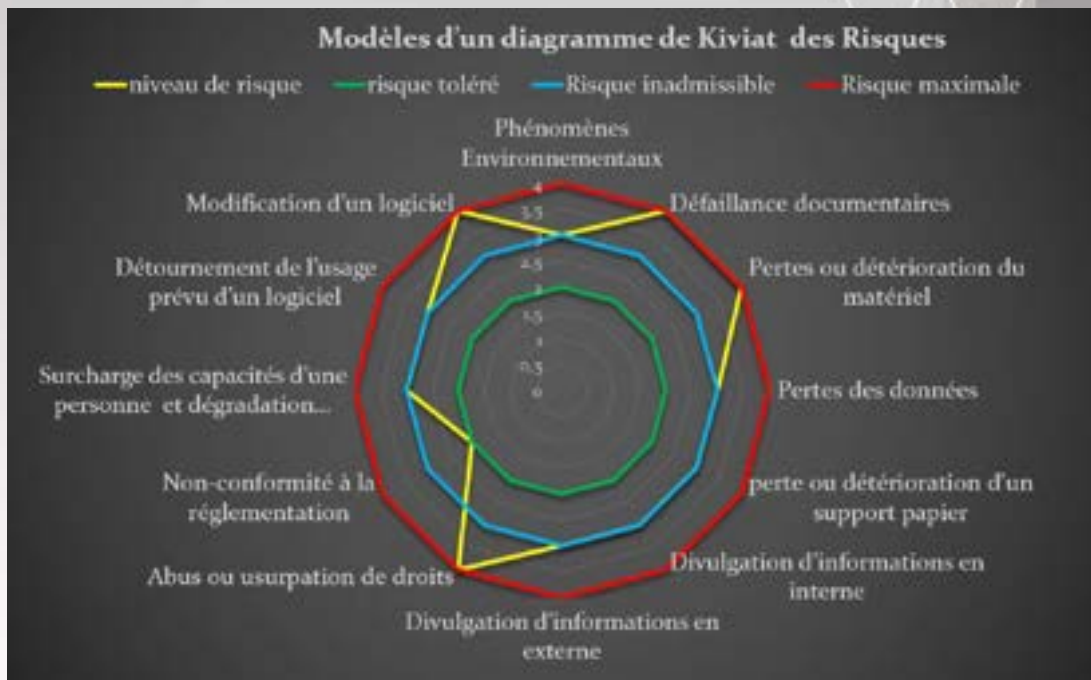
Intervalle de gravité	Gravité du risque
1	Risque toléré
2	Risque modéré
3	Risque inadmissible
4	Risque inacceptable

DESCRIPTION	NIVEAU D'IMPACT
Mineur	1
Modéré	2
Majeur	3
Catastrophique	4

DESCRIPTION	DURÉE	VALEUR
Très peu probable	1 fois tous les 10 ans et plus	1
Peu probable	1 à 2 fois tous les 10 ans	2
Probable	> 2 fois par an	3
Très probable	> 1 fois tous les trois mois	4



Synthèse DE L'ANALYSE DES RISQUES



STATISTIQUES DES AUDITS

Structures auditées	Ministères	ECM	EPA	Opérateurs et FAI	Total
<b>Total</b>	37	21	69	11	138
Types de structures	Niveau de maturité par axe			Maturité Moyenne	
	Organisationnel	Physique	Technique		
Ministères	28%	34%	28,93%	30%	
Services déconcentrés des Ministères	22,34%	25%	16,41%	21,25%	
Etablissements publics	34,78%	40,31%	34,26%	36,45%	
ECM	62,81%	69,83%	61%	64,55%	
Opérateurs et FAI	60,11%	66,66%	62,56%	63,11%	
Catégories de structures	Nombre de vulnérabilités par Axes			Total	
	Organisationnel	Physique	Technique		
Départements ministériels	2142	1245	5405	8792	
Etablissements publics	1726	769	4181	6676	
Opérateurs et FAI	373	181	1004	1558	
ECM	536	230	1176	1942	
<b>Total</b>	<b>4777</b>	<b>2425</b>	<b>11766</b>	<b>18968</b>	



**DIFFICULTES RENCONTREES**

- Refus de certaines structures à se soumettre à l'audit de sécurité ;
- Absence de mesures administratives et/ou réglementaires contraignantes relatives à la mise en œuvre obligatoire des recommandations issues des audits de sécurité ;
- Défaut de budgétisation des activités liées à la sécurité des systèmes d'information par certaines structures à auditer ;
- Absence d'un cadre administratif et/ou réglementaire contraignant les Administrations publiques à respecter les référentiels techniques élaborés par l'ANTIC ;
- Sanctions réglementaires relatives aux audits de sécurité pas assez contraignantes ;
- Non-respect des délais réglementaires de paiement des prestations d'audits réalisées par l'ANTIC.

**RECOMMANDATIONS**

- Modifier le cadre légal et réglementaire afin :
- d'astreindre certaines structures sensibles à l'audit de sécurité obligatoire et périodique de leurs systèmes d'information ;
- de renforcer les sanctions relatives aux audits de sécurité.
- Définir un cadre administratif et/ou réglementaire afin de rendre obligatoire la mise en œuvre des recommandations contenues dans les rapports d'audit de sécurité ;
- Rendre obligatoire pour les Organismes Publics, le respect des référentiels élaborés par l'ANTIC en matière de cybersécurité ;
- Mettre en place des mécanismes de budgétisation systématique de l'activité d'audit de sécurité.



# PANEL 2

## STRATÉGIES DE MISE EN ŒUVRE DE LA CYBERSÉCURITÉ AU CAMEROUN



**MODERATEUR**



**NDONGO Paul Petit**

Inspecteur Général des Services au MINPOSTEL

## PANEL 2

## STRATÉGIES DE MISE EN ŒUVRE DE LA CYBERSÉCURITÉ AU CAMEROUN

## Exposé 1

CYBERSÉCURITÉ DANS LE RÉSEAU DE  
TÉLÉCOMMUNICATIONS DE CAMTEL

Presenté par : **Armel MEBANDE,**  
**Expert Certifié Réseau & Cyber sécurité**

Armel MEBANDE, est ingénieur informatique et consultant senior international. Il est spécialisé dans la sécurité des réseaux et des TI. Il a plus de 10 ans d'expérience de haut niveau à travers le monde et de nombreuses certifications de niveau Expert. Il a démontré ses connaissances dans de nombreuses entreprises et administrations comme CAMTEL, la présidence de la République, le point d'échange Internet du Cameroun, etc. Armel est également consultant permanent pour CISCO Inc comme Security Expert Matter, et Fondateur-PDG d'AFRILANE

## PLAN DE L'EXPOSE

- I. Présentation;
- II. Etat des lieux Infrastructures;
- III. Evaluation des Risques;
- IV. Stratégie de Lutte ;
- V. Opérationnalisation de la stratégie;
- VI. Difficultés rencontrées;
- VII. Suggestions/Recommandations.



**I- PRESENTATION DE LA CAMEROON TELE-COMMUNICATIONS (CAMTEL)**

- Opérateur historique du CAMEROUN;
- Dispose d'une dorsale nationale à fibres optiques de plus de 12000 km;
- Exploite les Points d'atterrissement des câbles à fibres optiques Sous-marin;
- Infrastructures, Produits et Services;
- Téléphonie;
- Les solutions Internet;
- Liaisons spécialisées urbaines, interurbaines, internationales;
- Réseaux d'entreprise;
- Solutions Wi-Fi;

- Sécurité;

**II- ETAT DES LIEUX DES INFRASTRUCTURES**

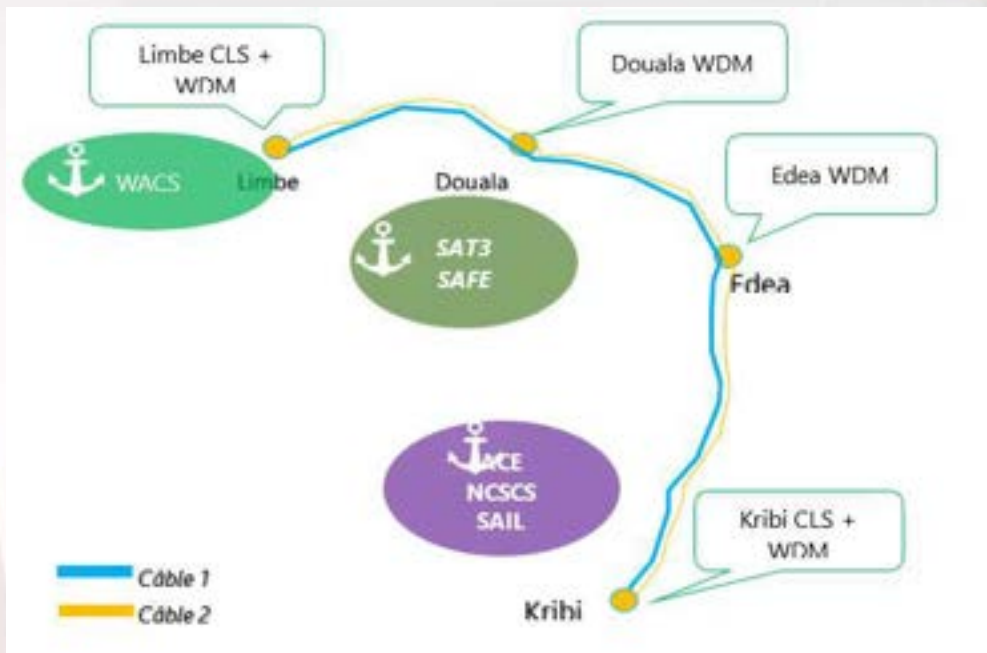
**CAMTEL : Le Socle de l'Economie Numérique**

**Transport : International**

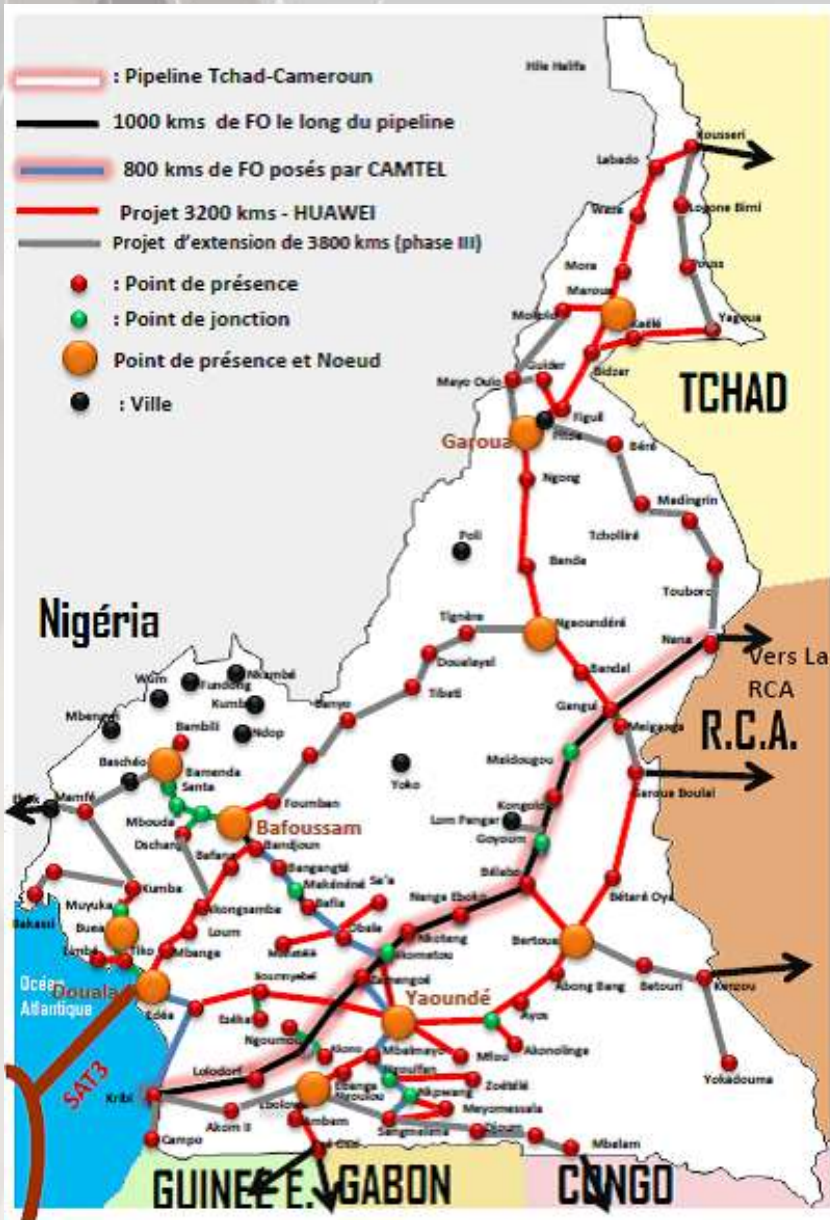
Quatre câbles sous-marins opérationnels. Capacité totale : 400 Gbps, dont 100 Gbps d'Internet

Infrastructure de CAMTEL comme moteur de l'économie numérique au CAMEROUN

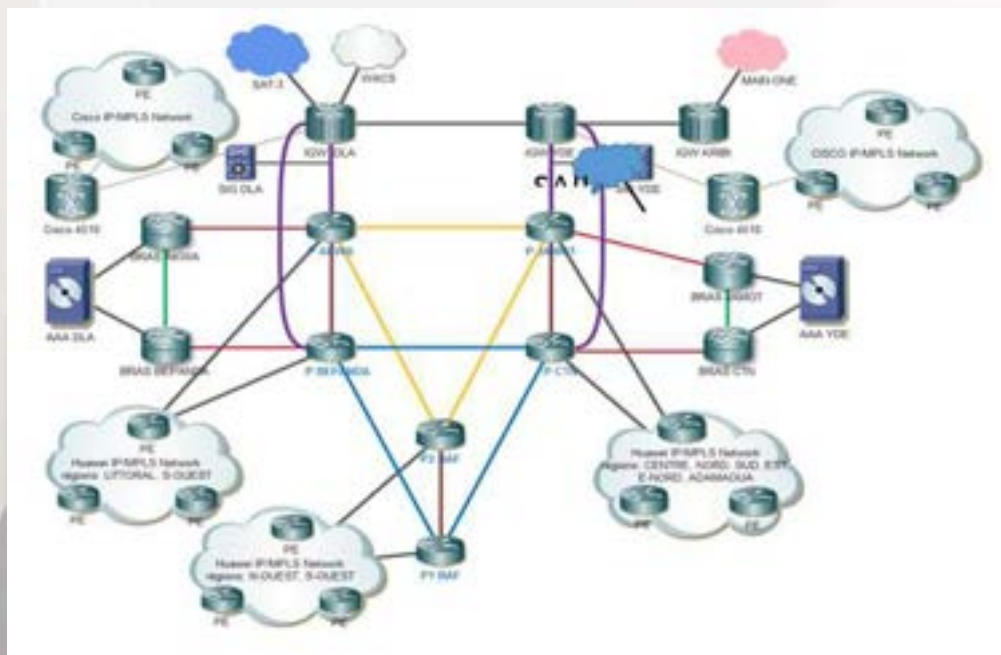
- Points d'atterrissement;



Transport : National  
Plus de 12 000 km de fibre optique activés

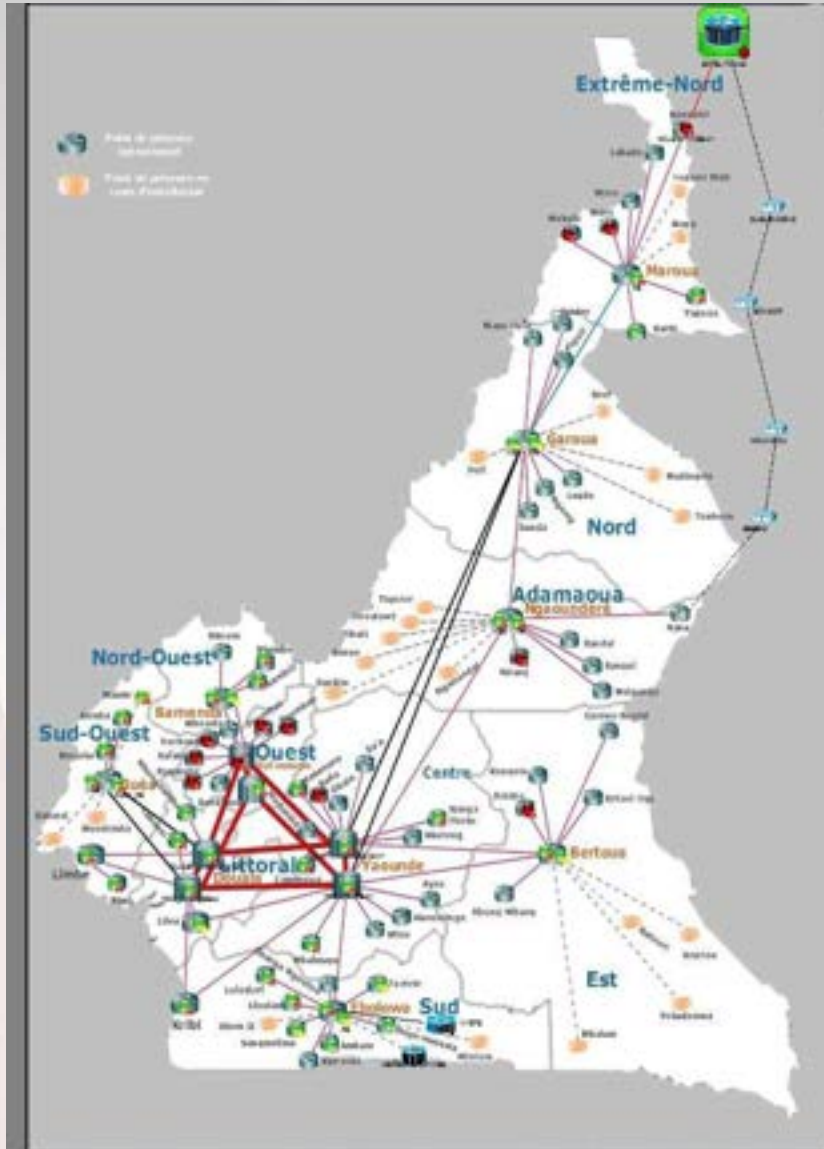


Backbone National Fibre optique : Plus de 12 000 Km activés

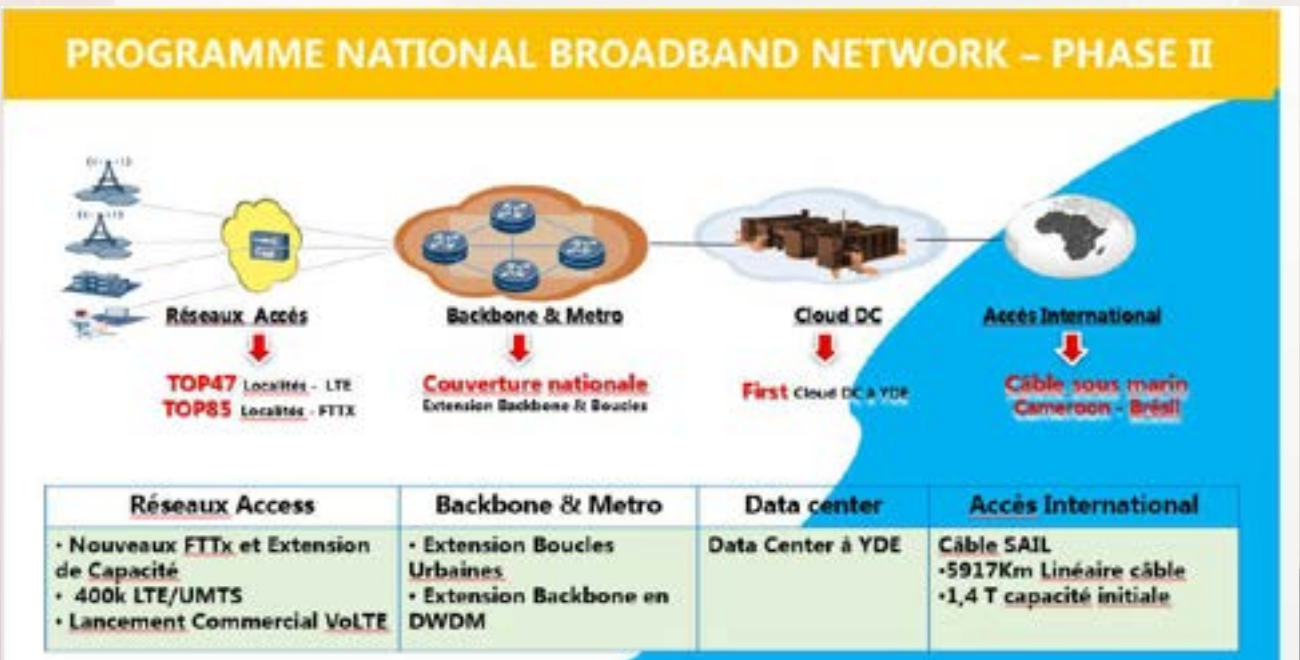


Dorsale nationale IP/ MPLS : Plus de 50 points de présence dans les dix régions



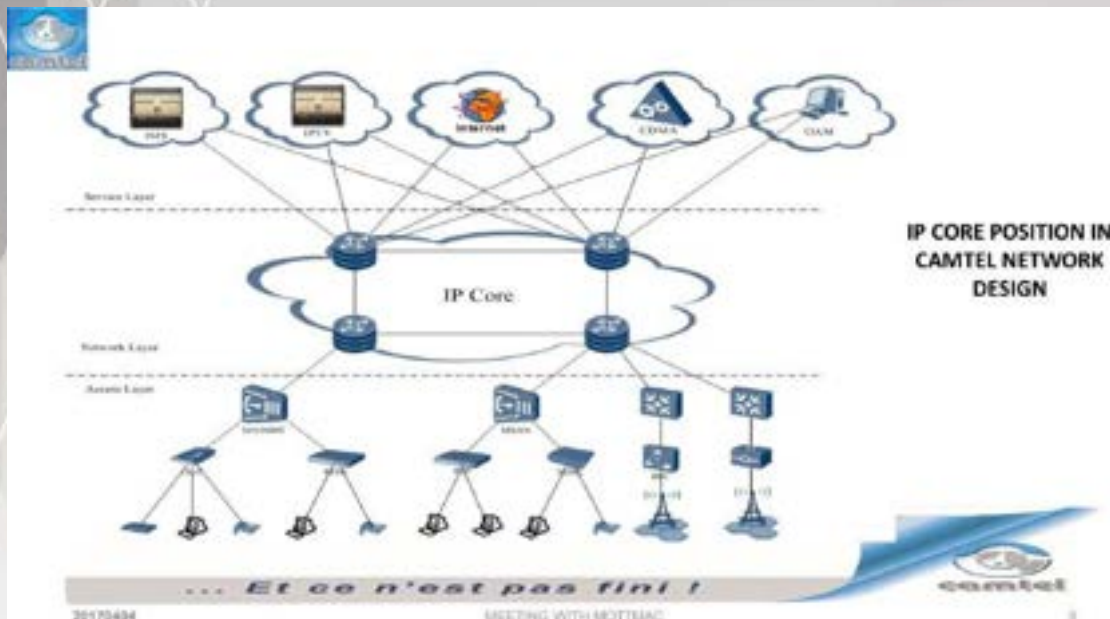


Infrastructure de CAMTEL comme moteur de l'économie numérique au CAMEROUN





UNE NOUVELLE VISION POUR LES SERVICES INNOVANTS



III- LES RISQUES

Mission statutaire de CAMTEL : Top 3 des Risques

- Indisponibilité de fourniture du service internet ;
- Deni d'accès aux infrastructures et nœuds réseaux;
- Visibilité et control du trafic entrant et sortant;
- Activité frauduleuse;
- Espionnage;
- Etc.

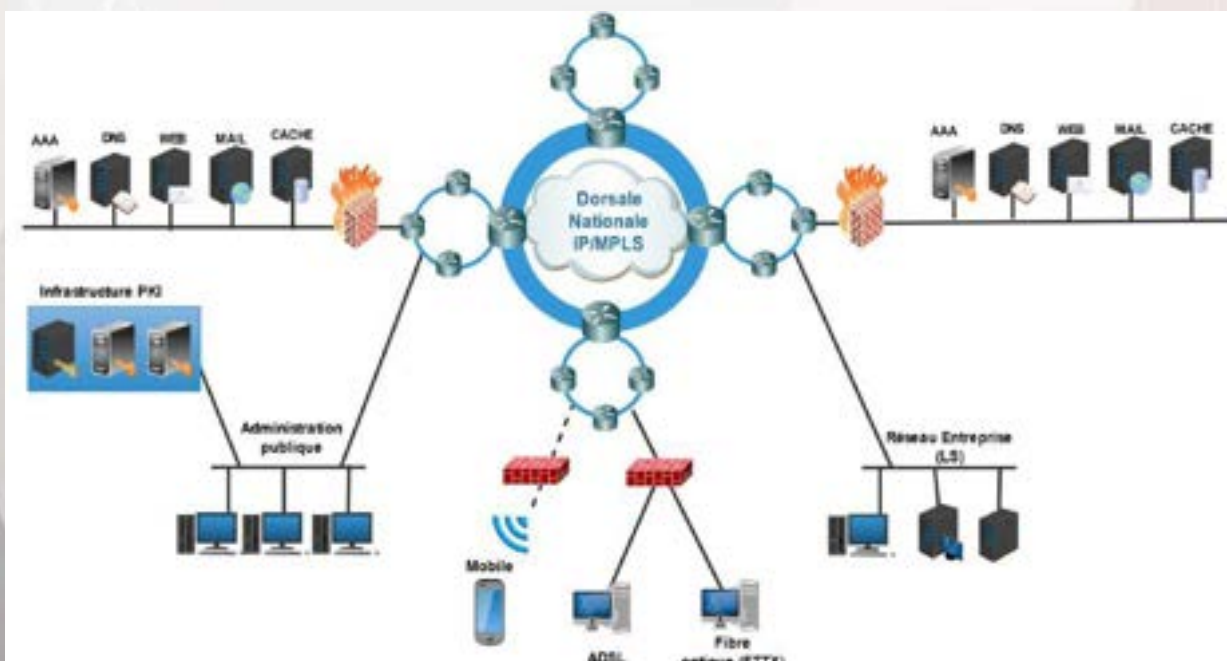
IV- STRATEGIE DE CAMTEL

- Souscription des liens Internationaux avec

Protection DDOS;

- Mise en place progressive d'une solution MSSP (Managed Security Service Provider);
- Mise en Place d'un Centre National de Supervision du Réseau;
- Etroite collaboration avec services et entreprises chargés des aspects de la sécurité
- Plusieurs projets en cours allant dans le sens du renforcement de la Sécurité;

V- OPERATIONNALISATION



## VI- DIFFICULTES

- LA CULTURE DE LA SÉCURITÉ VS NÉGLIGENCE;
- FINANCEMENT DES SOLUTIONS ;
- NORMES/INSTRUCTIONS/REFERENCES ;
- ACCOMPAGNEMENT DE L'ETAT POUR LA PRESERVATION DE LA SOUVERAINETE.

## SUGGESTIONS ET RECOMMANDATIONS

Le niveau de sécurité du cyberspace Camerounais est celui de l'acteur le plus faible:

Niveau 1 : Opérateurs

Niveau 2 : Entreprises et Administrations

Niveau 3 : Utilisateurs finaux

La Sécurité c'est donc une affaire de tous

## MESURES D'URGENCE

- Cyberspace une affaire de tous (MINATD-MINPOSTEL-CAMTEL-ANTIC-...);
- Politique Nationale de sécurité : Un Guide/Référentiel très important;
- Tous les acteurs du cyberspace doivent avoir un RSSI (Responsable de la Sécurité du Système d'Information) ;
- CIRT Locaux : Relai du CIRT National;
- Un comité permanent d'experts en support pour la gestion des situations critiques/complexes.

## MOYEN & LONG TERME

Mettre en place une coopération solide et gagnant - gagnant avec :

- GAFAM (Google-Apple-Facebook-Amazon-Microsoft)
- BATX (Baidu – Alibaba – Tencent – Xiaomi)

## PANEL 2

## STRATÉGIES DE MISE EN ŒUVRE DE LA CYBERSÉCURITÉ AU CAMEROUN

## Exposé 2

**LA CYBERSÉCURITÉ DANS LE RÉSEAU DE  
TÉLÉCOMMUNICATION DE NEXTTEL  
CAMEROUN**

Presenté par : **BAMA SI MFOUM Franck Arnold**  
NEXTTEL-Cameroun

Titulaire d'un diplôme d'Ingénieur des Télécommunications, il est Expert en Sécurité des Systèmes d'Information, il occupe le poste de Chef de la Division de la Sécurité des Systèmes d'Information à Nexttel.

**Plan**

01

**Définition de la cybersécurité**

02

**Architecture du réseau et points critiques**

03

**Mesures de sécurité**

04

**Protection des abonnés**

05

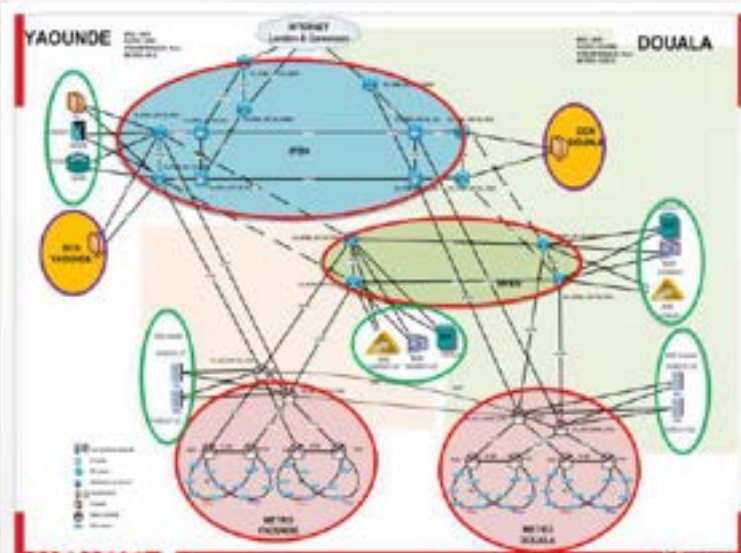
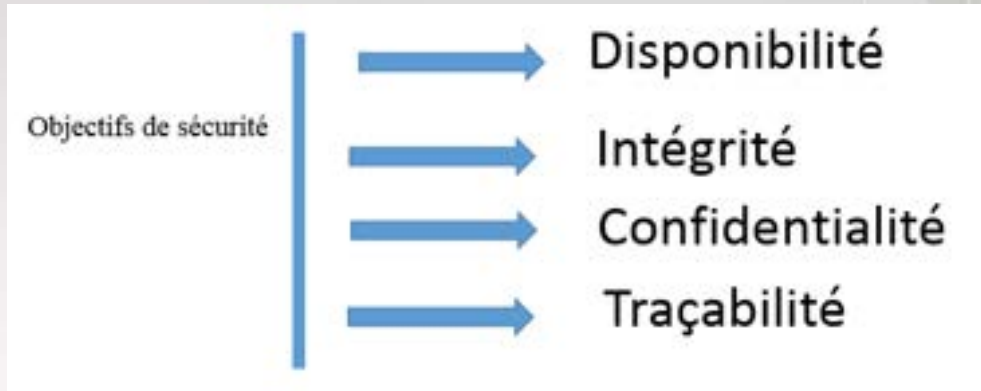
**Lutte contre la fraude**



Exposé 2 : LA CYBERSÉCURITÉ DANS LE RÉSEAU DE TÉLÉCOMMUNICATION DE NEXTTEL CAMEROUN

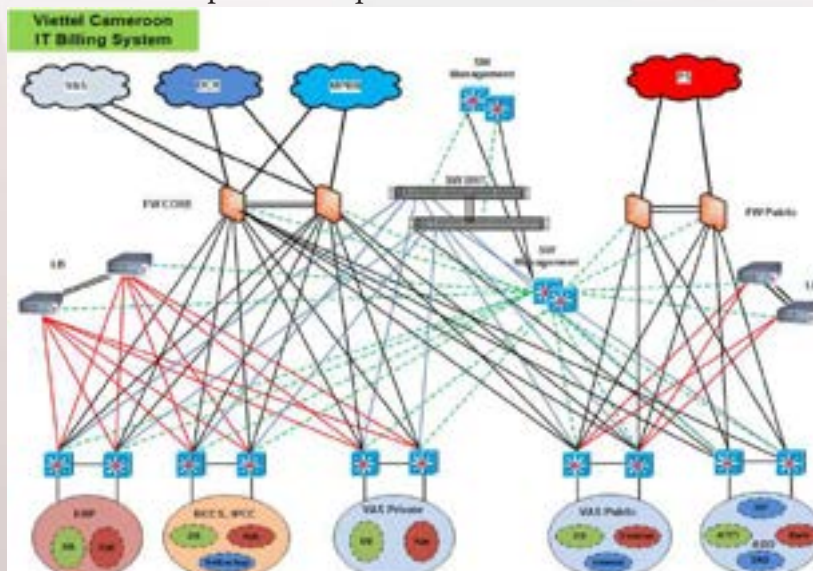
1. Définition de la cybersécurité

« Ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes. » (source loi sur la cybercriminalité)



Architecture hiérarchique du réseau de transport  
 Nœuds de collecte  
 Nœuds d'agrégation  
 Cœur du réseau des services  
 Services de base  
 Services à valeur ajoutée

2. Architecture du réseau et points critiques





Les menaces

### Hameçonnage & ingénierie sociale

L'hameçonnage (« phishing ») qui vise à abuser de la « naïveté » des clients ou des employés pour récupérer leurs identifiants (code PIN, identifiants de connexion à une BD, ...)

