La logique de la géostratégie des menaces de l'espace virtuel, de la Mondialisation-Globalisation, mais surtout de la Glocalisation, impose des approches de solutions de sécurité collective et commune efficaces. Ces dynamiques insécuritaires sont soutenues à la fois par l'exceptionnalité de l'espace virtuel, l'ingénierie sociale ondoyante et diverse, et éprouvent les capacités des Etats, dans leurs prérogatives régaliennes de sécurisation des biens et des personnes. En effet, cet espace échappe encore à la conscience, la compréhension et l'action régulatrice des Etats.

Les défis et les enjeux de lutte contre la cybercriminalité et la cybersécurité se posent en termes de prise de conscience des réalités de l'espace virtuel, de renforcement de la confiance numérique, de sécurisation de l'espace virtuel, d'actualisation des politiques et des pratiques, mais également en termes de responsabilisation de tous les acteurs (Etats, administrations, entreprises, etc.) pour réduire les vulnérabilités inhérentes à cet espace.

L'organisation de ce séminaire, qui s'inscrit dans la perspective de ses missions de formation et de recherche, a permis à l'Ecole Internationale des Forces de Sécurité (EIFORCES), à travers son Centre de Recherche et de Documentation, ainsi qu'aux acteurs publics et privés, d'éveiller les consciences sur les menaces de l'espace virtuel, de dresser un état de lieux, de manière à identifier et à nommer ces menaces; et à évaluer les politiques, stratégies pour y répondre efficacement et, le cas échéant, pro-agir avec résultat.

www.eiforces.com

Revue scientifique éditée par l'EIFORCES

VIGIE Edition Hors Série Les défis et enjeux de la cyber-criminalité et la cyber-sécurité en afrique centrale

VIGIE BULLETIN D'ANALYSE STRATÉGIQUE ET PROSPECTIVE

E-mail: baspvigie@gmail. com Edition Hors Série

Actes du séminaire de recherche sur :

"Les défis et enjeux de la cyber-criminalité et la cyber-sécurité en Afrique Centrale"

Sous la coordination scientifique et technique
du Pr Wulson Mvomo Ela Directeur du Centre de Recherche et de Documentation de l'EIFORCES
et du Dr BELL B. G. Ph.D Sciences Techniques en Cyber Sécurité ; Expert en Cyber Criminalité

Préface du Général de Brigade,
André Patrice BITOTE
Directeur Général de l'EIFORCES

LES ACTES DU SEMINAIRE DE RECHERCHE SUR LES DEFIS ET ENJEUX DE LA CYBERCRIMINALITE ET LA CYBERSECURITE EN AFRIQUE CENTRALE

Du 05 au 08 Décembre 2018, à l'Hôtel SAWA, à Douala

Sous la coordination scientifique et technique du

Pr Wullson MVOMO ELA
Directeur du Centre de Recherche et Documentation de l'EIFORCES

et du

Dr. BELL B.G.,
PhD Sciences techniques en cyber sécurité
Expert Formateur en sécurité des systèmes d'information

Préface du Général de Brigade,
André Patrice BITOTE
Directeur Général de l'EIFORCES

SOMMAIRE

PRÉFACE

En inscrivant cette problématique dans son agenda, dans le cadre d'une activité associant les experts universitaires et professionnels de la sécurité, l'Ecole Internationale des Forces de Sécurité (EIFORCES), ce faisant, entend assumer la plénitude de ses missions de recherche à la fois pour contribuer au renouvellement des curricula de formation et pour la dissémination des standards et de bonnes pratiques dans cet espace-temps virtuel si complexe à cerner.

Appréhender la phénoménologie en termes de défis et enjeux de la cybercriminalité et de la cybersécurité appelle, entre autres, à prendre en compte les réalités complexes, notamment celles liées à la manipulation des consciences et des opinions à travers les Fake news. Par leur charge psychologique répétée, celles-ci s'affirment de plus en plus comme des menaces tangibles à la stabilité des Etats, à la cohésion nationale et sociale. En effet, les enjeux (sociaux, économiques, politiques, etc.) du monde réel, transposés dans l'espace-temps virtuel, y trouvent un cadre idéal pour l'exacerbation des antagonismes. En compromettant l'intégrité, la confidentialité, voire la disponibilité des données personnelles et biens des usagers, la cybercriminalité, à travers une ingénierie sociale, crée chez ces derniers, un choc émotionnel et psychologique à caractère terroriste ou proto-terroriste.

Ce contexte critique et interlope pose en termes d'impératifs, la prise de conscience du cyberespace et des dynamiques y afférentes, sa normalisation, sa régulation. D'où, l'exigence d'un aggiornamento de la vision, la politique, la stratégie, au profit de l'adéquation et de l'efficience. Loin de s'inscrire dans une logique responsive, et donc réactive, les solutions en matière de lutte contre la cybercriminalité et la cyber insécurité ne sauraient trouver toute leur pertinence, en dehors d'une perspective préventive et préemptive collective et commune. Ce, de manière à renforcer le cadre de notre cyber sécurité.

Adresser les problématiques liées aux enjeux et contraintes de la lutte contre la cybercriminalité et la cybersécurité, participe du devoir légitime de l'EIFORCES. La Recherche et la Formation, en tant que champs prioritaires du mandat de l'Institution, deviennent donc les canaux idoines pour la prise de conscience, la compréhension et la recherche de solutions pour faire face aux menaces de l'espace virtuel.

Général de Brigade,

André Patrice BITOTE

Directeur Général de l'EIFORCES

PLENIERE N°1 – CYBERCRIMINALITE : ORIGINES, MANIFESTATIONS ET ENJEUX

Dark Web, Deep Web, DDoS, Ingénierie sociale, Attaques informationnelles, FakeNews, Lois, Code de procédures, Techniques d'investigations, interceptions légales, analyses forensiques…

La criminalité organisée investit aujourd'hui de nouveaux territoires liés à l'émergence d'horizons comme le Cyber-Espace. Cette nouvelle forme de criminalité prend son essor dans les usages récents de l'informatique que nous déployons ; Mobilité, Smartphone, Hyper-connectivité, Services Cloud, Réseaux Sociaux. Au travers de la cartographie d'espaces comme le Dark Web ou le Deep Web, nous mettrons en évidence les risques ou opportunités qu'ils représentent, les profils et motivations des acteurs, et essayerons de donner des clés de lecture pour comprendre ces nouveaux phénomènes.

MODERATEUR : Mr. MASSIMA Jean Jacques, Représentant A/C UIT

INTERVENANT N°1 : M. BATONGUE Alain, Secrétaire Général Exécutif GICAM

Fake news, structuration des perceptions et des représentations : une menace pour la cohésion sociale et la stabilité étatique en Afrique ?

L'expansion des nouveaux outils technologies de l'information et de la communication connaît une croissance remarquable, depuis une dizaine d'années. Le développement de nouveaux moyens et supports de communication permet à plusieurs entreprises et personnes physiques de partager des informations en temps réel et ainsi d'influencer le management, le rendement, la notoriété, …

Ainsi, après la citoyenneté qui est le fait pour un individu, pour une famille ou pour un groupe, d'être reconnu officiellement comme citoyen, c'est-à-dire membre d'une ville, avec des droits (comme celui d'avoir accès à l'information), mais aussi des devoirs, il s'est développé, avec ces nouveaux outils technologiques, la cyber-citoyenneté, avec donc une identité numérique, une identité virtuelle.

Cela donne des droits aussi : entre autres, comme cité plus haut, le droit à l'information, l'accès du plus grand nombre à l'internet pour consommer ce nouveau modèle de communication.

Plusieurs solutions sont proposées de nos jours et permettent ainsi aux dirigeants, aux milieux d'affaires et à des individus pris individuellement, de proposer de manière différente les produits et services. Je cite ici l'avènement du marketing digital qui est en train de révolutionner la vente et la communication des entreprises.

La présentation des sites internet a considérablement évolué et ces différentes entités utilisent de plus en plus les réseaux sociaux pour communiquer avec leurs différents stakeholders.

Exemple le plus emblématique : l'actuel chef d'Etat Américain, Donald Trump, qui a vulgarisé la communication et le partage des décisions politiques par tweet. Faisant ainsi d'internet et ses multiples facilités un outil légitime dans l'exercice du pouvoir.

Mais, ce nouveau modèle de communication entraine lui aussi des

devoirs. Il y a derrière chaque information véhiculée une audience. Cela engage (ou devrait engager, la responsabilité pénale de ceux qui utilisent ces espaces virtuels pour la circulation des informations.

Car autant un journal physique (papier) ou une télévision peuvent être identifiés, autant les différents sites et blogs, ou encore des informations encore plus anonymes qui se répandent sur les réseaux sociaux et qui deviennent virales (ce qu'on appelle désormais cyber-espace), échappent à cette identification.

Avec les enjeux de contrôle du pouvoir, avec les enjeux de sécurité, l'utilisation des fakes news (entendues comme informations volontairement fausses et destinées à abuser ou manipuler les lecteurs/consommateurs pour des fins autres), de telles dérives ont des conséquences désastreuses pour le développement économique, la cohésion sociale ou la stabilité des Etats.

Exemple N°1. Rumeur sur le décès de Marcel NIAT NJIFENDI, Président du Sénat du Cameroun.

Le 26 septembre 2018, 11 jours avant l'élection présidentielle du 07 octobre dernier, une rumeur se répand sur la toile, annonçant le décès du Président du Sénat tantôt à Genève, tantôt à Paris. A mesure que la journée avance, les détails les plus invraisemblables s'accumulent. Puis aux environs de 19h, une dépêche qui semble plus précise se répand sur la toile :

"M NIAT NJIFENDI Marcel, Président de la Chambre Haute du Parlement (SENAT), vient de rendre l'âme à GENEVE. Source : GICAM»

Comme vous le constaterez, l'information en elle-même n'a pas changé, Mais une signature de poids a été identifiée pour la crédibiliser : le GICAM…

Réaction immédiate, une demie heure plus tard, signée du Secrétaire Exécutif du GICAM :

«Manipulation : Une dépêche en circulation sur les réseaux sociaux annonce le décès du Président du sénat et indique comme source de cette information le GICAM. Le GICAM tient à préciser qu'il n'a pas d'information sur ce sujet. Et qu'il n'a par conséquent publié aucun communiqué à cet effet. Le

GICAM rappelle qu'il dispose d'un site officiel www.legicam.cm à travers lequel il communique ses annonces et prises de position." Alain Blaise BATONGUE, Secrétaire Exécutif du GICAM

Aussitôt, nous arrosons les mêmes réseaux sociaux, à l'effet de neutraliser la première information. Groupes WhatsApp, Facebook, Twitter, et publication sur notre site officiel. Si nous avions besoin d'une preuve pour savoir qu'il ne s'agissait pas d'un simple caprice d'un aventurier des réseaux sociaux, la réponse des initiateurs du message sera brutale. Le site web du GICAM sera aussitôt bloqué et inaccessible, contribuant à semer davantage la panique. Nos techniciens ont dû être mobilisés une bonne partie de la nuit, dans un combat à distance, pour rétablir aux environs de 23 heures, notre site.

Exemple N°2 : Rumeurs sur le décès d' Ali BONGO ONDIMBA, chef de l'Etat gabonais.

Toujours au départ les réseaux sociaux, puis un relais (de bonne ou de mauvaise foi) par une télévision camerounaise de grande audience, Vision4, qui a semblé avoir authentifié cette rumeur, en lui donnant un écho encore plus large. D'où, la panique générale qui s'en est suivie, avec des mesures énergiques prises par les autorités gabonaises contre cette télévision (signal coupé au Gabon).

Comme on peut le constater à travers ces deux exemples (mais il y en a tellement qui peuplent notre quotidien), cette nouvelle manière faire n'est pas sans risque. On ne le dit pas assez, au-delà des informations (fake news), il y a les hackers qui entrent dans les systèmes des banques et même des entreprises en général pour manipuler les données et les chiffres, faisant perdre d'énormes sommes d'argent. Aussi la désinformation et l'espionnage sont des phénomènes qui prennent de l'ampleur ces jours.

Cette situation est soulignée ici pour vous montrer en effet qu'il est important de profiter des Technologies de l'information et de la communication (TIC), mais il faut surtout savoir comment s'en servir.

Comment, dans ces conditions, une organisation de défense comme l'EIFORCES peut-elle se positionner, en termes de géopolitique par rapport à un outil aux ravages innombrables et dont l'opinion pense (à tort ou à raison), qu'il n'a pas toujours la maitrise parfaite ?

Quel type de réponse préventive ? Quels moyens d'identification et de répression ? Quels outils pour traquer ? Le débat est ouvert et les travaux permettront sans doute de dégager des pistes de solutions.

Pour notre part, nous en dégageons quelques-unes :

- Pour couper l'herbe sous les pieds des professionnels des fake news, il faut communiquer dans la transparence sur les principaux sujets de chaque institution, et occuper les différents sites des réseaux sociaux ou de communication publique pour les neutraliser ;
- Il faut poursuivre la sensibilisation des citoyens à l'utilisation et donc, au danger des réseaux sociaux (dernier message à la jeunesse du chef de l'Etat)
- Multiplier les espaces de mutualisation des efforts pour dégager les meilleurs outils techniques susceptibles de traquer et d'identifier les semeurs de fake news et d'attaques de sites, afin de les exposer aux rigueurs de la loi et de la règlementation.

Le GICAM, qui se positionne comme un patronat au service de ses membres, et développe une capacité d'influence et développe des outils d'intelligence économique, est disposé à apporter sa contribution et sa collaboration. Il dispose, en son sein, de diverses commissions opérationnelles dont la Commission en charge de l'Economie Numérique, qui pourrait donc être un appui certain pour EIFORCES. Cela pourrait se faire, entre autres, en matière de cyber stratégie, de formation et renforcement de capacités sur la cyber régulation et la cybercriminalité ; mais aussi, en termes de solutions techniques pour la mise en œuvre de mécanismes de cyberdéfense.

INTERVENANT N°2 : C/E MBOUOPDA, Expert en droit pénal cybernétique

Cadre légal et règlementaire, procédures d'investigations et fonctionnement des juridictions

Les infractions cybernétiques sont monnaie courante de nos jours. Que prévoit la législation ? Quel est le cadre des procédures en la matière ? Que vaut la preuve numérique ? Comment fonctionnent les juridictions sur ces questions ? Les structures d'investigation et d'enquête sont-elles outillées ? Ces questions, et beaucoup d'autres, trouveront réponses lors des débats prévus dans cet espace.

Idée maitresse

Lutter efficacement contre la cybercriminalité passe par une approche préventive qui consiste à rendre le cyberespace moins favorable à l'expression de la criminalité et à réduire les opportunités criminelles.

En effet, il faut élever le seuil de difficulté de réalisation des cyberattaques (augmenter les coûts en termes de compétences et de ressources pour le malveillant et diminuer les profits attendus) et accroître les risques pris par les criminels d'être identifiés, localisés et poursuivis.

Plan

- Cadre légal et règlementaire
- Procédures d'investigation
- Fonctionnement des juridictions
- Quelques problématiques

ETAT DES LIEUX A LA GENDARMERIE NATIONALE

Cas connus

PERIODE DE 03 ANS			
ANNEE	**NOMBRE DE CAS TRAITES**	**NOMBRE DE CAS RESOLUS**	**MONTANT en FCFA**
2016	95	39	265.279.298
2017	389	106	3.465.389.425
2018	61	28	112.527.768
TOTAL	**545**	**173**	**3.843.196.491**

Actes malveillants

	TYPE D'INFRACTIONS	**Nbr de dossiers**	**%**
1	Attaques sur les systèmes d'information	8	1.9%
2	Fraudes sur compte mobile/bancaire	27	3.2%
3	Usurpation d'identité	35	5.4%
4	Arnaques (à l'héritage, aux sentiments, par sociétés fictives, triangle bamoun, aux grains, œufs, scamming etc.)	389	71.3%
5	Vols de données personnelles / vol d'appareil des tics	97	17.8%
6	Spoliation de compte mail	6	4.5%
7	Fraudes informatiques (imprimés de l'Etat, timbres, ticket de péages, quittances diverses, etc.)	23	2.8%
8	Chantages à la vidéo/téléphone	4	0.8%

Origine des cas signalés (2016-2018)

MINREX	56
ADMINISTRATIONS PUBLIQUES ET ASSIMILEES	90
ADMINISTRATIONS/SOCIETES PRIVEES	117
AUTRES	282

Nombre d'affaires par pays

	PAYS (Victime/suspect)	Nbr de dossiers	%
1	CAMEROUN	279	66.3%
2	NIGERIA	26	6.2%
3	BENIN	24	5.7%
4	CÔTE D'IVOIRE	25	5.9%
5	BURKINA FASO	10	2.4%
6	UKRAINE	3	0.7%
7	SUISSE	3	0.7%
8	BELGIQUE	2	0.5%
9	ANGLETERRE	4	1.0%
10	USA	5	1.2%
11	POLOGNE	7	1.7%
12	ALLEMAGNE	1	0.2%
13	SLOVENIE	8	1.9%
14	FRANCE	18	4.3%
15	CANADA	6	1.4%

Illustrations

Scamming et triangle bamoun

- Un individu ou une société qui se propose de vendre des animaux domestiques (chien, chat, perroquet …), se propose également de gérer le transport de ces animaux jusqu'à votre domicile en vous présentant ou non des certificats de transit ou agrément d'une compagnie d'assurance pour animaux moyennant le versement de quelques acomptes

- Il vous est proposé d'acheter des objets d'arts en provenance des chefferies traditionnelles BAMOUN (Ouest Cameroun) à des prix relativement bas, pour les revendre dans un délai très court à un autre acheteur qui vous propose un prix alléchant et vous établit un contrat d'achat

REPUBLIQUE DU CAMEROUN
Paix-travail-patrie
AMBASSADE DE FRANCE
MINISTERE DE LA CULTURE
DIRECTION UNESCO-ICOM

REPUBLIC OF CAMEROON
Peace-work-fatherland
MINISTRY OF CULTURE
DIRECTION UNESCO-ICOM

PROTOCOLE INTERNATIONAL DE VOYAGE

enreistrement n°:.....

