

RESUMÉ CONFÉRENCE 26/04/21

Thème : LA ZLECAF face aux défis de la cybercriminalité

Organisée par : Africa Cyber Sécurité.

Date : Lundi 26 Avril 2021 de 15h30 – 17h30 GMT.

Introducteur (MC) : Reine TOUNGUI

Panélistes : Yves ICKONGA , Kag SANOUSSI , Eric BÂREZUNG , Armel MUMBERE , Jean Claude KAWADI.

Il y a une lueur d'espoir pour le continent africain dû à la souveraineté que de nombreux états peuvent avoir maintenant sur les données numériques. La numérisation des données économiques, sociales, sociétales sont désormais le cheval de guerre de nombreux états africains. La question centrale est quelle Afrique voulons nous , souhaitons nous , et rêvons-nous à l'horizon 2063. Pour arriver à atteindre cette Afrique, Quels outils utiliser et comment les utiliser ? La question de la cybercriminalité au sein du développement de l'Afrique devient centrale.

Panéliste 1 : Yves Ickonga Conseiller Spécial numérique, Présidence République Démocratique du Congo.

Thème : La dette africaine face aux attaques cyber.

Les questions de la dette africaine autour de la menace cyber est une question centrale. Nous pouvons faire émerger notre continent malgré la dette avec le numérique. La mise en œuvre de la ZLECAF montre que nous devons atteindre la maturité numérique. Le développement et la transformation du numérique est le point central du développement de la ZLECAF. Mais L'Afrique est-elle prête ? Il faut innover dans la démarche de la mise en place du projet de la ZLECAF. Nous devons croire en nous et dans nos capacités d'autonomisation numérique. L'heure n'est plus au questionnement mais au rassemblement des compétences.

Les types de cybercriminalité :

- Le traçage des échanges économiques.
- Le suivi des transactions monétaires.
- Fraude commerciale
- Usurpation d'identités
- Extorsion de fond
- Fuite de capitaux
- Escroquerie sur internet.

Panéliste 2 : KAG SANOUSSI. Expert en intelligence négociation elle , Président de l'institut national de gestion des conflits. **IGC**

La gestion des crises et la place de la négociation. Des temps anciens aux temps présents , les conflits ont jalonné l'humanité sans pour autant s'imposer comme étant une fatalité , mais en une réalité tangible. Elle peut conduire au pire , comme au meilleur. La bonne gestion des conflits, permet une ouverture durable. Le numérique aussi n'est pas épargné par les conflits avec l'apparition de la cybercriminalité. Une approche exigée des risques numérique , nécessite une approche. Le cyber est un cadre de défis pluriel. L'accélération du numérique a engendré des conséquences inattendus et parfois imperceptibles. Cependant cette nouveauté rencontre des problèmes de pirates, du sabotage des réseaux informatiques , de la mauvaise foi des hackers , mais aussi le développement d'une nouvelle forme de proximité humaine. La cyber sécurité se doit de se présenter en préventif et aussi en curatif.

Les pratiques de négociation doivent s'inscrire aussi dans le numérique. Gagner, le défi de la cyber-sécurité reviens à prévoir et ensuite savoir négocier.

Utilisation de deux outils pour la prévention et la gestion dans le cadre de la cybercriminalité. L'outil **A-V-A** : (Anticiper – Visualiser – Oser) . Il anticipe, et permet quand tout va mal à réfléchir et donne des perspectives sur des bases solides. *Les différentes étapes de l'outil A-V-A sont celles – ci :* a) Bien recenser, b)Former , c) Organiser , d) Planifier , e) Exécuter , f) vérifier.

- Plan **O-S-E-R.** = Plan d'Organisation pour la Sécurité des États Responsables.

Panéliste 3 : Eric Bärenzung, Senior Cybersecurity Consultant / CISO / Suisse

Thème : La gestion des nouvelles menaces cybercriminelles.

L'Afrique est comme tous les continents du monde, il y a le côté positif et le côté négatif. Malheureusement l'Afrique est victime de la cybercriminalité. La cybercriminalité a évolué. La digitalisation et le développement ne pourra continuer que si les populations ont confiance dans l'utilisation de leurs données. Mais si les menaces criminelles, ne sont pas vite réglées, la peur du numérique empêchera le développement. En 2020 le cout de la cybercriminalité était de 4 milliards de dollars. L'Afrique se positionne après la chine dans l'utilisation du numérique. La cyber sécurité est une priorité pour l'agenda de l'UA 2063. Il faut engager tous les pays à se sentir en sécurité face au nouveau projet numérique.

- 21 Janvier 2021 : L'Afrique de l'Ouest : La CEDEAO a adopté une stratégie commune contre la cybercriminalité.
- Le 16 Mars 2021 : La BAD a investi 2 millions de dollars USD dans sa lutte contre le cyber crime.
- Le 22 Mars 2021 : Les acteurs de préventions au Burkina Faso , formés en technique d'infiltration en ligne et cyber patrouille.
- Le 2 Avril 2021 : L'UNIVGA lance une licence en cyber sécurité , une première au Gabon. (La licence cyber-sécurité de l'UNIVGA d'une valeur totale de 800.000 F CFA permet à l'étudiant d'acquérir à la fois des compétences théoriques grâce à son programme de cours mais également des compétences pratique à travers des projets, des stages obligatoires en entreprise et des soutenances devant des experts de la sécurité membres du CESIA. À la fin du cycle, grâce à son réseau de partenaire, les stages sont des pré-embauces. Pour son lancement, D2S offre 3 bourses d'étude. Le bureau du CESIA retiendra 3 candidatures sur des critères suivants : Être gabonais, résider au Gabon , avoir au plus 23ans au 1er mai 2021, Avoir réussi au baccalauréat série C, D ou E en 2018, 2019 ou 2020, avoir une moyenne supérieure ou égale à 12/20 au baccalauréat).