- Réception d'un mail flatteur;
- Demande pour effectuer une opération comme la mise-à-jour des données personnelles ou la confirmation du mot de passe;
- Connexion à un faux-site identique à celui de l'entreprise et contrôlé par l'attaquant;
- Récupération par l'attaquant des identifiants/mots de passe (ou tout autre donnée sensible) saisie par le client sur le faux site.

L'« ingénierie sociale » constitue une « attaque ciblée » qui vise à abuser de la « naïveté » des employés de l'entreprise :

pour dérober directement des informations confidentielle, ou pour introduire des logiciels malveillants dans le système d'information de l'entreprise



Par téléphone



par réseaux sociaux



par e-mail

### Virus informatique

Les virus informatiques constituent des « attaques massives » qui tendent à devenir de plus en plus ciblées sur un secteur d'activité (télécommunication, banque, défense, énergie, etc.) et de plus en plus sophistiquées et furtives.

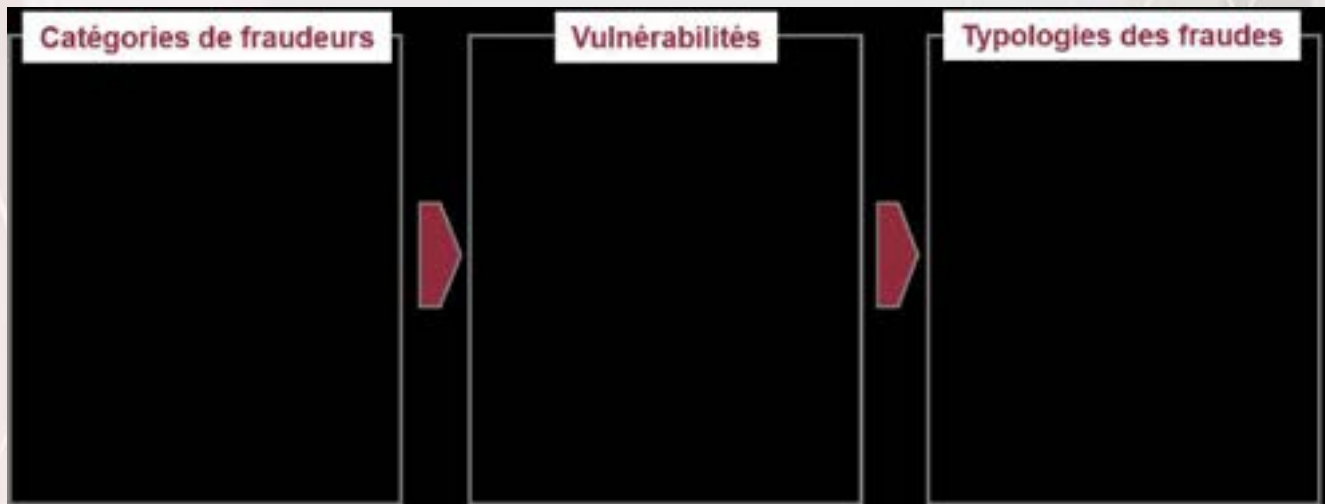
Les principaux vecteurs d'infection :

- Message avec pièce-jointe;
- Support amovible (clé USB...);
- Site Web malveillant ou piraté;
- Partages réseaux ouverts, systèmes vulnérables etc.;

Avec comme conséquences potentielles:

- Installation d'un « cheval de Troie » pour accéder au poste de travail à distance d'un administrateur;
- Récupération de données ciblées : identifiants/mots de passe...;
- Surveillance à distance des activités : capture des écrans, des échanges, ...;
- Destruction des données;
- Chiffrement des données pour une demande de rançon.

**Fraude interne**

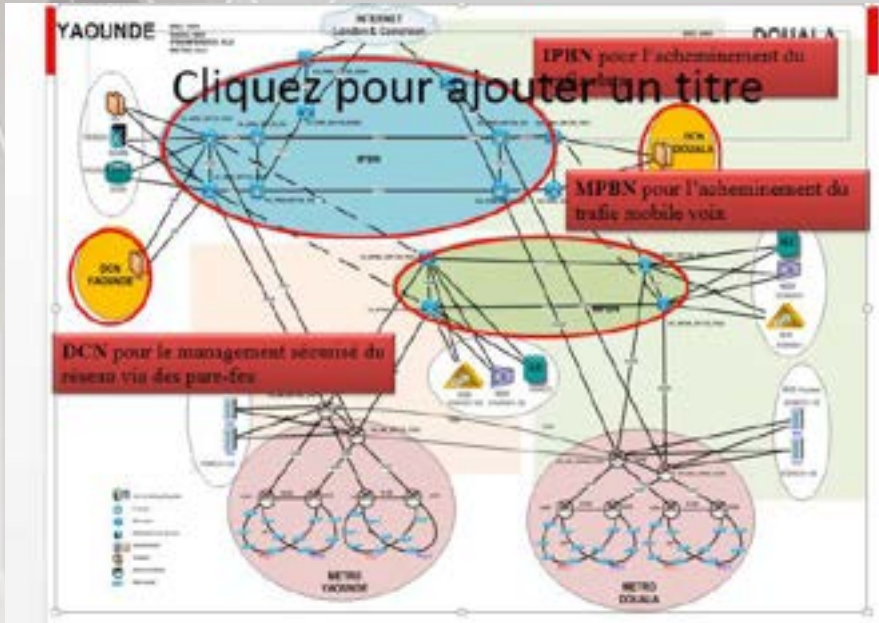


## Indisponibilité de service

Due....

Rupture de lien  
Équipement, carte, ... défectueux  
Erreur humaine

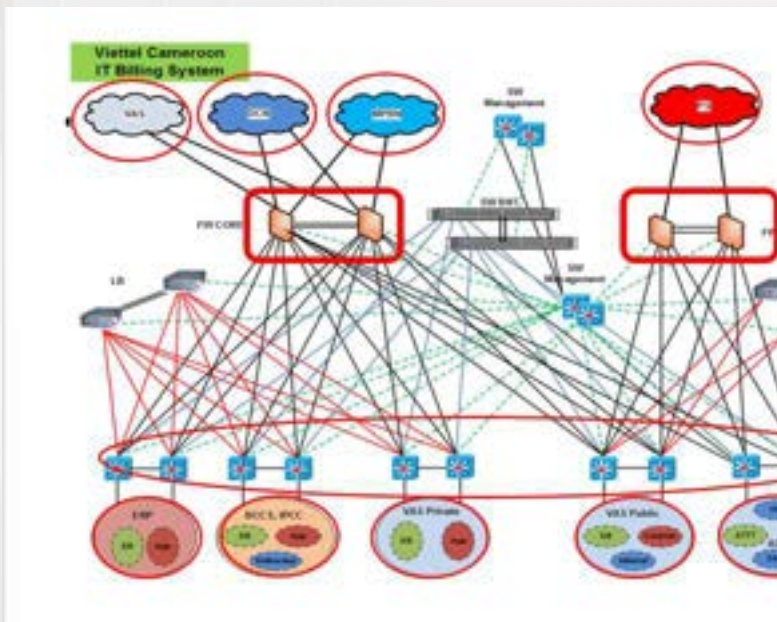




**Dans l'architecture du réseau**

- Redondances à plusieurs niveaux;
- Des boucles
- Redondances de liens
- Redondance de nœuds
- Redondances de cartes de traitement des données
- Partage de charge
- Cloisonnement du réseau;
- Durcissement des réseaux;
- Environnement de fonctionnement des équipements du réseau.

**3. mesures de sécurité**



**Dans la gestion du réseau**

- Contrôles d'accès et gestion des identités;
- La maintenance préventive;
- Les audits journaliers, mensuels et annuels;
- Stratégies et plans de sauvegarde des données etc...

**Dans l'organisation**

- Une division sécurité des systèmes d'information
- Politiques de sécurité
- Charte d'utilisation des moyens informatiques
- Cartographie + Plan de gestion des risques
- Plan de Continuité d'Activités + gestion des incidents
- Formation et sensibilisation du personnel aux bonnes pratiques (cyber hygiène)
- Etc

**4. protection des abonnés**

- Identification des abonnés
- Chiffrement des données des abonnés (profiles, transactions)
- Limitation et contrôle d'accès aux données des abonnés
- Contrôle de la puissance d'émission

## 5. lutte contre la fraude

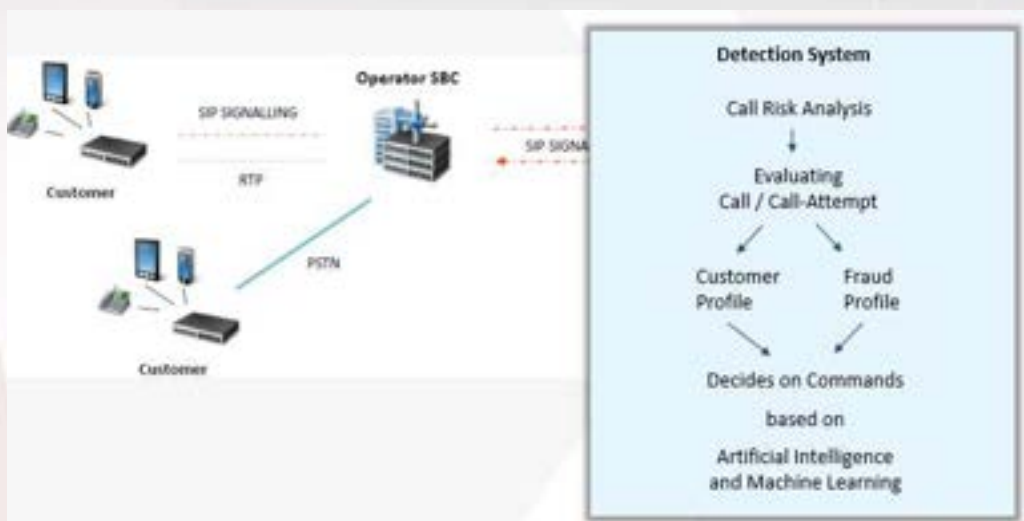
### Fraude interne

Renforcement des procédures permettant la traçabilité de toutes les actions entreprises

### Fraude dans les échanges de trafic.

- Communication: partage fréquent d'informations sur les anomalies et examens à intervalles réguliers;
- Définition de seuils déclenchant une enquête;
- Examen des accords d'interconnexion.

### Détection -> Prévention des Fraudes (en cours)



### Difficultés et perspectives

- Adhésion de tous les employés dans l'implémentation des procédures de sécurité;
- Intégration de la culture de la cyber hygiène au quotidien par le personnel de l'entreprise.

### Conclusion

Nexttel a compris les enjeux de la cybersécurité dans l'accomplissement de ses missions et alors entrepris de minimiser le risque cyber par des solutions techniques d'une part, mais aussi des solutions organisationnelles et procédurales d'autre part.

Toutefois, beaucoup reste à faire, notamment dans la sensibilisation et la formation des employés et des clients en ce qui concerne les bonnes pratiques cybernétiques afin de réduire les cybermalveillances.

## PANEL 2

### STRATÉGIES DE MISE EN ŒUVRE DE LA CYBERSÉCURITÉ AU CAMEROUN

## Exposé 3

# CYBERSÉCURITÉ À ORANGE



Presenté par : **Pascal Oum**

Senior Manager en charge de la Sécurité à Orange Cameroun

#### La cybersécurité à Orange

- De la Technologie: systèmes, solutions et outils de **sécurité**.
- Des Processus : politiques de sécurité, lignes directrices.
- Des Hommes et des Femmes: organisations, expertises, formation, sensibilisation,

Tous destinés à **protéger les actifs et le système d'information** de l'Organisation

Disponibilité - Intégrité - Confidentialité - Traçabilité - Non répudiation





### La cybersécurité à Orange: pourquoi ?

#### L'économie numérique : une bataille planétaire

"L'économie numérique ne peut exister que grâce à des réseaux performants et sécurisés: il est essentiel de protéger les systèmes critiques et les données de nos clients et collaborateurs"

Stéphane Richard, PDG d'Orange, FIC-2016

<https://www.youtube.com/watch?v=bMy3HM-Oe0s>



### Les Menaces liées aux métiers Telco



## Quelques impacts sur les Telco



## La cybersécurité chez Orange: Retour d'expérience?



## PANEL 2

## STRATÉGIES DE MISE EN ŒUVRE DE LA CYBERSÉCURITÉ AU CAMEROUN

## Exposé 4

**CYBERSECURITE DANS  
LES RESEAUX BANCAIRES**

Presenté par : **EKOLLO Françoise**  
RSSI / BC-PME



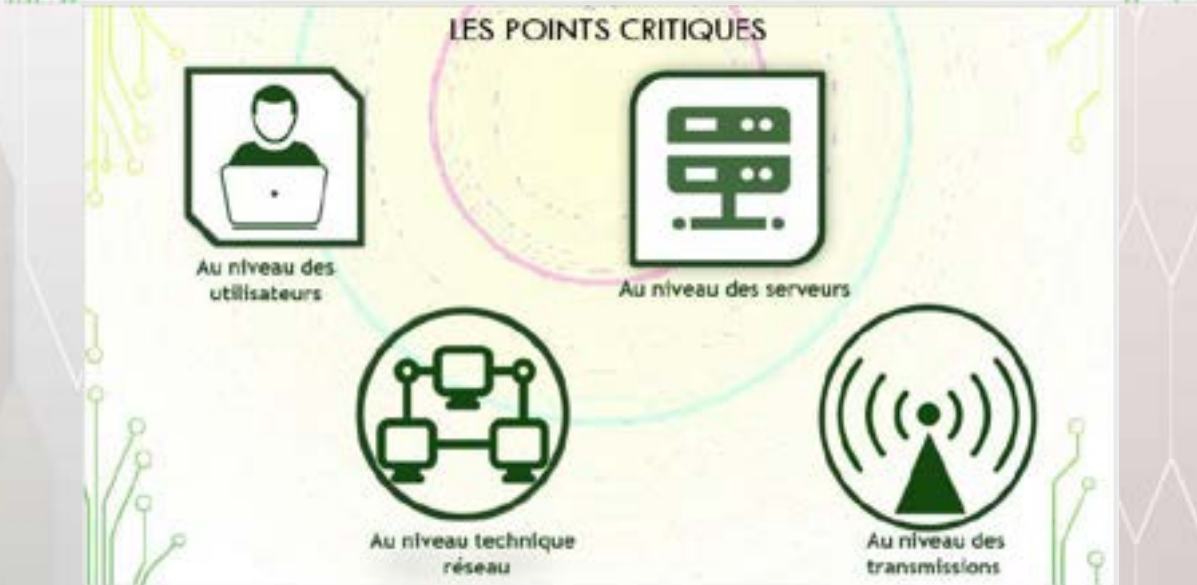
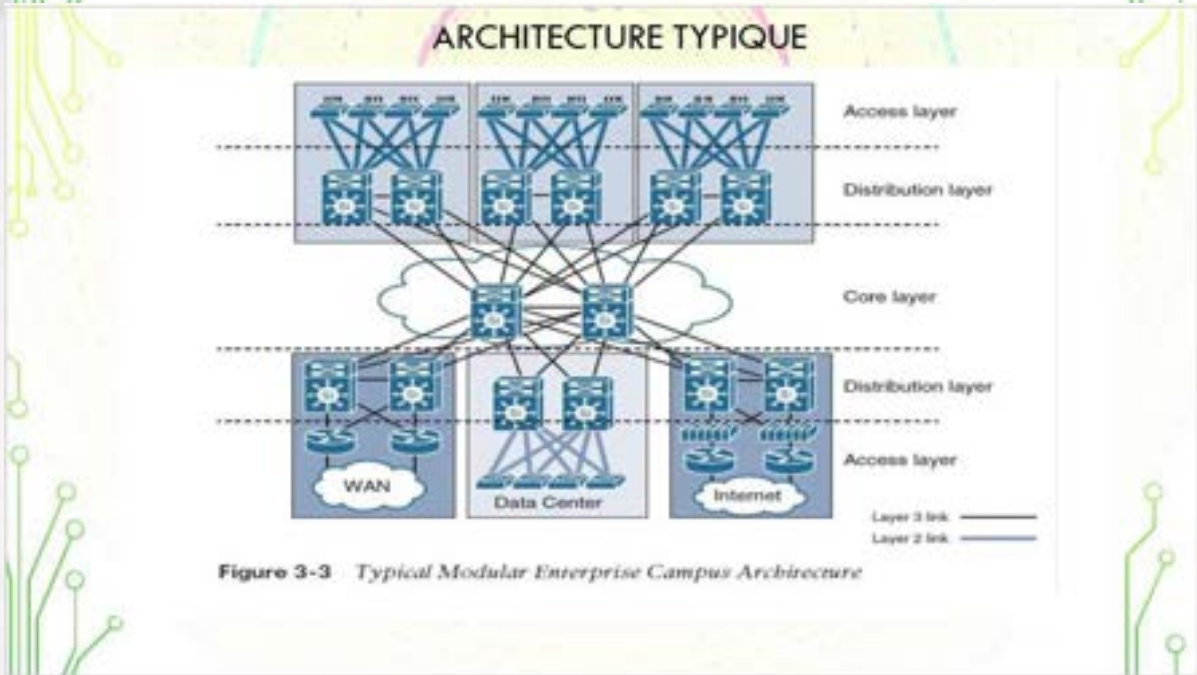
Responsable de la sécurité des systèmes d'information à la Banque des PME depuis sa création en 2015, elle bénéficie d'une longue et riche expérience dans la gestion de projet et la mise en œuvre de solutions financières (comptabilité générale, clients et fournisseurs et intégration avec modules logistiques (achat, vente, production, maintenance, ...)).

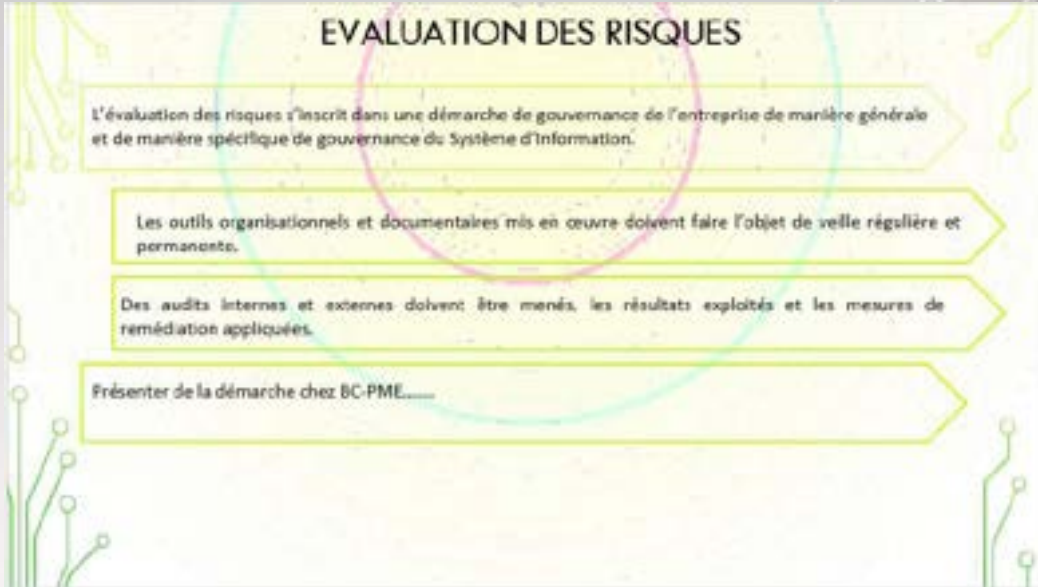
Dans les systèmes d'information, notamment en France où elle a occupé le poste de consultant, Expert Fonctionnel, Business analyste et Chef de projet durant 16 années. Pendant 2 années chez SYNTEGRA - Filiale de British télécom une SSII à la défense, ensuite pendant 14 années, chez ALSTOM à la Défense en région Parisienne, avant de mettre son expérience à la disposition de son pays d'origine.

Depuis 2014, elle exerce au sein de la BC PME où elle a participé au projet de création de ladite banque pour la mise en œuvre du système d'information bancaire. Depuis la création de la banque en 2015, elle occupe la fonction de RSSI, où elle met en œuvre le système de management de la sécurité de l'information ; Mme Ekollo Françoise est détentrice d'une certification PECB ISO 27001 LEAD IMPLEMENTER obtenu en 09 /2018.











## GRANDES VULNÉRABILITÉS

1

- Les postes de travail qui ont des ports de service ouvert (la pile smb) qui est exploité pour lancer des attaques DOS, DDOS et même ransomware,
- L'absence des mises à jour et correctifs de système d'exploitation

2

- Les applications web banking publiées directement derrière les Firewall sans la présence des Reverse Proxy dont le rôle est principalement de lutter contre les attaques et menaces avancées sur les services HTTP et HTTPS

## LUTTE CONTRE LES VULNÉRABILITÉS

1

La fermeture des ports de service non utilisés

2

La gestion centralisée des mises à jour et patches du système d'exploitation

3

L'installation de système de contrôle de l'accès des utilisateurs

4

Le renforcement de la sécurité des serveurs de messagerie par le déploiement des protocoles SPF, DKIM et DMARC

## CAS DES CYBERCRIMES





### PRINCIPALES ATTAQUES : QUELQUES CHIFFRES (ANTIC, MONDE ET ENIX)

- ➔ 3 388 cas d'usurpation d'identité sur les réseaux sociaux ont été recensés depuis la fin d'année 2018, et 2 595 ont été supprimés. 31 pages/comptes ont été certifiés par l'ANTIC ;
- ➔ Plus de 2 050 plaintes reçues depuis 2018 au niveau du CIRT, relatives au cas de scamming, phishing etc ;
- ➔ Près de 5 milliards de pertes dues au scamming
- ➔ Près de 6 milliards de pertes relatives aux fraudes bancaires ;
- ➔ Plus de 20 cas de SIM SWAP signalés et ayant ciblés les hauts cadres.

### PRINCIPALES ATTAQUES

**L'attaques des cartes de crédits et des distributeurs**


- Le clonage des cartes de crédit (Avec accès physique et Clonage des cartes magnétiques à distance)
- Attaques des distributeurs avec les logiciels malveillants (Profilés des cybercriminels ; en général des employés internes, Ex : ATMick, Alica, etc)


**Hacking des applications et plateformes financières en ligne**


**Crimes liés aux données**


- Collecte des informations sensibles à travers les solutions mal sécurisées
- Collecte des informations à travers des logiciels non testés
- Revente illégale des informations des clients (Se souvenir du cas Cambridge Analytica)

### CAS D'UN FLASHAGE DE COMPTE BANCAIRE

  
**Hackers**  
(Généralisme au Bénin, Côte d'Ivoire)

  
**Banque en ligne**

  
**BANK**  
Banque où est stocké le compte de la victime

  
**Complice au sein de la banque**  
(Fourni les données clients et se charge des retraits)

Les pertes sont généralement énorme mais difficile à être connu au sein de la banque



### PRINCIPALES ATTAQUES VERS LES CLIENTS

- 1 • **Le scamming:** Forme d'ingénierie sociale très répandue sur le continent Africain. Généralement le cybercriminelle envoi un email ou un SMS afin d'abuser la confiance du client et obtenir de l'argent.
- 2 • **Le phishing :** attaque découlant du social engineering

**Moyens de lutte:** L'installation des solutions de lutte antispam, de protection de DNS et l'éducation et la sensibilisation des utilisateurs sur les types et contenus de courriels reçus. Et surtout la dénonciation des cas





## PANEL 2

### STRATÉGIES DE MISE EN ŒUVRE DE LA CYBERSÉCURITÉ AU CAMEROUN

## Exposé 5

# STRATEGIES ET MESURES DE REGULATION SUR L'IDENTIFICATION DES ABONNES DES OPERATEURS DES TELECOMMUNICATIONS

Presenté par : **MENGANG BEKONO**

**Directeur Technique de l'ART**



- Ingénieur des Télécommunications
- Titulaire d'un diplôme d'Ingénieur Industriel en Electronique de Institut Supérieur Industriel Catholique du Hainaut à Charleroi (Belgique) et d'un diplôme d'Ingénieur Principal des Travaux des Télécommunications de l'ENSPT de Yaoundé ;

Parcours professionnel, il est tour à tour :

- 1999-2002 Cadre à la Division de la Coopération Internationale au MINPOSTEL
- 2002-2006 Chef Section Technique ART/Douala ;
- 2006-2010 Chef Centre de Contrôle des Fréquences ART/Douala ;
- 2010-2013 Chef Service des Infrastructures des Télécommunications ART/ Yaoundé;
- 2013-2015 Délégué Régional de l'ART pour le Centre, le Sud et l'Est;
- Depuis 2015, Directeur Technique à l'Agence de Régulation des Télécommunications (Yaoundé).

### L'IDENTIFICATION?



C'est le fait de collecter les informations inscrites sur un document officiel d'identification d'un abonné lors de la souscription d'un abonnement auprès d'un opérateur

### SES OBJECTIFS

Produire des statistiques des abonnements au téléphone,  
permettre le traitement des réquisitions judiciaires,  
assurer l'identification de l'appelant des services d'urgence



## SES ORIGINES

Afin de faire face à la recrudescence des infractions commises au moyen du téléphone (vols, menaces, arnaques, chantages, injures, dénonciations calomnieuses, escroqueries, diffamations, attentas, actes terroristes, cybercriminalité, entre autres), les pouvoirs publics ont mis en place une réglementation visant à protéger les citoyens contre les abus des personnes inciviques et mal intentionnées.

## LA REGLEMENTATION

- Loi 2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun
- Décret du 03 septembre 2015 sur l'identification des abonnés et équipements terminaux dont la mise en œuvre devrait aboutir à :
  - l'identification systématique de tous les abonnés,
  - l'élimination de la commercialisation des cartes SIM pré-activées et leur vente dans la rue,
  - la limitation du nombre de puces pouvant être détenues par une personne physique,
  - la mise en place d'une base de données commune qui fédère les bases de données d'identification des opérateurs.

## LA MISE EN OEUVRE

- Des contrôles sont régulièrement effectués sur le terrain et dans les bases de données des opérateurs. Les statistiques les plus récentes pour l'ensemble des bases de données des opérateurs sont les suivantes:
    - Total de numéros dans les bases de données d'identification = 21 952 639;
    - Total des numéros non conformes et suspendus = 73 021;
    - Total des numéros actifs = 21 879 618;
    - Total des numéros actifs conformes = 21 878 835;
    - Total des numéros actifs non conformes = 783;
    - Soit un taux de conformité global = 99,99%.
- Pour les numéros actifs non conformes, les opérateurs ont été mis en demeure de procéder à la mise en conformité ou à la suspension

## LA PROBLEMATIQUE DE LA FIABILITE DES DONNEES CAPTUREES LORS DE L'IDENTIFICATION

Elle se caractérise par l'usurpation d'identité, la présentation des fausses pièces d'identité lors de l'identification, l'utilisation abusive des pièces d'identité retrouvées dans les rues etc.

Ces pratiques rendent complexe le rapprochement de la puce avec son utilisateur final, lequel n'est plus l'abonné préalablement identifié.

Les Perspectives face à la problématique de la fiabilité des données d'identification

Afin d'apporter des réponses à ces problématiques, il est prévu de mettre en place une plateforme numérique centralisée pour l'identification des abonnés et des équipements terminaux des communications électroniques comprenant l'accès distant et la base de données centralisée qui interagira avec les bases de données de la DGSN et la Gendarmerie

Les perspectives face à la problématique de la fiabilité des données d'identification

Pour la mise en place de cette solution, l'une des premières actions consistera à faire un état des lieux, un diagnostic de la situation actuelle et un apurement synchronisé des bases des données actuelles par leur fiabilisation.

L'état des lieux amènera notamment à procéder à un audit des systèmes d'identification des opérateurs (chaîne d'identification, bases des données d'identification, etc.),

Dans un second temps, il sera question d'authentification des données d'identification préalablement à l'activation des cartes SIM c'est-à-dire que les opérateurs vont continuer à identifier leurs abonnés. Les informations seront par la suite transmises à la base des données centralisée pour validation avant activation des cartes SIM.

## PANEL 2

## STRATÉGIES DE MISE EN ŒUVRE DE LA CYBERSÉCURITÉ AU CAMEROUN

## Exposé 6

**BLOCKCHAIN & CRYPTOMONNAIES: INTRODUCTION, APPLICATIONS DIRECTES ET IMPACT SOCIO-ECONOMIQUE AU CAMEROUN**

Présenté par : **MOUDZE TATSUM**  
Operations Manager  
| Blockchain Association of Cameroon

- Directeur des Opérations chez NGUETI IT SOLUTIONS, Logistiques et Planning
- Président et fondateur | NAMSOFIT
- Responsable communautaire Hyperledger-Cameroun
- Responsable du chapitre GBA | GBA Douala
- Membre de l'Association de la blockchain du Cameroun

**Agenda**

- Introduction;
- Définition & Importance de la Blockchain et des Cryptomonnaies;
- Applications & Usages de la Blockchain;
- Impact & Adoption de la Blockchain;
- Perspectives.

