FORUM BRAZZA CYBERSECURITY

RAPPORT D'ACTIVITÉS

FORUM BRAZZA CYBERSECURITY

ÉDITION 2021

DU 16 AU 17 SEPTEMBRE 2021

by SKYTECH CONGO

Table des matières

Remerciements & Aide-Mémoire

I. Remerciements

Nous adressons nos profonds remerciements à tous nos partenaires Institutionnels pour leurs engagement manifestés ;

Spécialement au Ministre des Postes, des Télécommunications et de l'Economie Numérique, **Monsieur Léon Juste IBOMBO** ; au Ministre de la Communication et des Médias, Porte-Parole du Gouvernement de la République du Congo, **Monsieur Thierry Lézin MOUNGALLA** ; au Conseiller du Président de la République du Congo, chef du département des Télécommunications et du Numérique, **Monsieur Yves ICKONGA** ; au Ministre de la Communication et des Médias, Porte-Parole du Gouvernement de la République Démocratique du Congo , **Monsieur Patrick MUYAYA,** au Conseiller Spécial du Président de la République Démocratique du Congo en charge du Numérique, **Monsieur Dominique MIGISHA,** au Ministre d'Etat, ex Ministre de la Défense du Bénin**, Monsieur Issifou KOGUI N'DOURO,** ainsi qu'à **l'Autorité Malienne de Régulation des Télécommunications, des Technologies de l'Information et de la Communication et des Postes (AMRTP).**

A tous nos sponsors et partenaires pour leur accompagnement et soutien ;

A tous nos panélistes et formateurs qui ont mis à notre disposition leur expertise en matière de cybersécurité ;

A tous nos invités qui nous ont honoré par leur présence aux différentes activités du Forum.

II. Aide-Mémoire

Le Forum Brazza Cybersecurity a eu lieu au Centre International de conférence de KINTELE du 16 au 17 septembre 2021 sous le thème : « La Cybersécurité, un enjeu stratégique pour les Etats, les entreprises et institutions en Afrique. »

Initié par la société SKYTECH CONGO, le Forum Brazza Cybersecurity est un évènement qui a donné rendez-vous aux décideurs, chefs d'entreprises et acteurs de la cybersécurité, qui jouent le rôle de facilitateurs en fournissant des informations et des solutions concrètes en matière de cybersécurité au profit des décideurs en Afrique.

Le Forum a permis, pendant deux jours, de présenter l'état de la cybersécurité en Afrique centrale et les enjeux de la transformation digitale d'identifier les enjeux majeurs imminents de la cybersécurité et les moyens pour renforcer la cyberdéfense, de sensibiliser sur le risque cyber en Afrique, de renforcer la résilience de la cybersécurité en Afrique en construisant un écosystème de cybersécurité solide.

Les différents échanges et débats ont conduit à l'identification des faiblesses techniques des systèmes d'information des Etats, des entreprises et des particuliers ; à l'évaluation des éventuelles menaces auxquelles sont exposés les systèmes défaillants présenté lors de la démonstration de hacking, à la pose des bases pratiques d'une gouvernance numérique sécurisée pour les pouvoirs publics, à la sensibilisation des jeunes étudiants à la culture de la cybersécurité et aux techniques de protection des données et de détection des menaces cyber.

III. Contexte

Engagé sur la voie du développement, le continent africain qui enregistre une forte croissance économique depuis plusieurs années, a connu des avancées significatives dans la promotion et la mise en place des infrastructures des Technologies de l'Information et de la Communication (TIC) et a accru son accessibilité à l'internet.

Toutefois, les TIC qui offrent à l'Afrique une opportunité de développement et d'ouverture internationale ont également favorisé l'explosion des pratiques malveillantes telle que la cybercriminalité ou cyberattaque. L'Afrique devrait de toute urgence accroitre ses efforts pour lutter contre les menaces aux TIC, en se dotant des installations et équipements qui protègent l'ensemble de la chaîne de valeur des Technologies de l'Information et de la Communication.

Les Etats, entreprises et particuliers se trouvent souvent démunis face à cette nouvelle forme de criminalité qui les affecte tant du point de vue de la sécurité de l'information que du point de vue financier. Il s'agit désormais pour tous ces acteurs aussi bien institutionnels que privés de réduire leur vulnérabilité par le développement des politiques et de mettre en place des techniques de cybersécurité adéquates.