Vu le décret N° 05698/du 15 juin 1989 portant rectification de la convention libre des personnes, des biens et des mesures a prendre pour empêcher l'importation et l'exportation des propriétés culturelles,

Conformément a la loi N° 89652336 du 20 octobre 1997

L'ambassade permet a tout corps administratifs de pouvoir être libre de toutes transaction,

Nous soussignés, L'ambassade, Mincult, ICOM et UNESCO certifions que ce document est valorisé pour toutes les transactions internationales afin que le propriétaire d'une collection de 08 objets d'arts ancienne en bois d'origine Ouest-Cameroun dont Mr LAURENT ESTEVE de nationalité Française (France) soit libre de faire une exposition vente ou vente dans tout le territoire international.

En foi de quoi la présente (PROTOCOLE INTERNATIONAL DE VOYAGE)
est établie pour servir et faire valoir ce que de droit

Fait à yaounde

Le Ministre de la Culture

UNESCO,

Ambassade de France

Mme Christine Robichon

ICOM

I/ LE CADRE LEGAL ET REGLEMENTAIRE

Clarifications conceptuelles

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.

Cyber-sécurité : 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. (loi N°2010/012 du 21 décembre 2010).

A/ Au niveau international : Convention sur la cyber-criminalité

Aussi connue comme la Convention de Budapest sur la cybercriminalité ou Convention de Budapest, il s'agit du premier traité international qui tente d'aborder les crimes informatiques et les crimes sur Internet (y compris la pornographie infantile, l'atteinte au droit d'auteur et la discours de haine) en harmonisant certaines lois nationales, en améliorant les techniques d'enquêtes et **en augmentant la coopération entre les nations** et la protection adéquate des droits de l'homme et des libertés.

B/ Au niveau continental : La Convention de l'Union Africaine (UA) sur la Cyber sécurité et la protection des données à caractère personnel

La Convention est divisée en 4 chapitres :

Chapitre 1 : les transactions électroniques

Chapitre 2 : la protection des données à caractère personnel

Chapitre 3 : promotion de la cyber sécurité et lutte contre la cybercriminalité

Chapitre 4 : dispositions finales

C/ Au niveau national

- **Loi n°2016/007 du 12 juillet 2016 portant Code Pénal**
- **Loi N° 2005/007 du 27 juillet 2005 portant Code de Procédure Pénale**

Autres textes de lois

Libellé acte	N°	Date	Objet	Objectif
Loi	2010/012	21 décembre 2010	Relative à la cybersécurité et la cybercriminalité au Cameroun	- Instaurer la confiance dans les réseaux de communications électroniques et des systèmes d'information; - Fixer le régime juridiques de la preuve numérique, des activités de sécurité, de cryptologie et de certification électronique.
Loi	2010/021	21 décembre 2010	Régissant le commerce électronique au Cameroun	Vise à réguler l'ensemble des transactions commerciales sur le cyberespace au Cameroun

Article 66.- (1) Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 1.000.000 (un million) à 2.000.000 (deux millions) F CFA ou de l'une de ces deux peines seulement, celui qui entraîne la perturbation ou l'interruption du fonctionnement d'un réseau de communications électroniques ou d'un équipement terminal, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles les données.

Article 75.- (1) Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) F CFA ou de l'une de ces deux peines seulement, celui qui enregistre et diffuse à but lucratif, par la voie de communications électroniques ou d'un système d'information sans le consentement de l'intéressé, des images portant atteinte à l'intégrité corporelle.

Article 78.- (1) Est puni d'un emprisonnement de six (06) mois à deux (02) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui publie ou propage par voie de communications électroniques ou d'un système d'information, une nouvelle sans pouvoir en rapporter la preuve de véracité ou justifier qu'il avait de bonnes raisons de croire à la vérité de ladite nouvelle.

Libellé acte	N°	Date	Objet	Objectif
LOIS PROMULGUEES				
Loi	2010/012	21 décembre 2010	Régissant les communications électroniques du Cameroun	- Vise à promouvoir le développement équilibré des réseaux et services de communications électroniques, en vue d'assurer la contribution de ce secteur au développement de l'économie nationale, et de satisfaire les besoins multiples des utilisateurs et de la population. - Fixe les modalités d'établissement et d'exploitation des réseaux ainsi que de fourniture des services de communications électroniques dans le respect des prescriptions exigées par la défense nationale et la sécurité publique ; - Encourage et favorise la participation du secteur privé au développement des communications électroniques dans un environnement concurrentiel.

Libellé acte	N°	Date	Objet	Objectif
LOIS PROMULGUEES				
Loi	2011/012	06 mai 2011	Portant protection du consommateur au Cameroun	- La présente loi fixe le cadre général de la protection du consommateur - Elle s'applique à toutes les transactions relatives à la fourniture, la distribution, la vente, l'échange de technologies, de biens et de services portant sur la protection du consommateur ; - Ces transactions concernent notamment les secteurs de la santé, la pharmacie, l'alimentation, l'eau, l'habitat, l'éducation, les services financiers, bancaires, du transport, l'énergie et les communications.

Libellé acte	N°	Date	Objet	Objectif
LOIS PROMULGUEES				
Décret	2012/308	26 juin 2012	fixant les modalités de gestion du Fonds Spécial des Télécommunications	1- L'Agence de Régulation des Télécommunications s'assure de l'effectivité des versements des contributions des opérateurs ; 2- Les opérateurs de réseaux et les fournisseurs des services des communications électroniques sont tenus d'effectuer le paiement de leurs contributions de l'année écoulée au plus tard le 31 mars de l'année suivante ; 3- L'Agence de Régulation des Télécommunications assure le contrôle de la sincérité des chiffres d'affaire déclarés par les opérateurs des réseaux et des fournisseurs de services de communications électroniques. 4- En cas de doute sur la sincérité du chiffre d'affaire déclaré, l'Agence de Régulation des télécommunications se réserve le droit de commettre un audit aux frais de l'opérateur et/ou de l'exploitant.

Libellé acte	N°	Date	Objet	Objectif
Décret	2012/309	26 juin 2012	fixant les modalités de gestion du Fonds Spécial des Activités de Sécurité Electronique (FSE)	- L'Agnece Nationale des Technologies de l'Information et de le communication s'assure de l'effectivité des versements des contributions des autorités de certification accréditées, des éditeurs de logiciels de sécurité agréés ; - Les autorités de certification accréditées, les auditeurs de sécurité, les éditeurs de logiciels de sécurité et des autres prestataires de services de sécurité agréés, sont tenus d'effectuer le paiement de leurs contributions de l'année écoulée au plus tard le 31 mars de l'année suivante.

II - LES PROCEDURES D'INVESTIGATION

A/ L'informatique Légale (digital forensic)

Cette procédure consiste à :

- apporter des preuves numériques à la demande d'une institution de type judiciaire
- Utiliser des connaissances et méthodes pour collecter/conserver/analyser des preuves issues de supports numériques en vue de les produire devant une juridiction.

B/ La perquisition

Concrètement, il s'agit :

- D'établir qu'une infraction spécifique a été commise.

Le FAI peut être sur le territoire mais l'hébergeur (Datacenter) à l'étranger. Dans ce cas, il faut une CR pour poursuivre la perquisition.

Seules les données présentes sur le territoire peuvent être rapidement perquisitionnées. Aussi toute législation interne relative à la procédure pénale doit prévoir des pouvoirs de perquisition et de saisie d'objets tangibles.

En l'absence de loi, les règles de perquisitions qui peuvent être retenues sont celles en vigueur dans le cadre des infractions classiques (Heures légales).

C/ La Saisie

Elle consiste à :

- La récupération du support physique dans lequel les données ou les informations sont stockées (ou réaliser ou conserver une copie de ces données ou informations) ;
- L'utilisation du matériel/logiciel approprié pour extraire les données ;
- L'emport du support matériel sur lequel les données intangibles sont stockés (disque dur ou disquette) ;
- L'impression des données avant la saisie du support, les données originelles restant en mémoire (cas des mémoires volatiles).

1/ Quelques tâches qui répondent aux besoins d'enquête

- Récupérer des données effacées ;
- Faire sauter les mots de passe (d'amorçage au de session)
- Démontrer que des contacts par email ou par messagerie instantanée ont eu lieu ;
- Prouver l'existence des téléchargements illicites ;
- Montrer qu'un virus a été créé sur un poste ;
- Établir qu'un site au contenu illicite a été visité ;
- Dupliquer les éléments contenus sur le disque dur ou les clefs et ne travailler que sur les copies.

* Réquisition des OTM

- Appels téléphoniques reçus et émis.
- SMS reçus et envoyés, incluant les informations de l'expéditeur et du récepteur.
- Le numéro IMEI - numéro unique qui identifie un téléphone portable.

- Le numéro IMSI - numéro unique qui identifie une carte SIM - c'est ce à quoi le numéro de portable est lié.
- Le numéro TMSI - numéro temporaire régulièrement réassigné en fonction du changement de la situation géographique ou du réseau (couverture) qui peut être pisté par des systèmes d'écoute en vente dans le commerce.
- La cellule réseau dans laquelle le téléphone est situé. De quelques mètres jusqu'à plusieurs kilomètres, les cellules peuvent couvrir plusieurs tailles de zones géographiques, avec des cellules beaucoup plus petites dans les zones urbaines et encore plus petites dans les immeubles qui utilisent une antenne relais pour renforcer les signaux.
- La position géographique de l'abonné grâce à cette cellule. La situation géographique exacte du téléphone dépend de la taille de la cellule - plus une zone géographique est pourvue de tours-relais, plus la position géographique du portable sera précise.

* Réquisition des FAI/ISP

Les données de trafic et de connexion à internet sont collectées et relevées par les FAI. Elles comprennent :

- L'identifiant de l'utilisateur ; l'adresse IP qui lui est affectée; les dates et heures exactes de connexion et de déconnexion
- Le données caches du FAI qui contiennent tout type de données transmises (par exemple les activités de navigations sur le web, hors HTTPS, les messages instantanés non chiffrés) ainsi que le volume de données envoyées.

A chaque connexion de l'internaute sur le réseau, le FAI attribue a son ordinateur une adresse IP valable pour le temps de sa session.

2/ Pistes d'investigation : exploiter les traces technologiques laissées

Identifier le suspect

a Trouver l'identité virtuelle

- Adresse email

- Compte de réseau social ou forum (facebook, badoo, google+, twitter, etc)
- Compte de Chat/VoIP (skype, WhatsApp, Yahoo Msg, MSN, hangout, etc.)
- Numéros de téléphones utilisés (directement ou via comptes)

b Trouver l'identité réelle derrière l'identité virtuelle avec les fournisseurs de service tic

- Trouver les adresses IP et les identités des propriétaires (whois)
- Adresser des réquisitions aux opérateurs gérant les IP ou les numéros de tél.,
- Analyser les liens et le réseau du suspect (investigation traditionnelle).

Localiser le suspect

c Analyser les habitudes du suspect

- Lieux fréquentés (par analyse dossier banque, transferts d'argent, etc.)
- Contacts privilégiés,
- Lieux habituels de retrait des transferts,
- Utiliser les informations d'identification et d'adresses fournies lors des abonnements, etc.

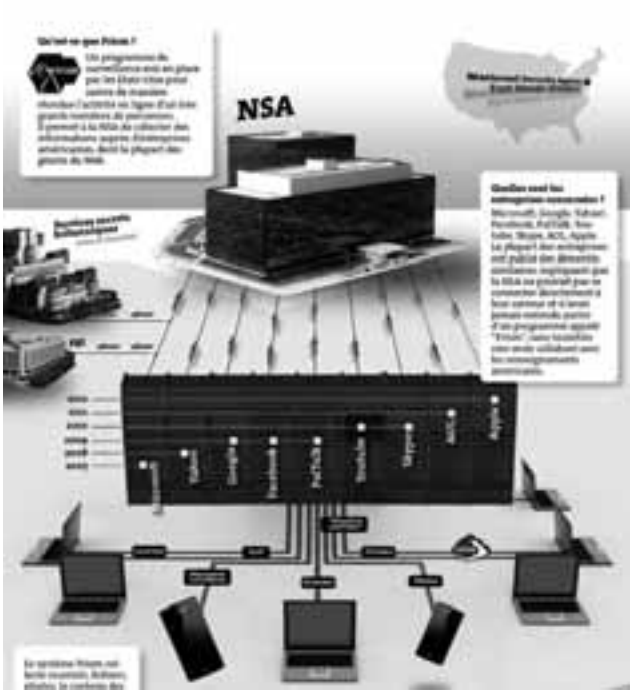
d Localiser physiquement et interpeler le suspect

- Surveiller les lieux identifiés,
- Rechercher des complices,
- Tendre des pièges avec l'aide des victimes,
- Enquêtes terrain classiques, etc.

3/ Aspect organisationnel

Activités liées aux investigations : laboratoire forensic

Enjeux de renseignement: Programmes de surveillance



Les pays les plus surveillés:

- Iran
- Pakistan
- Jordanie
- Turkie
- Inde

Autres programmes de surveillance

- Bullrun (États-Unis)
- Muscular (Royaume-Uni)
- Tempora (Royaume-Uni)
- XKeyscore (États-Unis)
- Programmes de surveillance électronique :
- Echelon
- Intelligent information system supporting observation, searching and detection for security of citizens in urban environment

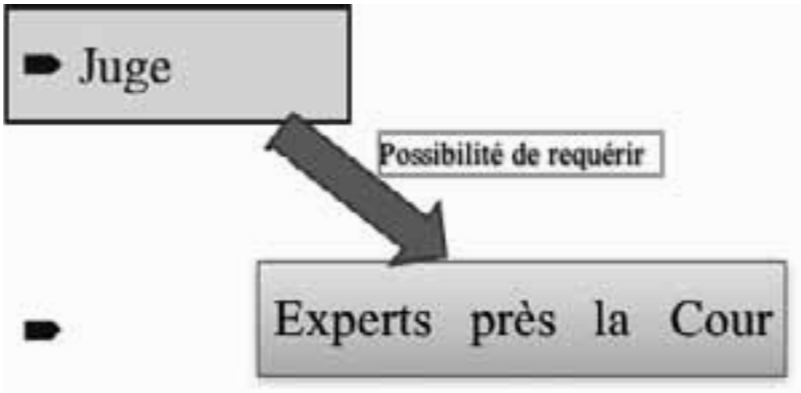
(INDECT, projet de surveillance Européen semblable à PRISM)

III - FONCTIONNEMENT DES JURIDICTIONS

Compétences

- Tribunal de Première Instance (TPI)
- Tribunal de Grande Instance (TGI)
- Tribunal Militaire (TM)

Poursuites pénales



IV - QUELQUES PROBLEMATIQUES

Les problèmes du point de vue juridique

- Absence d'une nomenclature des infractions
- Plusieurs infractions s'effectuant à travers le cyberespace de manière complémentaire à la criminalité classique ne sont pas pris en compte
- La valeur de la preuve numérique

Ratification de la convention de Budapest

Limite les capacités actuelles du Cameroun dans la lutte internationale contre la cybercriminalité qui se joue des frontières des Etats.

Les autorités judiciaires et policières obtiennent difficilement l'assistance des Etats membres à la Convention de Budapest (USA, France, Afrique du Sud, Japon etc.) ainsi que des acteurs globaux de l'Internet (Facebook, Youtube, Google, Gmail etc.) dans leurs investigations ainsi que de l'assistance technique et opérationnelle du Conseil de l'Europe.

Challenges permanent lors de la commission d'un délit

- bloquer un compte Face book diffusant des contenus frauduleux
- etc.

Difficultés à enquêter au plan technique

- Schémas sophistiqués et fastidieux (cas de virus, warns, botnets …),
- Processus rapide et volatilité des preuves,
- Opacité des services,
- Localisations multiples et internationales,
- Difficulté d'estimer les pertes,
- Difficultés de sensibilisation de façon adaptée à chaque culture,
- Participation active des victimes à la commission de l'infraction,
- Absence de témoin (en dehors de traces tech.)

Partage des informations : Recueil de traces détenues par de tiers parties privées, dans un contexte international et multi-législation.

Mutualisation des ressources

- base de données fichier criminel (Sûreté Nationale, ANTIC, etc.)
- base de données Douane
- base de données MINTRANSPORT (permis de conduire, Véhicules)
- base de données MINJUSTICE (registre de commerce, Casier Judiciaire, etc.)
- base de données conservation foncière
- base de données IMPOTS
- base de données SENAC
- Etc.

Avec les opérateurs de téléphonie mobile

- Réponses tardives aux réquisitions ;

- Difficultés de localisation dans un rayon très réduit ;
- Pas d'identification ou identification incomplètes ;

De manière générale, il s'avère que beaucoup d'usagers ne sont pas encore identifiés. Par ailleurs, les ventes des puces continuent à se faire sans identification préalable, indépendamment de l'opérateur de téléphonie.

CONCLUSION

Dans le cadre d'une action en justice, la collecte, la conservation et l'analyse de preuves (immatérielles) issues des supports informatiques supposent une approche probatoire spécifique qui conditionne leur admissibilité.

Les institutions en charge des TIC, les experts des entreprises, des Universités et des grandes écoles spécialisées ainsi que les Agences doivent collaborer pour mettre en place une stratégie nationale de cyber sécurité. Il pourrait en découler un plan national de formation en vue d'une reconnaissance de la spécialité de ''**Cyber enquêteur**''.