Introduction

Définition & Importance de la Blockchain et des Cryptomonnaies

**Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Avant la Blockchain | Bitcoin

Cryptocurrencies -		Exchanges -		Watchlist		USD ▾	Next 100 →	View All
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)	
1	Bitcoin	\$57,240,324,615	\$3,284.90	\$3,068,308,235	17,425,300 BTC	0.65%		---
2	XRP	\$11,937,982,309	\$0.291600	\$327,967,774	40,926,963,305 XRP *	0.56%		---
3	Ethereum	\$9,008,416,228	\$86.77	\$1,545,269,905	103,824,420 ETH	2.11%		---
4	Stellar	\$1,878,486,774	\$0.098070	\$93,969,738	19,154,492,208 XLM *	-0.00%		---
5	Tether	\$1,863,965,220	\$1.00	\$2,379,631,320	1,856,421,736 USDT *	0.25%		---
6	EOS	\$1,753,764,954	\$1.94	\$565,291,944	906,245,116 EOS *	4.53%		---
7	Litecoin	\$1,533,368,121	\$25.73	\$352,362,708	59,580,363 LTC	7.00%		---



EXPOSÉ 6 : BLOCKCHAIN & CRYPTOMONNAIES: INTRODUCTION, APPLICATIONS DIRECTES ET IMPACT SOCIO-ECONOMIQUE AU CAMEROUN

Ecosystème Bitcoin Map



The Blockchain Ecosystem Map V3,0



Ecosystème Blockchain Map

- Applications
- Associations
- Echanges
- Services Financiers
- Infrastructure
- Investissements
- Mining
- Information & Data
- Paiements
- Services
- Portefeuilles

Blockchain: C'est quoi Exactement ?



La blockchain est une base de données distribuée sécurisée avec des processus business partagés par tous les membres d'un réseau Blockchain.

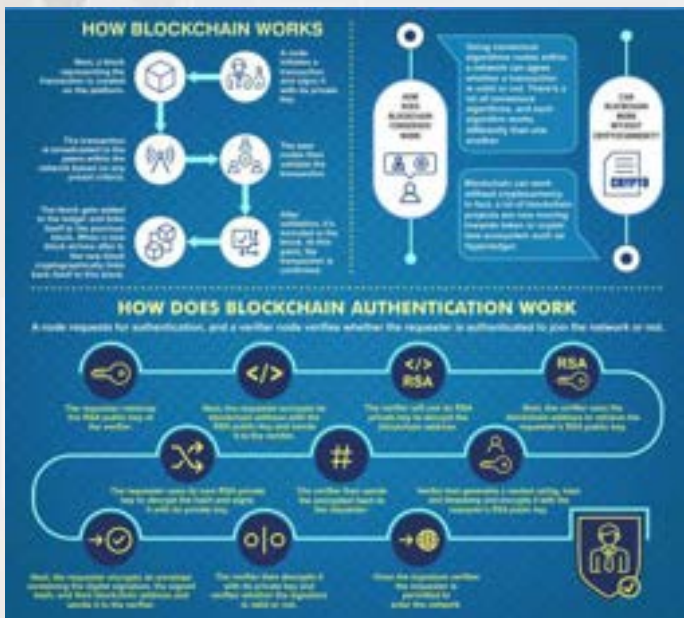
- Transfert d'actifs & Création de valeurs;
- Immutabilité;
- Transparence;
- Système Distribué;
- Consensus;
- Transaction Peer-to-Peer (P2P).



**En Résumé:**

Monnaie numérique utilisant des techniques de cryptage, utilisées pour régler la production d'unités monétaires et vérifier le transfert de fonds et fonctionnant indépendamment d'une banque centrale, qui nécessite l'utilisation d'un programme informatique pour visualiser, envoyer ou recevoir de l'argent. Le programme informatique utilise la cryptographie pour créer et vérifier les transactions. L'état de la propriété de la monnaie est déterminé par un certain consensus des ordinateurs qui partagent les informations sur les transactions et suivent le même code.

**Blockchain & Bitcoin | Fonctionnement**



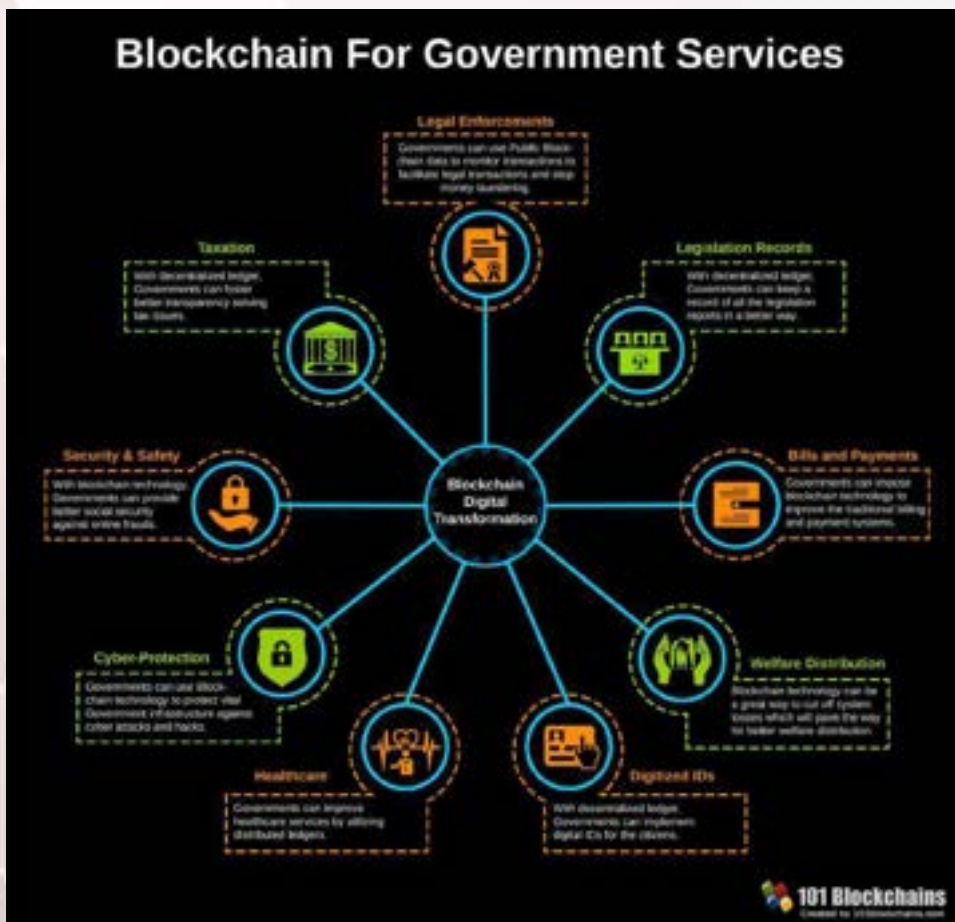
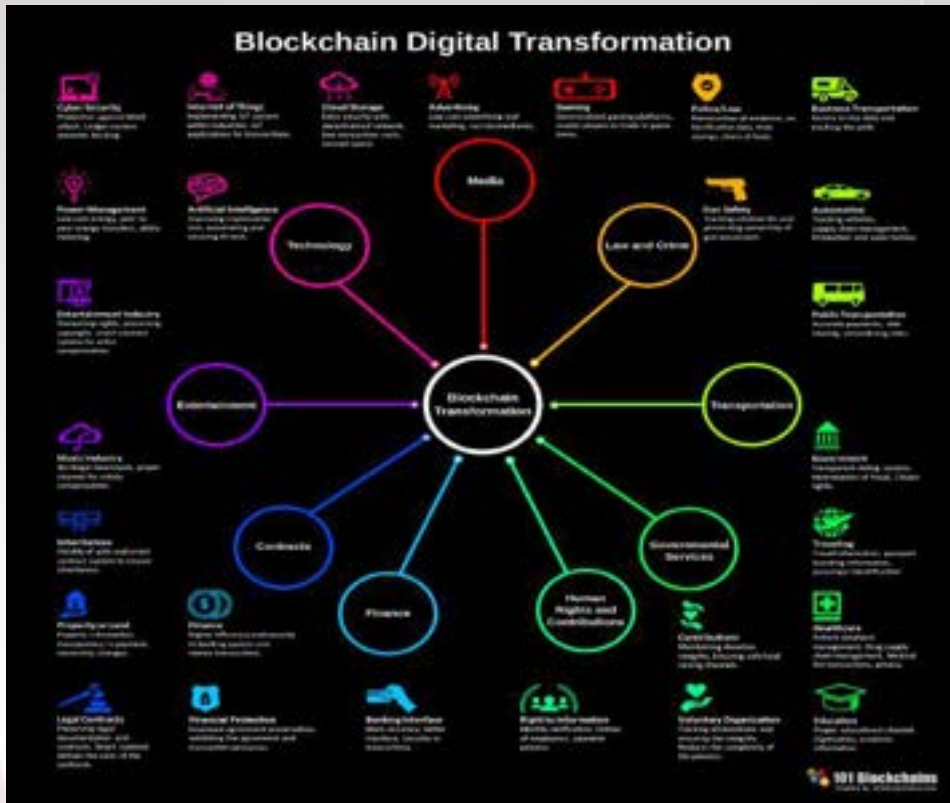
**Blockchain & Cryptomonnaies | Importance**

- La Blockchain & les cryptomonnaies inversent la concentration du pouvoir;
- Les gouvernements utilisent des institutions centralisées pour surveiller, influencer et contrôler:
  - Les Institutions Financières;
  - Les Compagnies d'Assurance;
  - Les mouvements de valeurs entre pairs érodent la visibilité, l'influence et le contrôle du gouvernement.
- Les gouvernements remplissent des fonctions vitales pour maintenir l'ordre dans les sociétés;
- Les cryptomonnaies utilisent des modèles non gouvernementaux pour maintenir l'ordre;
- Bitcoin possède plusieurs milliards de transactions sans banque centrale, ni régulateur gouvernemental, ni auditeur, ni tiers;
- De nouveaux modèles, algorithmes et technologies consensuels pourraient remplir des fonctions gouvernementales à l'avenir.



EXPOSÉ 6 : BLOCKCHAIN & CRYPTOMONNAIES: INTRODUCTION, APPLICATIONS DIRECTES ET IMPACT SOCIO-ECONOMIQUE AU CAMEROUN

Applications & Usage de la Blockchain Blockchain | Domaines d'Activités





## Exemples de Blockchain Pour la Santé

**Hashed Health**

Services Blockchain de conseil en matière de soins de santé

Quel problème ce service permet-il de résoudre ?

Hashed Health s'efforce d'utiliser des systèmes basés sur la Blockchain pour améliorer l'efficacité des transactions de soins de santé.

- Hashed Health se concentre sur le développement des technologies de chaînes de blocs et de registres distribués dans le secteur des soins de santé.
- Hashed Health fournit une variété de services liés à la Blockchain, tels que le conseil, le développement communautaire, la gestion des produits et le support technique.
- Hashed Health travaille avec les prestataires de soins de santé pour créer et gérer des solutions Blockchain pour une variété de problèmes auxquels l'industrie est confrontée

**Health Nexus**

Plate-forme de gestion des données médicales basée sur la Blockchain

Quel problème ce service permet-il de résoudre ?

Une solution blockchain pour la sécurisation des données des patients .

- Health Nexus et ConnectingCare sont des produits développés par SimplyVital Health. Ils espèrent réunir les prestataires de différentes organisations médicales sur une même plateforme, où ils pourront consulter les mêmes données pour des patients communs;
- Des algorithmes financiers et cliniques basés sur l'intelligence artificielle fourniront des informations exploitables à toutes les parties;
- La plateforme alimentée par blockchain, permet aux utilisateurs de suivre les patients ainsi que de réduire le coût des soins.

EXPOSÉ 6 : BLOCKCHAIN & CRYPTOMONNAIES: INTRODUCTION, APPLICATIONS DIRECTES ET IMPACT SOCIO-ECONOMIQUE AU CAMEROUN

Autres Cas



- Vérification de l'authenticité des médicaments retournés;
- Prévention de la contrefaçon de médicaments et de dispositifs médicaux;
- Conformité dans la chaîne d'approvisionnement pharmaceutique;
- Transparence et traçabilité du consentement dans les essais cliniques;
- Améliorer la qualité et la fiabilité des données sur les essais cliniques et beaucoup d'autres...

Impact & Adoption de la Blockchain  
Blockchain | Statistique Globale



Blockchain | Mosaïque d'utilisation



Blockchain | Cadre Réglementaire



Préoccupations

- Lutte contre le blanchiment d'argent;
- Connaître son client (KYC) et Connaître son entreprise (KYB);
- Protection des consommateurs;
- Perception et paiement des impôts.

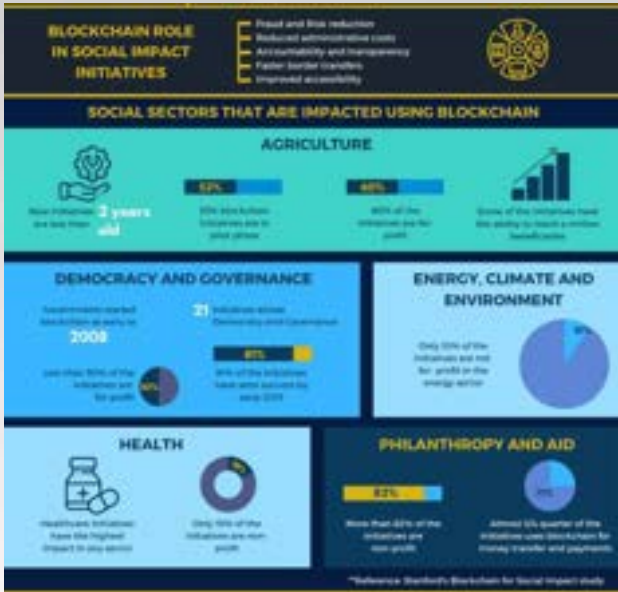
Opportunités

- Développement économique;
- Réduction des frictions;
- Gains d'efficacité;
- Coûts.

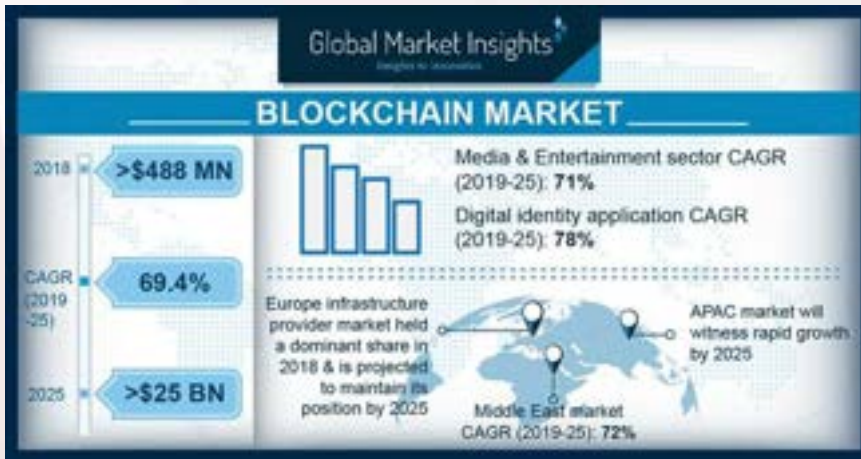
Blockchain | Mosaïque d'utilisation



EXPOSÉ 6 : BLOCKCHAIN & CRYPTOMONNAIES: INTRODUCTION, APPLICATIONS DIRECTES ET IMPACT SOCIO-ECONOMIQUE AU CAMEROUN



Blockchain | Perspective D'évolution



## PANEL 2

### STRATÉGIES DE MISE EN ŒUVRE DE LA CYBERSÉCURITÉ AU CAMEROUN

## Exposé n° 7

# STRATEGIES ET MESURES DE CYBERDEFENSE

Presenté par : **le Colonel NDONGO MVE Désiré,**  
**Chef de la Division des Transmissions**  
**de l'Electronique et de l'Informatique au MINDEF**



Titulaire d'un Master II en Stratégie, Défense et Gestion des catastrophes et breveté du Cours Supérieur Interarmées de Défense.

Officier des forces de défense issu de la 27ème promotion de l'Ecole Militaire Interarmes. Affecté dans l'Arme des Transmissions, il a effectué l'intégralité de sa formation dans la technique et dans l'emploi de cette Arme dans les écoles françaises et israéliennes.

#### Sur le plan professionnel

Il a été successivement instructeur au Centre d'Instruction des Transmissions des Forces de défense, Commandant dudit Centre, Chef du service Technique à la Division des Transmissions, de l'électronique et de l'informatique, Commandant du Bataillon des Transmissions, et enfin Chef de la Division des Transmissions, de l'électronique et de l'Informatique du Ministère de la Défense.

Il a géré les Systèmes d'Information et de la Communication dans les Missions de maintien de la paix au Soudan et en République Centrafricaine.

Dans le cadre de la coopération multilatérale avec les organisations régionales, sous régionales et les armées étrangères, il a participé à plusieurs opérations et initiatives dans le domaine des Systèmes d'Information et de la communication, en partenariat avec l'Union Africaine, la CEEAC, la CEMAC, et les armées française et américaine.

#### PREAMBULE.

L'importance sans cesse grandissante du cyberespace le place au cœur des enjeux sociaux, moraux, politiques, sécuritaires et le confirme dans sa dimension de nouveau domaine de la pensée stratégique. Si le cyberespace est un multiplicateur de force, il est aussi un multiplicateur de vulnérabilité, et cela vaut aussi pour les forces de défense qui se trouvent désormais exposées à des cyberopérations.

A cet effet, la défense des intérêts fondamentaux du Cameroun commande que soit rapidement entreprise la coordination de l'action d'un grand nombre d'acteurs publics et privés afin de passer d'une posture de protection passive à une véritable opérationnalisation de la stratégie nationale de cyberdéfense.

#### PLAN DE L'EXPOSÉ

##### I. GENERALITES.

##### II. APPROCHE EXOGENE DE L'IMPACT DES ACTIVITES DANS LE CYBERESPACE SUR LES FDC.

##### III. APPROCHE ENDOGENE DE L'IMPACT DES ACTIVITES DANS LE CYBERESPACE SUR LES FDC.

##### IV. STRATEGIES ET POSTURES DE CYBERDEFENSE

##### V. PERSPECTIVES ENVISAGEABLES DANS LE DOMAINE DE LA CYBERDEFENSE.



**I – GENERALITÉS.**

**1- Clarification des concepts**

**Le cyberspace :** Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

**Cyberattaque :** Acte malveillant de piratage informatique dans le cyberspace.

**Cybercriminalité :** Ensemble des infractions s'effectuant à travers le cyberspace par des moyens autres que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique.

**Cyberdéfense :**

• Ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberspace pour garantir l'effectivité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère.

• Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberspace les systèmes d'information jugés essentiels.

**2- Topologie des Cybermenaces.**

- Les acteurs;
- Les modes d'action;
  - Le deni de service;
  - Hameçonnage;
  - Ransomware;
- Les finalités
  - Cybercriminalité;
  - Espionnage;
  - Sabotage;
  - Atteinte à la démocratie; ou recherche de déstabilisation



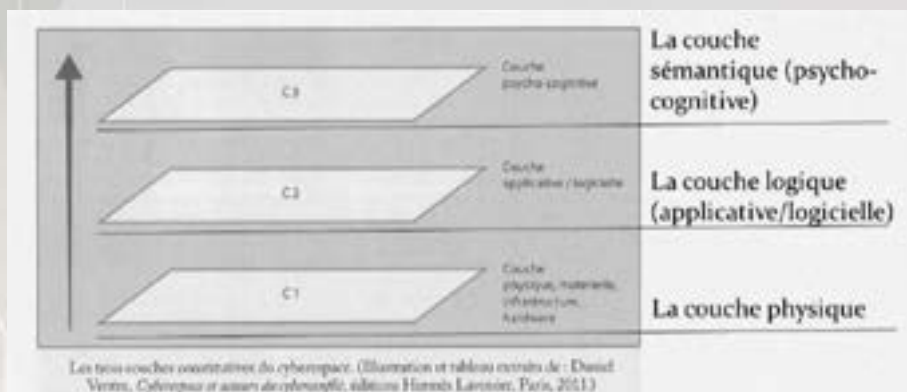
**3- Caractéristiques du cyberspace.**

- Intangibilité, perception de la donnée difficile ;
- Instantanéité, tout va très vite ;
- Furtivité, difficile pour les schéma militaires classiques ;
- Opacité, difficile traçabilité, usurpation d'identité ;
- Ubiquité, substitution des acteurs, attaques de multiples provenances ;
- Létalité indirecte, utilisation fréquente de l'action cyber en combinaison avec une offensive militaire classique.



La schématisation du cyberspace s'appuie sur trois couches :

- La couche physique (les câbles, les infrastructures, ...)
- La couche logicielle (hacking, moteurs de recherche, ...)
- La couche psycho-cognitive (defacing, propagande, les réseaux sociaux, ...), c'est la couche la plus intangible, la plus difficile à géolocaliser ;



		Caractéristiques	Forme d'attaques possibles contre la couche
C3	Couche haute	Couche cognitive fichiers, sites, adresses et codes de connexion, e-mails, pseudonymes, adresses IP, pages sur les réseaux sociaux, blogs, numéros de téléphone, avatars	Modifier l'affichage des ordinateurs, défigurer des sites, introduire des messages modifiant les perceptions, mener des opérations de propagande, hacking cognitif
C2	Couche médiane	Couche applicative : les données, logiciels, algorithmes, applications, couche des bits, du code, des normes, des protocoles, langages logiciels	Attaques par le code : hacking, diffusion de virus...
C1	Couche basse	Couche physique, matérielle, hardware, câbles, réseaux, satellites, ordinateurs, matériels communiquant, infrastructures connectées	Couper des câbles sous-marins, détruire des satellites, détourner des satellites de leur trajectoire, bombarder des bâtiments accueillant des serveurs, bombarder des infrastructures de communication, utilisation de bombes impulsions électromagnétiques...

#### 4- Les enjeux dans le cyberspace

- Enjeux économiques
  - espionnage industriel et économique,
  - le vol de propriété intellectuelle et de secrets industriels.
- Enjeux socio-culturels
  - les langues,
  - les dogmes, soft power, islamisme, ...
  - les cultures.

- Enjeux stratégiques
  - La territorialisation des données ;
  - Le contrôle des algorithmes de routage ;
  - La production de contenus.
- Enjeux militaires  
L'enjeu militaire principal concerne le renseignement cyber qui prend une place de plus en plus importante dans les outils de défense

II - APPROCHE EXOGENE DE L'INFLUENCE DU CYBERESPACE SUR LES FDS

1- Approche exogène de l'impact du cyberspace sur les FDS.

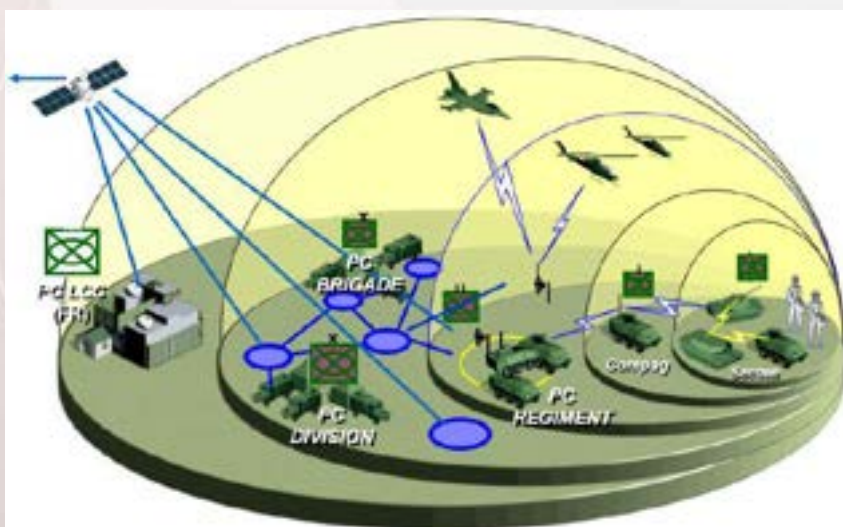
- Le cyberspace a pénétré la société de telle manière que tous les conflits ont désormais une dimension cyber.
- Les belligérants utilisent le cyberspace pour se renseigner, informer, désinformer, influencer, communiquer, organiser l'action.

Cette omniprésence de la dimension cybernétique se manifeste depuis plus de deux décennies dans les conflits qui se déroulent dans le monde.

2- Approche exogène de l'impact du cyberspace sur les FDS.

Année	Cyber-attaquants	Cyber-victimes	Motifs	Description
2007	Israël	Syrie	Raid aérien de F-15 Israéliens contre un radar syrien	Cyberattaque brouillant et mettant hors service les radars syriens (interruption des signaux électromagnétiques)
2008	Russie	Géorgie	Guerre russo-géorgienne	Vagues d'attaque informatiques mettant à terre les infrastructures géorgiennes
2010	USA & Israël (soupçons)	Iran	Contre le programme de développement du nucléaire iranien	Vers Stuxnet ayant détruit des centrifugeuses nucléaires en Iran
2013	Chine (soupçons)	USA	Espionnage	Plans d'armes américaines dérobés (F35-F18-missiles Patriot, Radar Aegis)
2016	Russie	Ukraine	Territoire Est-ukrainien	Malware « BlackEnergy » aurait infecté 03 fournisseurs d'électricité

3- Approche exogène de l'impact du cyberspace sur les FDS.



Les systèmes d'armes sont informatisés et potentiellement vulnérables à des cyberattaques.



## 4- Approche exogène de l'impact du cyberspace sur les FDS.



## 5- Approche exogène de l'impact du cyberspace sur les FDS.



Au Cameroun, l'utilisation du cyberspace à des fins de troubles à l'ordre public et de déstabilisation a atteint des niveaux inégalés

## 6- Approche exogène de l'impact du cyberspace sur les FDS.



Certains acteurs infra étatiques qui contestent l'autorité de l'état cherchent à agir dans les champs psychologiques des populations cibles en utilisant les réseaux sociaux à des fins de distorsion de la réalité.

A cet effet, des nouvelles fausses sont propagées avec la célérité reconnue aux réseaux sociaux finissent par influencer l'opinion publique, et plus grave, écorner l'image du Cameroun.

**Cette guerre du sens activement entretenue par certains groupes et leaders d'opinion vise à donner une légitimité à leur action**



### 7- Approche exogène de l'impact du cyberspace sur les FDS.



L'action pernicieuse des réseaux sociaux à cette occasion a favorisé la survenance d'importants troubles à l'ordre public dans la ville de Douala, et à une perception très négative à l'extérieur de l'administration et des services de santé du Cameroun.

**Affaire Monique KOUMATEKE à Douala le 28 mars 2016**

### 8- Approche exogène de l'impact du cyberspace sur les FDS.



Les réseaux sociaux à cette occasion ont grandement facilité la diffusion d'informations visant à traumatiser les populations en focalisant sur l'incapacité des forces de l'ordre et de leurs partenaires institutionnels à gérer une situation de catastrophe de grande ampleur.

**Catastrophe ferroviaire survenue à Eseka le 21 octobre 2016**

### 9- Approche exogène de l'impact du cyberspace sur les FDS.



Les réseaux sociaux à cette occasion ont également facilité la diffusion d'images insoutenables visant à choquer les populations et mettre en exergue les difficultés des forces de l'ordre et de leurs partenaires institutionnels à assurer la sécurité des établissements scolaires dans les zones en crise.

**Assassinat des élèves dans une école à Kumba le 24 /10/2020**

### 10- Approche exogène de l'impact du cyberspace sur les FDS.

#### Le cyberspace plateforme de recrutement des groupes terroristes



L'utilisation du cyberspace est en forte croissance au Cameroun. A mesure que se développe l'accessibilité aux ordinateurs et aux smartphones, il en est de même pour la propagande terroriste.

**Les efforts des pouvoirs publics pour la réduction de la fracture numérique sont exploités au Cameroun par les organisations terroristes pour leur expansion.**

**11- Approche exogène de l'impact du cyberspace sur les FDS.****Le cyberspace plateforme de recrutement des groupes terroristes**

Le cyberspace facilite la communication et le recrutement des groupes terroristes en laissant souvent proliférer sur leurs plateformes, des contenus faisant l'apologie du terrorisme.

**La réglementation qui s'adapte à la nouvelle donne n'est pas toujours appliquée avec la célérité à laquelle on serait en droit de s'attendre.**

**12- Approche exogène de l'impact du cyberspace sur les FDS.****Le cyberspace, plateforme d'expression des activités criminelles**

Facebook semble particulièrement prisé par les organisations terroristes. Les affichages peuvent être disponibles au public de sorte que personne n'est tenu à s'inscrire à une page spécifique pour visionner l'information.

**Un affichage peut comporter un seul membre, et être regardé par des milliers d'utilisateurs.**

**13- Approche exogène de l'impact du cyberspace sur les FDS.****Le cyberspace, plateforme d'expression des activités criminelles**

Faisant référence à certains affichages sur Facebook, il a été établi que les mêmes informations qui y sont disponibles l'étaient également à peu près au même moment dans certains forums radicaux en langue arabe.

**Une certaine convergence semble établie entre les contenus radicaux disséminés sur Facebook et certains forums islamistes extrémistes.**

**14- Approche exogène de l'impact du cyberspace sur les FDS.****Le cyberspace plateforme de recrutement des groupes terroristes**

Des centaines de jeunes au chômage, et souvent diplômés se sont orientés vers des activités criminelles sur Internet, favorisant ainsi la naissance sur le territoire camerounais d'un Darkweb dont les effets se font ressentir chaque jour d'avantage.



**15- Approche exogène de l'impact du cyberspace sur les FDS.**

**Mise en œuvre des technologies de chiffrement sensées protéger les données**



Sur les terminaux de nouvelle génération, les réseaux sociaux implémentent des algorithmes complexes de chiffrement sensées protéger les données personnelles de leurs utilisateurs.

**L'absence des "Back doors" rend particulièrement difficile l'exploitation de ces terminaux dans le cadre des enquêtes de sécurité**

**16- Approche exogène de l'impact du cyberspace sur les FDS.**

**Le cyberspace plateforme de recrutement des groupes terroristes**



L'usurpation des identités des hauts responsables de l'administration publique et des forces de défense a connu un développement rapide avec l'avènement des réseaux sociaux

**III - APPROCHE ENDOGENE DE L'INFLUENCE DU CYBERESPACE SUR LES FDS.**



**La méconnaissance des capacités réelles des réseaux sociaux et l'inobservation des règles élémentaires de sécurité sont à la base des effets pernicious imputables aux personnels des forces de défense.**

**1- Approche endogène de l'impact du cyberspace sur les FDS.**



En général, l'utilisation des réseaux sociaux par les militaires s'effectue au détriment des règles élémentaires de sécurité. Par ces canaux de communication, ils peuvent partager des informations avec des milliers de personnes, et c'est précisément cette possibilité qui constitue un danger pour les forces de défense

**Si les RS donnent la possibilité de divulguer des informations sensibles, Ils permettent également de colporter des informations erronées, ce qui pourrait avoir des conséquences tout aussi ravageuses.**



### 15- Approche endogène de l'impact du cyberspace sur les FDS.



Par ignorance et dans le but de partager leur vécu quotidien avec leur proches, certains personnels des FD diffusent sur les réseaux sociaux, des contenus (textes, photos, vidéo) relatifs à leurs activités professionnelles et à celle de l'institution militaire.