Plusieurs initiatives ont été amorcées par l'Union Africaine, les Communautés sous régionales et les Etats pour mettre en place des cadres juridiques et règlementaires sur la cybersécurité. Cependant, les solutions techniques et pratiques qui constituent des barrières de protection n'ont pas été assez promues.

Aujourd'hui plusieurs entreprises et institutions africaines sont connectées à internet. La digitalisation de ces structures constitue désormais une nécessité. La plupart travaille avec des logiciels en ligne et leurs données sont généralement stockées sur un cloud, à la portée des cybercriminels redoutables. Avec la venue du télétravail suite à la pandémie de covid-19, le risque cyber devient de plus en plus réel. Depuis plusieurs années, les cyberattaques ne cessent d'augmenter et des millions de données sont volées, ruinant des milliers d'entreprises et institutions en Afrique.

Cérémonie d’ouverture

IV. Cérémonie d'ouverture

Sous le patronage du Ministre des Postes, des Télécommunications, de l'Economie Numérique, Monsieur Léon Juste IBOMBO, la cérémonie d'ouverture du Forum Brazza Cybersecurity a eu lieu au Centre International de Conférence de KINTELE et a connu la participation de plus de trois cent personnes, en présence des membres du Gouvernement Congolais, des Chef d'entreprises, des représentants des Institutions internationales. Elle a été rythmée par les discours de la Coordonnatrice Générale du Forum Brazza Cybersecurity et maîtresse de cérémonie, Madame Horgerie GUEMPIAUT, suivi du mot de l'adjoint au Maire de la commune de KINTELE, du discours de Monsieur Arnaud AKEN ELION, Promoteur du Forum Brazza Cybersecurity ; de l'allocution du Monsieur Léon Juste IBOMBO, Ministre des postes, des télécommunications et de l'économie numérique du Congo.

Les travaux du Forum ont débuté dans l'imposante salle des banquets du Centre International de KINTELE par l'accueil et l'installation des participants.

La Coordonnatrice Générale du Forum BRAZZA CYBERSECURITY, Madame Horgerie GUEMPIAUT, a souhaité la bienvenue aux participants, suivant les usages de bienséance, qui ont auréolés l'évènement de leur présence. Par une présentation synoptique de l'agenda du Forum, la Coordonnatrice Générale a souligné les objectifs visés par la rencontre qui sont la mutualisation des réflexions pour favoriser l'expansion du secteur numérique en Afrique et les questions de cybersécurité.

Prenant ensuite la parole, l'adjoint au maire de la commune de KINTELE a présenté les remerciements de la Présidente du Conseil Municipal Député-Maire de KINTELE, Madame Stella MENSAH SASSOU NGUESSO, à l'endroit des organisateurs qui ont honoré la commune de KINTELE par la tenue d'un forum de haut gabarit. Il a fait part de ses attentes du forum qui portent sur la cristallisation des réflexions le long de l'événement en des résolutions utiles et pratiques sur les questions de cybersécurité en Afrique.

L'honneur étant accordé au Président du comité d'organisation et Promoteur du forum ; Monsieur Arnaud AKEN ELION, a salué la bonne volonté des participants aux assises du forum, dont la délégation de la République Démocratique du Congo (RDC) portée par l'éminent Conseiller Spécial du chef de l'Etat de la République Démocratique du Congo en charge du Numérique, Monsieur Dominique MIGISHA. Un mot particulier a été adressé au Gouvernement Congolais, à travers le Ministre des Postes, des Télécommunications et de l'Economie Numérique, Monsieur Léon Juste IBOMBO, hôte de l'évènement, pour la bonne conduite de la vision du chef d'Etat Congolais, Son Excellence Monsieur Denis SASSOU NGUESSO, dans le secteur du Numérique.

Il a évoqué le but du forum qui porte sur la nécessité de mesurer les impacts des risques de la forte numérisation de l'Afrique qui s'est lancée dans une opération irréversible. Les acteurs du secteur doivent saisir les enjeux de la sécurité liés aux données et à la vie privée pour rendre sûr l'espace cybernétique africain. On notera la prépondérante question législative, qui est un outil pour les Etats et organisations régionales, mais qui pourtant suscite un faible engouement, avec 25 pays sur 54 qui ont légiféré sur les questions de protection de données. Le potentiel du marché de la cybersécurité et la vulnérabilité des données des usagers des technologies digitales en Afrique doivent conduire les experts et les décideurs politique à prendre le train déjà en marche et implémenter des solutions pour tirer au mieux les bénéfices d'une bonne gestion de la question de la cybersécurité en Afrique.