Biographie

1) «LES ADMINISTRATIONS CHARGEES DE L'APPLICATION DE LA LOI FACE A LA CYBERCRIMINALITE : APPROCHE SUR LES MOYENS DE LUTTE», Publication de l'Association Miroir du Droit, Ed. Octobre 2011, Yaoundé, Cameroun.

2) «MULTI-PERPECTIVE CYBERCRIME INVESTIGATION PROCESS MODELING », International Journal of Applied Information Systems 2(8):14-20, June 2012. Published by Foundation of Computer Science, New York, USA.

3) «MODELING AND VERIFICATION OF GROUP SIGNATURES PROPERTIES», International Journal of Applied Information Systems 2(8):14-20, June 2012. Published by Foundation of Computer Science, New York, USA.

4) «A BASIC INTRUSION DETECTION MODEL FOR CYBERCRIME INVESTIGATION PURPOSES», Conférence Africaine sur la Recherche en informatique; Ecole nationale Supérieure Polytechnique, Cameroun, 2013.

5) «LEGAL FRAMEWORK FOR A DIGITAL FORENSIC PROCESS », International Journal of Computer Application 3(12):08-16, October 2013. Published by Foundation of Computer Science, New York, USA.

6) «A FORMAL FRAMEWORK FOR INTRUSION DETECTION WITHIN AN INFORMATION SYSTEM BASED ON WORKFLOW AUDIT», International Journal of Computer Application 3(12):08-16, October 2013. Published by Foundation of Computer Science, New York, USA.

7) «OBTAINING DIGITAL EVIDENCE FROM INTRUSION DETECTION SYSTEMS», International Journal of Computer Application 1(10):12-21, Juin 2014. Published by Foundation of Computer Science, New York, USA.

Projets de publication

«CYBERCRIME ACTIVITIES ANALYSIS» Université de YAOUNDE I, Département d'Informatique, Cameroun 2015.

«LA CYBER PATROUILLE AU CAMEROUN» Université de YAOUNDE I, Département d'Informatique, Cameroun 2015.

«LES ENJEUX DE LA PREUVE NUMERIQUE POUR LA JUSTICE CAMEROUNAISE» Université de YAOUNDE I, Département d'Informatique, Cameroun 2015.

INTERVENANT N°3 : Dr. BELL B.G.,
Ph.D sciences techniques en cyber sécurité ; Expert en cybercriminalité

Le facteur humain et l'ingénierie sociale

Pourquoi recourir à des kits d'exploitation, quand on peut tirer profit des utilisateurs ? Lors de cette intervention, on verra l'influence du Facteur Humain et de l'ingénierie sociale dans la commission d'infractions cybernétiques. Nous verrons notamment les stratégies pour leurrer leurs victimes et les amener à devenir leurs complices involontaires pour dérober les identifiants et transférer des fonds. Quel que soit le secteur ciblé et l'envergure de l'attaque, les cybercriminels tirent parti de l'ingénierie sociale pour inciter les personnes à effectuer une action qui, autrefois, nécessitait l'exécution d'un code malveillant. Les tendances sur les messageries, les réseaux sociaux et les applications mobiles dévoilent les stratagèmes des cybercriminels. Il est donc impérieux de recommander aux organisations des solutions pour protéger leurs systèmes contre le facteur humain.

LA CYBERSECURITE

La sécurité (y compris la cyber sécurité) se définit comme la gestion des risques (dans un environnement cybernétique). On reconnait cependant que gérer est une affaire d'humains. Car la gestion invoque constamment:

- Les prises de décisions ;
- Les analyses
- Les appréciations et interprétations y compris à caractère émotionnel

LA CYBERSECURITE EST UNE AFFAIRE D'HUMAINS

En cyber sécurité, on reconnaît trois niveaux d'interventions:

- Niveau stratégique (réservé exclusivement à la ressource humaine)
- Niveau organisationnel (réservé exclusivement à l'humain)
- Niveau opérationnel (partagé entre l'humain et les machines)

L'Homme apparaît comme la première ressource en cyber-sécurité. En effet:

- Il audite et constate les insuffisances en matière de cyber sécurité
- Il développe les stratégies, politiques et plans d'actions opérationnelles de mise en œuvre pour améliorer le niveau de sécurité
- Il conduit la mise en œuvre d'opérations de sécurité
- Il conduit des missions de formations et sensibilisation à la sécurité
- Il réalise des investigations pour trouver les preuves numériques en cas d'infraction

Par ailleurs, l'Homme est de surcroît le maillon le plus faible de la chaine de cyber sécurité. Il est donc le plus exploité pour commettre des infractions cybernétiques. L'homme représente ainsi une importante vulnérabilité pour la cyber sécurité.

Question: D'où vient cette vulnérabilité ? Et de quelles façons se manifeste elle?

CARENCES DE COHESION EMOTIONNELLE ENTRE HUMAINS ET SOLUTIONS TECHNIQUES

L'EMOTIONEL PROBLEME OU PROBLEME D'EMOTIONS?

- Il se peut que dans la conception et la réalisation des solutions techniques utilisables en cyber sécurité, le facteur émotionnel n'est pas assez pris en compte.
- De la même façon dans le fonctionnement au quotidien de l'humain, la décision est motivée et toujours accompagnée d'émotions

INGENIERIE SOCIALE

Origines

Cette insuffisance de liens émotionnels entre les solutions techniques et humaines en cyber sécurité, permet de possibles détournements d'intérêts et d'attention des humains vers les appâts émotionnellement piégés par des cybercriminels pour amener les utilisateurs à mettre en difficulté eux-mêmes les solutions techniques de sécurité mises à leur disposition. La manifestation artistique de ce phénomène est communément appelée «INGENIERIE SOCIALE»

Les ressources utilisées pour la commission de ces délits sont : la peur - la paraisse - la convoitise - le stress - l'amour - la haine - les croyances - la pitié Etc…

Les environnements exploités pour compromettre l'intégrité, la confidentialité ou la disponibilité sont multiples et variés :

- Violation du contrôle d'accès aux actifs informationnels (biens essentiels et biens supports);
- Utilisation abusive d'actifs informationnels;
- Exploitation abusive de la messagerie électronique
- Désinformation;
- Espionnage électronique et interception de communications;

- Usurpation d'identités;
- Infections virales;
- Répudiation d'action cybernétique Etc…

Les victimes sont toujours démunies face à la sophistication des attaques et aux approches psychologiques utilisées.

Après un clic dans un email de phishing, un utilisateur peut recevoir un coup de téléphone et le cyber criminel peut essayer de le manipuler en jouant sur la peur et la responsabilité :

- «si vous ne le faîtes pas, votre chef vous en tiendra responsable...»;
- «Vous ne voulez pas m'aider ? Je pensais que vous étiez quelqu'un de bien...»;
- «Si vous m'aidez,vous en retirez un grand bénéfice…».

Exploiter simultanément les failles systèmes et le facteur humain, tel est l'objectif principal des agents cybercriminels.

En effet, les cybercriminels construisent des stratégies d'attaques personnalisées. Ils collectent de l'information, identifient leurs interlocuteurs grâce aux informations personnelles disponibles sur Internet et les réseaux sociaux puis contextualisent leurs attaques pour gagner le combat émotionnel dans votre prise de décision.

Des détails bien respectés pour garantir la vraissemblance

Exemple:

Les opérations de phishing par exemple sont ainsi de plus en plus élaborées aucune faute d'orthographe, un design graphique strictement identique aux communications officielles de l'organisme usurpé et des mentions contextualisées parfois personnelles mais souvent pertinentes trompant la vigilance de l'utilisateur qui finalement prendra la mauvaise décision de cliquer sur une URL malveillante...

QUELQUES CAS UTILISANT L'INGENIERIE SOCIALE

Fraude 419 (Arnaque nigériennes)

Escroqueries au gain à une loterie

Escroqueries à la fausse loterie Microsoft

Escroquerie aux gains à une fausse loterie

Escroquerie à la fausse offre d'emploi 1

Escroquerie à la fausse offre d'emploi 2

Escroquerie à la fausse offre d'emploi 3

Escroquerie aux frais à la fausse vente

Arnaque - Bien à vendre à l'étranger AcompteEscroqueries au gain à un concours Arnaque - Pseudo service consommateurs

Arnaque - Faux paiement d'un achat

Arnaque au président

Escroquerie au faux président

Escroquerie à la fausse qualité

Escroquerie aux faux ordres de virement

Escroquerie FOVI faux ordre virement international

Escroquerie des auto-entrepreneurs au RSI

Escroquerie aux faux papiers

Escroqueries au colis en attente

Escroqueries au gain à un jeu

Escroqueries au gain à un tirage au sort Escroquerie à la romance amoureuse

Escroqueries à l'offre d'emploi

Escroqueries à l'offre d'une tâche ponctuelle

Escroqueries à la vente à prix dérisoire ou gratuite

Escroqueries à la vente d'œuvres d'art

Escroqueries à l'achat chèque plus élevé que prévu

Escroquerie au gain loterie Fondation Bill Gates

Escroquerie au gain Fondation Lance Armstrong

Escroqueries à la prisonnière espagnole

Escroqueries à la pitié / compassion

Quelques cas - suite

Escroquerie à la romance amoureuse

Escroqueries à l'offre d'emploi

Escroqueries à l'offre d'une tâche ponctuelle

Escroqueries à la vente à prix dérisoire ou gratuite

Escroqueries à la vente d'œuvres d'art

Escroqueries à l'achat chèque plus élevé que prévu

Escroquerie au gain loterie Fondation Bill Gates

Escroquerie au gain Fondation Lance Armstrong

Escroqueries à la prisonnière espagnole

Escroqueries à la fausse location Escroqueries au chantage à la Webcam

Escroquerie à la fausse offre de bourse

Escroquerie à la fausse offre de stage

Escroquerie à la fausse donnation

Escroquerie aux faux legs (faux héritages)

Escroquerie à la fausse location

Escroquerie à la fausse vente immobilière

Escroquerie aux marabouts

Escroquerie à la voyance

Escroquerie aux astrologues
Escroquerie aux options binaires

Escroquerie Interpol

Escroquerie aux faux techniciens Microsoft

Escroquerie aux chaine d'argent

Escroquerie aux ventes pyramidales

Escroquerie à la boule de neige

Escroquerie à la Pyramide de Ponzi

Escroquerie aux ventes multiniveau

Escroquerie au faux bon père de famille

Escroquerie Cercles de dons

Escroquerie Spam «Make Money Fast»

Escroquerie Fausses transactions commerciales

Escroquerie Utilisation frauduleuse de moyens de paiement

Escroquerie Fausse propositon de mariage

Escroquerie Fausse maladie grave

Escroquerie Escroqueries financières diverses

Escroquerie à l'annulation et demande de remboursement

Escroquerie à la fausse transaction immobilière
Escroquerie à l'astrologie

Escroquerie aux options binaires

Escroquerie investissements dans les terres rares

Escroquerie aux faux investisseurs

Escroquerie à Interpol

Escroquerie aux adresses e-Mail trompeuses

Escroquerie Wash Wash

Escroquerie Assistance victimes d'escroqueries

Escroquerie au blanchiment d'argent sale

Escroquerie au marabout voyant sorcier envoûteur

Escroquerie Spam « Make Money Fast »

Escroquerie Fausses transactions commerciales

Escroquerie Utilisation frauduleuse de moyens de paiement

Escroquerie Fausse propositon de mariage

Escroquerie Fausse maladie grave

Escroquerie Escroqueries financières diverses

Escroquerie à l'annulation et demande de remboursement

Escroquerie à la fausse transaction immobilière
Escroquerie à l'astrologie

Escroquerie aux options binaires

Escroquerie investissements dans les terres rares

Escroquerie aux faux investisseurs

Escroquerie à Interpol

Escroquerie aux adresses e-Mail trompeuses

Escroquerie Wash Wash

Escroquerie Assistance victimes d'escroqueries

Escroquerie au blanchiment d'argent sale

Escroquerie au marabout voyant sorcier envoûteur

LEÇONS

1 L'ingénierie sociale est en pleine croissance, elle est dopée par la socialisation et la globalisation de l'usage des technologies.

2 Les solutions à ce problème humain sont:

- Le renforcement de la formation et la sensibilisation permanentes des utilisateurs;
- L'intégration des contraintes psychosociales dans le développement de solutions techniques;
- L'intégration de l'intelligence artificielle;
- Le renforcement des capacités des services d'enquêtes opérationnelles.

CYBERMENACE N°1

- Les techniques d'ingénierie sociale constituent la menace N°1 pour la cyber sécurité;
- Dans le cadre de cyberguerres, la maîtrise de ces techniques représente un grand atout pour les services de sécurité dans un sens comme dans l'autre;
- La manipulation et la désinformation constituent des axes privilégiés de l'ingénierie sociale.

AU CAMEROUN

La crise dans les régions du Nord-Ouest et du Sud-Ouest, est une illustration de ce que peut représenter l'usage des techniques de l'ingénierie sociale.

Les atouts de l'ingénierie sociale pour les cybercriminels

- Solution peu coûteuse, facile, et efficace;
- Expérience de marche riche et adaptation facile pour de nouveaux schémas d'arnaque;
- Informations personnelles sur de potentielles victimes disponibles et accessibles facilement;
- La victime est complice inconsciente de son propre forfait. Elle s'en sort de là avec du complexe et de la honte. Ce qui limite sa motivation à la plainte;
- La victime accomplie elle-même une partie de la tâche à la place du cybercriminel, ce qui complique le cadre d'investigations.

PLENIERE N° 2 : CYBERSECURITE, PROTECTION DE L'INFORMATION ET DES SYSTEMES D'INFORMATION

Confidentialité des données, Big Data et Cyber-sécurité, Cryptographie, Signature numérique, BlockChain, Contrôle d'accès…

Détecter des attaques et y apporter des réponses est primordial pour la protection des organisations. La survie à une attaque va dépendre de la rapidité avec laquelle on va y apporter une réponse. Les techniques comme la blockChain, le chiffrement, la signature numérique, le filtrage des paquets de données, l'authentification et le contrôle d'accès, appliquées à la cyber-sécurité permettent aujourd'hui d'apporter des réponses significatives et nécessaires pour répondre aux problèmes de sécurité de l'information et des systèmes d'information, et réduire par la même occasion les risques liés aux infractions cybernétiques.

MODERATEUR : Mr. OTTOU, MINPOSTEL

INTERVENANT N°1 : Mme ASSAKO, ANTIC

Niveaux de responsabilités en cyber sécurité et lutte contre la cybercriminalité

Pour répondre aux préoccupations de cybercriminalité et à celles de la cyber-sécurité, il est important de définir les niveaux de responsabilités des acteurs de la société. Nous parlerons ici des responsabilités de l'Etat, des responsabilités des organisation/entreprises, et enfin des responsabilités individuelles/ personnelles.

SOMMAIRE

INTRODUCTION

FONDEMENT DE LA LIBERTE DE COMMUNIQUER

1 **La Déclaration des droits de l'homme et du citoyen (1789)** : la libre communication des pensées et des opinions est : «un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement».

2 **La Déclaration universelle des droits de l'homme (1948)** « Tout individu a droit à la liberté d'opinion et d'expression, en ce qui concerne le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répondre sans considération de frontières, les informations et les idées par quelque moyen que ce soit».

3 **Le règlement des Télécommunications internationales (1989)**: Adopté à Melbourne par l'UIT et signé par 88 Etats dont le Cameroun, Le RTI prévoit des dispositions relatives au droit de communiquer en ces termes : «En conformité avec la législation nationale, tout usager ayant accès au réseau international établi par une Administration a le droit d'émettre du trafic».

STATISTIQUES :

- 4,12 milliards d'internautes à travers le monde soit 54% de la population mondiale ;
- 3,36 milliards d'inscrits sur les réseaux sociaux, soit 44% de la population mondiale ;
- 65 vols de données par seconde ;
- 140 attaques de phishing par heure ;
- 41% : taux de succès d'un ransonware ;
- 10 min (temps utilisé pour casser un mot de passe)

Au Cameroun :

- 156 faux comptes Facebook des personnalités publiques ;
- 16 000 vulnérabilités détectées dans les SI;
- 28 attaques webdefacement sur les sites web des Administrations publiques.

I - NIVEAUX DE RESPONSABILITE en cyber sécurité

a L'ETAT

- Fixe la politique générale ;
- Défini la Stratégie ;
- Met en place les Institutions et fixe les rôles ;
- Prend des textes légaux et réglementaire pour asseoir la politique.

b LES STRUCTURES DE SECURITE

- Assurent la sécurité des personnes et des citoyens sur tous les champs (terre, mer, air, cyberespace ;
- Collabore avec les régulateurs.

c LES JUGES

- Chargés de l'application de la loi.

d LES REGULATEURS (L'ANTIC ET L'ART)

- Facilitateurs ;
- Suivi du respect de la Politique et des normes (lois, règlements, normes ISO) ;

- Opérationnalité (Audits de sécurité, veille sécuritaire, certification électronique, homologation des moyens de cryptographie) ;
- Régulation visible et régulation invisible.

e LES OPERATEURS DES RESAUX DE COMMUNICATIONS ET FOURNISSEURS DE SERVICES

- Fournir les services de communication électronique de manière équitable ;
- Assurer le secret des communications et protéger la vie privée des usager ;
- Sécuriser leurs SI (normes, politique sécurité, plan de continuité des services) ;
- Conserver les données de trafic pendant 10 ans ;
- Identifier les abonnées (voix et données) et les terminaux.

f LES AUTRES ENTREPRISES PRIVEES (Interconnectées, traitant des données automatisées) ET FOURNISSEURS DE CONTENUS ET DE SERVICES A VALEUR AJOUTEE

- Assurer le secret des communications et protéger la vie privée des usagers ;
- Sécuriser leurs SI (normes, politique sécurité, plan de continuité des services) ;
- Conserver les données de trafic pendant 10 ans ;
- Obligation d'accord préalable avant la conservation des données personnelles ;
- Obligation de fournir les données en clair sur réquisition;
- Accessibilité des données conservées au juge.