**Ces actes constituent une menace pour la sécurité des personnels de la défense, des opérations et de leur succès dans la mesure où ils renseignent des personnes mal intentionnées.**

### 15- Approche endogène de l'impact du cyberspace sur les FDS.



Une photographie est une source importante de renseignements. On peut citer principalement:

- La localisation / orientation,
- La sécurité,
- L'agencement,
- Les matériels,
- Les modes opératoires.

**Toute diffusion de photographies ou de vidéos informant sur les spécificités des camps militaires (entrée/sortie, agencement) et les missions (cartes, matériels, programmation) est strictement interdite.**

### 15- Approche endogène de l'impact du cyberspace sur les FDS.



En opérations, les postures et attitudes répréhensibles ci-après sont régulièrement observées:

- Prise de photographies,
- Géolocalisation des smartphones non désactivée.

**La prise de vues durant les opérations relève des prérogatives de certains structures spécialisées des forces de défense.**

## IV – STRATEGIES ET POSTURES DE CYBERDEFENSE.



### 1- Le cyberspace comme théâtre des opérations.



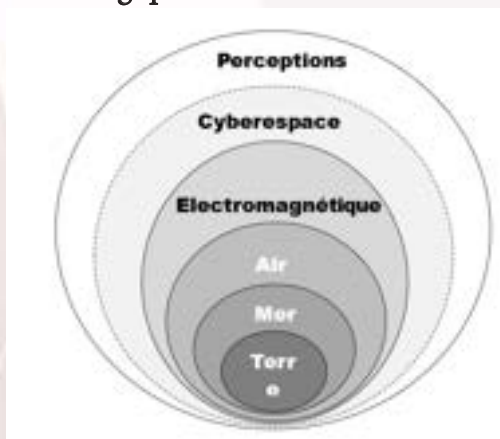
Quelle représentation stratégique peut – on se faire du cyberspace par rapport aux autres milieux stratégiques ?

### 2- Le continuum cybersécurité – cyberdéfense – cyberguerre.

L'approche cyberstratégique peut être précisée en distinguant les champs qu'elle recouvre:

- La cybersécurité traite de la sécurité intérieure et ressort d'une police générale. L'Etat en est responsable et utilise pour cela des organismes interministériels ou dépendant d'un ministère particulier.
  - 03 aspects: police, protection économique, sécurité technologique;
  - Protection des individus, des entreprises des organisations publiques.
- La cyberdéfense met en œuvre une politique de sécurité extérieure qui à une dimension interministérielle, et qui relève logiquement du Ministère de la défense. Lutte informatique offensive et défensive, protection des troupes et des services essentiels à la souveraineté de l'état, espionnage et contre espionnage. Prépare éventuellement une cyberguerre.
- La cyberguerre.

### 3- Les sphères stratégiques.



### 4- Le concept de base de la cyberdéfense.



Une opération de cyberdéfense, repose sur la coordination des différents moyens à disposition visant à comprendre une attaque informatique d'envergure en vue de l'entraver (la bloquer durablement). Elle se décompose en plusieurs phases.



## 5- Le mécanisme de la cyberdéfense.

### 1- La détection



Elle est parfois le fruit du hasard, mais plus généralement de la surveillance des systèmes avec des outils de supervision, ou d'une information fournie par un tiers ;

### 2- La qualification



Le but est de confirmer l'attaque et de la comprendre.

### 3- La remédiation



Elle vise à bloquer l'attaquant et à durcir la sécurité du système d'information pour l'empêcher de revenir.

## 6- Les initiatives sous le prisme d'une approche globale.

- Africa-CERT - 30 mai 2010 à Kigali au Rwanda, aider les pays africains à créer et à mettre en place des équipes de sécurité informatique et d'intervention en cas d'incident.
- Convention de Malabo – adoptée par l'UA en 2014 et visant la mise en place d'un cadre juridique pour la cybersécurité et la protection des données personnelles;
- Africa Cyber Defence Summit, ouverture de trois centres d'opérations de cyber-défense, au Nigéria, à l'Ile Maurice et au Sénégal, en plus de celui déjà ouvert en Afrique du Sud.



### 7- Option stratégique des FDC en matière de cyberdéfense.



<<les Forces Armées camerounaises, doivent également épouser leur temps, celui de la modernité, c'est-à-dire s'adapter aux changements aussi bien sur le plan technique et technologique que sur celui de la doctrine et de la stratégie >>.

**Le Président de la République le 31 mars 2000, à l'occasion du quarantième anniversaire des forces de défense à Ngaoundéré.**

### 8- Option stratégique des FDC en matière de cyberdéfense.



C'est dans ce contexte que le Chef d'Etat-Major des Armées a instruit les Etats-Majors Centraux de prendre en compte les exigences liées à la modernisation et à la professionnalisation des Armées.

**La finalité de l'entraînement militaire c'est le combat. Bien sélectionné, bien formé et bien équipé, le soldat doit pouvoir être projeté sur tous les théâtres en toute sécurité.**

### 9 - La cyberdéfense et les FDC.

Assurer ses missions régaliennes dans un contexte géostratégique en pleine mutation a conduit les FDC à repenser leur organisation.

Les armées ont intégré le changement important qu'a constitué l'émergence du cyberspace en allant au delà de la numérisation du champ de bataille et de la mise en réseau des forces.

### 10- La cyberdéfense et les FDC.

- DTEI (Division des Transmissions de l'Electronique et de l'Informatique) ;
- CRM (Centre de Renseignement Militaire) ;
- Les services spécialisés de la Gendarmerie Nationale (pleinement actifs dans le domaine de la lutte contre la cybercriminalité);
- Création d'unités/cellules en charge de la cyberdéfense dans certaines formations opérationnelles.

**Des projets de réforme sont en cours pour ériger un organe spécialisé, dédié à la cyberdéfense.**

### 11- La Stratégie de la cyberdéfense dans les FDC

- Instruction, entraînement et aguerrissement ;
- La coordination interministérielle;
- Coopération sous régionale;
- Coopération multilatérale.

**12- Postures recommandées aux personnels des FDC dans le cyberspace.**

- Initier les personnels aux pratiques de sécurité relatives aux réseaux sociaux;
- Faire prendre conscience aux personnels qu'ils constituent des cibles privilégiées pour des personnes ou des groupes;
- Rappeler le devoir de réserve pour tous les faits, documents ou informations dont ils ont connaissance dans l'exercice de leur fonction;
- Séparer les outils numériques et usages personnels et professionnels;
- Choisir, gérer et protéger les mots de passe.

**13- Postures recommandées aux personnels des FDC dans le cyberspace.**

- Stimuler l'entraînement et l'aguerrissement par l'acquisition des environnements de simulation informatique;
- Renforcer la résilience des systèmes d'armes;
- Systématiser l'analyse comportementale pour détecter les intrusions;
- Renforcer la coopération avec les autres acteurs de la sécurité cybernétique.

Les militaires se trouvent face à un environnement informationnel qui bouscule les us et coutumes ainsi que les frontières physiques et virtuelles.

**V - LES PERSPECTIVES ENVISAGEABLES DANS LE DOMAINE DE LA CYBERDEFENSE.****1- Identification des insuffisances et des faiblesses.**

- Pas assez de coordination entre les organes en charge de la sécurité informatique ;
- Moyens financiers et humains insuffisants;
- Sensibilisation et maturité insuffisantes des utilisateurs et des dirigeants face à la menace dont ils ne perçoivent pas les risques.

**2- Identification des insuffisances et des faiblesses**

Mener à leur terme les réflexions juridiques sur la cyberconflictualité ;

- Structures d'hébergement insuffisantes ou à relocaliser;
- Risque de «cyber-colonialisme»
- Institutionnalisation des « FAKE NEWS ».

**3- Perspectives en matière de cybersécurité**

- ORGANISATION, parachever la mise en place d'une structure cyber au sein du Ministère de la Défense ;
- FORMATION, poursuivre le renforcement en capacités au travers de divers partenariats;
- FAVORISER UNE COLLABORATION ACCRUE, entre les différents services participant à la préservation de la souveraineté numérique du Cameroun, mais aussi au niveau sous régional et régional;
- INFRASTRUCTURES, de communication et Datacenter à travers le pays ;
- SURVEY STRATEGIQUE, développement des équipes d'intervention d'urgence ;
- RENSEIGNEMENTS D'ORIGINE CYBER, à renforcer afin d'anticiper les menaces, de caractériser l'adversaire et d'adapter ainsi les systèmes de défense.





Etant donné l'influence positive comme négative désormais reconnue au cyberspace, les forces de défense ne peuvent se permettre d'ignorer son rayonnement sans précédent.

Toutefois, les progrès technologiques et la libéralisation des télécommunications ne devraient pas favoriser le désordre et la déstabilisation.

A ce titre, une veille sécuritaire et la surveillance des réseaux sociaux semblent naturellement s'imposer afin d'en tirer le meilleur, et optimiser leur utilisation au profit de la nation toute entière.

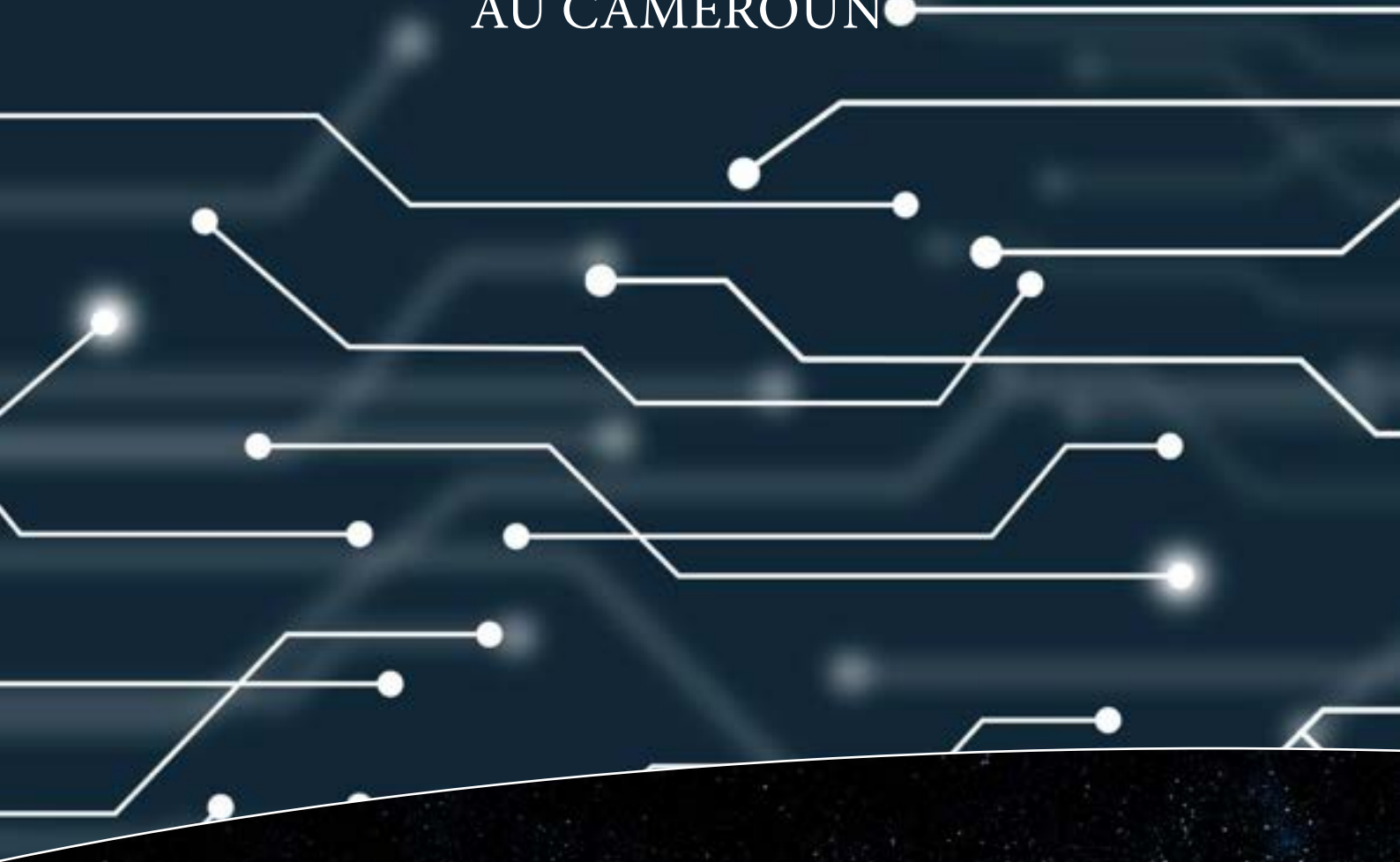
**LA VALEUR DES HOMMES RESTE LE CŒUR DU SYSTÈME ET LA CLEF DE LA VICTOIRE.**





# PANEL 3

LUTTE CONTRE LA CYBERCRIMINALITÉ  
AU CAMEROUN



# MODERATEUR



## M. OTTOU Valery

Inspecteur N°1, à l'Inspection Générale Chargée des Questions Techniques  
au Ministère des Postes et Télécommunications.





# PANEL 3

## LUTTE CONTRE LA CYBERCRIMINALITÉ AU CAMEROUN

### Exposé 1

## PROCEDURES ET TECHNIQUES D'INVESTIGATIONS NUMERIQUES



Presenté par : Dr. BELL B.G.

Expert Judiciaire

Laboratoire-Digital-Légal

- Cryptologue, Titulaire d'un PhD en Technical sciences In Methods and Systems of protection of the information, Information security- Cryptologist;
- Diplômé en National Advanced School of engineering-University of Yaounde 1;
- Enseignant dans plusieurs universités et grandes écoles du Cameroun
- Directeur Général de ITS ;
- Membre d'Information Systems Audit and Control Association (ISACA);
- Membre d'International Association for Cryptologic Research (IACR);
- Expert judiciaire auprès des Cours d'Appels du Centre et du Littoral.

### Cyber-infractions

On peut observer trois phases dans les actions liées aux infractions cybernétiques:

1. Avant l'infraction (les événements dépendent de la robustesse des systèmes de sécurité mis en place);
2. Pendant l'infraction( les événements dépendent de la robustesse du système de sécurité et de son système de gestion mis en place);
3. Après l'infraction( les événements dépendent du système de sécurité, de son système de gestion et du contexte règlementaire).

### Deux catégories d'infractions

- infractions directement liées aux technologies numériques ;
- Les infractions dont la commission a été facilitée ou liée à l'utilisation de ces technologies. .

### Catégorie 1

Dans le premier cas, le numérique est l'objet même du délit ; on parle alors d'infractions nu-

mériques pures. On y rencontre, notamment, les atteintes aux systèmes de traitement automatisé de données, la diffusion de programmes permettant de commettre une atteinte à un système de traitement automatisé de données, les infractions à la loi Informatique et liberté sur la protection des données personnelles, les infractions aux cartes de paiements (dont la diffusion de programmes permet de fabriquer de fausses cartes de paiement) et les infractions à la législation sur la cryptologie.

### Catégorie 2

Dans la seconde catégorie, le numérique, tout comme sert à commettre une infraction. Alors, la technologie tient lieu d'adjuvant, de moyen. Ici, l'on se trouve confronté aux infractions liées aux nouvelles technologies du numérique. Ce sont, par exemple, la diffusion de contenus illicites, les escroqueries par utilisation frauduleuse de numéro de carte bancaire pour une transaction en ligne, les escroqueries par fausse vente sur un site d'enchères en ligne, les contrefaçons de logiciels ou d'œuvres audiovisuelles.



### Problèmes

Les problèmes posés par ce type d'infraction et qui sont à résoudre rapidement sont ceux de la mise en place de cadres de justice adaptés, et notamment de la création de nouvelles méthodes et procédures d'enquêtes, de saisie des scellés et l'exploitation des rapports.

### Actions à mener

- Saisir des équipements numériques de question;
- Rechercher des données effacées, cachées, cryptées;
- Retrouver toutes traces visibles;
- Prouver toute fraude numérique au sein ou à l'encontre de.....;
- Prouver tout usage abusif ou illicite du numérique;
- Constituer des preuves numériques en vue d'une action (judiciaire ou privée);
- Engager des procédures contentieuses ou précontentieuses.

### Investigation numérique

Terme adapté de l'anglais « computer forensics », l'expression « investigation numérique » représente l'utilisation de techniques spécialisées dans la collecte, l'identification, la description, la sécurisation, l'extraction, l'authentification, l'analyse, l'interprétation et l'explication de l'information numérique. Ces techniques sont mises en œuvre quand une affaire comporte des questions relatives à l'usage d'un ordinateur et de tout autre support d'information, ainsi qu'à l'examen et l'authentification de données en faisant appel aux techniques d'analyse du fonctionnement des ordinateurs ou à la connaissance des structures de données. L'investigation numérique est une branche spécialisée de l'informatique qui requiert des compétences allant au-delà de celles nécessaires à la maintenance et à la sécurité informatique.

### Preuve numérique

Terme adapté de l'anglais « digital evidence », l'expression « preuve numérique » représente toute information numérique pouvant être utilisée comme preuve dans une affaire de type judiciaire. La collecte de l'information numérique peut provenir de l'exploitation de supports d'information, de l'enregistrement et de l'analyse de trafic de réseaux (informatiques, téléphoniques ...) ou de l'examen de copies numériques (copies-images, copies de fichiers ...). Les copies-écran d'informations numériques ne sont pas des preuves numériques au sens de la pré-

sente définition, mais elles peuvent servir de point de départ pour la recherche ultérieure de preuves numériques.

### Rapport d'investigation

Terme adapté de l'anglais « chain of evidence », l'expression « rapport d'investigation » représente un enregistrement des étapes d'une investigation numérique permettant de garantir qu'une preuve numérique est issue de manière irrévocable d'une information numérique. Ce rapport décrit comment l'information numérique originale a été préservée, donne son empreinte numérique, décrit les moyens logiciels et matériels de blocage en écriture utilisés, décrit les opérations réalisées et les logiciels mis en œuvre, expose les éventuels incidents rencontrés et notamment les modifications de l'information numérique analysée, énonce les preuves réunies et donne les numéros de série des supports d'information utilisés pour leur enregistrement. Ce rapport est un rapport judiciaire si et seulement s'il est produit à la demande d'une institution de type judiciaire et s'il est associé à un rapport de garde.

### Rapport de garde

Terme adapté de l'anglais « chain of custody », l'expression « rapport de garde » représente un rapport ou procès-verbal établi lors de la saisie ou de la réception d'une information numérique et de son support, comportant toute information sur le détenteur antérieur (propriétaire, usager, gardien), les lieux et conditions d'acquisition (saisie, transmission), la nature du support d'information (description physique avec photographie, numéro de série), la description éventuelle de l'information numérique (méta-données, structure des données, empreinte numérique), la situation d'accès aux données (accessibles ou non), la présence de sceau (avec identification), le libellé de l'étiquette d'accompagnement, les dates d'ouverture et de fermeture du support, la mention des modifications éventuelles (suppression de mot de passe) et l'état de restitution du support (scellé, accessibilité aux données, étiquette) avec photographie.

### Empreinte numérique

Terme adapté de l'anglais « hash value », l'expression « empreinte numérique » représente une empreinte digitale d'une information numérique produite par un algorithme mathématique appliqué à cette information (disque physique ou logique, fichier).

Cet algorithme par essence à sens unique doit être tel qu'il soit impossible (en pratique) de changer l'information numérique sans changer la valeur de l'empreinte. Autrement dit, si l'empreinte numérique d'un fichier n'a pas changé, alors ce fichier n'a pas été modifié et réciproquement. Pour être certaine, l'empreinte numérique doit être calculée de deux manières indépendantes (pour les disques durs en particulier). Parfois désigné par «valeur de hachage».

### Copie-image

Terme adapté de l'anglais « forensic copy », l'expression « copie-image » représente une copie bit à bit intégrale de l'information numérique présente sur un support d'information, y compris espaces non utilisés, espaces non alloués et queues de clusters, effectuée à l'aide d'un logiciel spécifique. Réalisée dans le cadre d'une investigation numérique légale, une copie-image doit être pure et parfaite ; dans le cas contraire, le rapport d'investigation explique les raisons de l'impureté ou de l'imperfection.

Une copie est dite « pure » quand son empreinte numérique est identique à celle confirmée de l'information numérique dont elle est la copie ; elle est en outre dite « parfaite » quand cette information numérique originale n'a pas été modifiée par l'opération de copie.

### Démarche administrative

- Les textes qui organisent le fonctionnement du système judiciaire au Cameroun prévoient qu'en situation de nécessité technique dans une procédure judiciaire, selon les cas:

- L'enquêteur, le juge d'instruction, le procureur, ou le tribunal peuvent selon le rôle respectif de chacun solliciter l'assistance d'une personne experte pour mener des investigations aux fins de trouver et mettre à leur disposition des éléments de preuves permettant de conduire le dossier en présence;

- Réquisition (Procureur);
- Ordonnance (Juge d'instruction);
- Un jugement ADD (Tribunal);

Chacun de ces trois types de documents engage l'expert dans l'exécution de sa mission de manière indépendante....

Le livrable est un rapport d'expertise répondant aux questions posées à l'expert.

### Démarche Technique

Les PC, PDA (assistants personnels), téléphones mobiles et appareils photos numériques, sont des média qui contiennent de nombreuses informations produites ou (et) échangées avec des tiers, qu'un expert peut retrouver, quand bien même les fichiers originaux auraient été effacés.

La recherche d'éléments ou de traces peut conduire à la constitution d'indices, des faisceaux d'indices, voire de preuves. L'expert est neutre : les indices et preuves peuvent être à charge ou à décharge

### Techniques utilisées

- Recherches des données;
- Cryptanalyse;
- Stéganalyse ;
- Restitution des données;
- Analyse d'images et de son;
- Biométrie;
- Le chiffrement de données;
- Compression et décompression de données
- Recherche de code malveillant;
- Surveillance numérique et recherche d'identités digitale;
- Desanonymat.

### Equipements utilisés

- Ordinateurs divers;
- Téléphones divers;
- Lecteurs de mémoires divers;
- Logiciels spécialisés divers;
- Sondes et équipements d'interconnexion divers;
- Outils d'interception légale.

### Informations et traces

Les informations et traces recherchées peuvent être :

- Des images ;
- Des documents bureautiques (lettres, documents, feuilles de calcul ...);
- Les adresses électroniques ;
- Les courriers électroniques ou SMS envoyés et reçus (si cela a été explicitement autorisé par le Magistrat);
- Les sites Internet visités ;
- Des mots de passe mémorisés ;
- Les cookies (informations personnelles d'accès à un site Internet donné);



- Les logiciels installés;
- Les dates d'activités du PC (dates de création et de dernière modification d'un fichier ...);
- Les numéros appelés ou reçus.

Les informations présentes sur un support numérique, peuvent être visibles, mais aussi être délibérément cachées ou détruites (certaines pouvant être restaurées).

### Validité de la preuve numérique

- La preuve apportée est à sens unique : l'absence de preuve n'est pas la preuve de l'absence.
- L'investigation numérique peut en effet déboucher sur le constat de l'absence des informations recherchées. Compte tenu des techniques d'enregistrement des données numériques, ces informations peuvent pourtant avoir été présentes sur le support analysé et avoir été recouvertes ensuite par d'autres.
- Autrement dit, si l'investigation numérique ne trouve pas l'information recherchée, cette preuve ne vaut qu'en l'état du support et au moment de son analyse. Il ne peut en aucun cas en être déduit que ce support n'a jamais comporté l'information en cause.

### Exploitation des traces

L'identité de l'auteur est parfois difficile à établir. Il est nécessaire d'effectuer des recoupements, si possible avec des indices externes au média analysé. En effet, les indices découverts sur un PC peuvent avoir été produits par un tiers qui aurait alors pris son contrôle à l'insu de son propriétaire (Par exemple par un accès à distance via Internet). On dit alors que le PC a été compromis. Il est assez difficile de prouver qu'un ordinateur n'a pas été compromis, car un intrus avisé peut avoir effacé les traces de son intrusion. La nécessité du recoupement des indices est un nouveau défi technologique car il faut établir les liens reliant l'indice aux différents médias utilisés.

- Les informations mémorisées peuvent être incompréhensibles car chiffrées (disque dur des ordinateurs portables, fichiers encryptés proposés par les nouvelles versions de Windows XP Professionnel). Le décryptage est une science et une pratique plus ou moins difficile selon le système de chiffrement utilisé. Banal dans certains cas, le décryptage peut s'avérer très difficile dans d'autres.
- Plusieurs logiciels, dont EnCase, WinHex, Forensic Toolkit (FTK), SMART, The Coroner's Toolkit (TCT), The Sleuth Kit (TSK), Safeback, Snapback et matériels dédiés, dont Forensic Recovery of Evi-

dence Device (FRED), gamme Logicube, ainsi que X-Ways (X-Ways Software Technology AG), CelleBrite (CelleBrite Mobile Synchronizarion) pour les téléphones) ont été développés pour répondre à la forte croissance des besoins (justice, experts judiciaires, police et gendarmerie, laboratoires d'informatique légale, services secrets, officines privées.

### Points forts du Cameroun

- Loi traitant des questions de cybercriminalité disponible;
- Des conventions internationales en la matière signées;
- Des enseignements dispensés dans les parcours de formation de la police, des magistrats et des greffiers;
- Des idées d'organisation d'unités spécialisées naissent.

### Limites

- Code de procédure non adapté au contexte du numérique;
- Rupture dans la chaîne d'expertise notamment au niveau des unités d'enquête et des juridictions.

### Activités d'investigations numériques au Cameroun

- ANTIC
- LES UNITES DE POLICE ET DE GENDARMERIE
- LES LABORATOIRES SPECIALISES

### REFERENCES DU LABORATOIRE DIGITAL LEGAL

Sur les trois dernières années, plus de 250 dossiers sensibles expertisés.

Dans près de 30 Juridictions parmi lesquels:

- Le TCS;
- Les 10 tribunaux militaires du Cameroun;
- Les TGI, TPI et Autres juridictions;
- Plus de 20 villes couvertes;
- Plusieurs dossiers expertisés dans d'autres pays de la CEMAC.



# PANEL 3

## LUTTE CONTRE LA CYBERCRIMINALITÉ AU CAMEROUN

### Exposé 2

## LA POLICE CAMEROUNAISE FACE A LA CYBERCRIMINALITE : QUELS DEFIS ET QUELLES ATTENTES



Presenté par : **OBA ELLE GUY ROLAND**  
**OFFICIER DE POLICE DE 2ème GRADE**  
**Ingénieur des Télécommunications**  
**Master en Systèmes d'Informations**  
**Administrateur Réseaux**  
**et des Bases de Données à la DGSN**

#### INTRODUCTION

La Sûreté Nationale, à l'instar d'autres administrations, fait face aux défis de sécurisation du cyber espace camerounais. La révolution numérique qui a facilité la structuration et l'émergence du crime organisé en ligne, a entraîné le développement de nombreuses pratiques cybercriminelles.

Dans le même temps, des publications virales à connotation haineuse, irrédentiste et diffamatoire prolifèrent sur les réseaux sociaux, troublant gravement l'ordre public numérique, la paix publique, la sécurité des internautes et celle des infrastructures critiques de l'information nationale.

Pour y faire face, la Sûreté Nationale a entrepris d'arrimer son dispositif de sûreté et de sécurité aux évolutions technologiques et aux formes de menaces nouvelles et émergentes. Pour ce faire, elle s'emploie à affiner sa stratégie opérationnelle de cyber sécurité afin d'assurer, par le Maintien de l'Ordre Public Numérique, la protection des personnes, des biens, des entreprises et de l'Etat ainsi que la sécurisation des infrastructures critiques de l'information nationale.