Pour sa part, Monsieur Léon Juste IBOMBO, Ministre des Postes, des Télécommunications et de L'économie Numérique du Congo, a souligné l'honneur qui était sien de prendre part à cette rencontre d'information et de sensibilisation sur la question de la cybersécurité. Poursuivant par des remerciements à l'endroit d'un auditoire mixte constitué de différents profils professionnels, de

différentes nationalités et de tout niveau d'expertise sur les questions liées au numérique et à la cybersécurité.

Rassurant du soutien du Gouvernement dans l'accompagnement de cette initiative qui offre aux différents acteurs un cadre inclusif d'échange et de réflexion sur la cybersécurité, il a également souligné l'importance majeure qu'occupe la question de la protection des données à caractère personnel au Congo, ceci à travers la politique éclairée du Chef de l'Etat Son Excellence Monsieur Denis SASSOU NGUESSO, en dotant le Congo d'un arsenal juridique en matière de cybersécurité. Aussi, la volonté du Congo de contribuer à la collaboration régionale et internationale par la ratification de la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel dite Convention de Malabo est au centre des réflexions du Gouvernement Congolais, qui est également en pourparler pour ratifier la convention de l'Union Européenne sur la cybercriminalité dite de Budapest.

Il a rappelé le projet de mise en place de l'Agence Nationale de Sécurité des Systèmes d'Information ainsi que l'adoption de la loi portant création de la Commission Nationale de Protection des Données, qui viennent enrichir le carquois des pouvoirs publics.

Le moment du Sponsor officiel

Monsieur Gaëtan SOLTESZ, Directeur Général de SILICONE CONNECT, n'a pas caché le plaisir qui était le sien et celui de la structure qu'il représente d'être mis à l'honneur au cours d'un événement de portée internationale.

Relativement au principe de la séquence du moment du sponsor, il a présenté la structure SILICONE CONNECT à travers ses objectifs et ses missions. La vocation de SILICONE CONNECT est de desservir en réseau fibre optique les grandes entreprises, les opérateurs de télécom et les institutions. Avec son projet de construction d'un data center, SILICONE CONNECT vise à contribuer à la gouvernance souveraine des données du Congo Brazzaville.

De ce qui a attrait à la cybersécurité, SILICONE CONNECT prend la question très au sérieux avec des mesures préventives de sécurité sur ses installations et celle de sa clientèle.

Pour comprendre l'identité de SILICONE CONNECT, il faut partir de la genèse du projet. La société nationale d'électricité E²C a construit pour son compte l'un des plus grands réseaux de fibre optique au Congo et l'exploitation de ce réseau est concédé au groupe YAO CORP en 2020 à travers un partenariat public-privé, l'Etat conservant la propriété des infrastructures. SILICONE CONNECT est donc créée à cette occasion pour devenir la filiale Télécom du groupe YAO CORP.

Les 1300 km du réseau sont segmentés de la façon suivante :

- Une dorsale (backbone) sud entre Pointe-Noire et Brazzaville de 550 km de linéaire. Cette partie du réseau est construite sur le câble de garde de la ligne très haute tension (THT) qui relie PNR à BZV.
- Une dorsale (backbone) nord entre Brazzaville et Owando. Cette partie du réseau est également construite sur le câble aérien de la THT.
- Deux boucles métropolitaines complètent le réseau : une à Pointe-Noire et une autre à Brazzaville. Ces boucles connectent les agences E²C entre elles, créant ainsi des points de distribution partout en ville. Ces segments sont majoritairement souterrains.

- Des segments en construction ou en projet viennent compléter le diagramme avec notamment des extensions prévues vers Dolisie, Ouesso et Kinshasa pour connecter le réseau aux pays voisins.

Etant devenue omniprésente dans les vies au quotidien, la technologie par la révolution du digital transforme la façon de vivre, de travailler, d'apprendre, de se soigner, de se divertir et même de se loger.

Forts de ce constat, SILICONE CONNECT a pour mission de "garantir un accès à internet au plus grand nombre" car la connectivité est devenue un enjeu stratégique pour les sociétés, les entreprises, et les Etats.