L'échange des formations et des compétences est nécessaire pour une bonne gestion des nouvelles menaces cybercriminelles. Deux supports internationaux peuvent aider nos pays : Premièrement, **GLACY +** qui est un programme d'aide offert par l'Union Européenne. Et ensuite : **SIPAO** qui est le système d'information policière d'Afrique de l'Ouest.

Par ailleurs, de nombreux intérêts de la part des grandes puissances, qui ont déjà des stratégies face à ses attaques cybercriminelles. Nous pouvons consulter ses stratégies dans :

- Global Law Enforcement Network
- Digital Strategy 2022 – 2024
- International coopération on cyber terrorisme and cyber crimes

Il ne faut toutefois pas négliger la vie privée. En Zambie de nombreuses personnes ont levé le doigt , par rapport aux nouvelles mesures numérique qui violent la vie privée. Les coopérations régionales , réfléchissent à faire mieux et surtout accompagner les décideurs, dans l'application des mesures efficaces.

Panéliste 4 : Armel MUMBERE . Mathématicien. Manager chez Deloitte.

Thème : L'importance de se mettre ensemble dans la ZLECAF.

La ZLECAF a démarré en 2021 (54 États) permettant aux pays de l'Union africaine d'œuvrer et d'échanger librement sans barrières tarifaires. Sans internet, nous ne pourrions pas parler de cybercriminalité. Le taux de pénétration d'internet est de 11% , et 48% des pays africains ont accès à internet. Internet, permet aujourd'hui au système financier africain d'atteindre les endroits les plus reculés. Le secteur aussi de l'E-commerce fut développer grâce à Internet. Un Cyber crime est une infraction pénale faite sur un réseau. La cybercriminalité est une activité criminelle qui vise un réseau , un ordinateur ou une appareil connecté à Internet. On estime à 600 milliards de dollars, l'impact des actes criminalistiques qui ont eu lieu sur l'économie mondiale.

3 catégories de cybercriminalité : La cybercriminalité contre la propriété, La cybercriminalité individuelle , la cybercriminalité gouvernementale

Les enjeux de la ZLECAF face à la cybercriminalité. Selon le cabinet McKinsey, les gains que peuvent retirer l'Afrique dans les différents secteurs d'activités s'élèvent à 148 – 198 milliards de dollars. Ces objectifs ne peuvent être atteint que si les risques liés au cyber-crime sont correctement identifiés. Par ailleurs, les opérateurs économiques présents dans la ZLECAF doivent aussi être mis à l'abri des attaques cybercriminelles.

Le secteur de l'énergie est en plein essor sur notre continent, avec le barrage de la renaissance , qui crée un léger conflit entre l'Éthiopie, l'Égypte et le Soudan et le projet INGA aussi en RDC. Ces deux projets peuvent permettre à l'Afrique d'avoir une bonne autonomie énergétique. Ce sont des projets à fort potentiel sur le développement de l'Afrique.

Panéliste 5 : Jean Claude KAWADI.

Thème : La RDC carrefour de la ZLECAF.

Pour que l'Afrique réussisse la ZLECAF, il faut regarder la RDC, car ce pays a une position stratégique. Il a 9 voisins et facilite les échanges entre le nord, le sud, l'est et l'Ouest. C'est un carrefour d'informations, de personnes, des services et des biens. Il y avait beaucoup de réticence au niveau de la RDC pour entrer dans la ZLECAF. En tant que carrefour d'une Afrique prospère, la RDC peine encore dans la signature de certains contrats. Je cite ici : le contrat de CERT (Computer Emergency Security Team) qui est un centre d'alerte et de réactions aux attaques informatiques destiné aux entreprises et administrations. Il y a déjà un actif numérique considérable en RDC. La RDC est une zone de libre échange continentale africaine, mais aussi une zone de libre-échange de la mort. La mise en place d'une stratégie de sécurité des systèmes d'information est en place. La RDC doit se montrer exemplaire, car elle est aussi présidente de l'Union Africaine. Par ailleurs, elle souhaite stimuler la **cyberdiplomatie**. La cyberdiplomatie a pour but : De renforcer la résilience, de bâtir la confiance, de prévenir les conflits, de protéger les droits humains, de promouvoir le multilatéralisme. Pour atteindre ses buts, elle le fera par le moyen de : des cyberdialogues avec les états et régions partenaires, des collaborations avec la société civile et le secteur privé, des campagnes d'informations et de sensibilisations, le renforcement des capacités techniques, les démarches de déclarations et des prises de décisions diplomatiques. La numérisation est croissante surtout en cette période de crise sanitaire. Le cyberspace est maintenant un espace qui influence fortement les politiques étrangères et les intérêts nationaux. La gestion de cyberspace est devenue un point de discussion géopolitique majeur. La 5G, l'intelligence artificielle, l'informatique quantique, le *blackchain* ont un impact potentiel sur les rapports de force et l'économie à l'échelle mondiale.

Conclusion : Il y a une dynamique en marche en ce qui concerne la lutte et la gestion des nouvelles menaces en Afrique. Nous devons encourager la RDC qui est présidente de l'Union Africaine, car elle sera responsable du prochain tournant africain. Nous arrivons à une Afrique où les frontières ne seront plus matérielles, mais aussi cybernétique. Les pays doivent s'activer dans la gestion et la sécurité cybernétique, car elle est le passage pour un monde nouveau. La bonne gestion des outils susmentionnés 2030 et 2063,