II - ATTEINTES EFFECTUEES A TRAVERS LES RESEAUX

a LES ATTEINTES AUX SYSTEMES D'INFORMATION

- Atteintes à Intégrité ;
- Atteintes à la Confidentialité ;
- Atteintes à la Disponibilité ;
- Atteintes aux systèmes automatisés ;
- Atteintes aux systèmes de cryptographie.

b LES ATTEINTES A L'ORDRE PUBLIC

- Terrorisme;
- Diffusion de nouvelles fausses;
- Racisme.

c LES ATTEINTES A LA VIE PRIVEE

- Droit à l'image;
- Diffamation;
- Usurpation d'identité.

d LES ATTEINTES AUX MŒURS ET A LA PUDEUR

- Diffusion des images portant atteinte à la pudeur;
- Pédophilie et pornographie.

III - SANCTIONS ADAPTEES AUX ATTEINTES

e LES ATTEINTES AUX SYSTEMES D'INFORMATION

- Atteintes à la confidentialité (accès frauduleux à un système d'information : articles 65,66 et 68) ;
- Atteintes à l'intégrité des systèmes d'information : articles 67, 69, 70, 86 et 87 ;
- Atteintes à la disponibilité des systèmes d'information :

article 71 et 72 ;

- Atteintes aux systèmes automatisé des données: article 64 et 85 ;
- Atteintes aux systèmes de cryptographie : article 60 et 88.

f LES ATTEINTES A L'ORDRE PUBLIC

Diffusion de nouvelle sans preuve de véracité (Loi cyber sécurité)

Article 78.- (1) Est puni d'un emprisonnement de six (06) mois à deux (02) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui publie ou propage par voie de communications électroniques ou d'un système d'information, une nouvelle sans pouvoir en rapporter la preuve de véracité ou justifier qu'il avait de bonnes raisons de croire à la vérité de ladite nouvelle.

Racisme (Loi cyber sécurité)

Article 77.- (1) Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 2.000.000 (deux millions) à 5.000.000 (cinq millions) FCFA, ou de l'une de ces deux peines seulement, celui qui, par la voie de communications électroniques ou d'un système d'information, commet un outrage à l'encontre d'une race ou d'une religion.

(2) Les peines prévues -à l'alinéa 1 ci-dessus sont doublées lorsque l'infraction est commise dans le but de susciter la haine Ou le mépris entre les citoyens.

Terrorisme

g LES ATTEINTES A LA VIE PRIVEE

Atteinte à la vie privée et diffamation (Loi cyber sécurité)

Article 74.- (1) Est puni d'un emprisonnement de un (01) à deux (02) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) F CFA, quiconque, au moyen d'un procédé quelconque porte atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant, saris le consentement de leur auteur, les données électroniques ayant un caractère privé ou confidentiel.

(4) Est puni d'un emprisonnement de six (06) mois à deux (02) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) F CFA ou de l'une de ces deux peines seulement, le fait de collecter par des moyens illicites, des données nominatives d'une personne en vue de porter atteinte à son intimité et à sa considération.

(5) Les peines prévues à l'alinéa 4 ci-dessus sont doublées, à l'encontre de celui qui met, fait mettre en ligne, conserve ou fait conserver en mémoire informatisée, sans l'accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître ses origines tribales, ses opinions politiques, religieuses, ses appartenances syndicales ou ses mœurs.

France : CA de METZ (publication sur la toile dès 1999 du «Grand Secret» interdit d'édition en 1996 ;

Tribunaux d'instance de Puteaux 1999 diffusion d'une page «comment AXA nous prend pour des Cons»

h LES ATTEINTES AUX MŒURS

Diffusion des images portant atteinte à la pudeur (Loi cyber sécurité)

Article 75 (1) Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) F CFA ou de l'une de ces deux peines seulement, celui qui enregistre et diffuse à but lucratif, par la voie de communications électroniques ou d'un système d'information sans le consentement de l'intéressé, des images portant atteinte à l'intégrité corporelle.

Pédophilie et pornographie (Loi cyber-sécurité)

Article 76.- Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui confectionne, transporte, diffuse, par voie de communications électroniques ou d'un système d'information, un message à caractère pornographique enfantine, ou de nature à porter gravement atteinte à la dignité d'un enfant.

IV - ANALYSE CRITIQUE DE LA REGLEMENTATION du dispositif

VIDE JURIDIQUE SUR :

- L'usurpation d'identité sur Internet ;
- La Vengeance pornographique ;
- L'escroquerie à l'aide des réseaux sociaux (scamming) ;
- Le Droit à l'image ;
- La protection des données à caractère personnel ;
- La mise en œuvre des recommandations issues des audits de sécurité ;
- Les sanctions administratives en cas de non conservation des données de trafic.

CONCLUSION

Quelques pistes de solution

- Mise en œuvre effective de la Stratégie nationale de migration de l'IPv4 à L'IPv6 ;
- La mise en place d'un Data Center national de grande capacité;
- La révision du cadre légal pour sa mise en conformité au contexte national (prise en compte des crimes récurrents, réduction du délai de conservation des données de trafic etc.);
- Ratification des conventions de Budapest et de l'UA ;
- Déploiement des dispositifs de sécurité dans toutes les infrastructures sensibles ;
- Mise en place d'un Observatoire multi acteurs pour l'identification en temps réel des détenteurs d'adresses IP.

INTERVENANT N°2 : M. BELEOKEN Hervé,
Head of Sales & Business Development French Sub-Sahara Africa and Indian Ocean Motorola Solutions

Solutions intégrées de sécurité et de communications critiques pour la protection des villes et la prospérité des entreprises

La sécurité est une science de gestion. Elle se définit comme la gestion des risques. En ce qui concerne la sécurité des systèmes d'information, elle ne fait pas exception à cette situation. Les nouvelles technologies sont devenues des outils indispensables dans la vie de tous les jours. Nous en sommes depuis longtemps convaincus qu'il ne peut y avoir de développement sans sécurité. Par conséquent, il est crucial pour tout un chacun de se sentir plus responsable. Aussi, la puissance publique doit s'assurer de la protection des citoyens et des biens ainsi que de l'intégrité du pays.

De ces engagements dépendra la capacité des entreprises à investir localement ou à accroître leurs investissements, entreprises qui par ailleurs et selon leurs secteurs d'activité, éprouveront le besoin d'acquérir des solutions de communications critiques favorisant leur prospérité et apportant des réponses opérationnelles à des situations de prévention ou de risque.

Plan

I - MOTOROLA SOLUTIONS

II - LA TECHNOLOGIE AU SERVICE DE LA SECURITE PUBLIQUE

A – Des solutions manuelles/analogiques aux solutions digitales

B – Voix/Vidéo/Données: approche globale et intégration

I - MOTOROLA

Mobiliser et connecter les personnes au moment où il importe le plus

MOTOROLA SOLUTIONS – LEADER MONDIAL DES SOLUTIONS DE COMMUNICATIONS CRITIQUES

NOTRE PORTÉE INTERNATIONALE NOUS PERMET D'INTERAGIR AVEC NOS CLIENTS N'IMPORTE OÙ

PRESENCE DANS 160+ PAYS

20m EMPLOYÉS DANS **65** PAYS

1,800 VENTES DIRECTES

20m PARTENAIRES INDIRECTS

3,600 PERSONNELS D'INTÉGRATION, ASSISTANCE DE TERRAIN & SOLUTIONS

R&D DANS 6 PAYS, INNOVATION 2 PAYS

PLUS DE 10,000 BREVETS

A/ MOTOROLA EN AFRIQUE

Motorola a démarré ses activités en Afrique en 1966, et aujourd'hui nous disposons de fonctions de ventes et de services sur l'ensemble du continent. La région couvre 50 pays africains.

PAYS D'AFRIQUE CENTRALE ET DE L'OUEST : Cameroun, RD Congo, Côte d'Ivoire, Sénégal, Niger, Gabon, Tchad, Guinée, Mali, Bénin, Burkina Faso, Togo, RCA, Congo Brazzaville, Mozambique, Malawi, Namibie, Madagascar, Seychelles, Maldives.

AFRIQUE ORIENTALE : Kenya, Ouganda, Éthiopie, Érythrée, Tanzanie, Djibouti, Somalie, Burundi, Rwanda, Comores.

PAYS DE L'AFRIQUE AUSTRALE : Afrique du Sud, Angola, Botswana, Swaziland, Zimbabwe, Zambie, Ile Maurice, Lesotho, Comores, Mozambique, Malawi, Namibie, Madagascar, Seychelles.

VISION & OBJECTIFS

- Innover pour créer des applications, des solutions d'infrastructure et de services ;
- Aider les gouvernements à construire des villes plus sûres;
- Aider les entreprises à devenir des organisations plus robustes, donc plus profitables;
- Fournir des solutions de bout en bout adaptées aux besoins de nos clients;
- Maintenir notre leadership en tant que partenaire de choix et intégrateur de référence en Afrique et dans le monde en matière de communications critiques et sécurisées.

NOS SOLUTIONS

Mobiliser les informations nécessaires pour vous permettre de prendre les meilleures décisions à temps;

Produire sans compromis des solutions intelligentes de sécurité pour garantir l'efficacité de vos missions.

MOTOROLA = CONSTRUCTEUR ET INTEGRATEUR

- CENTRE DE COMMANDEMENT ET DE CONTROLE INTEGRE;
- SOLUTIONS DE RADIO COMMUNICATIONS;
- VIDEO SURVEILLANCE INTELLIGENTE;
- CONTROLE D'ACCES, afis, DRONES, …
- SOLUTIONS DE COMMUNICATIONS MULTI-SUPPORT (FO, hf, VSAT, WIFI, …)

2018 : ACQUISITION D'AVIGILON, un leader dans les solutions avancées de sécurité et de surveillance /intelligence artificielle.

- Nouveaux Produits et Solutions
- Analyse vidéo, logiciel et matériel de gestion de vidéo sur IP, caméras de surveillance et solutions de contrôle d'accès.
    - Infrastructure critique, aéroports, installations gouvernementales, lieux publics, soins de santé, commerce de détail et plus encore.

Nous créons une solution de bout en bout pour les clients afin de protéger leurs employés, leurs clients et leurs actifs. Nos solutions sont utilisées par des clients commerciaux et gouvernementaux

II - MOTOROLA : LA TECHNOLOGIE AU SERVICE DE LA SECURITE PUBLIQUE

LES DEFIS OPERATIONNELS

- **SECURITE PUBLIQUE : Protection des villes, des citoyens, des sites stratégiques et biens divers**
    - Les menaces et conflits exigent une réponse polyvalente, déployable et des efforts conjoints;
    - Capacité d'anticiper, de prendre les bonnes décisions et de réagir rapidement;
    - Protection des biens et des personnes;
    - Lutte contre la (cyber) criminalité, le banditisme et l'insécurité;
    - Lutte contre tout type de trafic.
- **Gestion sécurisée des systèmes d'information**
- **Sécurité et sûreté** : assurer des conditions de sécurité et de travail de qualité dans des environnements opérationnels complexes
- **Communiquer**

Obtenir, gérer et transmettre des volumes de données et d'informations entre différents groupes de travail, et ce, pour permettre des opérations efficaces.

LES OBJECTIFS OPERATIONNELS : une approche globale nécessaire

- Des plateformes de communications sécurisées appropriées pour les différents groupes de travail aux environnements opérationnels complexes;
- Améliorer la rapidité et l'efficacité des opérations;
- Sécuriser au mieux les réseaux, les sites et les lieux sensibles;
- Assurer la protection des personnes et des biens;
- Gérer et traiter efficacement des situations d'urgence;

- Accroitre le sentiment de sécurité des citoyens et des utilisateurs;
- Assurer l'intégrité du territoire national et de l'espace web;
- Donner une image encore plus rassurante du pays pour rassurer les potentiels investisseurs (prospérité des entreprises).

DES SOLUTIONS MANUELLES / ANALOGIQUES AUX SOLUTIONS DIGITALES

Les 5 raisons majeures de passer au numérique

- Sécurité;
- Interopérabilité;
- Meilleure couverture;
- Capacité de données;
- Proactivité & réactivité.

Les objectifs stratégiques

- Des équipements adaptés pour la lutte contre l'insécurité (d'où qu'elle vienne);
- La capacité d'analyse pour prendre rapidement les bonnes décisions;
- Des réseaux de communications sécurisées pour transmettre de manière intègre et fiable des informations sensibles inter services ou sur le terrain;
- Interopérabilité avec les réseaux existants et interconnexion;
- Protection contre les interférences (radio, virus...);
- Solutions opérationnelles et des outils efficaces de contre-attaques.

Objectif : Fluidité de la communication (transmission de l'information) et efficacité dans l'action

Rendez votre organisation plus efficace et mieux connectée, s'ouvrir au monde digital : Les transmissions sécurisées numériques

Quelques fonctionnalités d'Appels :

- Appels de groupes ou individuels/ Appels d'urgence;
- Qualité de communication, enregistrement et écoute;
- Messages textes courts;
- Géolocalisation via GPS;
- Téléphonie;
- Solutions de Computer Aided Dispatch;
- Applications diverses sécurisées;
- Couverture nationale sécurisée.

B/ VOIX / VIDÉO / DONNÉES : APPROCHE GLOBALE ET INTÉGRATION

Des villes sûres et intelligentes à travers le Safecity concept

- Amélioration de la qualité de vie;
- Terre d'attractivité;
- Un juste équilibre entre sécurité, mobilité et environnement;
- Intégrité territoriale.

La criticité du temps est un facteur clé pour maintenir un pays et ses villes en sécurité. Les opérations de sécurité publique sont de plus en plus dépendantes des informations obtenues (voix, vidéo, data), de leur analyse et de leur utilisation. La collaboration est donc essentielle pour maintenir une ville en sécurité et ceux qui décident en sont de plus en plus conscients.

Aujourd'hui, les responsables gouvernementaux nous demandent :

Comment accueillir/intégrer d'autres agences, partager avec elles et en toute sécurité des données et gérer des ressources?

Comment être responsable de données reçues d'une autre agence sans compromettre sa sensibilité ?

Comment pouvons-nous lier et hiérarchiser?

Les données structurées et non structurées et conduire des résultats corrects. ?

Comment les données peuvent-elles être liées à des métadonnées géo spatiales et autres méta-informations opérationnelles d'une manière efficace ?

Comment passer d'une attitude réactive à un comportement proactif et mettre en place ce concept de ville/pays plus sûr

Les analyses complexes révèlent des schémas invisibles, fournissent une vue d'ensemble et recommandent l'allocation des ressources.

Comment diffuser l'intelligence pour des rôles appropriés sur nimporte quel réseau et vers n'importe quel support?

Comment pouvons-nous garder les utilisateurs conscients de la situation sans distraire ou accabler et faciliter la prise de décision critique ? Comment prévenir ou lutter contre les risques ?

Les données prolifèrent partout dans le monde - y compris dans le domaine de la sécurité publique. Le public est de plus en plus exigeant. En effet, 98% Des officiers demandent des technologies plus sophistiquées (Police Executive Research Forum (PERF)) et 91% des citoyens pensent que les agents de sécurité publique devraient utiliser des technologies plus avancées afin de prévenir et de résoudre des crimes (Police Executive Research Forum (PERF)).

D'ou la necessité :

- d'élaborer des solutions intelligentes de sécurité publique
- de transformer les données en intelligences;
- d'avoir des données analyses intelligentes;
- de transformer vos opérations grâce au renseignement.

SOUTENIR

Command Central Inform : Prenez des décisions plus rapides sur le terrain grâce à des renseignements géospatiaux en couches.

Command Central Aware : Gérez plus efficacement les opérations grâce à des renseignements intégrés constitués de voix, données et vidéos.

PLANIFIER

Command Central Analytics : Transformez la planification stratégique en action tactique grâce à une analyse mobile descriptive. Patrouillez en anticipant grâce à des prévisions intelligentes sur les délits commis dans la zone.

RECUEILLIR

Command Central Vault :

Unifié. Simplifié. Intelligent. Logiciel de gestion numérique des preuves.

La réalité de la VIDEO PROTECTION

« La plupart des flux vidéo ne sont jamais visionnés. Dans certains cas, il s'agit de 99% du volume des données collectées ».

Guide de conception de surveillance vidéo IP

Selon Fredrik Nilsson, «Un taux stupéfiant de 99% de toutes les vidéos de surveillance enregistrées sont effacées avant même d'avoir été visionnées».

Aussi, «L'efficacité décroît car regarder un écran de moniteur – où dans 99% des cas rien ne se passe et où vous vous efforcez à chercher des moments suspects – est une tâche pratiquement impossible».

Vie sécurisée.

Dans la même lancée - Charles Palmer, Directeur Technique de Département Sécurité et Vie Privée chez IBM Research « L'un des plus gros problèmes avec la surveillance est que 99% du temps est d'un ennui profond »

En quoi consistele «Vidéo Synopsis» ? Comment ça marche? Et il y a en plus … Vidéo Syndex!

- Filtrage par direction
- Filtrage par couleur
- Filtrage par taille

Protection à 5 niveaux intégrés

Motorola Solutions offre une solution à grande échelle pour les centres de contrôle fixes, les postes de commandement déployés, et des moyens de surveillance de sites sensibles.

5 niveaux de protection :

- Barrière électronique / physique / Contrôle d'accès;
- Radars et Caméras thermiques longue distance;
- Communications critiques (services de localisation incluses);
- Drones;
- Centre de contrôle.