SILICONE CONNECT se présente comme l'opérateur des opérateurs sur le territoire national. Sa politique est l'accès ouvert envers les autres opérateurs et de créer des points de mutualisation des infrastructures partout au Congo.

Des interconnexions transfrontalières viendront mailler notre réseau avec nos pays voisins.

SILICONE CONNECT veut être un moteur du développement de la fibre optique nationale avec ses partenaires stratégiques : E²C, les Ministères de tutelle, le Ministère de la Coopération Internationale et de la Promotion du Partenariat Public Privé, le Ministère des Grands Travaux, et les porteurs de projets de futurs câbles sous-marins.

Il se positionne résolument sur le segment B2B avec une activité déclinée en 3 métiers à destination des grandes entreprises, des institutions et des opérateurs de télécom.

Avec des services comprenant:

- L'accès à internet professionnel ;
- L'interconnexion de sites en interurbain et en intra-urbain ;
- La vente de capacité de gros aux opérateurs de télécom et aux FAI nationaux et régionaux.

SILICONE CONNECT soutient les opérateurs régionaux en développant des points de présence (des POP) sur l'ensemble du territoire national et à l'international. Ces POPs sont ensuite mis en exploitation et ouverts à nos clients opérateurs.

Aussi, l'infrastructure est à la fois le vecteur des attaques, et est elle-même constamment sous attaque.

Pour un réseau de fibre optique, il faut composer entre les agressions physiques et les attaques logiques. La sécurité revêt donc deux aspects différents mais complémentaires.

Les attaques propres aux services sont les cyber attaques, qui attaquent le réseau ou les équipements connectés.

La cybercriminalité peut être qualifiée selon le type d'attaque prodigué :

- Escroquerie,
- Attaques en provenance de l'internet (exploits, DoS),
- Espionnage industriel,
- Phishing,
- Usurpation d'identité,
- Vol de données,
- Ransomware …

D'où la nécessité de mesures préventives – donc la cybersécurité – et de mesures curatives c'est à dire d'une riposte à chaque nouvelle brèche de sécurité découverte car les infrastructures sont des cibles de choix pour les criminels.

Pour protéger nos infrastructures et les données de ses clients, SILICONE CONNECT emploie des experts du domaine pour sécuriser son infrastructure.

Déroulement des activités – Jour 01

V. Déroulé des activités au programme

Jour 1

Plénière d'ouverture :

Thème : « Cybersécurité et géopolitique »

Modérateur :

Jean Pierre GOMA,
Consultant en Communication Institutionnelle

Panélistes :

Monsieur Léon Juste IBOMBO,
Ministre des Postes, Télécommunications et
de l'Economie numérique de la République du Congo

Monsieur Yves ICKONGA,
Conseiller du Président de la République du Congo, chef du Département des Télécommunications et du Numérique, Membre d'**Afrik@ CyberSecurity**

Monsieur Dominique MIGISHA,
Conseiller Spécial du Chef de l'Etat en charge
du Numérique (République Démocratique du Congo)

Ambassadeur Mohamed EL NOKALY,
Directeur Conseil Egyptien Européen (Egypte),
Membre d'**Afrik@ CyberSecurity**

Callixte TUZOLANA, Directeur de Cabinet Adjoint du Ministre du Numérique (République Démocratique du Congo)

Sur la question de la cybersécurité et de la géopolitique, les intervenants ont soutenu la nécessité des Etats africains d'adopter des mesures correctives et évolutives sur les questions du numérique dont la cybersécurité. Cette prise de décision ce doit être faite au niveau national puis sous-régional. A cet effet, il a été souligné l'exemple du Congo Brazzaville, pays hôte du forum, qui donne le ton par l'adoption depuis 2019 d'une stratégie nationale du numérique. Le projet de mise en place de l'Agence Nationale de Sécurité des Systèmes d'Information en République du Congo, qui illustre les efforts se

faisant localement pour implémenter les enjeux de la cybersécurité dans l'écosystème numérique au Congo.

La République Démocratique du Congo pour sa part traite la question de cybersécurité dans toutes les couches de son Plan National du Numérique horizon 2025, qui se décline sous les axes d'infrastructure, de la production et la gestion du contenu, l'usage applicatif et le dernier volet qui se constitue de la régulation et de la gouvernance.

Les dispositions des Etats africains en matière de politique nationale de cybersécurité favorisent des élans sous régionaux pour gérer de manière efficiente ses questions de sécurité d'un nouveau genre qui se posent au-delà des frontières régaliennes. A des niveaux régionaux et sous-régionaux, les efforts sont dans la synchronisation législative sur les questions de cybersécurité.