#### PLAN

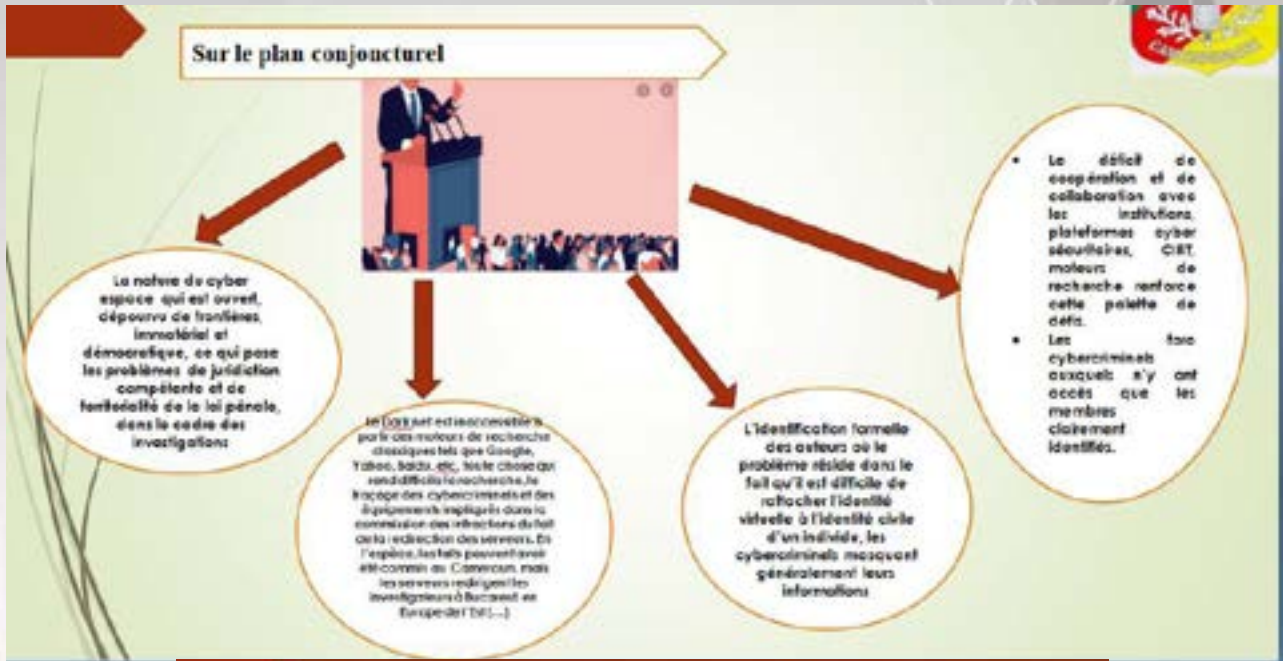
LES PRINCIPAUX DEFIS AUXQUELS FAIT FACE LA DGSN DANS LA LUTTE CONTRE LA CYBERCRIMINALITE

LA RIPOSTE DE LA SURETE NATIONALE CONTRE LE FLEAU

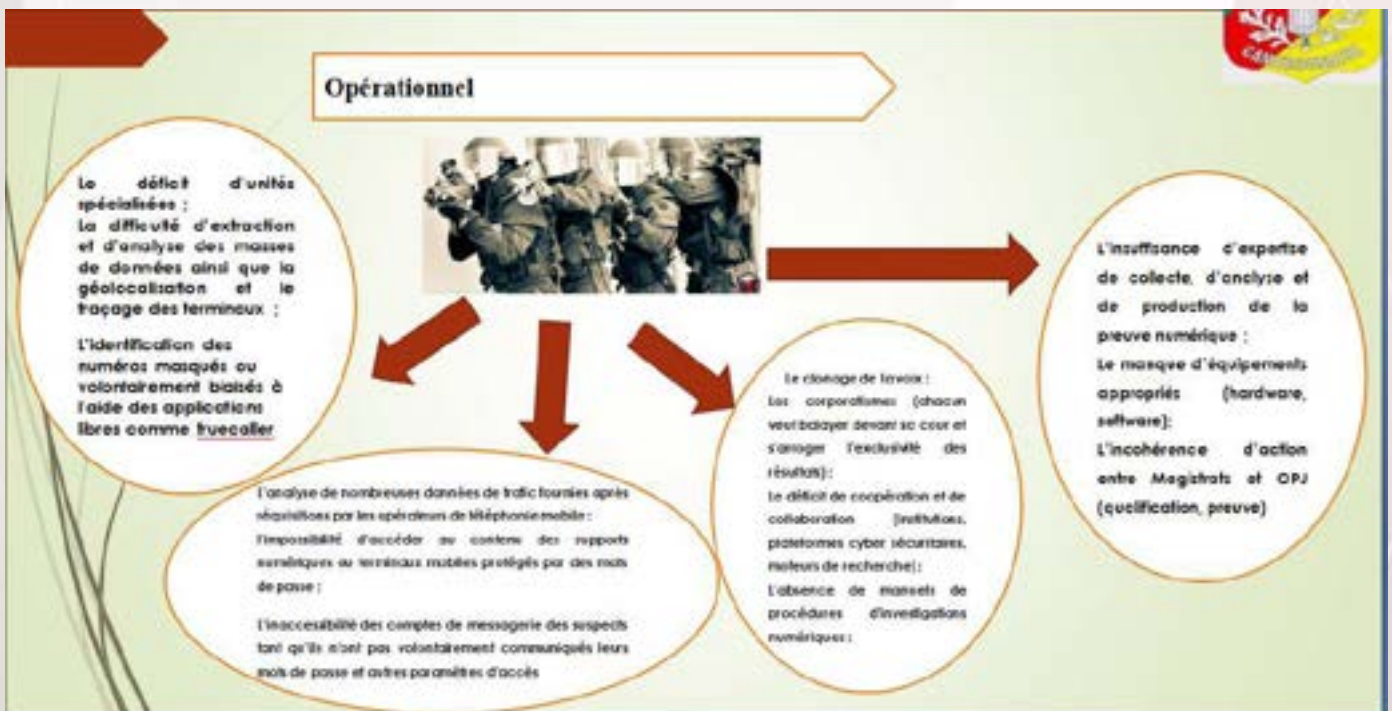
LES ATTENTES DE LA DGSN

LES PRINCIPAUX DEFIS AUXQUELS FAIT FACE LA DGSN DANS LA LUTTE CONTRE LA CYBERCRIMINALITE

Sur les plans Conjoncturel et Structurel, Juridique et Technique et Opérationnel









LA RIPOSTE DE LA SURETE NATIONALE CONTRE LE FLEAU

Création de l'USLUCC



Développement et renforcement de partenariats



TRAVAUX EN PLENIERE

Exposé 2 :LA POLICE CAMEROUNAISE FACE A LA CYBERCRIMINALITE : QUELS DEFIS ET QUELLES ATTENTES

LES ATTENTES DE LA DGSN Au niveau stratégique



Au niveau tactique

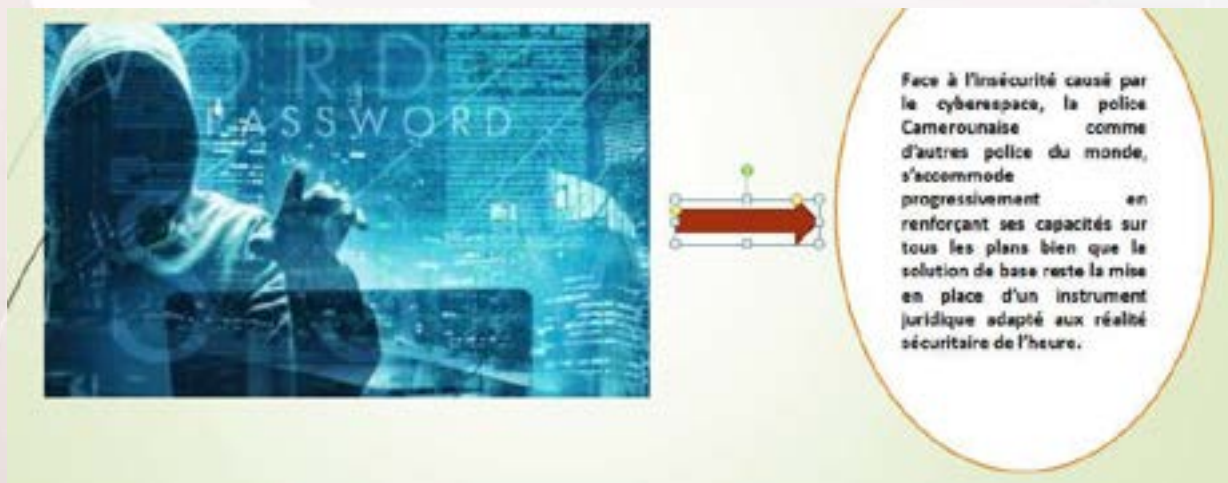




Au niveau opérationnel



CONCLUSION





## PANEL 3

## LUTTE CONTRE LA CYBERCRIMINALITÉ AU CAMEROUN

## Exposé n° 3

## CYBERCRIMINALITÉ ET RÉPONSE DE JUSTICE PÉNALE DANS LE CYBERESPACE



Presenté par : Monsieur LOGMO II Achille,  
Magistrat,  
Sous-Directeur de l'Action Pénale  
à la Direction des Affaires Pénales et des Grâces,  
Ministère de la Justice

## Introduction

## I- Le Cadre Normatif de la Répression de la Cyber Criminalité

- Sur le plan International
  - Convention de Budapest du 23 Novembre 2001;
  - Convention de l'Union Africaine sur la Cyber sécurité et la protection des données, adoptée à Malabo le 23 juin 2014.
- Sur le plan National
  - Loi n° 2016-7 du 12 juillet 2016 portant code pénal;
  - Loi n° 2005/007 du 27 juillet 2005 portant code de procédure pénal;
  - Loi n° 2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun •
  - Loi n° 2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun ;
  - Loi n° 2010/012 du 21 décembre 2010 relative à la Cyber sécurité et à la Cybercriminalité;
  - Loi n° 2015/007 du 20 avril 2015 régissant l'activité Audiovisuelle au Cameroun.

## II- Mise en œuvre de la répression des infractions cybernétiques

- La constatation des infractions cybernétiques;

- La poursuite des infractions cybernétiques;
- Le jugement des infractions cybernétiques.

## III- Les difficultés d'appropriation et d'application de cette législation spéciale

- Culture numérique embryonnaire des populations;
- Formation insuffisante (voire absente) des acteurs de la chaîne de répression de ce phénomène criminel;
- Le déficit des moyens logistiques;
- Le caractère évolutif et transnational des crimes cybernétiques.

## IV- Perspectives pour une amélioration de la riposte contre la cybercriminalité

- Relever le niveau de culture numérique des populations;
- Renforcer les capacités des acteurs de la chaîne de répression.
  - Relire la loi n° Loi n° 2010/012 du 21 décembre 2010 relative à la Cyber sécurité et à la Cybercriminalité;
  - Accroître la coopération régionale et internationale.





## PANEL 3

## LUTTE CONTRE LA CYBERCRIMINALITÉ AU CAMEROUN

## Exposé 4

## RÉSEAUX SOCIAUX : OPPORTUNITÉS ET MENACES, SIMULATIONS PRATIQUES



Présenté par : **Dr EYOUM GÉRARD**  
DIRECTEUR GÉNÉRAL CYBERIX  
EXPERT EN CYBER SÉCURITÉ

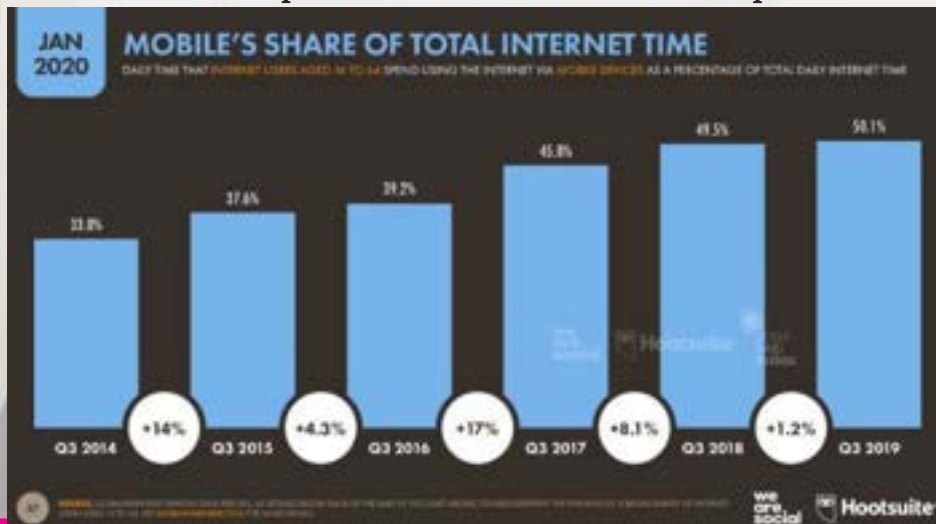
Titulaire d'un doctorat en cyber renseignement

- Expert en cybersécurité et spécialiste des questions de cyberrenseignement stratégique;
- Membre de l'International Association of counter Terrorism.

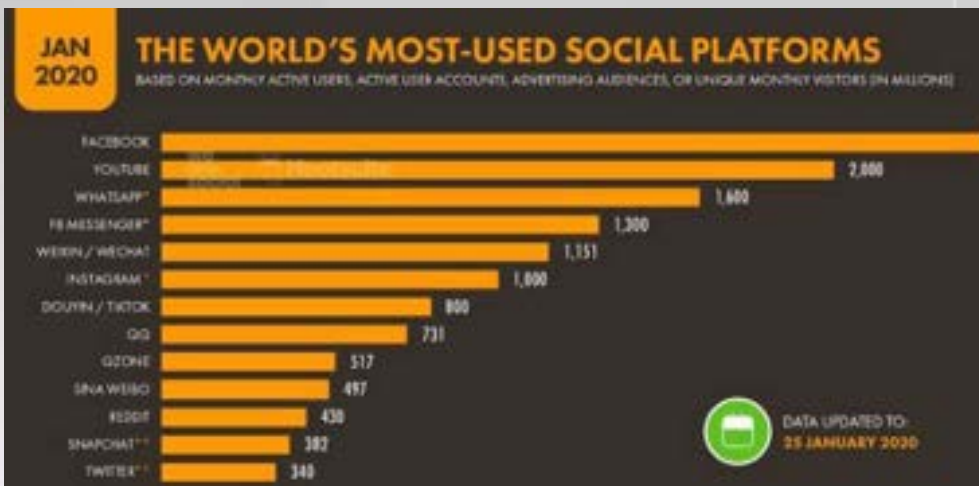
## RÉSEAU SOCIAL

- En sciences humaines et sociales, l'expression réseau social désigne un agencement de liens entre des individus et/ou des organisations, constituant un groupement qui a un sens : la famille, les collègues, un groupe d'amis, une communauté, etc.
- Le mot réseau est très ancien. Il s'écrivait alors réseuil, rets, et il fut à l'origine un mot féminin. De ces mots, le plus connu est rets. La fable de

La Fontaine fait référence au lion pris dans des rets, délivré par un rat. L'on se souvient aussi du rétiaire, gladiateur armé d'un filet pour immobiliser l'adversaire et d'un trident pour le tuer. Plus globalement, la réseuil est un filet pour capturer des animaux. Le réseau est donc à l'origine un instrument de capture, un moyen d'empêtrer, d'immobiliser. On ne parlait pas de réseau, sauf pour évoquer l'action clandestine, le complot, le piston... toutes situations dans lesquelles chacun est tenu par les autres.



*TAUX D'UTILISATION  
DES SMARTPHONES  
POUR ACCÈS INTERNET*



RÉSEAUX SOCIAUX  
LES PLUS UTILISÉS  
AU MONDE



UTILISATION  
D'INTERNET AU  
CAMEROUN



STATISTIQUES  
SUR LES MÉDIAS  
SOCIAUX

### BUTS EXOGÈNES DES RÉSEAUX SOCIAUX

Les réseaux sociaux sont des moyens modernes de communication, de partage et d'expression permettant d'instaurer un dialogue avec sa communauté, et donc une relation concrète :

- Ils ont pour but de renforcer la sociabilité chez leurs utilisateurs, tout en développant les interactions sociales, révélant un engagement de la part d'une communauté;
- Ils permettent de communiquer même en situation de mobilité;
- Augmenter la capacité de renseignement biographique et technique (identité, adresse, email, téléphone, amis, travail, scolarité, famille, lieux fréquentés, etc.);
- Obtenir un maximum d'informations sur les individus sans se déplacer ;
- Cibler une catégorie d'individus dans le but de les suivre ou de les influencer;
- Obtenir des informations dans le but de les revendre aux compagnies commerciales.





OSINT: LE REN-  
SEIGNEMENT DE  
SOURCE OUVERTE

The CIA 'Bin Laden' unit claimed that 90% of what they needed to locate and capture their target was Open Source Intelligence, while in 2005 W.M Nolte (Former deputy assistant director of the CIA) claimed that 95-98% of all information provided by the US intelligence services was OSINT based.

		LES ZONES GRISSES DE LA RECHERCHE D'INFORMATION		
		« LA FIN NE JUSTIFIE PAS LES MOYENS »		
		Les MOYENS utilisés		
		Ouverts	Organisés et déontologiques	Illégaux
La Fin : type d'info	Info noire (fermée, secrète)	<b>Interdit</b>	<b>Interdit</b>	<b>Espionnage (au sens strict)</b>
	Info grise (semi- ouverte)	<b>Intelligence économique</b>	<b>Intelligence économique</b>	<b>Bêtise dangereuse "border line"</b>
	Info Blanche (ouverte)	<b>Intelligence économique</b>	<b>Bêtise dangereuse</b>	<b>Bêtise dangereuse</b>

© Jacques Breillat

TYPOLOGIE DE  
L'INFORMATION

### CONSÉQUENCES (RISQUES) DES RÉSEAUX SOCIAUX

Le renseignement opérationnel, autrefois 100% opérationnel (HUMINT, SIGINT), est réalisé à près de 80% par OSINT, c'est-à-dire par l'exploitation des sources ouvertes, et particulièrement des réseaux sociaux.

L'information se classe en 3 catégories : blanche (publique, ouverte), grise (limitée, réservée) et noire (confidentielle, secret). Aujourd'hui, l'information noire est devenue blanche ou grise grâce aux réseaux sociaux où l'utilisateur n'a pas toujours conscience de partager une information importante.

Les réseaux sociaux se substituent souvent aux médias pour le partage d'informations, ce qui multiplie le risque de propagation de fausses nouvelles car la transmission répond ici à un facteur émotionnel d'adhérence plutôt qu'à une éthique journalistique. La majorité des crises médiatiques naissent aujourd'hui dans les réseaux sociaux.

### SCANDALE CAMBRIDGE ANALYTICA – FACEBOOK



**RISQUES LIÉS AUX RÉSEAUX SOCIAUX**

**Risques pour les utilisateurs et les entreprises**

- Escroquerie ;
- Usurpation d'identité;
- Chantage;
- Vol d'informations;
- Cyber-harcèlement;
- Désinformation;
- Diffamation.

**Risques Étatiques**

- Manipulation de l'opinion public (par exemple Imposer et diffuser un narratif auprès d'une population, astroturfing);
- Propagation de fausses nouvelles;
- Opérations psychologiques.

- Cyber-terrorisme;
- Espionnage des États alliés;
- Espionnage des États ennemis;
- Menace à la souveraineté de l'État;
- Discréditer;
- Asseoir des intérêts politiques, économiques et diplomatiques.

**STRATÉGIE DE L'ÉTAT**

La stratégie de l'État devrait s'articuler autour de la maîtrise des réseaux sociaux dans le but de :

- Bloquer les opérations psychologiques (par exemple, le cas de PSY-GROUP)
- Bloquer les opérations de propagande
- Combattre la cybercriminalité

Les réseaux sociaux sont aujourd'hui à la fois les principaux vecteurs et outils de la guerre de l'information que mènent les acteurs étatiques et non étatiques dans le cyberspace.

**MOYENS DE RIPOSTE**

Il serait utile, dans la riposte de l'État, de :

- Mettre sur pieds une plateforme de surveillance des réseaux sociaux
- Créer des plateformes de répression
- Mettre sur pieds une plateforme de conformité et d'inter-échange d'information avec les réseaux sociaux
- Mener des opérations psychologiques pour combattre la cyber aliénation (ex: taxer le temps passé dans les réseaux sociaux)
- Créer des réseaux sociaux parallèles afin de riposter aux opérations psychologiques d'influence



**QUELQUES CAS PRATIQUES**

- SURVEILLANCE D'UN RÉSEAU SOCIAL;
- RECHERCHE OPÉRATIONNELLE ACTIVE;
- VEILLE D'INTÉGRITÉ D'UN COMPTE.



## PANEL 3 LUTTE CONTRE LA CYBERCRIMINALITÉ AU CAMEROUN

### Exposé 5

# GESTION ET PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL AU CAMEROUN



Presenté par : **Monsieur WANGUE DAVID BRICE**  
Ingénieur Informaticien /  
Diplomate Expert en Stratégies de cybersécurité  
et de lutte contre la cybercriminalité  
Chef de la Division des Etudes  
et Projets au CENADI/MINFI

#### PLAN DE L'EXPOSÉ

I. RAPPEL DES OBJECTIFS DE L'EXPOSÉ (Mission : VOIR TDR MINPOSTEL)

II. CONTEXTE ET INFORMATIONS GÉNÉRALES

III. PREMIÈRE PARTIE : LES DONNÉES À CARACTÈRE PERSONNEL, TRAITEMENT, PROTECTION : DE QUOI IL S'AGIT ?

IV. DEUXIÈME PARTIE : ESSAI D'ANALYSE DIAGNOSTIQUE DE LA SITUATION DE GESTION ET DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL AU CAMEROUN.

V. TROISIÈME PARTIE : BREF REGARD DE CE QUI SE PASSE AILLEURS (EXPÉRIENCES DES AUTRES ÉTATS)

VI. QUATRIÈME PARTIE : SUGGESTIONS ET RECOMMANDATIONS

## I- RAPPEL DES OBJECTIFS DE L'EXPOSÉ

### OBJECTIF GLOBAL

Présenter la problématique de la gestion et la protection des données à caractère personnel au Cameroun.

### OBJECTIFS SPÉCIFIQUES

- Présenter quelques éléments de langage (concepts et terminologies) liés aux données à caractère personnel ;
- Évoquer les enjeux autour de la gestion et de la protection des données à caractère personnel ;
- Analyser la situation de la gestion et de la protection des données à caractère personnel au niveau national, assorti des points forts et des faiblesses d'une part, et, au niveau international, des opportunités et menaces, d'autre part ;
- Justifier de la nécessité d'un cadre réglementaire spécifique, son processus d'élaboration, les parties prenantes, les stratégies de mise en œuvre, les structures étatiques de gestion ;
- Présenter l'expérience de quelques États sur le point susvisé, ainsi que les difficultés qu'ils rencontrent ;
- Formuler des suggestions et recommandations visant à améliorer le cadre de gestion et de protection des données à caractère personnel au Cameroun.

## II- CONTEXTE ET INFORMATIONS GÉNÉRALES

Les données en général, celles à caractère personnel revêtent une grande importance. Leur gestion et protection préoccupent les acteurs publics et privés (États, collectivités locales, entreprises du secteur privé, organisations de la société civile, médias, institutions de formation et de recherche etc.). La révolution numérique est incontestablement admise comme un véritable moteur de croissance économique et de développement politique et social. L'Internet s'appuie sur les données en général, qui représentent sa matière première. Parmi ces données, il existe celles relatives aux personnes physiques.

Exemple des données relatives aux personnes physiques: démographiques : nom, prénom, âge, sexe, statut marital ; comportementales : habitudes d'achats, durée de session... ; centres d'intérêts : couleur politique, hobbies; relatives à la navigation : le type d'appareil utilisé, la localisation précise ou encore le numéro de portable ou le numéro IMEI...

Susceptibilité d'identification d'une personne physique constituant des risques potentiels en terme

d'atteinte à la confidentialité, à l'intégrité et à la disponibilité de ces données personnelles, y partant de la violation de la vie privée des citoyens, dont l'État est garant de la protection en premier : vie privée ou intimité, vie sentimentale, relations amicales, nudité, pratiques sexuelles, l'état de santé, moyens d'existence, convictions religieuses...

La protection de la vie privée a été affirmée en 1948 dans la Déclaration universelle des droits de l'homme des Nations unies (art. 12), pour laquelle le Cameroun affirme son attachement aux libertés fondamentales y inscrites au plus haut niveau dans sa loi fondamentale (la constitution). les enjeux autour de la gestion et protection des données personnelles, dans le contexte actuel du tout numérique. Pour l'État :

- la nécessité de susciter en permanence la confiance des internautes quant à l'utilisation des TIC;
- l'amélioration de l'image du Cameroun en l'inscrivant dans le cadre des pays dont la législation protège de manière spécifique la vie privée sur le numérique et donc crédible pour commercer avec d'autres espaces bien avancés sur la question.

Pour les entités (organismes) chargées du traitement des données personnelles

- La maîtrise des risques que peut causer une mauvaise gestion et protection des données personnelles, notamment en termes d'impact négatifs qu'une telle situation pourrait générer sur le plan juridique (exposition à des sanctions), économique (les pertes financières), social (mauvaise presse, image) ; Pour les citoyens Camerounais :

- la maîtrise des droits nouveaux ainsi que les risques suscités par l'utilisation des Technologies de l'Information et de la Communication ;

- l'intensification de la culture de cyber sécurité par l'éducation, ô combien important pour intégrer la nouvelle société numérique.

Il se pose dans le cadre de la présente communication La question de savoir comment assurer une gestion efficace et un niveau de protection des données personnelles à la mesure des enjeux et dangers liés à leur traitement dans le contexte du tout numérique ?

Autrement dit, Comment procéder à l'identification des personnes d'une part et, quels cadre normatif et approches techniques pour protéger des données à caractère personnel traitées par les entités basées au Cameroun, de manière à faire respecter la vie privée des citoyens en responsabilisant les entités impliquées dans le traitement des dites données, à l'ère du numérique d'autre part ?



L'objectif ultime est la conciliation effective entre les exigences de respect de la dignité humaine et le développement du numérique.

En d'autres termes, il est visé ici la recherche par les voies normatives et technologiques, d'un équilibre entre l'usage des Technologies de l'Information et de la Communication et la protection de la vie privée des citoyens dans leur vie quotidienne ou professionnelle tout en garantissant la libre circulation des informations.

### III- PREMIÈRE PARTIE : LES DONNÉES À CARACTÈRE PERSONNEL TRAITEMENT, PROTECTION, IDENTITÉ NUMÉRIQUE : DE QUOI S'AGIT-IL ?

Il est question ici, au-delà des considérations philosophiques, d'essayer de définir techniquement quelques concepts liés à la question des données à caractère personnel.

#### 1- Définitions relatives aux données et aux traitements :

**En France :** Cette notion a été définie de façon extrêmement précise par le législateur français en 1978. Ainsi, selon l'article 2 de la Loi informatique et libertés de 1978 : « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

#### Union Africaine

Dans la convention de l'Union Africaine adoptée à Malabo la 23ème session le 27 juin 2014, les termes ci-après ont été définis.

#### En ce qui concerne les données

**Données informatisées :** toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;

**Données sensibles :** toutes les données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives;

**Données dans le domaine de la santé :** toute information concernant l'état physique et mental d'une per-

sonne concernée, y compris les données génétiques précitées ;

**Données à caractère personnel :** toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité ;

**Fichier de données à caractère personnel :** tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

**Information :** tout élément de connaissance susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, ou autres...

**Interconnexion des données à caractère personnel :** tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement.

#### S'agissant des traitements:

**Traitement des données à caractère personnel:** toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel.

**Destinataire d'un traitement des données à caractère personnel :** toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargés de traiter les données.

**Responsable du traitement :** toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités.

### Essentiel à retenir des données à caractère personnel Sur le plan technique

La nature des informations n'a pas d'importance. Illustration : « température d'un logement »

Si lien vers une personne, Donnée à caractère Personnel (DP). • Lien direct. Illustration : « température + nom » • ou indirect. Illustration : « température + ID client ENEO »

Personne identifiable si informations nécessaires détenues par : Responsable de traitement... Illustration : ENEO collecte « température + ID client ENEO ».

Ou n'importe qui dans le monde. Illustration : ENEO collecte « température + adresse IP du capteur »

(le FAI par exemple CAMTEL peut faire le lien entre une adresse IP et un client ADSL)

### 2- considération liée à l'identité numérique

**But :** Pour un État, une identité permet donc d'identifier de façon unique un individu afin de lui octroyer des droits et lui en réclamer les devoirs. Il existe plusieurs formes d'identités.

**Identité physique :** caractérisé par un nom, prénom

**Identité administrative :** caractérisé par un numéro matricule, CNPS ou un fiscal par exemple.

**Identité technologique :** permet à la technologie d'identifier les utilisateurs de façon unique. (nom d'utilisateur, son adresse IP, donc l'équivalent de son adresse postale sur Internet, des adresses mail, des identifiants Facebook ou des pages Internet). Aux identifiants, on peut associer des attributs de différents types qui sont des caractéristiques propres comme votre sexe, votre âge et donc il en existe différents types.

#### Types d'attributs:

Les attributs déclarés informations que vous déclarez volontairement quand vous allez vous enregistrer à un service. ( nom, prénom et commentaires) ;

Les attributs observés. Observation de nos faits et gestes sur Internet au travers de nos identifiants;

Les attributs inférés. À partir de nos actions, des personnes, des services vont essayer de découvrir de nouveaux attributs dans notre activité professionnelle;

Les attributs cachés, sont liés aux identifiants et qui sont liés à des technologies.

Enjeux. Tous les identifiants de l'identité numérique, sont des données à caractère personnel.

**Risque 1:** en tant que citoyen quand on va sur Internet, c'est qu'une personne soit capable de passer

de l'identité numérique à l'identité physique, du fait d'un mauvais choix d'identifiant ou de la corrélation qu'on peut faire entre les identifiants, les attributs et notre personne physique.

**Risque 2:** avec l'identité numérique, on peut découvrir de nouveaux attributs que nous n'avons pas déclarés, pas publiés sur Internet, en essayant de trouver des attributs qui sont incorrects sur notre personne.

En conclusion, notre identité numérique est définie par tous ces identifiants qui nous sont associés quand on se lie à une technologie, ainsi que les attributs que nous déclarons ou qui sont trouvés par la suite quand nous utilisons la technologie.

Tout ceci constitue des données à caractère personnel et sont ainsi susceptibles d'être protégées, ce d'autant plus que beaucoup de gens essayent de nous observer au travers de ces identifiants, et peuvent à partir de celles-ci porter atteinte à notre vie privée.

**État des lieux en interne :** National Examen du cadre législatif et réglementaire

#### Forces:

Existence d'une série de lois sur les TIC depuis 2010 qui avaient pour objectif principal de réguler le secteur des Nouvelles Technologies de l'Information et de la Communication en se concentrant sur la sécurité des réseaux de communications électroniques et les systèmes d'information.

#### Faiblesses :

1- Les lois de 2010 susvisés évoquent superficiellement la protection des données à caractère personnel, toutefois de manière dispersée.

#### À titre d'illustration :

Dans la loi N° 2010/012 du 21 décembre 2010 sur la cybersécurité et la cybercriminalité, la section IV est consacrée à la protection de la vie privée des personnes. La protection des « données à caractère privé ou confidentiel » est évoquée à l'article 74.

Dans la loi n° 2010/013 du 21 Décembre 2010 régissant les communications électroniques sur les communications électroniques lorsqu'elle consacre la notion d'exigence essentielle pour l'établissement et l'exploitation des réseaux ainsi que la fourniture des services de communications électroniques qui renvoie notamment à « l'interopérabilité des réseaux et celle des équipements terminaux, ainsi que la protection des données personnelles ».



Dans le Décret n° 2012/1639/pm du 14/06/2012 fixant les modalités de déclaration, ainsi que les conditions d'exploitation des réseaux et installations soumis au régime de la déclaration.

Dans le Décret n° 2012/1640/pm du 14/06/2012 Fixant les conditions d'interconnexion, d'accès aux réseaux de communications électroniques ouverts au public et de partage des infrastructures. Dans le Décret n° 2012/1638/PM du 14 Juin 2012 fixant les modalités d'établissement et/ou d'exploitation des réseaux et de fourniture des services de communications électroniques soumis au régime de l'autorisation qui précise que les opérateurs sont tenus « d'assurer la protection, l'intégrité et la confidentialité des informations à caractère personnel qu'ils détiennent et qu'ils traitent ».

Dans le Décret fixant les conditions d'interconnexion, d'accès aux réseaux de communications électroniques ouverts au public et de partage des infrastructures qui dispose que : « Les opérateurs précisent, dans leurs conventions d'interconnexion et d'accès, l'ensemble des mesures nécessaires pour garantir (...) la protection des données à caractère personnel liées à la vie privée et la confidentialité des informations traitées, transmises ou stockées ». Dans le décret fixant les modalités d'application de la loi n° 2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun qui précise que : « Toute personne qui exerce l'activité de commerce électronique au Cameroun a l'obligation de fournir aux consommateurs (...) les indications sur les dispositions relatives à la protection des données à caractère personnel ».

2- Les lois de 2010 semblent insuffisantes aussi bien du point de vue substantiel que processuel pour couvrir le champ des matières pertinentes susceptibles d'être abordées dans le cadre de la gestion et de la protection des données personnelles.

Illustration :

Le décret fixant les modalités d'établissement et/ou d'exploitation des réseaux et de fourniture des services de communications électroniques soumis au régime de l'autorisation, définit les notions de données à caractère personnel et même la notion de traitement des données à caractère personnel, sans préciser les modalités permettant d'établir sans ambiguïté le cadre de protection desdites données.

Dans le cadre de la loi sur la cybercriminalité, notamment l'article 74 où sont substantiellement déterminées les dispositions visant la protection des

données, Il se trouve que cette protection vise uniquement les usagers des services de communication électroniques, donc les abonnés, excluant une large part de la population susceptible d'être exposée à la violation des données à caractère personnel d'un côté et, est tacite sur l'énumération des droits dont les personnes disposent sur leurs données personnelles.

- Insuffisance de la protection internationale eu égard à la non internalisation des certaines règles de portée universelle sur la question.

Examen du cadre institutionnel

Forces:

Existence d'une multitude d'acteurs pouvant être impliqués dans le périmètre de ceux, responsables du traitement des données à savoir l'État, les collectivités territoriales décentralisées, les entreprises y compris celles qui n'interviennent pas directement dans le secteur des TIC comme les banques et les assurances.