EVOLUTION D'UN CENTRE DE COMMANDEMENT NOS SOLUTIONS POUR LES CENTRES DE COMMANDEMENT ET DE CONTROLE

Les défis d'un centre de commandement aujourd'hui: De multiples plateformes discrètes avec des impacts au niveau opérationnel, de performance et des coûts

- Interface utilisateurs uniques;
- Demandant ses propres consoles;
- Solutions de stockage individuel;
- Plusieurs systèmes de géocodage;
- Authentification séparée;
- Pas d'interfaces standard;
- Cartographie isolée unique.

Centre de commande et de contrôle intégré

- Interface utilisateurs uniques;
- Entièrement corrélé au niveau CAD, voix et vidéo;
- Données, requêtes et rapports unifiés;
- Système de géocodage commun;

- Authentification unique;
- Plate-forme flexible et évolutive;
- Cartographie commune et interactive.

Analyse des données : Transformer l'intelligence en information

Que s'est-il passé ? Descriptif – Tableaux de rapports

Pourquoi est-ce arrivé ? Diagnostic – La découverte des données

Que se passera-t-il ? Prédictive- Prévision, simulation

Ce que nous devrions faire ? Prescriptive - Planification, Optimisation

Exemple : MOTOCLOC SAFE CITY SOLUTION CONCEPT

MotoCLOC est un système intégré de commande et de contrôle comprenant :

- Cartographie;
- Géolocalisation;
- Gestion vidéo;
- Gestion des données;
- Gestion des évènements;
- Prises d'appels.

SOLUTIONS DE BOUT EN BOUT MOTOROLA = INTEGRATEUR

- Motorola intégrateur de solutions. D'où, le nom MOTOROLA SOLUTIONS;
- Expérience et capacité à gérer des projets en prenant le leadership en tant que Chef de projet;
- Capacité à gérer une multitude de sous-traitants en prenant la responsabilité complète du projet;
- Possibilité pour le maître d'ouvrage de s'appuyer techniquement sur Motorola pour garantir la bonne marche du

volet sécurité des communications et solutions de surveillance pour la conférence;

- Des solutions éprouvées, modernes et de dernière génération;
- Formation des clients et transfert de compétences des solutions installées;
- Assistance Motorola pour le déploiement de la solution;
- Possibilité d'assistance technique sur site durant la conférence;
- Possibilité d'aides pour la recherche de financement de projets.

MOTOROLA EN AFRIQUE Systèmes déployés en Afrique durant les 50 dernières années dans les pays suivants : Nigéria - Tanzania - Kenya - Côte d'Ivoire - Sénégal - Uganda - Cameroun - RDC - Rwanda - Guinée Equatoriale - Guinée Conakry - Sierra Leone - Botswana - South Africa - Angola - Benin.

DES PROJETS CLÉS POUR DES CLIENTS GOUVERNEMENTAUX EN AFRIQUE

MINISTÈRE DE LA DÉFENSE, GUINÉE ÉQUATORIALE : Expansion et mise à niveau du système de communication critique à la mission;

PRÉSIDENCE DU BOTSWANA : Expansion et mise à niveau du système TETRA;

RÉPUBLIQUE DÉMOCRATIQUE DU CONGO : Mise en place du système TETRA;

MINISTÈRE DE L'ENSEIGNEMENT, ÉRYTHRÉE : Mise en place d'un réseau large bande pour relier les écoles à Internet.

PRINCIPAUX PROJETS POUR LES CLIENTS DES SERVICES PUBLICS EN AFRIQUE

FORCES DE POLICE DU NIGERIA : Expansion et mise à niveau du système ASTRO MOTOTRBO de dizaines de milliers d'appareils;

POLICE D'AFRIQUE DU SUD : Plusieurs systèmes TETRA Accords de service extensifs;

POLICE DU KENYA : TETRA COMMUNICATIONS Système;

POLICE DE L'OUGANDA : Système de communication TETRA;

POLICE DE L'ANGOLA : Communications TETRA système.

PRINCIPAUX PROJETS – AFRIQUE POUR DES CLIENTS DES SERVICES PUBLICS, PÉTROLE & GAZ, MINE CLIENTS

KPLC – SOCIÉTÉ D'ÉLECTRICITÉ KENYA – expansion de mise à niveau et du système ASTRO;

RIO TINTO & CBG Système de communication TETRA;

SHELL NIGERIA Système TETRA;

CHEVRON NIGERIA Système ASTRO;

CHEVRON ANGOLA système ASTRO.

INTERVENANT N°3 : Dr. BELL B.G.,
Ph.D sciences techniques en cyber sécurité

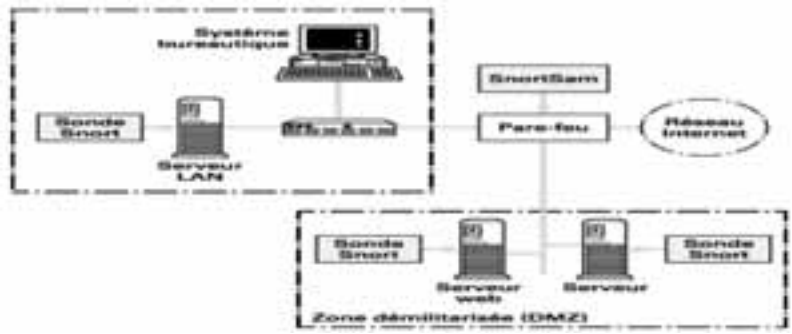
Solutions techniques, crypto, blockchain, Systèmes de détection et prévention d'intrusions, de malveillance et contrôles d'accès aux systèmes d'information

Les systèmes de détection et prévention d'intrusion sont des solutions permettant de réduire l'impact des attaques hautement orchestrées par des adversaires humains ou matériels sophistiqués. Les attaques orchestrées représentent aujourd'hui l'une des formes les plus dangereuses pour les responsables des systèmes d'informations. Ces systèmes combinent différentes technologies pour apporter des réponses contre des adversaires humains organisés en utilisant des combinaisons sophistiquées d'outils et de techniques dans les environnements informatiques complexes. D'autres formes d'attaques liées à l'ingénierie sociales et aux fake news trouvent leur réponses grâce aux techniques de sensibilisation humaines et à une organisation des procédures adaptée au contexte. Nous parlerons également de la cryptographie qui apporte des solutions de chiffrement, de signature et de certification numérique, ainsi que la blockchain pour sécuriser les transactions électroniques diverses.

SERVIR L'OPERATIONALISATION DE LA CYBERSECURITE

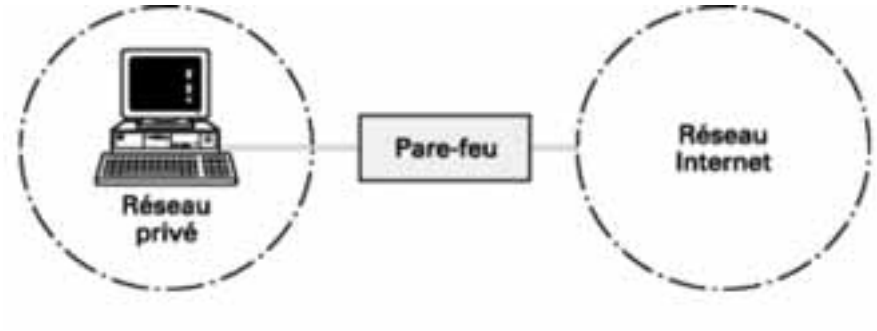
- Les solutions techniques en cyber sécurité servent l'opérationnalisation des mesures. A travers :
    - Les techniques de détection et prévention;
    - Les techniques de filtrage;
    - Les techniques d'investigations;
    - Les techniques cryptographiques, PKI et Blockchain.

I - Techniques de détection et prévention



- Détecter et prévenir les intrusions dans les systèmes d'information;
- Détecter les programmes malveillants (Virus, chevaux de Troie; programmes espions etc…);
- Détecter les failles et vulnérabilités dans les systèmes d'information.

II - Techniques de filtrage



Ces procédés permettent de filtrer les contenus et flux d'entrée et de sortie dans un système d'information. Ils servent entre autre pour :

- Le contrôle d'accès et de sortie dans un système d'information;
- La vérification d'identités lors des requêtes de services dans un système d'information;
- La lutte contre les attaques de déni de services informatiques;
- La construction des zones démilitarisées;
- La création des structures de défense en profondeur.

Quelques architectures de défense

III - Techniques d'investigations

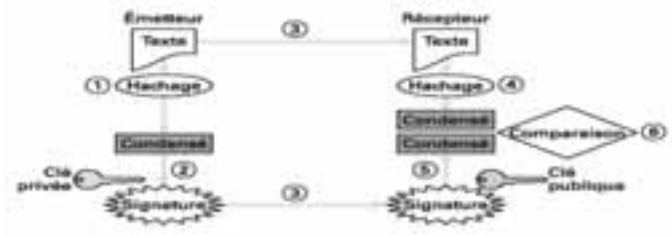
Elles se déclinent à travers les actions suivantes :

- L'interception de communications;
- L'écoutes de canaux de transmission;
- L'analyse de contenus;
- La reconnaissance biométrique (voix, forme etc…);
- La vérification d'intégrité des contenus Etc…

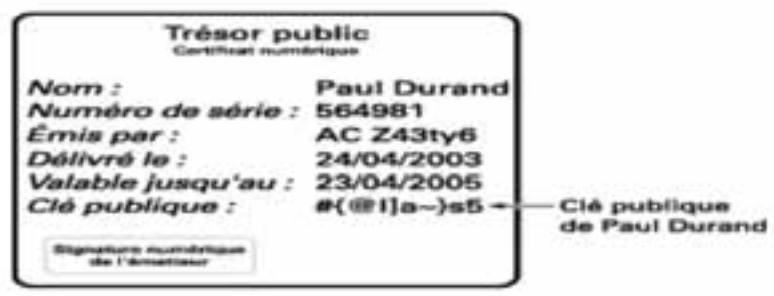
Systèmes cryptographiques

Ces systèmes sont très éfficaces pour :

- la confidentialité via le chiffrement;
- l'intégrité via le hachage, le MAC et la signature numérique;
- l'uthenticité de l'auteur via la certification numérique;
- La non répudiation des actes numériques via la signature et la certification numérique.
- Schéma de signature numérique

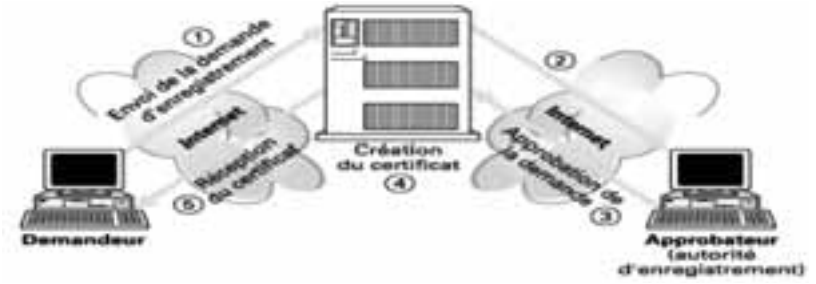


CERTIFICAT NUMERIQUE



Processus technique de demande de certificat numérique

Processus technique de demande de certificat numérique



A/ Cryptographie et fonctions de confiance

Les techniques cryptographiques ont à terme permis de construire les fonctions de confiance dans les systèmes d'information. Il s'agit de la signature et la certification numérique. Ces fonctions de confiance ont permis de construise des systèmes ou chaines de confiance numériques:

- PKI (Public Key Infrastructure);
- Bockchain.

Modélisation de la question du problème-confiance

- Nous constatons dans l'étude des problèmes, qu'il y a une constante à tous les problèmes. Cette constante est la crise de confiance;
- C'est-à-dire, tout problème d'où qu'il vienne, de quelque nature que ce soit et quelles que soient ces conséquences entraine une crise de confiance.

Modèle de confiance

- La confiance existe sous forme de chaine, qui va de la boucle de confiance (confiance en soi) à la relation de confiance (confiance aux autres). C'est donc une relation entre deux ou plusieurs entités qui parfois dans une construction prend la forme de fonction, dite de confiance. La confiance se construit généralement sous deux formes :
    - La chaine de confiance verticale ;
    - La chaine de confiance horizontale.

1/ La chaine de confiance verticale

Elle est basée sur une autorité de confiance racine et unique qui étend la confiance vers d'autres nœuds de confiance sur un modèle de chaine privée. Dans ce modèle, on ne peut vérifier que le nœud le plus proche. S'il y a rupture dans un nœud de confiance antérieur, la chaine peut être compromise sans que les entités n'en soient informées. Et si un nœud se compromet, presque toute la chaine de confiance sera corrompue

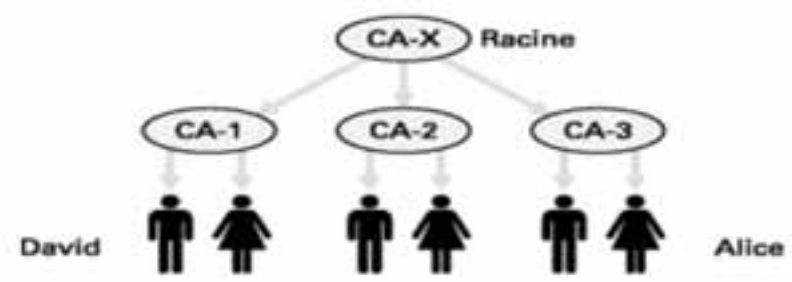
Pour faire confiance à une entité dans la société, on est obligé de consulter l'autorité de confiance. Et si cette dernière est compromise, ca devient une situation de corruption et de faux généralisé. Dans cette situation, les valeurs échangées perdent complètement leur contenu.

Exemple : L'Etat qui repend la confiance dans les documents comme (pièces d'identité ; la monnaie, les diplômes etc…).

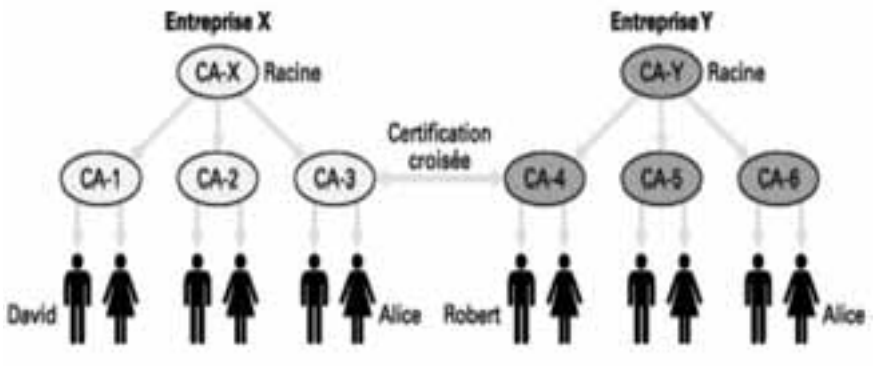
Spécificités de la chaine de confiance verticale

- Ce modèle est coûteux et risqué pour l'utilisateur;
- Il ne peut pas s'appliquer dans les conditions d'échange intensifs comme l'échange d'information;
- Ce modèle a beaucoup de lacunes;
- Impossible de vérifier toute la chaine de confiance, d'où, le risque d'accepter le faux;
- Ce modèle permet de construire les PKI.

Hiérarchie de confiance verticale



Extension de la chaine de confiance verticale par re-connaissance mutuelle



B/ Aboutissement de la chaine de confiance verticale : PKI

APPLICATIONS DE LA PKI

- Réseaux privés virtuels;
- La sécurisation de la messagerie électronique (chiffrement et signature des messages et pièces jointes);
- La télé déclaration (TVA, Impôts, salariés, etc.);
- Systèmes de paiement électroniques;
- Appels d'offres;
- Industrie pharmaceutique;
- Notaire en ligne;
- Cartes d'identité (CNI, passeport, carte d'électeur...).

2/ Chaine de confiance horizontale

Pour ce modèle :

1 Il n'y a pas d'autorité de confiance unique;

2 Tout le monde vérifie tout le monde et concourt à la crédibilité de tout le monde par des actions d'opinion;

3 La confiance est distribuée de manière presqu'équitable auprès de toutes les entités de la société;

4 Pas de centre de certification unique et donc pas de risque de saturation du système de certification lors des grands échanges;

5 Pas de dictat d'une autorité unique de confiance;

6 Moins de risque de corruption lors des échanges;

7 Chacun donne son appréciation sur les valeurs échangées et certifie ses actions dans un nœud d'échange public;

8 Tous les nœuds de confiance peuvent être vérifiées par chacune des entités. Ce qui limite l'acceptation du faux;

9 Ce modèle est à la base de la blockchain.

C/ Blockchain

Le Blockchain un système technique permettant de réaliser une

transaction entre deux ou plusieurs parties via un registre informatique d'informations, ouvert à toutes les parties pérennantes et infalsifiable. A travers sa transparence, il favorise l'ouverture à toutes les parties concernées. Le Block Chain a la particularité d**'être** infalsifiable, intègre et authentique.

Blockchain et cryptographie

Cette technologie a la particularité d'être : Accessible, Traçable, Vérifiable, Intègre, Authentique et Non-répudiable. Il apparait clairement que pour construire une blockchain, il faut impérativement implémenter les fonctions de confiance cryptographique.

QUELQUES APPLICATIONS

Problème du faux (falsification) et rupture de la chaine de confiance

- Le faux n'est possible que parce qu'il y a très souvent rupture de la chaine de confiance verticale, c'est-à-dire, à un moment donné, nous ne pouvons plus vérifier et sommes obligés de faire confiance sans vérifier.
- Ce problème est à la base de l'équilibre de base : expert-marchand-client

Solution blockchain à la contrefaçon

- L'utilisation d'un tag unique pour chaque produit dont les données sont stockées dans la Blockchain permet de vérifier les informations concernant ce produit : provenance, lieu de

stockage, authenticité, certificat de propriété et historique. La blockchain peut donc connaître les produits contrefaits, les produits détournés de leur utilisation première, la marchandise volée et les transactions frauduleuses qui touchent notamment les secteurs du luxe, de la pharmacie, l'électronique ou la joaillerie, les documents officiels, les billets de banque etc...