A cet effet, les panélistes ont souligné les efforts qui se font sur la question du numérique au niveau de la ZLECAF, de l'Union Africaine avec la Convention de Malabo. Ces actions collectives menées doivent donner lieu à une gouvernance sécuritaire commune tant dans les domaines politiques et législatifs que sur le plan technique.

Sur les défis et des difficultés qui se posent à chaque Etat, les panélistes ont convenu que des efforts doivent être fait pour assurer une souveraineté numérique. La cybersécurité doit être gérée premièrement comme problème de sécurité nationale, en confiant celle-ci aux compétences locales. Pour y parvenir, les Etats doivent anticiper les besoins et commencer au plus tôt à rapatrier et former les compétences.

Démonstration Hacking

« L'ABC de la sensibilisation aux risques de cybersécurité »

Intervenants :

Monsieur Clément DOMINGO
Hacker Ethique (France)

Monsieur Sanson CHAIGNON,
Expert en sécurité informatique (France)

Une présentation concrète des risques de cyberattaque a été faite pour édifier l'auditoire sur certains procédés d'hacking et comment en prendre garde.

On retiendra essentiellement de cette démonstration la nécessité :

- Pour les entreprises : avoir un code de procédure interne qui définit les règles d'hygiène informatique
- Pour le personnel d'entreprise : observer scrupuleusement les règles de sécurité édictées par l'entreprise et délimiter de manière claire le domaine professionnel et personnel ;
- Pour toute personne : redoubler de vigilance et de toujours privilégier les canaux officiels en cas de doute.

Study report :

Quelle stratégie de cybersécurité pour accompagner la transformation digitale ?

Intervenant :

M. Chrysostome NKOUMBI-SAMBA,
Président AfriK@ Cybersécurité (France)

La stratégie est un ensemble d'actions coordonnées, d'opérations habiles, de manœuvres en vue d'atteindre un but précis. En matière de cybersécurité, la stratégie se divise en quatre phase :

- Donner un sens et du sens
- Orienter la finalité
- Définition de la performance
- Partager l'information

Il faut, premièrement, donner un sens et du sens à la stratégie en lui traçant une ligne à suivre, créer une activité dans le long terme.

Deuxièmement, savoir faire des choix, c'est-à-dire, se questionner, collecter des données, confronter, développer les alternatives, évaluer les risques et bâtir le business model.

Troisièmement, rendre réalisable, c'est-à-dire, mettre en œuvre, affecter le personnel adéquat, assurer les moyens, allouer les ressources suffisantes et piloter la performance.

Quatrièmement, corriger, améliorer, analyser la créativité collective et saisir les stratégies émergentes.

En cybersécurité, il sied de bannir de mythe du risque zéro. Il convient de garder à l'esprit en permanence dans un univers numérique, de plus en plus complexe, incertain et dangereux, le risque zéro n'existe pas. S'il y a une vulnérabilité elle sera exploitée. Les hackers exploitent toujours les vulnérabilités d'un système. Aucun système n'est infaillible. Ce qui est créé par les humains, peut être défait par les humains, ceci dit, il n'y a pas de machines malveillantes, il n'y a que des hommes.

Le vrai problème de la sécurité se trouve entre le siège et le clavier. En sécurité, nous avons 20% de technique et 80% d'organisation. La sécurité est donc une question de comportement et de culture, bien au-delà de la sensibilisation.

L'acculturation, bien que peu utilisé comme terme, est plutôt pertinent, car elle désigne la capacité d'un homme à acquérir une culture qui lui est étrangère. Cas de l'inclusion de la culture de la cybersécurité au Congo.

Table-Ronde 01

Thème : Digitalisation, dématérialisation et économie numérique

Modération :

Serge Parfait GOMA,
Co-founder Open-source Community 242 (République du Congo)

Panélistes :

M. Abdoulaye COULIBALY, Secrétaire exécutif de l'Autorité Malienne de Régulation des Télécommunications, des Technologies de l'Information et de la Communication et

M. Chrysostome NKOUMBI-SAMBA, Président **Afrik@Cybersécurité** (France)

M. Steven Frederic ONDONGO, Juriste, spécialiste en cyber stratégie, ancien Conseiller administratif et juridique du Ministre de l'Économie numérique du Congo (République du Congo)

Monsieur Lié-Rupert GOUARI Directeur des Systèmes d'information et de la certification Électronique au GUOT (République du Congo)

La Digitalisation a apporté un changement significatif dans le domaine du commerce extérieur : la rapidité du service, la traçabilité de la marchandise et des opérations financières, la transparence dans les transactions en sont une illustration.