Faiblesses :

- Non existence d'une structure administrative autonome hautement qualifiée et légitime pour adresser de manière globale et efficace la gestion et protection des données à caractère personnel au Cameroun, notamment en assurant la garantie du respect;

- Focalisation des responsabilités et obligations sur les opérateurs/fournisseurs de services de communications électroniques et les entreprises qui exercent des activités de commerce électronique, comme l'illustre le Décret n° 2012/1642/pm du 14/06/2012 fixant les conditions d'attribution et d'utilisation des ressources en numérotation, art.2;

- Absence d'une loi spécifique sur la gestion et la protection des données personnelles donnant un sentiment de vide juridique, notamment en ce qui concerne les droits des internautes camerounais sur la question, ainsi que la responsabilité des acteurs impliqués dans le traitement desdites données.

#### IV- TROISIÈME PARTIE : BREF REGARD DE CE QUI SE PASSE AILLEURS (EXPÉRIENCES DES AUTRES ÉTATS)

En externe : Supranational ONU  
**Opportunités :**

- La nomenclature mondiale des instruments juridiques de protection des données à caractère personnel est bien fournie.

-La protection des données à caractère personnel repose sur certains instruments fondateurs.

**Au niveau universel et onusien,** il y a d'abord la Déclaration universelle des droits de l'Homme, notamment en son article 12 : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

La résolution 45/95 adoptée le 14 décembre 1990 par l'Assemblée Générale des Nations Unies qui fixe les principes directeurs en matière de protection des données à caractère personnel, à savoir la définition du corps des règles qui devraient être appliquées aux fichiers contenant des données à caractère personnel, ainsi que la consécration de l'autorité chargée de veiller à l'application de ces règles.

Les principes directeurs élaborés par un groupe d'experts de l'OCDE, permettant de sauvegarder les libertés face à l'utilisation croissante de l'informatique tout en offrant la possibilité de transmettre ces données nominatives à l'étranger.

**Limites:** Absence du caractère non contraignant des principes directeurs des Nations Unies qui

sont formulés sous forme de recommandation et qui n'ont pas de force obligatoire pour les États, vu que ces derniers sont libres de les mettre en pratique.

##### **Cadre américain :**

Aux États-Unis, la protection des données à caractère personnel est assurée au niveau fédéral par le Privacy Shield, entré en vigueur le 1er août 2016, et les législations diverses des États fédérés dont la plus emblématique est le California Consumer Privacy Act of 2018, entré en vigueur le 1er janvier 2020.

##### **Cadre Asiatique:**

La Chine a la Loi Cybersécurité depuis 2016 et entrée en vigueur le 1er juillet 2017 ;

L'Inde se base sur son Information Technology Act de 2011 pour procéder à la protection des données à caractère personnel en y incluant des dispositions y afférentes ;

Le Japon avait élaboré et renforcé respectivement en 2003 et 2017 sa loi sur la protection des données, encore dite Protection of Personal Information Act (APPI) ;

La Corée du Sud fonctionne avec le Personal Information Protection Act (PIPA).

##### **Cadre Européen (Union Européenne) :**

Le Règlement général sur la protection des données (RGPD), entré en vigueur le 25 mai 2018, et qui définit les droits des personnes physiques, fixe les obligations des personnes qui effectuent le traitement des données et de celles qui sont responsables de ce traitement, et définit les méthodes visant à assurer le respect des dispositions prévues ainsi que l'étendue des sanctions imposées à ceux qui enfreignent les règles.

La Directive relative à la protec-

tion des données sur le plan répressif, entré en vigueur le 5 mai 2016, dont le rôle vise à garantir le droit des personnes physiques à la protection des données à caractère personnel les concernant tout en assurant un niveau élevé de sécurité publique. Ladite directive s'applique aux opérations de traitement de données effectuées à la fois au niveau transfrontière et au niveau national par les autorités compétentes des États membres à des fins d'application du droit pénal.

##### **Cadre régional Africain**

La Convention de l'Union africaine (UA) sur la cybersécurité et la protection des données à caractère personnel, appelée aussi « Convention de Malabo », adoptée le 27 juin 2014 est le principal instrument fédérateur à vocation continentale dans le domaine.

##### **Cadre sous régional**

L'adoption du Règlement N° 03 /16-CEMAC-UMAC-CM du 21 décembre 2016 relatif aux systèmes, moyens et incidents de paiement a donné l'occasion aux autorités communautaires d'apporter quelques éléments dans le sens de l'encadrement juridique de la question de la protection des données personnelles collectées à l'occasion des transactions qui naissent des relations relatives aux divers services. Toutefois, les dispositions susvisées sont limitées aux données collectées dans le cadre de la relation bancaire, bien qu'elles pourraient augurer d'une généralisation future de ces mesures.



### Cas de quelques états Africains

**Bénin :** Commission nationale de l'informatique et des libertés (CNIL) Créée en 2009 Cadre juridique national : loi n° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin Effectif: 11 commissaires Réalisation récente : Présidence du RAPDP depuis 2016 Devenue Autorité de Protection des données Personnelles avec le vote de la loi portant code du numérique en République du Bénin en instance de promulgation. Cette loi confère à l'autorité béninoise une autonomie financière. Exemple de coopération avec l'AFAPDP. La CNIL est membre de l'AFAPDP et à ce titre, participe à toutes les activités qu'elle organise, notamment les conférences annuelles et les réunions de l'Assemblée Générale.

**Au Burkina Faso:** Commission de l'informatique et des libertés (CIL) Créée en 2004, démarrage de ses activités en 2007 Cadre légal : Loi n°010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel.

Effectifs : 26 agents et 9 commissaires Réalisation récente : Campagne d'éducation au numérique au profit des jeunes des lycées et collèges du Burkina Faso lancée le 28 janvier 2014. Organisation de la Conférence annuelle et de l'Assemblée Générale de l'AFAPDP en septembre 2016. Organisation du 2nd Forum africain des Autorités de protection des données personnelles en marge duquel le Réseau Africain des Autorités Protection des Données Personnelles (RAPDP) a été créé et les statuts adoptés. Tenue d'un séminaire de sensibilisation au profit des députés de l'Assemblée Nationale du Burkina Faso, pour les sensibiliser sur les nécessités de la réforme de la loi 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel. Élection de la Présidente de la Commission comme membre du Comité exécutif de la Conférence internationale, représentant la région Afrique.

**Au Gabon:** Loi n°001/2011 du 27 septembre 2011 relative à la protection des données à caractère personnel. Art1 la présente loi, prise en application des dispositions des articles 1er et 47 de la constitution, détermine les règles relatives au traitement des données à caractère personnel et a pour objet, de mettre en place un dispositif permettant de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage. Le Gabon se dote d'une commission

nationale pour la protection des données à caractère personnel (CNPDCP).

**Au Maroc :** Commission Nationale de contrôle de la protection des données à caractère personnel (CNDP) Créée en 2010 Cadre juridique : Article 24 de la Constitution du Maroc. Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Décret 2-09-165 du 21 mai 2009 pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

**En Tunisie :** Instance nationale de protection des données personnelles (INPDP) Créée en 2008 Cadre juridique national : Constitution (article 24). Loi organique 20404-63 du 27 juillet 2004 relative à la protection des données personnelles, Décrets 2007-3003 et 3004 relatifs à l'organisation de l'Instance et aux procédures devant elle : Circulaire du Chef du Gouvernement numéro 17 du 12 octobre 2016, Délibération 2016-1 de l'INPD du 13 mai 2016 déterminant les États à protection adéquate. Délibération 2016-2 de l'INPD du 20 octobre 2017 relative à la protection des données dans l'activité politique et à l'occasion des élections.

## V. QUATRIÈME PARTIE : SUGGESTIONS ET RECOMMANDATIONS

### V1- Volet juridique et organisationnel

**I. À moyen terme:** travailler dans le sens d'aligner la question de la gestion et de la protection des données à caractère personnel, ainsi que l'ensemble des initiatives inhérentes, sur une stratégie nationale de cybersécurité. Ladite stratégie à l'image du modèle préconisé par l'UIT peut reposer sur au moins les cinq axes ci-après : Juridique; Organisationnel; Infrastructurel; Renforcement de capacité; Coopération internationale.

**II. À très court terme:** élaborer une loi spécifique sur la gestion et la protection des données personnelles. L'intérêt d'une telle loi repose sur au moins deux points : d'abord politique en ce que le droit à la protection des données personnelles est un excellent marqueur de démocratie. Il reconnaît les nouveaux droits, installe une nouvelle autorité indépendante pour protéger les libertés fondamentales.

L'État lui-même se soumet au contrôle de la dite autorité. Ensuite, économiquement parce que le droit susvisé participe à la construction d'une société numérique juridiquement sécurisée et respectueuse des droits de l'homme. Les aspects ci-après doivent être pris en compte dans l'élaboration du cadre juridique national de gestion et de protection des données personnelles.

#### A. Les grands principes devant garantir les droits des citoyens

1. le principe de licéité et de loyauté dans la collecte, le traitement et l'utilisation des données ;

2. le principe d'exactitude des données enregistrées ;

3. le principe de finalité en vue de laquelle est créé un fichier et son utilisation conforme à cette finalité spécifiée, ce principe incluant le principe de proportionnalité, en particulier la durée de conservation qui ne doit pas excéder celle permettant d'atteindre la finalité déclarée ;

4. le principe de l'accès des personnes concernées, ce qui suppose le droit d'obtenir des rectifications ou des destructions de données erronées ou illicites et de connaître les destinataires ;

5. le principe de non-discrimination énoncé dans les termes suivants : " Sous réserve des cas de dérogations limitativement prévus sous le principe 6 (faculté de dérogation), les données pouvant engendrer une discrimination illégitime ou arbitraire notamment les informations sur l'origine raciale ou ethnique, la couleur, la vie sexuelle, les opinions politiques, les convictions religieuses, philosophiques ou autres, ainsi que l'appartenance à une association ou un syndicat, ne devraient pas être collectées";

6. la faculté de dérogation: " des dérogations aux principes 1 à 4 ne peuvent être autorisées que si elles sont nécessaires pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publiques ainsi que, notamment, les droits et libertés d'autrui, spécialement de personnes persécutées (clause humanitaire), sous réserve que ces dérogations soient expressément prévues par la loi ou par une réglementation équivalente prise en conformité avec le système juridique interne qui en fixe expressément les limites et édicte des garanties appropriées. Les dérogations au principe 5 relatif à la prohibition de la discrimination, outre qu'elles devraient être soumises aux mêmes garanties que celles prévues pour les dérogations aux principes 1 à 4 ne pourraient être autorisées que dans les limites prévues par la Charte internationale des droits de l'homme et les autres instruments pertinents dans le domaine de la protection des droits de

l'homme et de la lutte contre les discriminations".

7. le principe de sécurité pour protéger les fichiers contre les risques naturels et humains. Sur la base des principes ci-dessus, certains droits peuvent être proposés aux internautes dès lors que ces données font l'objet d'un traitement, afin de garantir le respect de leur vie privée et assurer leur protection.

#### B. Droits à proposer aux internautes

**Droit d'information :** L'information doit être concise, lisible et facilement accessible. Concrètement, un utilisateur n'a pas besoin d'être un expert pour prendre connaissance de la charte de confidentialité d'un réseau social ou d'une banque et comprendre ce qu'il adviendra de ses données personnelles.

**Droit d'accès :** L'exercice du droit d'accès permet d'obtenir la communication de vos données traitées dans un format compréhensible. Il offre également la possibilité de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer.

**Droit d'opposition :** Le droit d'opposition permet de vous opposer à ce que vos données soient utilisées par un organisme pour une raison précise. Il suffit donc d'arguer « de raisons tenant à votre situation particulière », sauf en cas de prospection commerciale, à laquelle vous pouvez vous opposer sans motif.

**Droit de rectification :** Le droit de rectification permet de corriger des données inexacts vous concernant ou de compléter des données en lien avec la finalité du traitement. Le responsable du fichier est alors en charge de communiquer aux autres destinataires des données sur les rectifications apportées.

**Droit à la limitation du traitement :** Ce droit est associé à ceux de rectification et d'opposition. Si vous contestez l'exactitude des données utilisées par l'organisme ou que vous vous opposez au traitement de vos données, la loi autorise l'organisme à procéder à une vérification ou à l'examen de votre demande pendant un certain délai. Pendant ce délai, vous avez la possibilité de demander à l'organisme de geler l'utilisation de vos données. Inversement, vous pouvez demander directement la limitation de certaines données dans le cas où l'organisme souhaite lui-même les effacer. Cela vous permettra de conserver les données par exemple afin d'exercer un droit.

**Droit à l'oubli numérique ou droit d'effacement :** Le droit à l'oubli numérique existe bel et bien. Qu'il s'agisse d'une photo gênante qui traîne de vous sur la toile ou d'une information collectée par un organisme que vous jugez inutile,



vous pouvez obtenir son effacement si au moins une de ces situations correspond à votre cas : Vos données sont utilisées à des fins de prospection commerciale ; Les données ne sont pas ou plus nécessaires au regard des objectifs pour lesquelles elles ont été initialement collectées ; Vos données ont été collectées lorsque vous étiez mineur dans le cadre de la société de l'information (blog, forum, réseau social ou site web)...

### **Droit au déréférencement**

Vous pouvez faire déréférencer un résultat vous concernant (il doit être associé à votre nom et prénom) depuis un moteur de recherche. Cette suppression ne signifie pas l'effacement de l'information sur le site internet source. Il vous suffit de remplir un formulaire à cet effet.

## **C. Les formalités préalables aux traitements des données**

Dans ce type de cadre national, certaines formalités sont instituées en vue de la protection des données à caractère personnel. Il s'agit de la déclaration, de l'autorisation et de l'avis.

### **1. La déclaration**

Certains traitements de données à caractère personnel obéissent au régime de la déclaration préalable. C'est le régime de droit commun pour la plupart des traitements, qu'ils émanent du secteur public ou de personnes privées. Seulement, certaines dispenses sont prévues. De même, pour les catégories les plus courantes de traitement de données à caractère personnel dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, l'obligation de déclaration peut être simplifiée.

### **2. L'autorisation**

Les traitements de données à caractère personnel peuvent être soumis à autorisation préalable du fait, soit de la nature des données en cause, soit des procédures, conditions ou modalités particulières du traitement. Ainsi, lorsqu'il s'agit de données génétiques ou portant sur la recherche dans le domaine de la santé, de données relatives aux infractions, condamnations ou mesures de sûreté ou enfin de données biométriques, l'autorisation préalable de l'Autorité de protection des données personnelles est requise. Il en est de même lorsque les traitements en cause ont pour objet soit l'interconnexion de fichiers, soit un numéro national d'identification ou tout autre identifiant de portée générale.

## **3. L'avis**

L'avis motivé de l'Autorité de protection des données personnelles est nécessaire pour tous les traitements automatisés d'informations nominatives opérés pour le compte de l'État, d'un établissement public ou d'une collectivité territoriale ou d'une personne morale de droit privé gérant un service public.

Ces traitements portent sur :

1. la sûreté de l'État, la défense ou la sécurité publique ;
2. la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;
3. le recensement de la population ;
4. les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

**La création d'un organe à l'image de la CNIL en France, de la Commission des données personnelles au Sénégal, ou celle du Maroc, notamment une Autorités indépendante pour protéger les libertés fondamentales.**

## **D. Description de l'organe protecteur des données**

La protection des données à caractère personnel devrait être assurée sur le plan organique par une autorité administrative indépendante chargée de veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions légales. Elle informe les personnes concernées et les responsables de traitements de leurs droits et obligations et s'assure que les Technologies de l'Information et de la Communication ne comportent pas de menaces au regard des libertés publiques et de la vie privée. Par ailleurs, elle peut homologuer des chartes d'utilisation qui lui sont présentées et tient un répertoire des traitements de données à caractère personnel. Elle conseille les personnes et organismes qui ont recours au traitement de données à caractère personnel ou qui procèdent à des essais ou expériences de nature à aboutir à de tels traitements

Elle formule les avis, reçoit les déclarations et délivre les autorisations préalables au traitement lorsque celles-ci sont requises. Elle autorise, dans les conditions les transferts transfrontaliers de données à caractère personnel et présente au Gouvernement toutes suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données. Elle coopère avec les autorités de protection des données à caractère personnel des autres pays, publie les autorisations accordées et les avis émis. Elle produit un Rapport annuel de ses activités.

### E. Les contrôles et sanctions

En vue d'assurer les missions qui lui sont confiées, l'autorité administrative indépendante par l'intermédiaire de ses membres et agents peut avoir accès aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel. Elle peut prononcer les mesures suivantes :

1. un avertissement à l'égard du responsable du traitement ne respectant pas les obligations découlant de la présente loi ;
  2. une mise en demeure de faire cesser les manquements concernés dans le délai qu'elle fixe
- Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, Elle peut prononcer à son encontre, après procédure contradictoire, les sanctions suivantes :

1. une sanction pécuniaire dont le montant est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.
2. une injonction de cesser le traitement.
3. l'interruption de la mise en œuvre du traitement pour une durée maximale de 3 mois ;
4. le verrouillage de certaines données à caractère personnel traitées pour une durée maximale de 3 mois ;
5. l'interdiction temporaire ou définitive d'un traitement contraire à la loi.

### F. LES PARTIES PRENANTES ET LES STRUCTURES DE GESTION

- MINPOSTEL/ANTIC/ ART;
- MINFI/ANIF/ CENADI;
- MINAT/ MINDEVEL/BUNEC;
- PRC /DGSN;
- BEAC.

IV. Intensifier le volet coopération internationale en collaboration avec les instruments comme le RGPD, la convention de l'Union Africaine, la Convention 108, la Convention de Budapest du 23 novembre 2001 d'une part et, le renforcement des partenariats institutionnels avec des organisations telles AFAPDP (Association Francophone des Autorités de Protection des Données Personnelles), d'autre part.

V. Accorder la priorité à la communication et à la formation, étant donné que le droit à la protection des données personnelles est un droit relativement nouveau et peu connu.

V-2- Volet technique concernant les organismes chargés de la gestion et la protection des données à caractère personnel

Les organismes chargés de la gestion et la protection de données doivent en permanence, suivant une approche de maîtrise des risques sur lesdites données pouvant porter atteinte à la vie privée des internautes, évaluer leurs niveaux de sécurité. Cette évaluation, pourrait se référer au cadre global constituée des quatre étapes suivantes :

1) Recenser les traitements de données à caractère personnel, automatisés ou non, les données traitées (ex : fichiers client, contrats) et les supports sur lesquels elles reposent :

Les matériels (ex : serveurs, ordinateurs portables, disques durs) ;

Les logiciels (ex : système d'exploitation, logiciel métier) ;

Les canaux de communication (ex : fibre optique, WiFi, Internet) ;

Les supports papier (ex : document imprimé, photocopie)

2) Apprécier les risques engendrés par chaque traitement :

1. Identifier les impacts potentiels sur les droits et libertés des personnes concernées, pour les trois événements redoutés suivants :

- accès illégitime à des données (ex : usurpations d'identités consécutives à la divulgation des fiches de paie de l'ensemble des salariés d'une entreprise) ;

- modification non désirée de données (ex : accusation à tort d'une personne d'une faute ou d'un délit suite à la modification de journaux d'accès) ;

- disparition de données (ex : non détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient).



2. Identifier les sources de risques (qui ou quoi pourrait être à l'origine de chaque événement redouté ?), en prenant en compte des sources humaines internes et externes (ex : administrateur informatique, utilisateur, attaquant externe, concurrent), et des sources non humaines internes ou externes (ex : eau, matériaux dangereux, virus informatique non ciblé)

3. Identifier les menaces réalisables (qu'est-ce qui pourrait permettre que chaque événement redouté survienne ?). Ces menaces se réalisent via les supports des données (matériels, logiciels, canaux de communication, supports papier, etc.), qui peuvent être :- utilisés de manière inadaptée (ex : abus de droits, erreur de manipulation) ;- modifiés (ex : piégeage logiciel ou matériel – keylogger, installation d'un logiciel malveillant) ;- perdus (ex : vol d'un ordinateur portable, perte d'une clé USB) ;- observés (ex : observation d'un écran dans un train, géolocalisation d'un matériel) ;- détériorés (ex : vandalisme, dégradation du fait de l'usure naturelle) ;surchargés (ex : unité de stockage pleine, attaque par dénis de service)

4. Déterminer les mesures existantes ou prévues qui permettent de traiter chaque risque (ex :

contrôle d'accès, sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation).

5. Estimer la gravité et la vraisemblance des risques, au regard des éléments précédents (exemple d'échelle utilisable pour l'estimation : négligeable, modérée, importante, maximale).

6. Mettre en œuvre et vérifier les mesures prévues. Si les mesures existantes et prévues sont jugées appropriées, il convient de s'assurer qu'elles soient appliquées et contrôlées.

7. Faire réaliser des audits de sécurité périodiques. Chaque audit devrait donner lieu à un plan d'action dont la mise en œuvre devrait être suivie au plus haut niveau de l'organisme.

#### **Conclusion :**

En l'état actuel, en ce qui concerne les données personnelles, l'internaute camerounais a la difficulté d'appréhender ses droits et de les faire respecter.

Les organismes qui manipulent les données personnelles au sein du territoire Camerounais n'ont pas assez de contraintes s'agissant de leur engagement quant à la sécurisation des données personnelles.



# PANEL 4

## COOPÉRATION INTERNATIONALE ET RENFORCEMENT DES CAPACITÉS

### MODERATEUR



### Dr. BANGA MBOM Calvin David

Titulaire d'un Doctorat/PhD en Traitement du Signal et Télécommunications de l'Université de Rennes 1 (France), obtenu en 1995.  
Ingénieur Général des Télécommunications (Hors Echelle), diplômé de l'Ecole Nationale Supérieure des Télécommunications de Bretagne (France), promotion 1990.

Il a effectué sa carrière professionnelle au Ministère des postes et télécommunications où il a occupé les fonctions suivantes :

- 1-) Directeur de la Coopération Internationale (2000-2005) ;
- 2-) Conseiller Technique N°1, Chargé du Secteur des Télécommunications (2005- 2009) ;
- 3-) Directeur de la Réglementation du Secteur des Télécommunications (2009- 2013) ;
- 4-) Directeur de la Sécurité des Réseaux et des Systèmes d'Information (2013- 2018) ;
- 5-) Secrétaire Général par intérim (2017-2018).

Actuellement en Retraite, il est Promoteur du Cabinet DIGITALIS.cm, qui fait dans l'expertise et le conseil dans la transformation numérique des administrations et des entreprises.



## PANEL 4 COOPÉRATION INTERNATIONALE ET RENFORCEMENT DES CAPACITÉS

### Exposé 1

# Coopération internationale en matière de cybercriminalité : opportunités et menaces pour le cyberspace national



Presenté par : **Me Balbine MANGA,**  
**Avocat au Barreau du Cameroun**

- Expert Consultante en droit des TIC, de la Cybersécurité, de la cybercriminalité et de la gouvernance de l'internetm;
- Coordinatrice de @JURISTIC ;
- Membre active de la communauté Internet africaine et mondiale.

#### AGENDA

- NOTIONS ET DEFINITIONS;
- ETAT DES LIEUX DE LA CYBER-EXPERTISE;
- QUELQUES ORGANISMES ET INSTITUTIONS;
- COORDINATION MONDIALE DE LA CYBER-EXPERTISE ( le GFCE);
- PERSPECTIVES ET RECOMMANDATIONS.

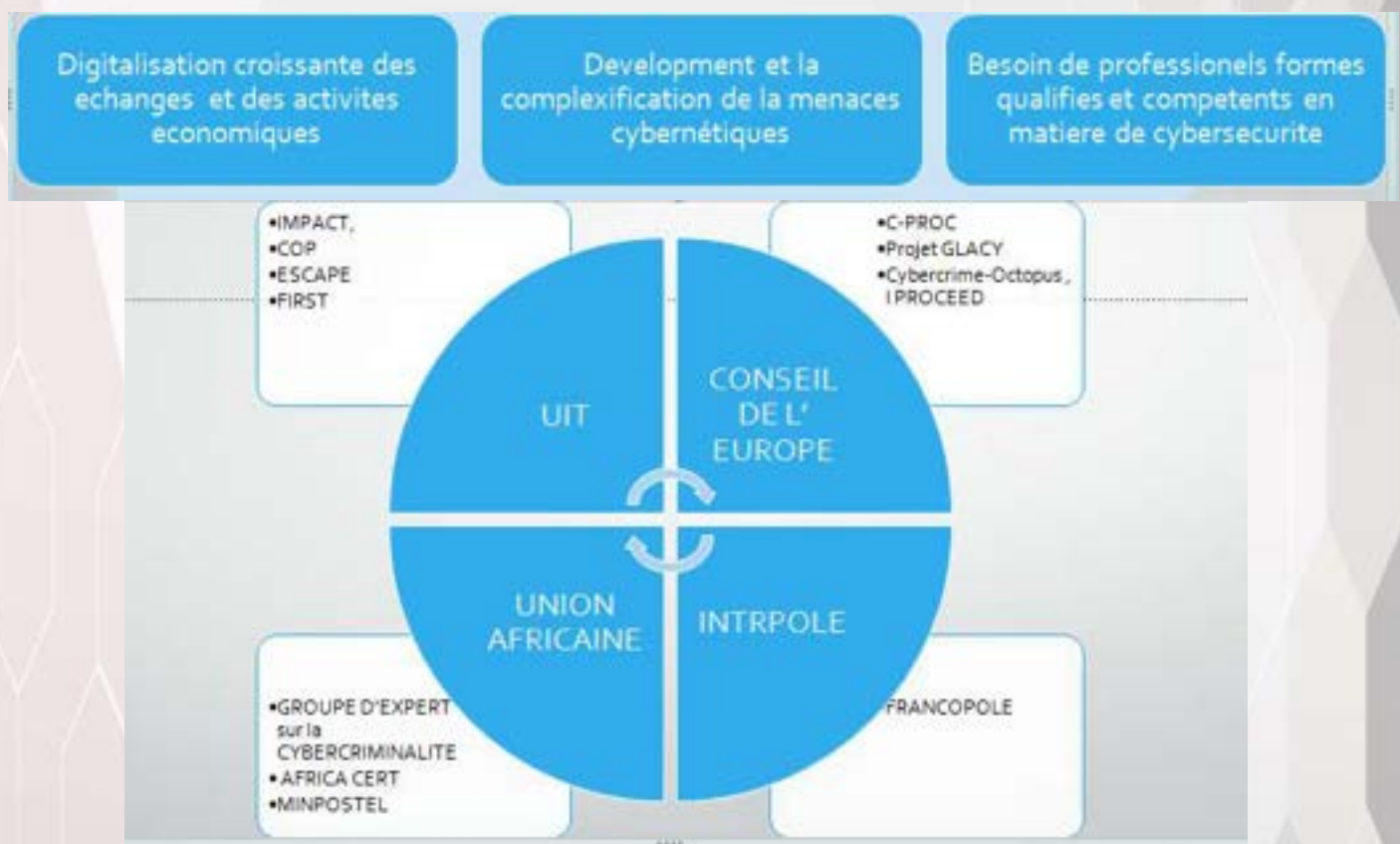
## NOTIONS ET DEFINITIONS

- **CYBERSECURITE:** Moyens, dispositifs, outils, mis en place par les Etats, gouvernements, entreprises pour assurer la protection des systèmes d'information et des données contre les cyber attaques. Installation d'anti- virus, configuration de serveur, gardiennage de data center ou des bureaux

Réaction contre les risques liés à l'omniprésence des TIC et leur capacité d'interconnexion et d'échange de données ; progressivement la cybersécurité se constitue comme une nouvelle discipline, une spécialité;

- **CYBERCRIMINALITE :** Ensemble des infractions et comportements malveillants, commis à l'aide ou au moyen d'un système informatique généralement connecté à un réseau,notamment l'internet;
- **CYBER-RESILIANCE:** Fait référence à la capacité pour une entité, notamment une entreprise à se préparer à affronter de nouvelles menaces, à réagir apres une cyberattaque afin de sauver son activité ;

## ETAT DES LIEUX DE LA CYBER-EXPERTISE



### Le GFCE

Crée le 16 Avril 2015 à la HAYE, lors de la conférence mondiale sur le cyberspace, le Global Forum on Cyber-Expertise (GFCE)

L'objectif majeure est l'identification des politiques, des bonnes pratiques et des projets afin de les dupliquer à l'échelle mondiale;

86 membres dont 06 pays Africains ( TUNISIE, SENEGAL, MAURICE, TANZANIE KENYA, RWANDA)

34 Partenaires

51 événements

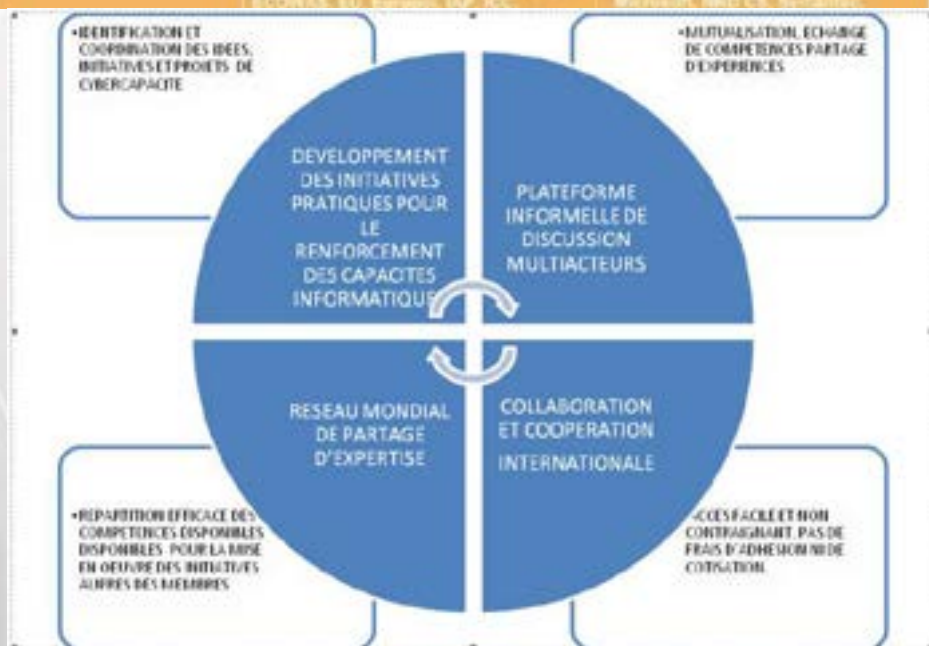




ORGANIGRAMME



Countries	IGOs	Private Organisations
38 states	African Union, Council of Europe, G70, ECOWAS, UN, European IAP, ICC	AT&T, Cisco, HP, Huawei, IBM, Microsoft, NPD CS, Samsung



## LES PERSPECTIVES DU GFCE

- Porte comporte un agenda mondial sur le renforcement des capacités en matière de cybercriminalité, celui-ci a été arrêté lors de la conférence mondiale sur l'espace cybernétique tenue en 2017 à New DHELI ;
- En effet 5 thèmes prioritaires ont été retenus pour le renforcement des capacités cybernétiques avec appel à l'action pour un renforcement conjoint des cybercapacités mondiales;

## AGENDA DU GACCB



## RECOMMANDATIONS

- 1/ Adhésion du CAMEROUN au GFCE pour profiter pleinement des multiples avantages de cette plateforme de travail;
- 2/ Ratifier la Convention de MALABO et celle de BUDAPEST;
- 3/ Voter la loi sur la protection des DCP et veiller à son implémentation;
- 4/ Pérenniser les initiatives nationales existantes, pour la sensibilisation, la formation la collaboration entre entités étatiques, la coopération...