Tokenisation comme extension de solution de stabilisation de la valeur marchande

- Dans le but d'authentifier un élément physique unique, les éléments sont associés à un jeton numérique correspondant.
- Cela signifie que les jetons sont utilisés pour lier les mondes physique et numérique. Ces jetons numériques (appelés «tokens») sont utiles pour la gestion de la chaîne d'approvisionnement, la propriété intellectuelle et la détection de la contrefaçon et de la fraude.

Blockchain contre fake news

- Si tout le système de publication de l'information sur Intenet est fait sous le modèle de blockchain, nous aurons :
    - Chaque information publiée sera signée numériquement par son auteur (responsabilité et traçabilité);
    - Chaque auteur sera identifié dans une chaîne de certification numérique publique (chaine de blocs);
    - Chaque action sur une information (sa création, sa publication, les commentaires sur elle, son appréciation et autre) sera signée avec marque de l'identité de l'auteur, et tout ceci sera public et accessible à tous les utilisateurs;
    - Il se dégagera donc de manière automatique le pourcentage de véracité de l'information qui trahira alors à chaque fois le faux dans la chaine de publication des informations.

Problème de l'identité numérique

Le modèle actuel de gestion de l'identité numérique oblige certains

utilisateurs à se servir du même mot de passe pour de nombreux comptes différents. D'autres utilisent des fournisseurs d'identité centralisée ; comme Facebook ou Google qui leur permettent certes de diminuer la charge de login et mot de passe. Par conséquent, ils deviennent des cibles d'autant plus intéressantes pour les hackers.

Solution blockchain à l'identité numérique

Le fonctionnement de la blockchain va à l'inverse de la centralisation des mots de passe. Les utilisateurs sont entièrement responsables de la sécurité de leur compte par la préservation et la protection de leur clé privée. Ainsi, il sera beaucoup moins intéressant économiquement pour un hacker de pirater cette clé privée que de s'en prendre à un serveur contenant des millions de mots de passe. En plus, toutes les identités étant publiques et laissant leurs traces sur les actes numériques, la blockchain résoud le problème de l'attaque de l'homme du milieu et celui de l'anonymat. Et par conséquence celui de la responsabilité sur les actes numériques posés

Transport et mobilité

En synchronisant en temps réel les places non utilisées dans une voiture et les besoins de transport des utilisateurs, une plateforme décentralisée pourrait appartenir à la communauté des utilisateurs en proposant une rémunération «juste» pour les développeurs, les utilisateurs et les contributeurs de la communauté. Avec l'avènement des voitures autonomes, l'impact de la blockchain pourrait être énorme dans le quotidien de millions de gens.

Stockage des données (cloud distribué)

La blockchain peut être appliquée en tant que solution de stockage cloud décentralisée. Outre la sécurité, c'est le prix du stockage des données qui est intéressant ici. Grâce à la blockchain, vous pouvez vendre la bande passante ou la mémoire inutilisée de votre ordinateur à d'autres utilisateurs qui en ont besoin pour stocker leurs données ou exécuter des programmes.

Santé publique

Plusieurs cas d'usage sont envisageables dans le secteur de la santé. La blockchain pourrait notamment servir à la traçabilité des médicaments,

à la sécurisation des données de santé, et à la gestion des données des patients.

Energie

La multiplication des auto-producteurs (les foyers dotés de panneaux photovoltaïques par exemple) pose d'importants problèmes aux réseaux de distributions traditionnels, conçus historiquement de façon univoque. La solution prônée pour y répondre est celle de la multiplication des réseaux locaux intelligents, les smart-grids. Des smart contracts pourront ensuite régir les règles d'utilisation de l'énergie produite par ces smart-grids, et naturellement les tarifs des producteurs.

Contrats intelligents

Les smart contracts sont dit «intelligents» car lorsque les conditions d'exécution de ces engagements sont réunies, ceux-ci s'exécutent automatiquement sur la blockchain, en prenant en compte l'ensemble des conditions et des limitations qui avaient été programmées dans le contrat à l'origine. Imaginez que vous êtes agriculteur, et signez un «smart contract» avec un assureur, stipulant qu'un versement est effectué après 30 jours sans précipitations. Après un mois de sécheresse, l'entité qui gère ce smart contract déclenche automatiquement le paiement grâce à des données externes sans que vous ayez besoin de déclarer ou de revendiquer quoi que ce soit.

Gouvernance publique

La blockchain peut agir comme une méthode fiable et transparente rendant possible le vote en ligne. Cette solution pourrait être particulièrement intéressante pour des pays ou des partis politiques sujets à des problèmes de fraude et de comptage difficile de voix.

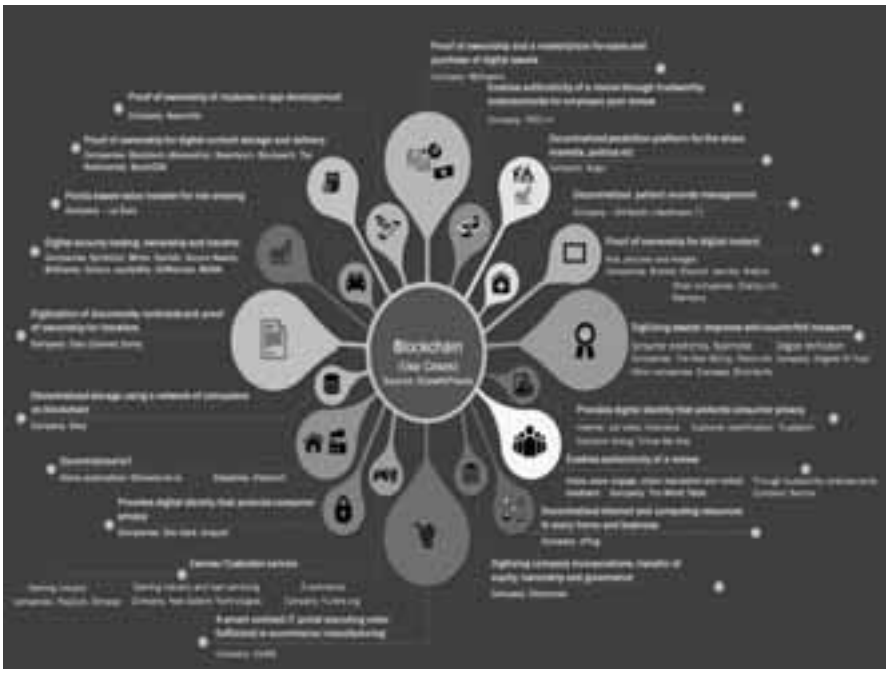
Dans de nombreux pays en développement, certaines terres ne sont pas enregistrées dans une base de données officielles, le cadastre. Certains habitants n'ont donc même souvent pas de véritable adresse. En répertoriant l'intégralité de son territoire sur une blockchain, on sait exactement à qui appartient les terres, et on ne peut plus remettre en cause le cadastre.

Egalement, l'influence directe de la décentralisation des opérations dans les services financiers aura un impact sur le secteur public.

Les applications possibles de la blockchain pour les gouvernements sont donc nombreuses et complexes.

Domaines d'application

- Sécurisation des diplômes et autres documents;
- La sécurisation foncière;
- Le collecte de la TVA et Impôts;
- Le recouvrement de crédits;
- L'optimisation de la production et de la consommation de l'énergie;
- Les compensations financières;
- La monnaie;
- Les marchés de valeurs et les bourses;
- Contrats intelligents;
- Commerce;
- Propriété intellectuelle;
- Internet des objets;
- Le covoiturage et partage des ressources diverses;
- Micro-hébergement informatique distribué;
- Tracking des produits, et mobiliers.


Blockchain
(Use Cases)

INTERVENANT N°4 : Mr. MEYO,
Chef service des audits de sécurité, MINPOSTEL

Audits, évaluations et contrôles de la sécurité des systèmes d'information

De nos jours, les services de sécurité informatique font face à un défi difficile : les attentes contradictoires de la performance de l'entreprise et la sécurité de l'information. En d'autres termes, plus on augmente les niveaux de contrôle, plus on ajoute des restrictions aux utilisateurs tout en laissant les criminels poursuivre leurs activités. Ainsi, la sécurité informatique devrait davantage compter sur la surveillance, le contrôle et les audits. Les décisions de sécurité intelligentes ont toujours besoin d'un contexte, d'une évaluation du niveau de sécurité. Cela signifie, adapter la sécurité à son contexte via une étude de l'environnement, des besoins et du niveau de sécurité. Ce travail est réalisé dans le cadre des audits de sécurité.

PLAN

- **Introduction**
- **Définitions**
- **Cadre Juridique**
- **Objectifs d'un audit de sécurité**
- **Identification des acteurs du processus d'audit et définition de leurs responsabilités**
- **Normes et Méthodes**
- **Déroulement d'une mission d'audit**
- **Intervention du MINPOSTEL**
- **Conclusion**

Introduction

Au cœur du bon fonctionnement des entreprises et de l'Etat, les systèmes d'information sont devenus des cibles d'attaques informatiques privilégiées (virus, intrusion, usurpation, dégradation, etc.) dont l'impact est extrêmement préjudiciable à l'Etat.

Comment les audits de sécurité peuvent-ils contribuer à la construction d'une société de l'information sécurisée ?

I. Définitions

Système d'Information (S.I): Ensemble de moyens (matériels, logiciels et organisationnels) destinés à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information. Il représente un patrimoine essentiel pour une organisation.

Sécurité du S.I: Ensemble de mesures de sécurité physique, logique, administrative et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer :

- La confidentialité des données de son système d'information;
- La protection de ses biens informatiques ;
- La continuité de service.

Audit de sécurité : Examen méthodique des composantes et des acteurs de la sécurité, de la politique, des mesures, des solutions, des procédures et des moyens mis en œuvre par une organisation, pour sécuriser son environnement et effectuer des contrôles de conformité de son système d'information.

II. Cadre Juridique

Loi N° 2010/012 du 21 décembre 2010 relative à la Cyber-sécurité et à la Cybercriminalité au Cameroun.

Décret N° 2012/1643/PM du 14 juin 2012 fixant les conditions et les modalités d'audit obligatoire des réseaux de communications électroniques et des systèmes d'information.

Arrêté conjoint N° 00000013/MINPOSTEL/MINFI du 10 mai 2013

fixant les frais perçus par l'ANTIC.

Décision N°00000094/MINPOSTEL du 30 mai 2013 fixant les frais d'audit de sécurité des systèmes d'information et des réseaux de communications électroniques.

III. Objectifs d'un audit de sécurité

Les objectifs de l'audit de sécurité visent principalement à :

- Protéger les actifs informationnels des menaces et vulnérabilités de façon organisés ;
- Élaborer une conception de sécurité ;
- Analyser les risques pesant sur les actifs;
- Proposer des solutions palliatives.

V. Identification des acteurs du processus d'audit et définition de leurs responsabilités

Acteur	Responsabilités
MINPOSTEL	• Suivi de la mise en œuvre de la politique nationale en matière d'audit de sécurité des réseaux de communications électroniques et des systèmes d'information ; • Signe les agréments des auditeurs externes après une étude préalable des dossiers par l'ANTIC ; • Définit les niveaux de gravité d'impact suite à l'exploitation les rapports d'audit de sécurité, produits par l'ANTI et des Auditeurs Agrées
ANTIC	• Elabore les procédures et référentiels d'audit ; • Audits des entités sensibles (Administrations publiques, opérateurs de services de communications électroniques) ; • S'assure de la régularité et de l'effectivité des audits ; • Examine la conformité des rapports des Auditeurs externes suivant les procédures élaborées ; • Accompagne les structures auditées dans la mise en œuvre des mesures correctives.
AUDITEURS EXTERNES	• Evalue le niveau de sécurité des structures en se basant sur les référentiels et procédures élaborées par l'ANTIC ; • Formule les recommandations pour remédier aux failles de sécurité décelées ; • Accompagne éventuellement les structures auditées dans la mise en œuvre des recommandations.

Entités	Responsabilités
ART	• En collaboration avec l'ANTIC, participe à la régulation, au contrôle et au suivi des activités liées à la sécurité des réseaux de communications électroniques et des systèmes d'information.
STRUCTURE AUDITEE	• Fournit à l'auditeur la documentation technique nécessaire (Architecture détaillée des systèmes d'information, topologie physique et logique, plan d'adressage, références des équipements, Procédures d'acquisition et de maintenance des équipements et des logiciels, Schéma directeur TIC, Manuel de procédures, Politique de sécurité du système d'information, Plan de réaction en cas d'incident) au bon déroulement de la mission d'audit de sécurité de son système d'information ; • Assiste les auditeurs lors des différentes phases de la mission; • Met en œuvre les recommandations formulées à l'issue de la mission d'audit suivant les délais prescrits.

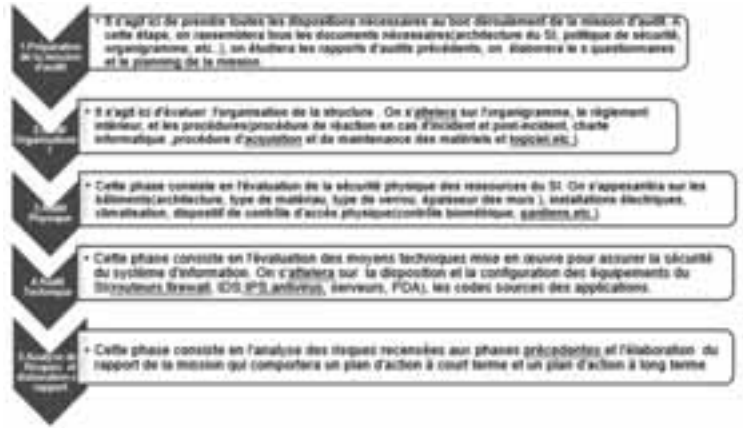
VI. Normes et Méthodes

Les audits de sécurité s'effectuent suivant les normes et les standards de sécurité, qui définissent les exigences, les spécifications, les lignes directrices ou les caractéristiques à utiliser pour assurer un maximum de sécurité.

Schématiquement, la démarche de la sécurisation des systèmes d'information adoptée par l'ANTIC passe par 4 étapes de définition :

- Périmètre à protéger (liste des biens sensibles);
- Nature des menaces;
- Impact sur le système d'information;
- Mesures de protection à mettre en place.

VII. Déroulement d'une mission d'audit de sécurité



VIII. Intervention du MINPOSTEL

- Assure la supervision de l'activité d'audit de sécurité des réseaux de communications électroniques et des systèmes d'information ;
- Exploite les rapports d'audit de sécurité, réalisés par l'ANTIC et les Auditeurs agréés ;
- Tient les données statistiques relatives aux vulnérabilité des réseaux de communications électroniques et des systèmes d'information.

Avec pour objectif de proposer au Gouvernement des orientations stratégiques pour l'activité

En 2014 le Ministre des Postes et Télécommunications a attribué les agréments, à sept (07) aux Auditeurs de sécurité et cabinets-conseils en sécurité des réseaux et des systèmes d'information, il s'agit de :

1 ERNST & YOUNG;

2 PRICE WATERHOUSE;

3 INFORMATION-TECHNOLOGIE-SECURITE (ITS);

4 TABI DIRECT INVESTMENTS;

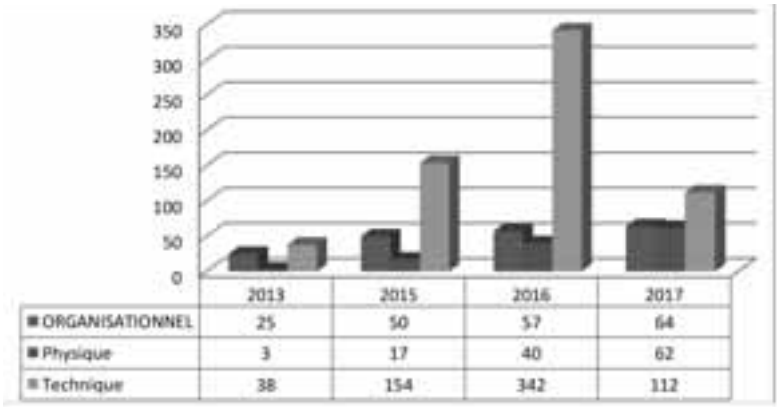
5 EVOLVING CONSULTING;

6 ISVA IT CO Ltd;

7 GETSEC.

Année	Ministères	Institutions financières/ assurances	EPA	Opérateurs de téléphonie et FAI	TOTAL
2013	14	4	1	4	23
2014	20	8	5	0	33
2015	1	4	1	3	9
2016	7	0	4	4	15
2017	10	0	8	4	30
Avril 2018	5	3	5	0	13
TOTAL	**57**	**19**	**24**	**15**	**123**

Évolution de l'activité de l'audit de sécurité 2013 à Avril 2018



	2013	2015	2016	2017
ORGANISATIONNEL	25	50	57	64
Physique	3	17	40	62
Technique	38	154	342	112

Évolution du nombre de vulnérabilités dans les réseaux des Opérateurs de téléphonie mobile de 2013 à Avril 2018

Conclusion

- Les pertes liées à un acte cybercriminel sont souvent très lourdes financièrement, pour les entreprises et l'Etat ;
- Les audits de sécurité participent activement au maintenir d'un cyberespace sain;
- Pour cette raison, chaque entreprise devrait procéder à un contrôle régulier du niveau de sécurité de son système d'information ;
- Ceci dans la perspective d'atteindre les objectifs fixés par l'Etat;

PLENIERE 3 : STRATEGIES ET REPONSES INSTITUTIONNELLES AUX PROBLEMES DE CYBERCRIMINALITE ET CYBERSECURITE

Cadre légal et règlementaire, structures et institutions en charge des questions de cybercriminalité et cyber-sécurité, stratégies et politiques en matière de cyber-sécurité, cyberdéfense et lutte contre la cybercriminalité

Les réponses aux challenges de cyber sécurité et cybercriminalité doivent être trouvées dans un cadre cohérent, faisant appel à des politiques et stratégies bien élaborées à l'échelle nationale et internationale. Ceci a pour avantage de bien organiser le travail au niveau institutionnel, et de mieux accompagner les structures opérationnelles du secteur.