Pour faciliter son développement, nous pouvons procéder, soit manuellement, c'est-à-dire, entrer une à une les données dans une terminal, soit utiliser une intelligence artificielle. A ce niveau, la formation des jeunes à la maitrise du numérique reste un véritable challenge pour le changement des mentalités, aussi le recours à l'expertise extérieur constituer une charnière pour évolution de la dématérialisation et de l'économie numérique.

La problématique de la production du contenu est essentielle car l'Afrique subi une influence culturelle, il faut d'une part, sensibiliser et rendre accessible à tous l'internet par la réduction des coûts et vulgariser les connaissances sur la production du contenu purement africain (application mobile, solutions numériques, etc.) , afin de faire la promotion de la culture, et d'autre part, le peuple africain étant une population de consommation, il faut préparer le public cible à recevoir et utiliser ce contenu local. Ainsi pour transformer avec le numérique, il faut réfléchir comme le numérique.

Atelier 03 : « Risques et défis en matière de cybersécurité pour le secteur financier »

Formatrice :

Madame Reine TOUNGUI,
Risk Manager et Membre d'Afrik@Cybersécurité.

L'univers du cyber ou cyberespace est l'ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs.

La notion de risque étant étroitement liée à la notion de sécurité, fait ressortir la volonté d'anticiper des solutions numériques face au danger éventuel plus ou moins prévisible que courent les données financières, qui empêcherait la fourniture des services financiers et qui aurait définitivement un impact sur nos activités quotidiennes.

Les opérateur et acteurs du développement, n'ont pas entrevu un événement aussi soudain qu'improbable que la crise de covid-19 en 2020, or la notion de gestion de risque doit, avec un certain nombre de ressources et informations en interne au sein d'une organisation, se poser la question de savoir : « Quelle serait le pire scénario qui pourrait arriver et qui empêcherait le bon déroulement des activités ? » afin d'en envisager des solutions.

L'émergence en Afrique des technologies multiples, l'autonomisation des utilisateurs des Mobile Money qui facilite les transactions financières a suscité la mise en place par les banques des services de Mobile Banking et de Banque Digitale, afin de se mettre à niveau par rapport à l'évolution exponentielle de l'écosystème. Nous serions passé en dix ou quinze ans du M-PESA qui a démarré au Kenya à la Block Chain aujourd'hui. Cette évolution dans la multiplication des outils de traitement des données financières a aussi fait ressortir la vulnérabilité des systèmes d'administration suite à la délocalisation des centres de gestion des opérations.

La finance digitale qui se veut inclusive et exige beaucoup de vigilance, démontre également des limites et de failles au niveau de la sécurisation des opérations car dans l'exécution d'une transaction des outils comme l'ordinateur, la connexion internet, le smartphone etc., sont sollicités et peuvent être la cible des personnes mal intentionnées qui réalisent des opérations en parallèle de ceux-ci pour détourner des fonds.

Atelier 04 : « L'influence de la cybersécurité dans le secteur maritime »

Formatrice :

Madame Armélia ITOUA,
Ingénieure en Management Maritime et Portuaire et Membre d'Afrik@Cybersécurité

A travers cet atelier, l'assistance, essentiellement composée d'agents de la gendarmerie nationale, a eu un aperçu de ce qui en est de la question de la cybersécurité dans le secteur maritime.

Un rappel du rôle indispensable que joue le secteur maritime dans l'économie mondiale a été évoqué, avec une étendue couvrant près de 2/3 de la surface terrestre, la mer est la voie par laquelle est acheminé 80% du volume mondial de marchandise. Par ce même canal transit les câbles internet sous-marin.

La migration des ports africains vers la 3e génération de port est fortement induite par le numérique. Au Congo par exemple, le port autonome de Pointe-Noire s'est vu doté, au cours de l'année 2020, de nouveaux équipements et de nouvelles infrastructures : deux nouveaux quais D et G pour recevoir des conteneurs de plus grande capacité, ce qui fait du port de Pointe-Noire l'un des ports les plus modernes de la sous-région. Ce progrès s'accompagne de risques importants, dont de risques de cyberattaques qui sont prises très au sérieux dans ce secteur, pour protéger les systèmes d'information et les infrastructures.