## PANEL 4 COOPÉRATION INTERNATIONALE ET RENFORCEMENT DES CAPACITÉS

### Exposé 2

# FORMATION ET RECHERCHE APPLIQUEE DANS LE DOMAINE DE LA CYBER-SÉCU- RITÉ AU CAMEROUN



Presenté par : **Dr. BELL B.G.**  
**PhD en sécurité des S.I.**  
**Cryptologue**

- Cryptologue, Titulaire d'un PhD en Technical sciences In Methods and Systems of protection of the information, Information security- Cryptologist.
- Diplômé en National Advanced School of engineering-University of Yaounde 1
- Enseignant dans plusieurs universités et grandes écoles du Cameroun
- Directeur Général de ITS ;
- Membre d'Information Systems Audit and Control Association (ISACA)
- Membre d'International Association for Cryptologic Research (IACR)
- Expert judiciaire auprès des Cours d'Appels du Centre et du Littoral

#### OFFRE DE FORMATION

- Management de la sécurité des systèmes d'information;
- Audits et contrôle de la sécurité des systèmes d'information;
- Management des risques de sécurité systèmes d'information;
- Investigations numériques;
- Architecture de sécurité des systèmes d'information;
- cryptographie.

#### Management de la sécurité des SI

##### Activités

- L'élaboration des stratégies et politiques de sécurité des systèmes d'information;
- Mise en place d'un système de management de la sécurité des systèmes d'information;

- Le développement d'un programme de sécurité des systèmes d'information;
- Conduite des projets de sécurité des systèmes d'information;
- Développement des normes et standards en sécurité des systèmes d'information.

#### Audits et contrôle de la sécurité des SI

##### Activités

1. Inventaire et classification des actifs informationnels;
2. Évaluation des mesures de sécurité des SI ;
3. Contrôle et vérification de conformité des mesures de sécurité des SI;
4. Evaluation des impacts du non respect des règles de sécurité des SI.

## Management des risques de sécurité SI

### Activités

1. Inventaire et classification des actifs informationnels;
2. Etude des menaces et vulnérabilités en sécurité des SI;
3. Appréciation des risques de la sécurité des systèmes d'information et leur classification;
4. Evaluation des impacts potentiels;
5. Établissement des plans de traitement des risques;
6. Mise en place des plans de reprise et de continuité d'activités.

### Investigations numériques

#### Activités

1. Recherche de la preuve numérique;
2. Extraction des données cachées, effacées, stéganographiées ou cryptées;
3. Authentification des données numériques;
4. Authentification d'actes numériques;
5. Relevé d'empreintes numériques;
6. Étude et sécurisation de la scène numérique d'infractions;
7. Rédaction de rapports de garde et d'investigation.

## Architecture de sécurité SI

### Activités

1. Normalisation des besoins de sécurité en prenant en compte toutes les dimensions (système, métier etc...);
2. Elaboration des dispositifs techniques de sécurité répondant à des besoins de sécurité, en relation avec des experts techniques ;
3. Estimation du niveau de sécurité d'un dispositif ou système d'information;
4. Gestion des incidents de sécurité pendant la phase d'exploitation, pour en réduire les impacts.

## Cryptographie

- Systèmes de chiffrement;
- Systèmes de signature numérique;
- Systèmes de certification numérique ;
- PKI et applications de confiance verticale;
- Blockchain et applications de confiance horizontale;
- Protocoles de sécurisation de la messagerie et des réseaux.

## Aspects de compétences

1. Juridiques;
2. Techniques;
3. Managériaux.

### Niveaux de compétences

1. Professionnel (Maîtrise quelques tâches d'un domaine de la sécurité des SI);
2. Spécialiste (Maîtrise un ou quelques domaines de la sécurité des SI);
3. Expert (Maîtrise tous les domaines).

## Au niveau professionnel

### Certificats professionnels

- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems controls (CRISC);
- Certified Information Systems Security Professional (CISSP);
- CCNA Security ;
- CEH.

Certificats professionnels locaux (MINEFOP: sécurité des SI; Investigations numériques etc...)

## Au niveau spécialiste

1. Formations universitaires

Masters en sécurité des systèmes d'information dans plusieurs universités au Cameroun

### Masters

- MASSICO – Polytechnique de Yaoundé/AUF;
- MASTER en sécurité des SI – Polytechnique de MAROUA;
- MASTER IT(option sécurité des SI) – SUP'PTIC;
- Plusieurs offres de Master et Licence dans les IPES.

## Au niveau expert

1. Recherche scientifique dans le domaine de la sécurité des systèmes d'information ;
2. Expérience professionnelle forte à partir du niveau spécialiste.



**Recherche appliquée**

• Plusieurs thèmes de recherches abordées depuis plusieurs années, avec des articles scientifiques publiés et des chercheurs formés notamment au sein de l'école doctorale de l'Université de Yaoundé1, dans les laboratoires de recherche à polytechnique de Yaoundé et en faculté des sciences/département d'informatique;

• En 2020, plus de 05 articles publiés dans un groupe de recherche ciblé sur les questions de confiance numérique, notamment la blockchain et les cryptomonnaies, mais aussi sur d'autres question comme la toxicologie numérique.

**Laboratoires**

• Un laboratoire de recherche en cybersécurité disponible à polytechnique (financement FSE);

• Un autre laboratoire en cours d'étude pour mise en place très prochainement à polytechnique de Yde, et qui va s'occuper des questions de cryptologie et de la recherche stratégique.

**Métiers traditionnels en sécurité SI**

1. Manager de sécurité des systèmes d'information;
2. Architecte de sécurité des systèmes d'information;
3. Auditeur de sécurité des systèmes d'information (Profession);
- Investigateur numérique (Profession)
5. Opérateur de sécurité des SI.

**Nouveau Métiers en sécurité SI**

- Mineur cryptographique

Emplois

Postes:

- Responsable de la sécurité des systèmes d'information;

- Spécialiste de sécurité système d'information;

Organisations:

- Banques;

- Administrations et entreprises diverses.

Demande d'expertise:

Limitée du fait de la limitation de la prise en compte de la sécurité SI dans les organisations au Cameroun

**Offre:**

Limitée en qualité et quantité (secteur nouveau)

4 professions formalisées du secteur au Cameroun

1. Deux professions seulement sont agréées

- Auditeur de sécurité des S.I;

- Expert judiciaire en cybercriminalité.

2. Pas d'agrément pour les deux autres professions

- Pas d'agrément pour les éditeurs de logiciels de sécurité;

- Pas d'agrément pour les prestataires de cryptographie et de certification électronique.

**Propositions**

- Définir les profils professionnels et métiers (avec matrice de compétences);

- Formaliser les professions du secteur;

- Améliorer les offres de formations;

- Améliorer la recherche et l'innovation.

**Constat**

Il y a un grand potentiel à creuser dans les métiers de la cybersécurité, il faut donc investir plus dans les formations du domaine.



# *CEREMONIE DE CLOTURE*





# RAPPORT GENERAL

Par : Monsieur NLEND Raphaël,  
Conseiller Technique N°1 du MINPOSTEL,  
rapporteur Général du forum et l'allocution de clôture.



Titulaire d'un Doctorat en Télécommunications, Il occupe le poste de Conseiller Technique N° 1, au Ministère des Postes et Télécommunications.

- I. INTRODUCTION
- II. DEROULEMENT DU FORUM
  - II.1 - Cérémonie solennelle d'ouverture
    - II.1.1 Allocution du Représentant du Bureau de zone de l'UIT pour l'Afrique Centrale et Madagascar
    - II.1.2 Leçon inaugurale
    - II.1.3 Allocution de Madame le Ministre des Postes et Télécommunications
  - II.2 Travaux en plénière
    - II.2.1 Politique, législation et coopération internationale en matière de cybersécurité
    - II.2.2 Infrastructure et technologies de cybersécurité
    - II.2.3 Identification des abonnés
    - II.2.4 Sécurisation des infrastructures critiques
    - II.2.5 Réseaux sociaux
    - II.2.6 Sensibilisation, formation et gestion du changement
  - II.3 Salon d'exposition
- III. RECOMMANDATIONS

## 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 03 au 05 novembre 2020 au Palais des Congrès de Yaoundé, le premier Forum National sur la Cybersécurité et la Lutte contre la Cybercriminalité (FNCC) sur le thème : « cyberspace national et défis sécuritaires ». Le but de ce forum était de susciter des échanges entre experts nationaux autour des défis actuels auxquels l'utilisation du réseau numérique national est confrontée en vue de formuler des recommandations qui permettront de consolider les politiques et stratégies de cybersécurité et de lutte contre la cybercriminalité.

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 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 Représentant du Chef de Bureau de la Commission Economique des Nations Unies

pour l'Afrique Centrale. Elle a été ponctuée par deux (02) allocutions et une leçon inaugurale.

#### II.1.1 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 louer 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 richesse. Cependant, il a déploré les pertes engendrées par les cybercrimes qui sont de l'ordre de 6 milliards de dollars dans le monde entier. Il a affirmé que selon l'indice de cybersécurité mondial (GCI) daté de 2018, le Cameroun occupe le 13ème rang en Afrique et le 91ème rang mondial et qu'avec la dynamique enclenchée, il ne doute pas de l'amélioration de ce classement dans les années à venir. Il a indiqué qu'à l'occasion de ce forum, il conviendrait de faire un diagnostic sans complaisance des faiblesses relevées en matière de cybersécurité afin de proposer les solutions appropriées. D'ores et déjà, l'UIT accompagne les Etats dans le domaine et les principaux problèmes relevés par l'organisation sont notamment l'absence de politique de protection des enfants en ligne, le manque de partenariats régionaux entre les Etats dans la lutte contre la cybercriminalité, le manque de ressources humaines et matérielles, le manque d'interconnexion des infrastructures à l'instar des points d'échange internet des Etats. Face à ces manquements, l'UIT a élaboré et publié des documents importants, à savoir le nouveau guide d'élaboration des stratégies de cybersécurité, un recueil de meilleures pratiques en cybersécurité dans le monde et de nouvelles lignes directrices de protection des enfants en ligne. Il a clos son intervention en invitant les Etats à révolutionner leurs modèles sociétaux de vie et à considérer la cybersécurité comme élément clé de protection de leurs ressources critiques.



### II.1.2 Leçon inaugurale

La leçon inaugurale a été faite par Monsieur Jacques BONJAWO, Ingénieur en informatique, Spécialiste des Questions des TIC dans les pays en développement. En s'appuyant sur le thème du forum intitulé « cyberspace national et défis sécuritaires », l'expert a rappelé le vœu émis par le Chef de l'Etat qui est de faire du Cameroun une nation digitale. Il a défini les problématiques de la cybersécurité et de la cybercriminalité au Cameroun et a présenté le cyberspace en deux mondes, licite et illicite qui se côtoient. Il a relevé par ailleurs qu'il n'existe aucun mécanisme qui permet de garantir la bonne foi de l'internaute. Aussi a-t-il suggéré la mise en place d'un plan d'actions contenant une série d'activités à mener pour faire face aux menaces du monde illicite et qui nécessite de dresser un état des lieux et de faire un diagnostic adéquat. Ces activités sont entre autres l'identification des infrastructures critiques, la définition des mécanismes de protection des enfants en ligne et des données à caractère personnel, le renforcement des capacités humaines et infrastructurelles en cybersécurité, l'élaboration, la mise en œuvre et l'évaluation d'une stratégie nationale de cybersécurité.

### II.1.3 Allocution de Madame le Ministre des Postes et Télécommunications

Dans son allocution d'ouverture, Madame Minette LIBOM LI LIKENG, Ministre des Postes et Télécommunications a

commencé par souhaiter la bienvenue aux experts participants au forum.

Elle 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 temps, une étape supplémentaire de la mise en œuvre sur Très Haute Prescriptions du Chef de l'Etat, de la politique nationale de cybersécurité. Ce regroupement d'experts, a-t-elle ajouté, constitue une phase complémentaire de la réflexion devant accompagner la Campagne d'envergure nationale susmentionnée dont les objectifs sont :

- d'éveiller l'attention des citoyens camerounais sur les menaces en provenance du cyberspace mondial et de susciter leur adhésion dans la mise en place des mesures de cybersécurité ;
- d'attirer l'attention des décideurs et responsables des structures de l'Etat ainsi que des entreprises en vue d'une prise de conscience et de l'implémentation des protocoles de sécurité des réseaux ;
- de sensibiliser toutes les couches sociétales sur l'usage responsable des réseaux sociaux qui sont utilisés de plus en plus à des fins malveillantes ;
- de mettre en place une coalition nationale pour la promotion de l'utilisation citoyenne des réseaux sociaux

Ensuite elle 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, elle a indiqué les menaces auxquelles sont confrontés les usagers et les organisations dans le cyberspace et la nécessité de les endiguer en vue de garantir une confiance totale dans l'utilisation du numérique. Elle a énuméré quelques mesures prises par le Gouvernement camerounais pour lutter contre ce fléau. Enfin, au regard des menaces en constante évolution, elle a exhorté les experts à trouver des solutions appropriées pour assurer la sécurisation du cyberspace camerounais.

### II.2 Travaux en plénière

Quatre (04) panels, composés de vingt-quatre (24) exposés, ont meublé les travaux en plénière. Les présentations et les échanges ont couvert globalement les domaines suivants : politique, législation et coopération internationale en cybersécurité ; infrastructure et technologie de cybersécurité ; identification des abonnés ; sécurisation des infrastructures critiques ; sécurisation des réseaux sociaux ; sensibilisation, formation et gestion du changement.

#### II.2.1 Politique, législation et coopération internationale en matière de cybersécurité

S'agissant de la politique, de la législation et de la coopération internationale en matière de

cybersécurité, il a été relevé que le Cameroun dispose d'un plan stratégique de développement de l'économie numérique comportant un volet se rapportant au renforcement de la confiance numérique.

Le Cameroun dispose également d'une politique et d'une stratégie nationale de cybersécurité. Au registre des textes juridiques, il existe la loi N°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun et ses textes d'application ; la loi N°2010/013 du 21 décembre 2010 sur les communications électroniques au Cameroun, modifiée et complétée par la loi N°2015/006 du 20 avril 2015 ; la loi N°2015/007 du 20 avril 2015 régissant l'activité audiovisuelle au Cameroun, ainsi que le code de procédure pénale. S'agissant du cas particulier de l'encadrement des données à caractère personnel, il n'existe pas de cadre juridique spécifique encadrant la protection des données à caractère personnel. Par conséquent, l'internaute camerounais a des difficultés à faire prévaloir ses droits en la matière. Aussi, les organismes qui manipulent les données personnelles au sein du territoire camerounais n'ont pas assez de contraintes s'agissant de leur engagement sur la sécurisation des données à caractère personnel.

Dans le but de garantir un environnement numérique sain, plusieurs structures interviennent dans la mise en œuvre de la politique du gouvernement en matière de cybersécurité et de cybercriminalité, au rang desquelles on peut citer :

- le Ministère des Postes et Télécommunications qui, à travers sa Direction de la Sécurité des Ré-

seaux et des Systèmes d'Information, est chargé de l'élaboration et du suivi de la mise en œuvre de la politique nationale en matière de sécurité des communications électroniques et des systèmes d'information ;

- le Ministère de la Justice qui est chargé de la poursuite et du jugement des auteurs des infractions et éventuellement de leur répression ;

- le Ministère de la Défense qui est chargé d'assurer les missions de cyberdéfense à travers la création de plusieurs structures y dédiées, notamment les services spécialisés de la Gendarmerie Nationale et les unités/cellules en charge de la cyberdéfense dans certaines formations opérationnelles ;

- l'ANTIC qui assure pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des réseaux de communications électroniques en collaboration avec l'ART ;

- la DGSN, la DGRE et INTERPOL qui participent à la lutte contre la cybercriminalité, notamment en matière d'investigations numériques ;

- le Conseil National de la Communication (CNC) qui régule les activités des médias audiovisuels. S'agissant du cas spécifique des audits de sécurité, 138 structures ont été auditées à date. Il ressort des résultats issus des audits que les ministères et les établissements publics ont un niveau de maturité moyen de 29,23% qui est en deçà du seuil de 60% requis, tandis que les établissements de microfinance, les opérateurs ainsi que les FAI ont des niveaux de maturité respectifs de 64,55% et 63,11% supérieurs à la valeur requise.

Cependant, les disposi-

tions spécifiques liées aux investigations numériques ne sont pas clairement précisées dans le code de procédure pénale. Par ailleurs, il est noté un déficit d'expertise en cybercriminalité dans la chaîne judiciaire.

En outre, les demandes d'assistance avec des pays étrangers susceptibles d'héberger les auteurs d'infractions criminelles sur le territoire national n'aboutissent pas toujours du fait de l'insuffisance du cadre juridique existant en matière de coopération et d'entraide judiciaire. De même, la coordination des structures en charge de la lutte contre la cybercriminalité est insuffisante et manque de lisibilité. Quant à la cyberdéfense, les réflexions juridiques sur la cyber-conflictualité n'ont pas encore abouti. Concernant les audits de sécurité, il n'existe aucune réglementation qui contraint les structures auditées à appliquer les recommandations faites.

En ce qui concerne la problématique de la protection des enfants en ligne, il a été relevé qu'actuellement, un internaute sur trois est un enfant. L'internet regorge de nombreux avantages qui permettent aux enfants de séduire, se divertir et garder les liens sociaux avec leurs proches. Cependant, 51% des enfants sont exposés à divers risques et préjudices en ligne et 44% des enfants exposés à des menaces en ligne subissent des conséquences plus tard dans leur vie.



## II.2.2 Infrastructure et technologies de cybersécurité

Le Cameroun a mis en place plusieurs infrastructures de cybersécurité, notamment le Centre de prévention et de réponse aux incidents cybernétiques (CIRT), l'infrastructure nationale à clé publique (PKI) à l'ANTIC, les laboratoires d'investigation numérique à la DGSN et à l'ENSPY.

Le CIRT est chargé de monitorer en permanence le cyberspace dans le but de détecter les menaces cybernétiques et de les endiguer. Il a permis aux forces de maintien de l'ordre de conduire plus de cinq mille (5000) investigations numériques. Par ailleurs, 5000 vulnérabilités ont été détectées dans 85 sites web et applications sensibles de l'administration publique et des entreprises privées. Un taux de disponibilité moyen de 88% a été évalué sur 175 sites web monitorés. Le CIRT a également certifié 35 pages Facebook et comptes des Ministres et hautes personnalités de l'Etat.

Les problèmes rencontrés dans l'exploitation de cette infrastructure se rapportent à l'absence d'un cadre de collaboration avec les fournisseurs de service en ligne comme Google, Facebook, Yahoo, Amazon, WhatsApp. De même, il n'existe pas de cadre réglementaire et technique encadrant les activités du CIRT.

L'infrastructure à clé publique (PKI) vise à sécuriser les données et les échanges électroniques. Cette infrastructure a déjà sécurisé quatre (04) applications à savoir : l'application COLEPS du Ministère des marchés publics ; le site web et la messagerie électronique du MINESUP ; le Guichet Unique des opérations de commerce extérieure et l'application CAMCIS de la Douane camerounaise.

Cependant, l'insuffisance d'expertise en matière de sécurisation des applications, la non prise en compte du volet sécurité dans le développement des systèmes et la faible standardisation de l'infrastructure sont les faiblesses relevées dans le développement de la PKI.

La Blockchain est une technologie de stockage et de transmission d'informations transparente, sécurisée et fonctionnant sans organe central de contrôle. C'est une base de données sécurisée et dis-

tribuée qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. La blockchain peut être utilisée dans plusieurs domaines comme les finances, la santé, les transports, la fiscalité, etc.

Cependant, son utilisation au Cameroun n'est pas exempte de toutes préoccupations. Il n'existe pas de cadre réglementaire régissant la blockchain au Cameroun. Son utilisation fait courir au Cameroun le risque de blanchiment d'argent et d'escroquerie à grande échelle. Bien plus, l'expertise en la matière reste embryonnaire dans notre pays.

## II.2.3 Identification des abonnés

S'agissant de l'identification des abonnés, les statistiques révèlent que 99,99% des usagers des réseaux des opérateurs de télécommunications sont identifiés. Cependant, certaines identifications restent erronées du fait de l'usurpation d'identité, de la présentation des fausses pièces d'identité, et de l'utilisation abusive des pièces d'identité retrouvées dans les rues.

## II.2.4 Sécurisation des infrastructures critiques

Le Cameroun dispose d'infrastructures critiques dans plusieurs secteurs, notamment les infrastructures de télécommunications, et les infrastructures bancaires, etc.

Les infrastructures de télécommunications font généralement face aux menaces telles que les détournements de trafic, les infections virales, les dénis de service, les intrusions, les actes de vandalisme, les coupures récurrentes de la fibre optique, etc. Au registre des conséquences, l'on relève des pertes financières énormes, l'atteinte à l'image et à la réputation des entreprises victimes, l'interruption de services, la divulgation des données sensibles, le vol ou l'usurpation d'identité. Cette situation est amplifiée en raison de l'absence d'un cadre approprié pour la protection des infrastructures critiques au Cameroun.

Quant aux infrastructures bancaires, elles sont généralement victimes du phishing, du scamming, du hacking des cartes de crédits, des distributeurs et des applications et plateformes financières en ligne.

Les solutions proposées pour relever les problèmes rencontrés sont généralement la mise en place des outils de sécurité tels que les dispositifs de contrôle d'accès, la gestion des identités, la maintenance préventive, les firewalls, les logiciels ou applications de veille et d'audit, les audits journaliers, mensuels et annuels, les proxy.

### II.2.5 Réseaux sociaux

Le Cameroun compte 3,7 millions d'utilisateurs des réseaux sociaux correspondant à un taux de 14% de sa population totale. Les accès aux réseaux sociaux de l'ordre de 97% se font généralement à travers des terminaux mobiles. Ces réseaux sociaux permettent de renforcer chez leurs utilisateurs les interactions sociales.

Cependant, les usagers et les entreprises sont exposés aux risques d'escroquerie, d'usurpation d'identité, de chantage, de vol d'information, de cyberharcèlement, de désinformation et de diffamation. Par ailleurs, les Etats courent des risques de manipulation de l'opinion publique, de propagation de fausses nouvelles, de cyberterrorisme, d'espionnage, d'atteinte à la souveraineté. Bien plus, l'utilisation des réseaux sociaux s'effectue parfois au détriment des règles élémentaires de sécurité entraînant ainsi la divulgation des informations sensibles.

### II.2.6 Sensibilisation, formation et gestion du changement

Concernant la sensibilisation, des campagnes sont organisées par le Ministère des Postes et Télécommunications comme celle relative à la promotion de la culture de la cybersécurité et de l'utilisation responsable des réseaux sociaux faite de séminaires, d'ateliers de sensibilisation, de diffusion de messages à travers le réseau Internet, la presse écrite et les chaînes de radios et de télévision. Dans le même ordre d'idées, l'ANTIC tient des rencontres annuelles sur les questions de cybersécurité et de lutte contre la cybercriminalité. Ces campagnes sont appelées à se poursuivre dans les prochaines années.

Pour ce qui est de la formation, plusieurs universités offrent des masters en sécurité des systèmes d'information. Par ailleurs, certains instituts nationaux sont agréés pour offrir des formations certifiantes en cybersécurité, en partenariat avec des

organismes internationaux tels qu'ISACA, CISCO, etc. En outre, il existe au niveau international un forum global sur la cyberexpertise regroupant 86 pays membres dont six (06) pays africains et trente-quatre (34) partenaires et auquel le Cameroun ne fait pas partie.

Dans le registre des difficultés rencontrées, il n'y a que deux professions agréées en sécurité des systèmes d'information, le reste des professions opère dans l'informel. De même, l'offre en formation demeure insuffisante au regard des besoins en expertise. Par ailleurs, il n'existe pas encore de programme national formel de sensibilisation à la cybersécurité couvrant une grande partie de la population et les moyens alloués aux campagnes de sensibilisation sont insuffisants par rapport aux objectifs à atteindre. On note également que la recherche en cybersécurité est quasi inexistante.

### 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 Ministre des Postes et Télécommunications, a connu la participation des structures publiques et privées suivantes : le MINPOSTEL, l'ANTIC, CAMTEL, MTN, ALOE, AFRILANE, ENIX SARL, INTELLEM SYSTEMS SARL, ESOKA CYBERSECURITY DIVISION, INSTITUTE OF PROFESSIONAL EXCELLENCE (IPE), INFORMATION TECHNOLOGIE ET SECURITE (ITS), INTERTECH GROUP.

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 politique, de la législation et de la coopération internationale en matière de cybersécurité ;
- de l'identification des abonnés des réseaux de communications électroniques ;
- des infrastructures et technologies de cybersécurité ;



Pour ce qui est de la politique, de la législation et de la coopération internationale en matière de cybersécurité, il a été suggéré :

- de ratifier les conventions de Budapest sur la cybercriminalité et de Malabo sur la cybersécurité et la protection des données à caractère personnel ;
- de réviser la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun dans le but de renforcer le régime des sanctions administratives et pénales notamment la qualification des infractions et l'aggravation des peines liées aux infractions commises dans le cyberspace.
- d'élaborer, d'adopter et de promulguer la loi sur la protection des données à caractère personnel et de veiller à son implémentation ;
- de mettre en place une structure autonome en charge de la protection des données à caractère personnel ;
- d'élaborer un texte réglementaire contraignant les organisations à mettre en œuvre les recommandations issues des audits de sécurité;
- de réviser la réglementation relative aux audits de sécurité en vue d'astreindre les administrations publiques à un audit de sécurité annuel obligatoire ;
- de conduire à terme les réflexions juridiques sur la cyber-conflictualité ;
- de favoriser une collaboration accrue des services de cybersécurité au niveau national, sous régional et international ;
- de produire annuellement les statistiques dans le domaine de la cybersécurité et de celui de la cybercriminalité;
- de revoir les cadres organiques des départements ministériels afin d'y intégrer des structures spécifiques en charge de la sécurité des systèmes d'information;
- de favoriser le développement local des outils de cybersécurité et de cyberdéfense.
- de mettre en place un cadre juridique qui édicte les normes d'audit de sécurité des réseaux et des systèmes d'information ;
- d'allouer des budgets conséquents dédiés aux activités de cybersécurité dans les administrations publiques et privées;
- de mettre en place une plateforme de lutte contre la cybercriminalité en vue de renforcer les actions de coordination des différentes entités chargées de lutter

contre la cybercriminalité au niveau national, sous régional et international ;

- de mettre en place une coopération solide avec les géants du numérique que sont les GAFAM (Google-Apple-Facebook-Amazon-Microsoft) et BATX (Baidu – Alibaba – Tencent – Xiaomi) ;
- de mettre en place un cadre réglementaire régissant la blockchain au Cameroun ;
- de s'approprier les lignes directrices élaborées par l'UIT et d'autres organisations internationales œuvrant dans la protection des enfants en ligne ;
- de finaliser l'élaboration de la charte de protection des enfants en ligne, l'adopter et la vulgariser ;
- d'adhérer à l'initiative de protection des enfants en ligne de l'UIT ;
- de mettre en place un Groupe de Travail devant préparer l'environnement technique nécessaire aux exigences de coopération nationale et internationale en matière d'investigation numérique ;
- d'impliquer les administrations dans la préparation coordonnée de la participation du Cameroun à la Conférence Mondiale du développement des Télécommunications (CMDT) 2021 ainsi qu'à d'autres événements en charge des questions de cybersécurité ;
- de mettre en place un Groupe de Travail pour l'élaboration du manuel de procédures d'investigation numérique.

S'agissant de l'identification des abonnés des réseaux de communications électroniques. Il a été préconisé :

- de mettre en place une plateforme numérique centralisée d'identification des abonnés et des équipements terminaux des réseaux de communications électroniques interagissant avec les bases de données d'identification de la DGSN et des opérateurs de téléphonie.

S'agissant des infrastructures de cybersécurité. Il a été demandé :

- de privilégier dans la mobilisation de l'expertise nationale en matière de sécurité, la conduite des formations certifiantes ;

- de conformer la PKI nationale aux normes internationales;
- de sensibiliser les administrations à la prise en compte du volet sécurité dans le développement des applications ;
- de mettre en place un cadre réglementaire et technique encadrant les activités du CIRT (Computer Incident Response Team) et du SOC (Security Operating Center);
- de mettre en place un SOC national et des SOC sectoriels.

S'agissant de la sécurisation des infrastructures critiques. Il a été recommandé :

- de sensibiliser et de renforcer en permanence les capacités des équipes techniques en charge de l'exploitation des infrastructures critiques ;
- d'acquérir et de déployer des outils techniques de pointe afin de protéger les infrastructures critiques du cyberspace Camerounais ;
- d'assurer la veille sécuritaire des infrastructures critiques du cyberspace ;
- de promouvoir la création des datacenter sécurisés au niveau national ;

En ce qui concerne les réseaux sociaux. Il a été proposé :

- de mettre sur pied une plateforme de surveillance et de répression des actes illicites sur les réseaux sociaux ;
- de mettre en place une plateforme chargée de certifier l'authenticité des informations publiées dans les réseaux sociaux ;
- de promouvoir la création des réseaux sociaux nationaux afin de prévenir la manipulation des masses.

S'agissant de la sensibilisation, de la formation et la gestion du changement, il sera question :

- de définir les profils professionnels et les métiers avec des matrices de compétences ;
- de favoriser l'émergence d'une masse critique d'experts nationaux capables non seulement de développer et d'administrer une PKI mais également d'intégrer ses fonctionnalités dans les applications en ligne ;
- de formaliser les professions du secteur ;
- de faciliter l'appropriation des textes spécifiques du secteur par les acteurs institutionnels (magistrats, Of-

ficiers de Police Judiciaire) ;

- de former notamment les OPJ aux techniques d'investigation dans le cyberspace ;
- d'améliorer les offres de formations de cybersécurité;
- d'améliorer la recherche et l'innovation dans le domaine de la cybersécurité;
- de faire adhérer le Cameroun au Global Forum on Cyber-Expertise (GFCE) pour profiter pleinement des multiples avantages de cette plateforme de travail ;
- d'intensifier et de pérenniser les initiatives nationales existantes, pour la sensibilisation et la formation en matière de cybersécurité et de lutte contre la cybercriminalité ;
- de favoriser l'intégration des modules de formations relatifs à la blockchain dans les cursus académiques du domaine des TIC ;
- de renforcer les capacités des personnels de l'administration publique et du secteur privé en matière de blockchain ;
- d'allouer plus de ressources financières dédiées à la recherche en cybersécurité.