MODERATEURS : PR MVOMO ELA, CCRD-EIFORCES &
M. BELEOKEN, MOTOROLA

INTERVENANT N°1 : Mr. OTTOU, MINPOSTEL

Stratégies et politiques de cyber sécurité et lutte contre la cybercriminalité

La vision et l'organisation à toute échelle sont nécessaires pour apporter des réponses optimales aux problèmes liés à la cyber-sécurité et la lutte contre la cybercriminalité. Nous parlerons ici du cadre des stratégies et politiques en matière de cyber sécurité et cybercriminalité.

PLAN

- Politiques de sécurité des réseaux et systèmes d'information mises en œuvre au Cameroun (2000 - …);
- Stratégie de mise en œuvre.

PHASE 1: DÈS 2002

- Projet de mise en œuvre des services de transactions électroniques dans le cadre du e-Government avec l'appui de l'Union Internationale des Télécommunications (UIT), l'Union Européenne dans le cadre de la préparation du Sommet mondial sur la société de l'information ;
- Objectif : favoriser le développement des transactions électroniques au niveau du secteur et l'étendre au niveau du Gouvernement;
- Services identifiés : messagerie sécurisée, monnaie électronique;
- Technologie support : PKI.

PHASE 2 : 2010

Loi n°2010/012 du 21 décembre 2010 relative à la cyber sécurité et la cybercriminalité

Article 1er.- La présente loi régit le cadre de 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. A ce titre, elle vise notamment à :

- instaurer la confiance dans les réseaux de communications électroniques et les systèmes d'information ;
- Fixer le régime juridique de la preuve numérique, des activités de sécurité, de cryptographie et de certification électronique ;
- Protéger les droits fondamentaux des personnes physiques, notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, ainsi que les intérêts légitimes des personnes morales.

PHASE 3 : 2011

Décret n°2011/408 du 09 décembre 2011 portant organisation du Gouvernement

Article 8.- Les attributions des Ministres sont fixées ainsi qu'il suit :

Le Ministre des Postes et Télécommunications est responsable de l'élaboration et de la mise en œuvre de la politique du Gouvernement en matière de postes, des télécommunications et des technologies de l'information et de la communication. . A ce titre, :

- Il assure le développement des Technologies de l'Information et de la Communication (TIC) ainsi que des communications électroniques sous toutes leurs formes en liaison avec les Administrations concernées ;
- Il suit les activités liées au commerce électronique et les questions de cyber-sécurité et de cybercriminalité en liaison avec les Administrations concernées.

STRATÉGIE DE MISE EN ŒUVRE

- Réorganisation du MINPOSTEL avec la création de la Direction de la Sécurité des Réseaux et Systèmes d'Information au niveau de l'administration centrale et du Service de Sécurité des Réseaux et Systèmes d'Information au niveau des Délégations Régionales des Postes et Télécommunications ;
- Renforcement des missions de l'ANTIC (gestion du point cm, régulation des activités de sécurité, autorité de certification racine, audit de sécurité, etc.);
- Mise en place du Fond Spécial des Télécommunications (FST) et Fond Spécial des Activités de Sécurité Electronique (FSE) pour financer les activités de développement, R&D, etc.;
- Elaboration du Plan Cameroun numérique 2020 avec un axe privilégié sur le renforcement de la confiance numérique ;
- Restructuration de l'Ecole Nationale Supérieure des Postes, Télécommunications et TIC (SUP'PTIC);
- Projet d'élaboration de la Politique Nationale de Sécurité des réseaux de communications électroniques et des Systèmes d'information ;
- Participation à la concertation aux niveaux sous régional (COPTAC, CEMAC), régional (UAT) et mondial (UIT, CTO, OIF).

MANAGEMENT DE LA POLITIQUE DE SECURITE

- Type de management préconisé et mis en œuvre dans le Secteur pour tenir compte des contraintes de l'environnement: coaching;
- Accompagner les régulateurs et les opérateurs à exercer au mieux leurs activités, dans la résolution des problèmes inhérents à leurs activités.

INTERVENANT N°2 : Dr. BELL B.G.,
PhD Sciences techniques en cyber sécurité
Expert Formateur en sécurité des systèmes d'information

Solutions humaines à la sécurité des systèmes d'information, hommes-pare-feu, expertise, responsabilités, profils de formation, profils de postes, profils de compétences

La sécurité des systèmes d'information est avant tout une affaire d'expertise. Quels sont donc les compétences nécessaires à la sécurité des systèmes d'information ? Quelles sont les offrent de formations qui peuvent permettre d'acquérir ces compétences ; les profils académiques et professionnels qui peuvent découler de ces formations ? Ces questions et bien d'autres encore seront débattues lors de cette séance.

Marché des métiers de la sécurité des SI

- 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.

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

- Inventaire et classification des actifs informationnels;
- Évaluation des mesures de sécurité des SI;
- Contrôle et vérification de conformité des mesures de sécurité des SI;
- Evaluation des impacts du non-respect des règles de sécurité des SI.

Management des risques de sécurité SI

Activités

- Inventaire et classification des actifs informationnels;
- Etude des menaces et vulnérabilités en sécurité des SI;
- Appréciation des risques sécurité systèmes d'information et leur classification;
- Evaluation des impacts potentiels;
- Établissement des plans de traitement des risques;
- Mise en place des plans de reprise et de continuité d'activités.

Investigations numériques

Activités

- Recherche de la preuve numérique;
- Extraction des données cachées, effacées, stéganographiées ou cryptées;

- Authentification des données numériques;
- Authentification d'actes numériques;
- Relevé d'empreintes numériques;
- Étude et sécurisation de la scène numérique d'infractions;
- Rédaction de rapports de garde et d'investigation.

Architecture de sécurité SI

Activités

- Normalisation des besoins de sécurité en prenant en compte toutes les dimensions (système, métier etc.);
- Elaboration des dispositifs techniques de sécurité répondant à des besoins de sécurité, en relation avec des experts techniques;
- Estimation du niveau de sécurité d'un dispositif ou système d'information;
- Gestion des incidents de sécurité pendant la phase d'exploitation, pour en réduire les impacts.

Aspects de compétences

- Juridiques;
- Techniques;
- Managériaux.

Niveaux de compétences

- Professionnel (Maitrise quelques taches d'un domaine de la sécurité des SI);
- Spécialiste (Maitrise un ou quelques domaines de la sécurité des SI);
- Expert (Maitrise 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

- Formations universitaires.

Masters en sécurité des systèmes d'information dans plusieurs universités au Cameroun

Au niveau expert

- Recherche scientifique dans le domaine de la sécurité des systèmes d'information;
- Expérience professionnelle forte à partir du niveau spécialiste

Métiers traditionnels en sécurité SI

- Manager de sécurité des systèmes d'information;
- Architecte de sécurité des systèmes d'information ;
- Auditeur de sécurité des systèmes d'information (Profession);
- Investigateur numérique (Profession);
- Opérateur de sécurité des SI.

Nouveau Métiers en sécurité SI

- Mineur cryptographique.

Emplois

Postes :

- Responsable sécurité système d'information;
- Spécialiste de sécurité système d'information.

Organisations :

- Banques;
- Administrations et entreprises diverses.

Demande d'expertise : elle est limitée du fait de la limitation de la prise en compte de la sécurité SI dans les organisations au Cameroun

Pareillement l'offre est limitée en qualité et quantité (secteur nouveau)

Professions formalisées du secteur au Cameroun

1. Deux professions seulement sont agrées
    - 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 sécurité des réseaux et systèmes d'information

INTERVENANT N°3 : Mr MEYO Yves,
Direction de la sécurité des réseaux et systèmes d'information au MINPOSTEL

Organisation institutionnelle de la cyber sécurité et la lutte contre la cybercriminalité

L'administration des questions de cyber sécurité et lutte contre la cybercriminalité nécessite la création et la gestion d'organes et institutions étatiques en charges de ces questions pour permettre à l'Etat et aux communautés d'adresser des réponses efficaces à ces problèmes.

Plan

INTRODUCTION

QUELQUES DEFINITIONS

ORGANISATION INSTITUTIONNELLE

- **PLAN STRATEGIQUE**
- **PLAN OPERATIONNEL**

CONCLUSION

Introduction

Les TIC en général et internet en particulier constituent :

- Un excellent outil de recherche de l'information et du savoir ;
- Un excellent outil de distraction ;
- Un excellent moyen de communication ;
- Favorisent de nouvelles formes de commerce (commerce électronique);
- Favorise l'accès à beaucoup de service (e-administration, e-banking)

A côté de tous ces avantages, s'est développé une nouvelle forme de criminalité matérialisée par :

- Les arnaques ;
- Le vol ;
- Le cyber terrorisme ;
- Le cyber espionnage ;
- La cyberpornographie ;
- Etc.

Cette nouvelle forme de criminalité est appelée cybercriminalité. Elle n'a pas de frontière physique et ses conséquences sont néfastes dans tous les domaines, en particulier dans celui des transactions numériques. Ces conséquences ont amené les pays à adopter des nouveaux cadres institutionnels pour y faire face. C'est le cas du Cameroun.

I. QUELQUES DEFINITIONS

- **Cyberespace** : Espace de communication créé par l'interconnexion mondiale des ordinateurs (Internet) ; espace, milieu dans lequel naviguent les internautes (cybermonde).
- **Cybercriminalité** : Tout acte portant atteintes à la confidentialité, l'intégrité, la disponibilité des données ou des opérations de traitement commis dans un environnement

électronique impliquant un réseau de communication.

- **Cyber sécurité**: Désignant le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des états et des organisations (avec un objectif de disponibilité, intégrité & authenticité, confidentialité, preuve & non-répudiation)
- **Cyberdéfense** : Regroupe l'ensemble des moyens physiques et virtuels mis en place par un pays dans le cadre de la guerre informatique menée dans le cyberespace.

II. ORGANISATION INSTITUTIONNELLE

L'organisation de la cyber-sécurité et la lutte contre la cybercriminalité au Cameroun s'opèrent sur plusieurs plans.

PLAN STRATÉGIQUE DE L'ETAT

Ministère des Postes et Télécommunications est chargé de l'élaboration et de la mise en œuvre de la politique de sécurité des communications électroniques et des systèmes d'information en tenant compte de l'évolution technologique et des priorités du Gouvernement.

- Cadre législatif

La loi N°2010/012 du 21 décembre 2010 relative à la cyber sécurité et à la cybercriminalité :

- Régit le cadre de 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 ;
- Met en évidence des mesures répressives qui vont des amendes, à des peines privatives de liberté pour des infractions cybercriminelles.

- Cadre réglementaire

- Décret N°2012/512 du 12 novembre 2012 portant organisation et fonctionnement du Ministère des Postes et Télécommunications avec l'avènement de la DSR ;
- Décret N°2012/180 du 10 avril 2012 portant organisation et fonctionnement de l'Agence Nationale des Technologies de l'Information et de la Communication ;
- Décret N°2015/3759/PM du 03 septembre 2015 fixant les modalités d'identification des abonnés et des équipements terminaux des réseaux de communications électroniques ;
- Décret N°2012/309 du 26 juin 2012 fixant les modalités de gestion du Fonds Spécial des Activités de Sécurité Electronique ;
- 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;
- Décret N°2013/0399/PM du 27 février 2013 fixant les modalités de protection des consommateurs des services de communications électroniques.

- Cadre stratégique

- La stratégie de développement de l'économie numérique : "Cameroun numérique 2020", élaboré en 2016. Parmi ses 08 axes stratégiques, l'axe 5 intitulé "renforcer la confiance numérique" énumère des actions à mener pour sécuriser le cyberspace camerounais;
- La stratégie nationale de cyber sécurité est en cours de validation, a permis de:
    - Dresser un état des lieux et diagnostic de la sécurité des réseaux et des systems d'information au Cameroun;
    - Ressortir les différents problèmes rencontrés;
    - Définir 05 axes stratégiques;
    - Identifier les différents projets à mettre en œuvre pour organiser le cyber sécurité et mieux lutter contre la cybercriminalité.

PLAN OPÉRATIONNEL

- ANTIC est chargé d'assurer pour le compte de l'Etat la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques, et à la certification électronique;
- Elle est composée de structures spécialisées comme le CIRT, le Centre PKI et la Division des Audits de sécurité
- ART qui veille à la bonne exécution de l'opération d'identification des abonnés et des terminaux;
- Les forces de défense et de sécurité servent également d'appui et d'accompagnement des agents assermentés de l'ANTIC et de l'ART lors des investigations numériques et de l'interpellation des auteurs des actes cybercriminels;
- Les services judiciaires sont chargés de juger les auteurs reconnus coupables d'infractions cybernétiques.

CONCLUSION

Le Cameroun a effectivement pris conscience des menaces qui pèsent sur son cyberespace. Cela se traduit par le réajustement institutionnel du secteur des télécommunications par la création des nouvelles structures. Le pays a également lancé des initiatives comme :

- la politique nationale de cyber sécurité;
- le projet de l'identification et classification des infrastructures critiques;
- le projet de développement et réalisation d'une PKI par l'expertise nationale;
- des campagnes de sensibilisation et de formation des ressources humaines.

- Ce qui vise à mieux outillées l'Etat pour affronter la montée des cyberattaques qui sont véhiculés par les réseaux de communication électroniques et particulièrement dans les réseaux 3G et 4G dont les conventions viennent d'être révisées et signé.

INTERVENANT N°4 : C/E MBOUOPDA, SCRJ/SED

Formation et bonnes pratiques d'hygiène informatique

Le comportement dans un système d'information est la source des difficultés généralement rencontrées par les utilisateurs des systèmes d'information. La formation et un code de bonnes pratiques de l'hygiène informatique peuvent réduire le risque de manière significative.

Cyber espace comme moyen de commission des infractions

Attaque sur les systèmes d'information
Fraude sur compte mobile/bancaire
Vol de données personnelles / vol d'appareil des tics

Cyber espace comme cible des attaques

Usurpation d'identité
Arnaques (à l'héritage, aux sentiments, par sociétés fictives, triangle bamoun, aux grains, œufs, scamming etc.)
Spoliation de compte mail
Fraude informatique (imprimés de l'Etat, timbres, ticket de péages, quittances diverses, etc.)
Chantage à la vidéo/téléphone

Choix des mots de passe

Méthodes

- La méthode phonétique : « J'ai acheté 5 bonbons pour cent francs cet après-midi » : **ght5bb%f7am** ;

- La méthode des premières lettres : « mon époux et mes 5 enfants, quel bonheur ! » : **méem5e,qb!**

Définir un mot de passe unique pour chaque service sensible sans recourir aux outils de stockage de mots de passe.

Mise à jour régulière des logiciels

Dans chaque système d'exploitation (Android, IOS, MacOS, Linux, Windows,…), logiciel ou application, des vulnérabilités existent.

Bien connaître ses utilisateurs et ses prestataires

Accéder à un ordinateur avec des droits d'utilisation plus ou moins élevés (utilisateur, administrateur).

Effectuer des sauvegardes régulières

Faut-il les sauvegarder sur

- CD /DVD ???
- Cloud ???

Sécuriser l'accès Wi-Fi de l'entreprise

Un Wi-Fi mal sécurisé peut permettre à des personnes d'intercepter les données et d'utiliser frauduleusement la connexion Wi-Fi pour réaliser des opérations malveillantes malintentionnées.

Etre aussi prudent avec un ordiphone (smartphone) ou une tablette qu'avec un ordinateur

N'installer que les applications nécessaires et vérifier à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement.

Être prudent lors de l'utilisation de sa messagerie

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées, etc.).

Télécharger les programmes sur les sites officiels des éditeurs

Le téléchargement d'un contenu numérique sur des sites Internet dont

la confiance n'est pas assurée, conduit au risque d'enregistrer sur l'ordinateur des programmes ne pouvant être mis à jour, qui, le plus souvent, contiennent des virus ou des chevaux de Troie.

Être vigilant lors d'un paiement sur Internet

Avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- contrôler la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs) ;
- s'assurer que la mention « https:// » apparait au début de l'adresse du site Internet ;
- vérifier l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.

Si possible, lors d'un achat en ligne :

- privilégier la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS.

Séparer les usages personnels des usages professionnels

Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette, etc.) dans un contexte professionnel.

Prendre soin des informations personnelles, professionnelles et de l'identité numérique

Des personnes malveillantes pratiquent l'ingénierie sociale, c'est-à-dire récoltent les informations personnelles, le plus souvent frauduleusement et à l'insu de l'internaute, afin de déduire son mot de passe, d'accéder à son système informatique, voire d'usurper son identité ou de conduire des activités d'espionnage industriel.

PLENIERE N°4 : RESTITUTION DES TRAVAUX D'ATELIERS

RAPPORT GENERAL DES TRAVAUX

Du 5 au 8 décembre 2018 s'est tenu dans la Salle de Conférences n°1 de l'Hôtel SAWA de Douala, le Séminaire de recherche organisé par l'Ecole Internationale des Forces de Sécurité (EIFORCES), avec l'appui du Japon à travers le PNUD sur le thème «Les défis et enjeux de la cybercriminalité et la cyber sécurité en Afrique Centrale».