Au regard des attaques recensées dans le monde ciblant des sites portuaires, le secteur maritime s'est doté de directives et de moyens techniques pour lutter contre les cyberattaques. En 2017, une société danoise spécialisée dans le fret maritime a été victime d'une cyberattaque ; en 2020, l'Organisation Maritime Internationale a été la cible d'une attaque cybernétique ainsi que le groupe Bolloré en République Démocratique du Congo.

Ce petit synopsis sur le secteur maritime illustre l'importance de la question de cybersécurité dans ce secteur.

Atelier 05 : Collecte des données, renseignements offensifs

Formateur :

Daniel DONNET-MONAY,
CEO VICI Suisse Competitive Intelligence (Suisse)

VICI Swiss Competitive Intelligence est une agence d'investigation et de protection basée en Suisse. Sa mission consiste à protéger les intérêts de toute personne ou entreprise grâce à une exploitation optimisée de l'internet. Pour parvenir à ces buts, ses experts pluridisciplinaires mettent en place une stratégie adaptée à toute demande particulière et liée au domaine du numérique.

VICI Swiss Competitive Intelligence offre des services d'Investigation numérique avec DATA Prédictor, de Veille stratégique avec DATA Prédictor, d'Extraction de données sur un appareil numérique.

Il est important de comprendre le fonctionnement d'internet. Il est fait de données annexées c'est-à-dire le web de surface qui fonctionnent avec les moteurs de recherche, et des données non annexées qui représentent 98% de l'internet et qui ne sont pas accessible à tous. Ainsi, VICI Swiss Competitive Intelligence propose une formation continue dans l'analyse de l'information pour les militaires mais aussi pour les entreprises stratégiques avec des services sensiblement moins cher sur le marché.

Etant le continent le plus connecté du monde, l'Afrique est une cible potentielle présentant beaucoup de faiblesses exploitées par les puissances étrangères.

Déroulement des activités – Jour 02

JOUR 2

Study report :

Les enjeux et défis de la cybersécurité en Afrique centrale

Intervenant :

Didier SIMBA,
Fondateur et Président de CESIA (Gabon)

Le CESIA - CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE est le 1er réseau d'experts de la sécurité numérique en Afrique. Le CESIA compte près de 200 membres présents dans 20 pays d'Afrique qui sont tous Directeurs des Systèmes d'Information (DSI), Directeurs de la Sécurité des Systèmes d'Information (DSSI), Responsables des Systèmes d'Information (RSI) ou Responsables de la Sécurité des Systèmes d'Information (RSSI).

Le CESIA accompagne les entreprises dans leur démarche en cybersécurité.

L'Afrique, étendue sur 54 pays, ne dispose pas de chiffres exacts en ce qui concerne la cybersécurité, car les victimes d'attaques cyber ne reportent pas les estimations des dommages causées par ces dernières et aucune structure de régulation ne recense les attaques.

La crise sanitaire de covid-19 a révélé que moins de 10% des pays africains ont réussi à développer le dispositif du télétravail pour des raisons de non préparation, de sécurisation des données mais aussi de confiance garantissant l'exécution des taches à distance.

55% des entreprises en Afrique centrale disent ne pas être capables de survivre à une attaque cyber de grande ampleur.

82% des entreprises en Afrique disent avoir subi au moins 3 attaques d'impact majeur en 2020 ; cet impact peut être financier, organisationnel ou peut toucher à l'image de l'entreprise.

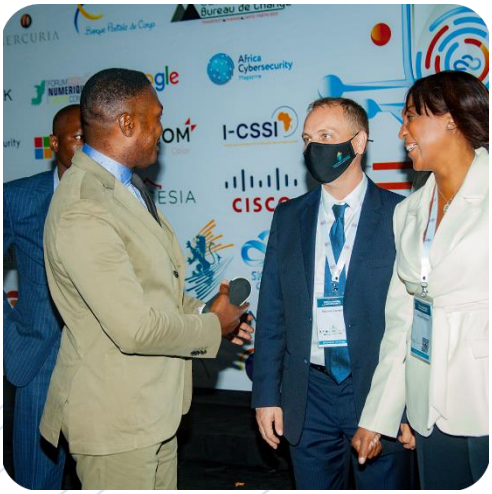


Table-Ronde 04

Thème : Cybersécurité : de la Cyberguerre à la Cyberdéfense

Modération :