Au vu des recommandations formulées au cours de ce forum et de l'importance de leur mise en œuvre pour l'émergence d'un cyberspace camerounais plus sûr, il a été suggéré, pour plus d'efficacité, de mettre en place un Groupe de Travail coordonné par le MINPOSTEL et chargé du suivi et de l'évaluation de leur implémentation./-



## DISCOURS DE CLOTURE DU REPRESENTANT DU MINISTRE DES POSTES ET TELECOMMUNICATIONS



Par : **Monsieur MOHAMADOU SAOUDI,**  
**Secrétaire Général du Ministère des**  
**Postes et Télécommunications**

**Monsieur le Représentant du Bureau de zone de l'Union Internationale des Télécommunications pour l'Afrique Centrale et Madagascar;**  
**Monsieur le Représentant du Bureau sous-régional de l'Afrique Centrale de la Commission Economique des Nations Unies pour l'Afrique;**  
**Monsieur le Représentant Résident de l'Institut Africain d'Informatique pour le Cameroun ;**  
**Messieurs les Inspecteurs Généraux ;**  
**Mesdames et Messieurs les Directeurs Généraux ;**  
**Mesdames et Messieurs les experts et représentants des administrations en charge de la sécurité des réseaux et des systèmes d'information ;**  
**Chers Invités.**

C'est avec un immense honneur et un plaisir renouvelé que je prends à nouveau la parole devant vous à l'occasion de la cérémonie de clôture du premier forum national sur la cybersécurité et la lutte contre la cybercriminalité au Cameroun, qui s'est déroulé du 03 au 05 novembre 2020 sous le

thème : « cyberspace national et défis sécuritaires ».

Ma joie est d'autant plus grande que j'ai suivi avec un intérêt grandissime le rapport général sanctionnant les travaux ainsi que les recommandations qui ont découlé de vos multiples et intenses réflexions. Des travaux, qui selon ce qui m'est revenu, se sont déroulés dans une ambiance sereine, participative et d'une assiduité exemplaire. En effet, pendant trois jours, vous n'avez ménagé aucun effort pour apporter votre contribution à l'édification d'un cyberspace camerounais sûr et sain.

**Distingués Invités ;**

**Mesdames et Messieurs ;**

L'organisation du premier forum national sur la cybersécurité et la lutte contre la cybercriminalité visait à regrouper autour d'une table les experts du domaine afin de confronter leurs points de vue dans le but d'avoir une vision commune de la lutte contre la cybercriminalité.

En effet, suite aux Très Hautes Prescriptions du Chef de l'Etat, le 31 décembre 2015, dans son traditionnel message de fin d'année à la nation je cite : «... Il nous faut rattraper au plus vite notre retard dans le développement de l'économie numérique. Celle-ci est un véritable accélérateur de croissance, en plus d'être une véritable niche d'emplois nouveaux pour notre jeunesse...», le Ministère des Postes et Télécommunications a pris ses responsabilités en élaborant le plan stratégique Cameroun numérique 2020, avec la participation des administrations publiques, privées et de la société civile. L'axe 5 de cette stratégie est consacré à la confiance numérique dont le plan d'actions prioritaires correspondant prévoit chaque année, l'organisation des fora nationaux dans le domaine de la cybersécurité. C'est dans cet optique que ce forum national a été organisé.

Le forum national sur la cybersécurité et la lutte contre la cybercriminalité aura été l'occasion d'un vrai brassage d'idées. Les experts venant des administrations publiques, privées, ainsi que de la société civile ont échangé et apporté leurs contributions à la réflexion sur les méthodes les plus efficaces pour sécuriser notre cyberspace.

Je saisis cette occasion pour vous faire savoir que Notre Département Ministériel est engagé sur d'autres fronts dans le domaine de la cybersécurité, notamment la mise à niveau du cadre juridique et réglementaire, l'élaboration d'un projet de loi sur la protection des données à caractère personnel, la

ratification des conventions de Budapest sur la cybercriminalité, de Malabo sur la cybersécurité et la protection des données à caractère personnel, l'élaboration d'une charte de protection des enfants en ligne et le renforcement du processus d'identification des abonnés pour ne citer que ceux-là.

Grâce à votre expertise avérée et à votre engagement, nous avons pu aboutir à des propositions constructives. De vos échanges, il en est sorti des recommandations pertinentes. C'est l'occasion de me réjouir des résultats éloquentes auxquels vous êtes parvenus au terme de vos travaux et dont je ne pouvais d'ailleurs douter au regard de la qualité des participants que vous êtes. Par conséquent, j'exhorte toutes les parties prenantes, chacun en ce qui le concerne à mettre en œuvre les recommandations issues de ce forum.

Je me réjouis également de l'ambiance qui a régné au sein des panels.

C'est le lieu pour moi de saluer fortement Monsieur Jacques BONJAWO pour sa leçon inaugurale et celle de tous les intervenants.

C'est sur cette note de satisfaction totale que je déclare clos les travaux du premier forum national sur la cybersécurité et la lutte contre la cybercriminalité au Cameroun.

**Vive le Cameroun ;**

**Vive Son Excellence Paul BIYA ;**

**Je vous remercie de votre aimable attention./-**



# AGENDA

PREMIERE JOURNEE : 03 Novembre 2020		
Horaire	Activité	Observations
08h30 – 09h30	Arrivée et enregistrement des participants/ <i>Participants registration</i>	
<b>Début des travaux</b>		
<b>PANEL 1 : Aperçu global de la <u>cybersécurité</u> au Cameroun</b>		<b>Modérateur</b> NGAE Denis
09h30 – 09h50	Cybersécurité : concepts, enjeux et défis	MINKA MI NGUIDJOI Thierry Emmanuel
09h50 – 10h10	Cadre institutionnel et réglementaire	POKOSSY BELLE EMMANUEL
10h10 – 10h30	Infrastructures et mesures techniques de cybersécurité : CERT national et SOC	M. MBUH Godlove MBUH
10h30 – 10h45	<b>Pause-café/ coffee break</b>	
10h45 – 11h05	Infrastructures et mesures techniques de cybersécurité : PKI national et E-GOV	M. GBITHICKI NDANGA Brice
11h05 -11h25	Infrastructures et mesures techniques de cybersécurité : Audits de sécurité	M. MOLEMB Beal Cyrille Augustin
11h25-12h45	<b>Echanges</b>	
<b>Cérémonie solennelle d'ouverture</b>		
13h00 – 14h00	<ul style="list-style-type: none"> <li>▪ Allocution du Représentant du Bureau de Zone de l'Union Internationale des Télécommunications (UIT) pour l'Afrique Centrale et Madagascar ;</li> <li>▪ Intermède ;</li> <li>▪ Leçon inaugurale par M. Jacques BONJAWO ;</li> <li>▪ Intermède ;</li> <li>▪ Discours d'ouverture de Madame le MINPOSTEL ;</li> <li>▪ Photo de famille ;</li> <li>▪ Coupure du ruban symbolique par Madame le MINPOSTEL et ouverture du salon ;</li> <li>▪ Visite des stands Madame le MINPOSTEL et sa suite;</li> <li>▪ Echanges avec la presse</li> </ul>	
14h00 – 15h00	<b>Buffet d'ouverture/Opening buffet</b>	
15h00 – 18h00	<b>Visite des stands par les participants et visiteurs</b>	
18h 00	<b>Fin de la journée</b>	

<b>DEUXIEME JOURNEE : 04 Novembre 2020</b>		
<b>Horaire</b>	<b>Activité</b>	<b>Observations</b>
<b>PANEL 2 : Stratégies de mise en œuvre de la cybersécurité au Cameroun</b>		<b>Modérateur</b> NDONGO Paul Petit
09h00 – 10h40 20 min/exposé	cybersécurité dans les infrastructures de télécommunications	CAMTEL/MTN/ORANGE/ NEXTTEL/ YOOME/ (5 exposés)
10h40- 11h00	<b>Pause-café/ coffee break</b>	
11h00 –11h20	Cybersécurité dans les infrastructures bancaires	<b>Mme EKOLLO</b> <b>Françoise</b>
11h20 –11h40	stratégies et mesures de régulation sur l'identification des abonnés des opérateurs de télécommunications	<b>M. MENGANG</b> <b>BEKONO</b>
11h40 –12h00	Blockchain et sécurisation de la cryptomonnaie	MOUDZE TATSUM Cédric
12h20 -12h40	Stratégies et mesures de cyberdéfense	Col. NDONGO MVE
12h40 -13h30	<b>Echange</b>	
13h30 –14h30	<b>Pause-déjeuner/ lunch break</b>	
<b>Panel 3 : Lutte contre la cybercriminalité au Cameroun</b>		<b>Modérateur</b> <b>OTTOU Valery</b>
14h30 – 14h50	Procédures et techniques d'investigations à la preuve numérique : Cas pratiques	<b>Dr BELL</b> <b>BITJOGA Georges</b>
14h50 – 15h10	La police camerounaise face à la cybercriminalité : Quels défis et quelles attentes	OP2. OBA-ELLE Guy Roland (DGSN)
15h10 – 15h30	Cybercriminalité et réponse à la justice pénale	LOGMO II Achille
15h30 – 15h50	Réseaux sociaux : opportunités et menaces	Dr. EYOUM Gérard
15h50 -16h05	<b>Pause-café/ coffee break</b>	
16h05 – 16h25	Stratégie de protection des enfants en ligne.	ZONGO Serge
16h25 – 16h45	Gestion et protection des données à caractère personnel	WANGUE David Brice
16h45 – 17h45	<b>Echanges</b>	
17h45	<b>Fin de la deuxième journée</b>	



<b>TROISIEME JOURNEE : 05 Novembre 2020</b>		
<b>Horaire</b>	<b>Activité</b>	<b>Observations</b>
<b>PANEL 4 : Coopération Internationale et renforcement des Capacités</b>		<b>Modérateur</b> BANGA MBOM Calvin
09h30 – 09h50	Coopération internationale en matière de cybercriminalité : opportunités et menaces pour le cyberspace national	Laurent GIUSEPPE-RENZO D'ARONCO
09h50 – 10h10	Coordination internationale des mesures légale et réponses aux incidents du cyberspace	INTERPOL
10h10 – 10h30	Cyber-expertise et organisations internationales	Me <u>Balbine</u> MANGA
10h30 -10h45	<b>Pause-café/ coffee break</b>	
10h45 – 11h05	Formation et recherche appliquée matière de cybersécurité dans les universités camerounaises.	<b>Dr BELL BITJOGA Georges</b>
11h05 – 12h05	<i>Echanges</i>	
12h05 – 13h05	Préparation du rapport et recommandations	Dr NLEND Raphaël Equipe des rapporteurs
13h05- 14h00	<b>Finalisation du rapport</b>	<b>Dr. Ing. NLEND Raphaël</b>
<b>14h00 – 15h00</b>	<b>Cérémonie de clôture du forum</b> <ul style="list-style-type: none"> <li>▪ Lecture du rapport final</li> <li>▪ Discours de clôture</li> </ul>	
<b>15h00 -15h30</b>	<b>Cocktail de clôture / Closing cocktail</b>	
<b>15h30</b>	<b>Fin de la troisième journée et fin forum</b>	

# LISTE DES PARTICIPANTS

Réf.	NOMS ET PRÉNOMS	TÉLÉPHONE	E-MAIL
1.	KAMEGNE FOM ERIC	693337018	rickyfom@yahoo.fr
2.	MBUH GODLOVE MBUH	676156932	godlove.mbuh@cirt.cm
3.	ANOGONO BENOIT THIERY	696086956	btanogono@gmail.com
4.	WITOMO LASSANDA	699690958	lassandaw@crtv.cm
5.	BRAHIM MOUTA . M	699508796	mounirmouta57@gmail.com
6.	BABEY DIMLA TONNY	675340041	babeytonna@gmail.cm
7.	SAMOU DPETCHOUA LESLIE	693968927	lesliesamou@gmail.com
8.	MINKA MI NGUIDJOI	675481433	
9.	OSSOU ONDO RODY	697171692	
10.	BANJEM ELISABETH	696155404	banjem02@yahoo.fr
11.	EVINA PIERRETTE ANNIE	699925191	bityebiyaa@yahoo.fr
12.	TEGOUFACK ZEUFACK MIREILLE	696733578	mimitegou@gmail.com
13.	NANA DIANE CAROLE	675792071	nadianecarole@yahoo.fr
14.	BIYONG SAMUEL	655975673	
15.	YVES ETOUNDI	693524528	Yvindongo614@gmail.com
16.	MENGUE ETEME	658553094	
17.	MAMOUKO RAISSA	679627907	mkraissa@yahoo.fr
18.	JAPHET DJETABE	674441734	Japhetdjetebe86@gmail.com
19.	FOTIE EUGÈNE	699456540	Eugene.fotie@minpostel.gov.cm
20.	GNOGA DIKDIM CHARLES	693072701	gdikdim@yahoo.fr
21.	ERNEST AKWA TAKU	677428525	ernstaku@yahoo.fr
22.	ATEMFACK TASSIADA CELINE	677436966	atemfackceline@gmail.com
23.	EFANDEN PATRICE OLIVIER	699436758	pefanden@gmail.com
24.	NGAE DENIS	693066376	denisngae@yahoo.fr
25.	NDO MBARGA SERGE	699434293	sergendos@gmail.com
26.	KOMBE HENRY PASANG	677522028	Kombeh91@gmail.com
27.	NGON NLEP ROMY	699341318	romynlep@gmail.com
28.	POKOSSY BEUE	699616567	bpokossy@yahoo.fr
29.	ESSONO NGUINI PARFAIT JOËL	699322518	eparfaitjoel@gmail.com
30.	TCHOUANANG ALAIN	699970483	alain.tchouanang@minpostel.gov.cm
31.	KAMGA PASCAL	690587576	kamgapascal@yahoo.fr



Réf.	NOMS ET PRÉNOMS	TÉLÉPHONE	E-MAIL
32.	KOULTCHOUMI SEHOU	699455493	ksehou@yahoo.fr
33.	EHET BEAL SYLVIN	665187707	Sylvin.ehet@nexttel.com.cm
34.	ERIC PENDA	677431019	ericpenzo@yahoo.fr
35.	NDE NINGO	677744180	ningonde@hotmail.com
36.	GAMO GAMO NADEGE	699045957	carine.gamo@antic.cm
37.	GBITHICKI NDANGA	699088538	brice.ndanga@antic.cm
38.	OBADA	698993887	
39.	TONGA TONGA YVES OLIVIER	677977488	yvestonga2002@yahoo.fr
40.	AZOMBO ZANG	699876262	azombozyl@yahoo.yahoo.fr
41.	BAMA-SI FRANCK	661000101	Arnoldbama2005@yahoo.fr
42.	AKONO THEODORE	699074925	<a href="mailto:akonothedore@yahoo.fr">akonothedore@yahoo.fr</a>
43.	NLEND RAPHAEL	693066386	rnlend@yahoo.com
44.	NGNOGA DIKDIM Charles	693072701	gdikdim@yahoo.fr
45.	DJASEP THIERRY	699553641	Djasep2000@gmail.com
46.	AWOULOU MENGUE FRANCK	699244165	Awoulou.franck@gmail.com
47.	BALBINE MANGA	699859388	babyambassa@yahoo.fr
48.	CHICK ESSENCE AMBE	677011279	Chickambe@yahoo.com
49.	MBENOUN MOUNCE	675355651	Benmbenoum@gmail.com
50.	BESSALA RAPHAEL II	677786814	Raphael2b@yahoo.fr
51.	RENGOU ABDEL BERNAZI	696554781	abdelsarki@yahoo.com
52.	NNEME NGA GABRIELLE	691183768	electrogaby237@gmail.com
53.	SM NJOWE PHILIPPE	679583153	
54.	EVODO CREPIN THIERRY	671288998	evodocrepin@gmail.com
55.	MOMO ONDOGO PONTADEM	695101454	georgesnmo@yahoo.fr
56.	NGO RANG NSIN	680955076	
57.	MEYO JEAN-YVES	655011455	yves.meyo@minpostel.gov.cm
58.	NJINANG GAETAN	677551121	Ulrich.njinang@mtn.com
59.	AYISSI ETEME ADOLPHE	699845957	Aayissi-eteme@yahoo.fr
60.	EVINA ZANGA HERMAN	699674278	evinazangaher@yahoo.fr
61.	ZAKEU ALOYS	656817414	aloyjerry@gmail.com
62.	MBOMBAP FORCHA HILARY	242002056	Hilary.mbobap@camtel.cm

Réf.	NOMS ET PRÉNOMS	TÉLÉPHONE	E-MAIL
63.	GNOWA SIMON	243000105	Simon.gnowa@camtel.cm
64.	MEBANDE ARMEL	242026511	armel.mebande@camtel.cm
65.	ABIA GEORGES PAULIN	675164003	georgespaulin@live.fr
66.	WANGUE DAVID	696262159	wangue-david@yahoo.fr
67.	GUIEGOU HELENE HORTENCE	670683024	horleneg@yahoo.fr
68.	KENMOE KAMGANG PATRICE	697583823	Kkpat4@gmail.com
69.	DENOUE YOUBI FABRICE	699419709	fabricedenoue@cubafoussam.cm
70.	ANGO WALWAL	698147031	ango-mol88@gmail.com
71.	KOUMOMOU GUEDEM LAUREL	675925443	sandylaurelle@yahoo.fr
72.	MBOUOPDA MOYO	675663557	fokajc@hotmail.com
73.	JOËL OBAM	650062723	Joel.obam@ccaa.aero
74.	SEMEONANA FRANCOIS	690834427	fsemeonana@yahoo.fr
75.	ABDOURASSOUL	670302988	abdourassoul@mintoul.gov.cm
76.	NDIFON SAMMUE	675462328	
77.	ESSOUME ROGER BRICE	655675991	rogerbricessoume@gmail.com
78.	WOKAM CLOTILDE	698384507	ndief72@yahoo.fr
79.	OSSELE CLOTAIRE DENIS	699323059	clotairedenis@yahoo.fr
80.	ABANDA EBANDA JULIENNE SANDRINE	694641751	sandyjuly85@yaoofr
81.	ZAMBO JOSEPH HERVE	690137725	Zajoh01@gmail.com
82.	PEH PEH FRANCK EBENEZER	658334309	pehfranck@gmail.com
83.	GAO JEAN	677696302	Jean.gao@cirt.cm
84.	AUZERKIN KERAWA	676888965	auzerkin.kerawa@globeleq.cm
85.	MFOKOUÉ LETOUTOUR	696918038	Brice.letutour@bc-pme.cm
86.	NDOUMBE JEAN	699630564	jean.ndoumbe@mindevel.gov.cm
87.	MEKOK MIMBE JEANNE	695226533	Mekok.mimbe@mindevel.gov.cm
88.	MOUAFO JOSEPH	674816544	josephmouafo04@gmail.com
89.	EVINDI BISSA JOSEPH PIERRE	676032561	joseph.evindi@adcsa.aero
90.	ABOUBAKAR ABDOULAYE	664909070	abdoulaye.aboubakar@nexttel.com
91.	TCHONHONG LINE	677753963	capdasiege@gmail.com
92.	BESSAGA BARNABE	677250193	
93.	AMOUGOU ROLAND ALOYS	659110740	rolandpro20@gmail.com

Réf.	NOMS ET PRÉNOMS	TÉLÉPHONE	E-MAIL
94.	YIAGNIGNI ABDEL AZIZ	696557644	abdelaziz.yiagnigni@gmail.com
95.	MOUDZE TATSUM CEDRIC	698389784	
96.	MBALA NKENGUE INGRID	656177229	ingridmbala97@gmail.com
97.	BIWOLE BIWOLE FRANCOIS D'ASSISE	676320782	fdbiwole@yahoo.fr
98.	NEMBOT KALACHI	674452411	Kalachi.nembot@minfi.cm
99.	GEORGES	665153636	
100.	BETCHE DAWAI	696811977	betche.dawa@yahoo.fr
101.	EYENGA GUY	697780796	guyeyenga@gmail.com
102.	MBE WAFFO RODRIGUE	676662324	mbewaffo@gmail.com
103.	ASSOMBANG MIREILLE	677824986	
104.	MBALLA OWONA CLARISSE	697378062	
105.	NDONGO EMMANUEL	679116655	EmmanuelNdongo@gmail.com
106.	SOZOGUE CYRILLE	696446932	sozocyr@gmail.com
107.	PATRICK ADINE	658519889	Patrick.Adine@j.ntechnologies.com
108.	GEHFE MACBETH	674766607	gmacbeth5@gmail.com
109.	KOMA NKANA JOSEPH CHARLES	699340342	Komaj@hotmail.com
110.	TABOU MARTIN	696631165	martin5tabu@yahoo.fr
111.	GONONG THIERRY	691834592	Yaneuro_002@yahoo.fr
112.	ASSEMBE BENOIT	674502010	assemblebenoit@yahoo.fr
113.	YOGO NTOMB PATRICE	699778445	
114.	NYANGONO EMMANUEL	693066342	enyangono@yahoo.fr
115.	DONTSA JIMMY ORHS	693159765	bromohoustark237@gmail.com
116.	BITET LANDRY JEAN	679419591	landry.bitet@yahoo.fr
117.	NYAKO WADJORE OLIVIER	699881351	El-wadjore@yahoo.fr
118.	MOUNIR NJI AMINE	655299370	aminenji@enix.cm
119.	NKOUTA ESSALA	651865679	siR5.GN@gmail.com
120.	ONDOBO MBASSI	696706222	emile.ondobo@art.cm
121.	WANGUE NADEGE	696110160	Wanadima1205@yahoo.fr
122.	ELOU'OU NDO SYLVIANE PRISCA	676925196	Prisca.elou2015@yahoo.fr
123.	NJEM TJEGA EMMANUEL		enjem@sni.cm
124.	NZOGANG RUFUS STEPHANE	675514838	mnozogang@sni.cm
Réf.	NOMS ET PRÉNOMS	TÉLÉPHONE	E-MAIL
125.	ENGUENE CLAUDE FRANCIS	650999145	fanguene@yahoo.com
126.	OUM PASCAL BLAISE	699949688	Pascal.oum@orange.cm
127.	FANLEU DJEU DA ULYSSE	683177068	ulyssedjeuda@gmail.com
128.	WITOMO LASSARADA	699690958	lzitomo@gmail.com
129.	NDONGO MVE DESIRE	699843612	desindongo@yahoo.fr
130.	MENGANG BEKONO	675141774	
131.	NSOGA NGUIMBOUS YVES		nsogan@gmail.com
132.	IBRAHIM MOUNIR MONTA	699508796	mounirmonta57@gmail.com
133.	MENANGA MENYE ANNE DIANE	668644795	dianemenye@gmail.com
134.	MOUDJONGUE DIBONG CLAIRE	674921111	Clairesolange09@gmail.com
135.	SOLANGE BADIJECK DIDIER	699914650	
136.	NDJOMOU HERMAN	693594785	hermandjomou@gmail.com
137.	SERNDIMA ALAMDOU SERGES	694476029	Serge.alamdou@elec.cm
138.	GHISLAIN NKOU DJOU	691612347	ghislain.nkoudjou@cca-bank.com
139.	NLEND JOSEE PRISCA	696600731	Josee.nlend@cca-bank.com
140.	DALI NKENFACK	673541130	dali.nkenfack@cca-bank.com
141.	ORU MIRABEL	679314403	Buten08@yahoo.fr
142.	AYISSI JEAN GERVAIS	695223852	J.Gervais@yahoo.fr
143.	LIONEL MBIANDJEU	242145618	
144.	GEORGES LOMBET		
145.	TCHASSEM CLAUDE	673000018	ctchassem@gmail.com
146.	ELOUNDOU BERTRAND	665000004	berteloundou@yahoo.fr
147.	NGNIMAN CHRISTIAN	678948068	cngniman@feicom.cm
148.	BOURDEU ALEX	694890250	
149.	PAUL LOPEZ	694885743	
150.	BENGALA MELINGUI	697709643	
151.	MOUELLE CYNTHIA-ROXANE	676321198	cycyroxane@gmail.com
152.	TCHOUABE TCHEUNANG FRANCIS	681362452	Ftchouabe2015@gmail.com
153.	MBALLA OWONA	697378062	
154.	ESSOMBA CHRISTIAN	690136227	essombajimm6@gmail.com
155.	SEME FRANCOIS	690834427	fsemeonana@yahoo.fr



Réf.	NOMS ET PRÉNOMS	TÉLÉPHONE	E-MAIL
156.	PATRICK MOUNKAM	699947162	yves.moukama@orange.com
157.	MASSOUGUEM LIDWINE ARANCE	695578114	lidwinemassou2@antic.cm
158.	KADJI INNOCENT	697600661	innocent.kadji@mntp.cm
159.	NKOY	696403601	
160.	YAMKAM FANKAM GAETAN	690662337	fankamgaetan@gmail.com
161.	ELEMUA FRANCINE	698303946	Francine.elemua@gmail.com
162.	LADREO LYCEL	655012059	
163.	ANGELE BATJOM	699948667	angele.batjom@orange.com
164.	ONANA ATANGANA YVES	699942905	yves.atangana@orange.com
165.	NGUEDJIO EMMANUEL	677739969	
166.	ONDOBO ESAI CELESTIN XAVIER	699425971	xavierpereceleste@yahoo.fr
167.	MZEUGANG ELVIS	655139286	
168.	EYOUM	650462172	levourien@cyberix.fr
169.	NKODO	697373677	
170.	TAGU	650590303	Harold@cyberix.fr
171.	ZONGO SERGE VALERY	41217305323	
172.	OBA ELLE GUY ROLAND	697955140	obaguy@yahoo.fr
173.	LOGMON II ACHILLE	696095002	achlog2@yahoo.fr
174.	DNJIKI HARAULD	675307322	harauld.dnjiki@afriland.cm
175.	IBOG BIYONG SAMUEL	655975673	
176.	MBENOUN MAURICE	675355651	
177.	TCHINDA MAXIME CARLOS	675055454	tmaximecarlos@gmail.com
178.	NGA EVOUNA REGINE	675379348	nerdada@yahoo.fr
179.	NGO PEGNWET ELISE FLORE	694159817	elformiss@gmail.com
180.	EPIE NGAME WILSON	682369737	epingom@gmail.com
181.	AGBOR OKON HERMANN	680177763	hermande2888@gmail.com
182.	OUMAROU LEKITIA	696684276	likitaOumarou@gmail.com
183.	NTSA BELA VICTOR CAROL	694746495	victorulrichtsabela@yahoo.fr
184.	EKOUMOU MVOLO ANDRE	699240946	issaekoumou@gmail.com
185.	BIYIHA NLEND JEAN AYMAR	676676523	aymarcm@yahoo.fr
186.	EWODO MARCEL BRICE	691714350	ewodo_marcel@yahoo.fr
187.	KWEDI NICK	698351570	nickkwedi@gmail.com
Réf.	NOMS ET PRÉNOMS	TÉLÉPHONE	E-MAIL
188.	KOMBE HENRY	677522028	kombeh91@gmail.com
189.	TCHONENG GERVAIS	697293422	ttgervais@yahoo.fr
190.	NGO MANG NSIN	680955076	
191.	OMGBA BERTRAND	694938986	omgbabertrand04@gmail.com
192.	GBI THICKI NDANGA BRICE	699088538	brice.ndanga@antic.cm
193.	MBAKOP NJANJA WILFRIED	656765551	Zilfriednjanja4@gmail.com
194.	OWONO Laurance Ornella	699320952	owono.laurance@gmail.com
195.	Etoua EVINA Simone Nicaise	698097937	simnicaise2014@gmail.com
196.	NKORO Fabrice	677701982	fabrice.nkoro@prc.cm
197.	EKOLLO Françoise	237699946189	francoiseekollo@yahoo.fr
198.	Balbine MANGA	699859388	babyambassa@yahoo.fr
199.	MENEKEU SONGMO Francine	237697964709	menekeuf@gmail.com
200.	NZIWOUE Wilfried	237676571376	wilfried.nziwoue@intelligentsia.biz
201.	TIOMENA FRANCOIS ROGER	237677092466	ftiomena@groupecommercialbank.com
202.	NGA MEBENGA Martien Landry	691603998	mebenga@banqueatlantique.net
203.	GBITHICKI NDANGA BRICE ARSENE	699088538	brice.ndanga@antic.cm
204.	Mouelle Cynthia-Roxane	676321198	cycyroxane@gmail.com
205.	NDEBI Elie-Roland	33628675078	elie.roland@orange.fr
206.	KENDJIO NZOGNING Pajesse Boris	237699076655	pajesse91fr@gmail.com
207.	EKOLLO ALAIN PASCAL	23799439129	alpas6@hotmail.com
208.	NKOA ERIC ARMAND	237695564156	eric.nkoa@yahoo.fr
210.	MBARGA Ferdinand Yves	695667027	mbargayves@gmail.com
209.	NDOUMGA ALEXIS	691575291	alexis.ndoumga@minpostel.gov.cm
211.	BIWOLE BIWOLE François d'Assise	237676320782	francoisdassisebiwole@gmail.com
212.	DACOBELL TACHAM NKWETA	237660274524	dacobelltacham@gmail.com
213.	DOH DONGDANGA ROSTAND	237677587873	ericdoh2002@yahoo.fr
214.	BENGALA MELINGUI Gilles Freddy	+237 6 97 70 96 43	gillesfrdd@gmail.com
215.	WANGUE Christian	237677779109	christian.wangue@prc.cm
216.	TEGOUFACK ZEFACK MIREILLE	696733578	mimitegou@gmail.com
217.	BABEY DIMLA TONNY	237658375425	babeytonny@blyscm.com

Réf.	NOMS ET PRÉNOMS	TÉLÉPHONE	E-MAIL
218.	YIAGNIGNI ABDEL AZIZ	696557644	abdelaziz.yiagnigni@gmail.com
219.	EVINDI BISSA Joseph Pierre	676032561	joseph.evindi@adcsa.aero
220.	MBOUMA SIK Martial Thadée	237675740766	martial.mbouma@globeleq.cm
221.	Hawaou Daoua Youssoufa	681582113	hawaoudaoua@yahoo.fr
222.	KOUOMOU GUEDEM Laurel Sandra	675925443	sandylaurelle@yahoo.fr
223.	KAMEGNE FOM Eric	693337018	rickyfom@yahoo.fr
224.	MBOLE ESIANE Annie:	697634205 /661445312	annie_mbole@yahoo.fr
225.	GBEL NKILI Hubert Parfait	697988486	parfaitgbel@gmail.com
226.	Chesi Azinwi	650770766	kendchesi2015@gmail.com
227.	ENOW DIVINE AKONG	661000080	edadilo86@gmail.com
228.	Yawat Gaetan	691178679	yawat@gmail.com
229.	kwedi essombe simone	237699509779	simone.essombe@minpostel.gov.cm
230.	CHEKAM TEBOU Arlette Grace	679582073	chekamtebou@gmail.com
231.	MANI Joseph Arthur	696552747	maniarthur@yahoo.fr
232.	NGO HIOBI Jackie Winnie Thatcher	237691865032	winnie.hiobi2016@yahoo.ca
233.	NANA DIANE CAROLE	675792071/691742677	nadianecarolr@yahoo.fr
234.	HOBEH Henry	678690150	h2hobeh@gmail.com
235.	OBAM NANGA Joël	655062723/222303090	joel.obam@ccaa.aero
236.	RENGOU ABDEL BERNAZI	696554781/672728610	abdelsarkir@yahoo.com
237.	DENOU YOUNBI Fabrice	237699419709	fabricedenou@gmail.com
238.	KOMA NKANA Joseph Charles	237699340342	komanj@hotmail.com
239.	DIKONGUE NDI Pierre Cedric	694165119/652349172	cedricndi66@gmail.com
240.	Keamwa Auberlain	237676888965	auberlain.kemawa@globeleq.cm
241.	NEMBOT DACHI Junior Le Prince	691170706	leprincenembot@gmail.com
242.	Tegno Emeric carlos	658022692	ctegno@gmail.com
243.	Naresh Kumar	971588299553	naresh.kumar@emtmeta.com,