Ledit séminaire s'est ouvert le mercredi 5 décembre 2018 sur une cérémonie solennelle présidée par Monsieur le Gouverneur de la Région du Littoral, en sa qualité de représentant du Ministre Délégué à la Présidence de la République, chargé de la Défense, Président du Conseil d'Administration de l'EIFORCES, en présence du Général de Brigade, Directeur Général de l'EIFORCES. Cette dernière a donné lieu, outre les discours officiels, à la présentation du cadre général des travaux par le Chef du Centre de Recherche et de Documentation de l'EIFORCES, qui a fixé le cap sur la nature et l'objectif des échanges ainsi engagés.

Par la suite, les travaux proprement dits se sont ouverts avec la première séance plénière sur le thème «**Cybercriminalité : origines, manifestations et enjeux**», sous la modération de S.E. Monsieur MASSIMA Jean Jacques, Ambassadeur, Représentant pour la zone Afrique Centrale et Madagascar de l'Union Internationale des Télécommunications (UIT). Après la transition qui s'est opérée de l'homo sapiens à l'homo communicatus rappelée fort opportunément dans le propos liminaire du modérateur, cette séance a permis d'exposer sur des thématiques aussi diverses que « les Fake news», appréhendées sous l'angle des perceptions et des représentations par **M. BATONGUE Alain** ; « Le cadre légal et règlementaire, procédures d'investigation et fonctionnement des juridictions» analysée par le **C/E MBOUPDA** ; et «Le facteur humain et l'ingénierie sociale» décryptée par le **Dr BELL**;

Il en ressort ce qui suit :

- d'abord, l'avènement des TIC s'accompagne de l'irruption d'une cyber citoyenneté travaillée par des manipulations de

tous ordres et productrice d'une forme de criminalité nouvelle, virtualisée;

- ensuite, à partir d'une lecture statistique et comparative des cas répertoriés de cyber crimes dans le monde, une typologie peut être dressée avec le constat, s'agissant du Cameroun, d'une recrudescence de l'escroquerie cybernétique. A ce sujet, outre le dispositif normatif adopté aux échelles nationale, régionale et internationale pour adresser ces questions, certaines Institutions policières et judiciaires ont reçu mandat pour leur prise en charge opérationnelle. Cependant, le cadre juridique y relatif reste marqué par une certaine vacuité s'agissant du traitement d'un grand nombre d'infractions ;

- enfin, si la gestion des risques cybernétiques relève de la responsabilité des hommes, la cyber sécurité recouvre quant à elle trois principales dimensions : stratégique, organisationnelle et opérationnelle. A ces dimensions, on peut ajouter une quatrième, déclaratoire pour sa part, qui procède d'une forme de discours mobilisé dans le cadre de la lutte contre la cybercriminalité. Pourtant, le paradoxe qui surgit ici, c'est bien que l'homme soit à la fois inventeur et maillon faible de l'espace et de l'outil cybernétiques. Par ailleurs, la variable émotionnelle complexifie la prise en charge d'une cybercriminalité adossée sur des mécanismes relevant de l'ingénierie sociale, qui procèdent du détournement des utilisateurs des activités sécurisées vers celles qui l'exposent davantage au cybercrime.

La question qui reste posée au final, c'est celle de la déterritorialisation du champ et de ces rapports de force qui une fois de plus, marquent la relation centre-périphérie et la transition vers la fin de l'exceptionnalité du cyberespace. Aussi, convient-il de souligner que la sécurité minimale pour toute Institution sensible à l'instar de l'EIFORCES passe aussi par la création de sites web et adresses email professionnelles qui elles, bénéficient d'une meilleure protection des données que les adresses à caractère personnel.

Faisant suite aux travaux en plénière, une intense discussion en atelier s'est tenue dans après-midi, sous la modération de **Mme Reine ESSOBMADJE.** De cet échange essentiellement pratique animé par des experts multi secteurs, il se dégage que :

- Au Cameroun d'une part, outre l'incurie du dispositif normatif encadrant le domaine de la sécurité numérique, le problème de l'évolution des mentalités et des comportements se pose dans un contexte encore marqué par la limitation des capacités techniques de l'Etat, des structures privées et des individus victimes de la cyber-insécurité. Trois grands axes d'intervention s'illustrent cependant, notamment : la veille sécuritaire, l'identification des failles sécuritaires et la certification électronique grâce à des outils tels que la Public Key Infrastructure (PKI) exploités par l'ANTIC, qui bénéficie notamment de l'appui gouvernemental ;

- Par ailleurs, en dépit des efforts engagés dans le champ des politiques publiques à l'instar de l'adoption par le MINPOSTEL d'un Plan Stratégique dont l'un des axes problématise la question de la confiance numérique, le besoin de formaliser et d'opérationnaliser une véritable politique nationale de sécurisation des réseaux et services informatiques servant de socle au cadre juridique continue de s'exprimer avec acuité ;

- De plus, il apparait clairement que la mutualisation des efforts, le partage des expériences et de l'expertise, de même que la sensibilisation et l'information des masses de cyber citoyens en général et du public jeune, principal animateur des réseaux sociaux en particulier, s'imposent comme des actions incontournables à renforcer, voire à entreprendre pour une meilleure prise en charge de ces problématiques.

- En effet, une approche stratégique voulue optimale devrait procéder non seulement d'une optique multisectorielle, mais aussi de la rationalisation d'une communication pertinente entre les acteurs intervenant directement ou indirectement dans le champ de la cyber sécurité d'une part, et entre ces acteurs et un public souvent peu ou mal informé sur les mesures prises dans ce domaine d'autre part.

Il convient toutefois de saluer le travail effectué par le Cyber incident response Team (CIRT) de l'ANTIC dans le domaine du monitoring en temps réel des réseaux et des systèmes d'information de tous les opérateurs.

Au final, c'est sur des échanges animés que se sont achevées les

activités de cette première journée.

Pour leur part, les travaux de la deuxième journée du séminaire de recherche de l'EIFORCES sur «Les défis et enjeux de la cybercriminalité et la cyber sécurité en Afrique Centrale», notamment le jeudi 6 décembre 2018, ont débuté avec la séance plénière n°2 consacrée à la «Cyber sécurité, protection de l'information et des systèmes d'information».

Sous la modération de M. OTTOU (MINPOSTEL), des thématiques telles que : les «Niveaux de responsabilité en cyber sécurité et lutte contre la cybercriminalité», «Les solutions intégrées de sécurité et de communication critique pour la protection des villes et la prospérité des entreprises», les «Solutions techniques, crypto, blockchain, systèmes de détection et prévention d'intrusions, de malveillance et contrôles d'accès aux systèmes d'information» et les «Audits, évaluations et contrôles de la sécurité des systèmes d'information» ont été analysées respectivement par Mme ASSAKO (ANTIC), M, BELEOKEN Hervé (Motorola), le Dr BELL et M. MEYO (MINPOSTEL).

Des exposés sus-évoqués, il se dégage que :

- Dans un monde de plus en plus connecté, avec un taux de pénétration digitale de l'ordre de 54% environ de la population mondiale connectée à internet et, d'environ 44% de cette population présente sur les réseaux sociaux, la cyber sécurité devient un enjeu politique, stratégique et économique majeur. En effet, à l'échelle nationale comme à celle internationale, le volume des activités criminelles perpétrées dans et à travers le cyberespace semble avoir atteint un seuil critique avec, s'agissant du Cameroun, environ 16 000 vulnérabilités détectées dans les systèmes informatiques et une prolifération à la fois fulgurante et dangereuse de faux comptes Facebook de personnalités publiques.

- Aussi assiste-t-on à une hiérarchisation des responsabilités consacrant le primat du politique sur les structures de sécurité (Police, Gendarmerie), appelées à travailler en coaction avec les organes régulateurs que sont les juridictions chargées d'appliquer les lois et les Instances spécialisées telles que l'ANTIC et de l'ART. Au demeurant, une meilleure cohésion s'impose entre ces différentes catégories d'acteurs dans leur déploiement au niveau opérationnel ;

- Au sujet de la répression des fakenews, la problématique se pose davantage du point de vue des perceptions et des représentations, sachant que la qualification d'un «fakenews» sera largement tributaire de la subjectivité de l'individu, du groupe d'individus ou de l'Institution qui le qualifie comme tel. C'est dire toute la complexité qui existe dans la conception et l'application d'un régime répressif en la matière ;

- Par ailleurs, une bonne appréciation de la charge critique de l'information est primordiale pour tout contrôle de sécurité qui se veut efficace. Car en effet, seule l'information critique, c'est-à-dire pertinente et traçable, mérite d'être mise en valeur ;

- Sur un autre plan et, dans une optique de sécurisation des systèmes informatiques des villes et partant, des pays, la technologie peut et doit être mise au service de la sécurité publique. Dans cette perspective, il importe de migrer des technologies manuelles vers celles digitales, en se rassurant toutefois de se doter de réseaux sécurisés. Ainsi, le partenariat avec des entreprises telles que Motorola, qui sont parvenues à concevoir des systèmes efficaces dans la prise en charge de ces impératifs sécuritaires, pourrait s'avérer hautement bénéfique ;

- Pourtant, dans l'absence de mesures coercitives susceptibles de contraindre les structures victimes d'attaques cybernétiques à se mettre à niveau, l'impact des avancées techniques et technologiques reste faible au sein de l'espace public ;

- En conséquence, les failles de sécurité informatique persistent dans un contexte dominé par la structuration d'une chaîne de confiance verticale plus vulnérable en matière de cyber sécurité qu'un système de confiance de type horizontal.

En définitive, le déficit de culture cyber-sécuritaire, qui se traduit entre autres par le volume relativement faible des audits sollicités par les consommateurs publics et privés des technologies numériques, tout comme les faibles capacités d'appropriation de ces outils par ces derniers, aggravent les vulnérabilités déjà prégnantes dans ce domaine.

La session en atelier organisée au cours de l'après-midi et placée sous la modération de M. MEYO (MINPOSTEL) a quant à elle été l'occasion de rendre compte, dans une perspective pragmatique et

critique, de l'existant en matière de mécanismes de lutte contre la cybercriminalité et de prévention d'éventuelles cyberattaques.

A ce propos, il faut d'emblée admettre que la sécurité en général, et celle cybernétique en particulier, étant essentiellement processuelle, il ne saurait exister un idéal en la matière, défini au sens du «risque zéro». Cependant, l'ajustement des comportements aura permis à la DGSN et à la Gendarmerie nationale de ramener les vulnérabilités à un niveau sinon satisfaisant, du moins acceptable.

Plus spécifiquement, l'impératif de préservation des ressources internes s'y traduit, entre autres mesures, par l'interdiction opposée aux équipements externes de l'accès à l'intranet, ou encore la formation des personnels à la sécurisation des opérations de système et à l'« ethical hacking» grâce à des partenariats conclus avec des Institutions spécialisées telles que l'IAI. Bien plus, la classification des données par niveaux de sensibilité permet également de réduire le risque de divulgation d'informations jugées critiques.

Pourtant, le faible degré de cloisonnement entre la sphère personnelle et celle professionnelle, avec notamment la mobilisation indifférenciée du matériel personnel pour des besoins professionnels et inversement, démultiplie les risques cyber sécuritaires.

De même, dans un contexte de limitation des capacités financières, le caractère onéreux des technologies de pointe en matière de cyber sécurité est bien souvent de nature à dissuader les consommateurs de biens et de services numériques. Toute chose qui rend relativement caduque toute ambition sérieuse de veille informatique.

Les débats se sont clos avec la formulation de certaines recommandations, dont l'économie a été faite dans un document y relatif ci-joint.

S'agissant de la troisième journée, du 7 décembre 2018, les débats en plénière survenus dans la matinée étaient consacrés aux «Stratégies et réponses institutionnelles aux problèmes de cybercriminalité et cyber sécurité» ont été modérés tour à tour par le Pr MVOMO ELA (CRD/EIFORCES) pour ce qui est de la première session, et par M. BELEOKEN (MOTOROLA) en ce qui concerne la seconde session.

Au cours de ces assises, les axes thématiques suivants ont été examinés par le panel constitué de M. OTTOU (MINPOSTEL), du Dr BELL

(expert en sécurité des systèmes d'information), de M. MEYO (MINPOSTEL) et du C/E MBOUOPDA (SED) à savoir : «Les politiques et les stratégies de cyber sécurité et de lutte contre la cybercriminalité» ; «Les solutions humaines à la sécurité des systèmes d'information» ; «L'organisation institutionnelle de la cyber sécurité et la lutte contre la cybercriminalité» et enfin «La formation et les bonnes pratiques d'hygiène informatique».

De ces intenses réflexions, il ressort que :

- **À propos des politiques et des stratégies de cyber sécurité,** et eu égard à l'avènement de l'usage de l'internet dans les entreprises et les Administrations publiques, une loi sur la cyber sécurité a été votée en 2010, concomitamment avec la loi sur le commerce électronique. L'adoption de cet instrument juridique a par ailleurs permis d'opérationnaliser certaines mesures telles que le guichet unique.

- Pourtant, si l'Etat a effectivement engagé plusieurs axes d'efforts dans ce sens sous la houlette du Ministère des Postes et Télécommunications, l'enjeu reste celui de leur adéquation avec la nature volatile et hautement complexe des menaces cybernétiques. Ledit enjeu problématise en effet, dans une optique aussi bien capacitaire que finalitaire, la vision et l'action de l'Etat, de ses déclinaisons institutionnelles que sont, pour le cas d'espèce, les juridictions et les organes de régulation comme l'ANTIC et l'ART et enfin, celles des opérateurs privés de télécommunication eux aussi appelés à s'investir dans la lutte globale contre la cybercriminalité et la cyber insécurité, dans le cadre de la mise en œuvre d'une approche partenariale public-privé ;

- **En ce qui concerne les solutions humaines**, elles se situent au cœur du processus de structuration d'une réponse efficiente dans le domaine de la lutte contre la cybercriminalité. Aussi, un impératif catégorique se dégage-t-il de manière claire : celui de la formation et du perfectionnement des ressources humaines et partant, du développement de compétences et d'une expertise endogène à même de porter à un niveau pertinent d'efficacité opérationnelle la vision et les axes stratégiques projetés dans le cadre des politiques publiques cyber sécuritaires dont l'activation, par ailleurs, reste encore attendue au Cameroun.

- Parallèlement, on peut déplorer le volume résiduel des sollicitations exprimées vis-à-vis de l'offre d'expertise cybernétique, du fait d'une faible conscience cyber sécuritaire observée au niveau des Organisations locales. La situation ainsi décrite est d'ailleurs aggravée par la nébulosité du champ des métiers y relatifs au Cameroun ;

- **Relativement à l'organisation institutionnelle de la cyber sécurité et de la lutte contre la cybercriminalité**, un important dispositif législatif servant de socle au Plan stratégique de l'Etat piloté par le MINPOSTEL a été adopté depuis 2010. Pourtant, l'implémentation de ces instruments continue de faire défaut, ce qui dénote un déficit d'articulation entre le niveau politico-stratégique et celui opérationnel.

- Bien plus, du point de vue de la géopolitique et de la géostratégie de l'information et de la communication, tout comme celui de la cyberdéfense, la question de la souveraineté sur les données d'identification des consommateurs de biens et de services numériques (les abonnées) se pose avec une acuité toute particulière, eu égard à la primauté sur le marché domestique d'opérateurs de télécommunication représentant des capitaux étrangers. Le fait qu'un secteur aussi stratégique puisse ainsi échapper au contrôle souverain de l'Etat constitue une vulnérabilité supplémentaire dont la capacité de nuisance potentielle se situe à un seuil absolument incompatible avec les besoins et les contraintes sécuritaires de tout Etat doué de conscience géopolitique et sécuritaire ;

- **Enfin pour ce qui est des bonnes pratiques**, elles devraient faire l'objet d'une appropriation autant au niveau des internautes pris individuellement qu'au niveau des Institutions, dont aucune ne saurait désormais échapper à l'imperium de la connectivité. Une telle ambition augure l'enracinement d'une culture de la vigilance et d'une «e-discipline» à la fois individuelle et collective fondée sur des principes et des mécanismes d'autocensure et de navigation responsable.

- Dans le même ordre d'idées, l'absence de différenciation entre les outils et le matériel informatiques utilisés à des fins privées et ceux mobilisés dans le cadre professionnel, tout comme la non sécurisation des réseaux intranet au niveau de certaines Administrations publiques, sont entre autres facteurs à risque

du point de vue de la cyber sécurité. Pourtant, des techniques relativement efficaces de management des systèmes d'information existent et sont largement appliquées avec résultat au sein des entreprises privées.

Faisant suite aux sessions plénières, la discussion en atelier modérée par M. OTTOU s'est structurée autour de plusieurs axes de réflexion, dont on peut retenir ce qui suit :

- D'abord, à la manipulation de l'information à travers internet et les réseaux sociaux s'oppose de manière paradoxale une faible capacité des dispositifs actuels de défense et de sécurité à anticiper et à endiguer les menaces induites telles que la cyber insurrection ou le cyber terrorisme ;
- Ensuite, le désengagement de l'Etat vis-à-vis de la prise en charge de l'identification numérique de ses habitants, couplé à l'absence de système de contrainte et de contrôle sur les opérateurs privés de télécommunication, ne rendent pas compte d'une véritable maturation des politiques nationales de lutte contre la cybercriminalité ;
- Enfin, le caractère volatile des menaces cybernétiques, boostées par l'évolution en permanence des techniques et des technologies numériques, constituera toujours une contrainte stratégique et opérationnelle dont les principaux acteurs de la cyberdéfense et de la cyber sécurité devront s'accommoder, dans un espace-monde de plus en plus interconnecté.

En définitive, la quatrième et dernière journée du samedi 8 décembre 2018 était consacrée aux amendements, à la validation et à la restitution du rapport final des travaux du séminaire, lequel prend fin avec la cérémonie solennelle de clôture présidée par Monsieur le Gouverneur de la Région du Littoral.