Olaf OQUEMBA,
Directeur de la logistique au CIRAS (République du Congo)

Panélistes :

M. Didier SIMBA,
Fondateur et Président chez CESIA (Gabon)

M. Daniel DONNET-MONAY,
CEO VICI Suisse Competitive Intelligence (Suisse)

M. Jean-Marius IBARA KIEBE KANIMBOET,
Directeur de la recherche technologique et stratégique, responsable de la cybersecurité au CIRAS, Membre d'Afrik@ Cybersecurité
(République du Congo)

M. Steven Frederic ONDONGO,
Juriste, spécialiste en cyber stratégie,
ancien Conseiller administratif et juridique du ministre de l'économie numérique du Congo

Cyberguerre peut être définie comme la guerre de l'information, la guerre par l'information ou la guerre à l'information, différente de la guerre classique. La cyberdéfense, quant à elle, doit être vue comme la dimension opérationnelle de la cybersécurité. La course à la donnée entre Etat a fait naître des systèmes de gestion d'information pour la sécurisation de celle-ci.

L'Afrique est le continent le plus connecté grâce à la présence des dernières technologies en matière de téléphonie mobile, d'ordinateurs et autres. La circulation intense des informations est contrôlée par le fournisseur à l'occident, qui analyse chacune des données émises afin de tenir sous son joug le continent africains. Les smartphones en Afrique constituent des canaux d'information pour les grandes puissances afin de gérer au quotidien et de façon minutieuse les richesses et potentiels de l'Afrique.

Aussi, aucune stratégie n'est possible pour faire face à une cyberattaque. L'africain ne croit pas à l'expertise locale et s'appuie sur l'expertise des puissances étrangères. La mise en place des moyens concrets suivant la Convention de Malabo qui invite les États à adopter des mesures législatives et réglementaires pour poursuivre la cybercriminalité, afin lutter contre la cybermenace qui doit être une préoccupation pour les institutions en Afrique, doit être exécuté pour de sécuriser les données et les utilisateurs.

Table-Ronde 05

Thème : Pièges Cyber

Modérateur :

Maixent FOUKOU,
Journaliste VOX TV

Panélistes :

Excellence Mohamed EL NOKALY,
Directeur Conseil Egyptien Européen,
Membre d'Afrik@CyberSecurité
(Egypte)

Daniel DONNET-MONAY,
CEO VICI Suisse Competitive Intelligence
(Suisse)

Serge Parfait GOMA
Co-founder Open-source Community 242
(République du Congo)

Reine TOUNGUI,
Risk Manager,
Membre d'Afrik@
CyberSecurité
(Gabon)

Yves-Valentin GBEYORO,
Analyste prévention des Conflits,
Membre d'Afrik@CyberSecurité
(RCA)

Ne pouvant pas reculer face à la digitalisation et la transformation numérique, il faut prendre conscience du risque d'être face aux multiples pièges contenus dans le cyberespace, pour cela il faut informer et sensibiliser les populations et vulgariser les connaissances de base dans l'utilisation de l'outil informatique.

Une négligence dans la manipulation de l'outil informatique peut représenter un piège cyber tout comme il est fondamental pour l'Afrique de produire un capital humain capable de se former selon les exigences des nouvelles technologies et de se défendre au piège cyber car le cyberespace africain reste jusqu'à lors dominé par les puissances étrangères, qui ont une main mise et un contrôle total sur les informations produites en Afrique et lui en refuse l'accès.

Il sied de reconnaître que la plupart des personnes, cibles d'une attaque, ne réalisent pas qu'elles en sont victimes, car ne disposant pas de méthodes adéquates de détection en temps réel d'une attaque cyber.

Il faut changer de mentalité en tant qu'utilisateur, ne pas s'attendre à une attaque mais utiliser les failles que présentent internet afin de prévenir et anticiper d'éventuelles attaques pour s'en défendre.

Le phishing vient essentiellement de la fuite des données, une entreprise ou un individu, potentielle cible, doit se munir des programmes et des procédures nécessaires pour se protéger des attaques car la menace est réelle.

Table-Ronde 6

Thème : « L'Afrique est-elle prête à tenir face à la menace cyber ? »

Modération :

Nelson CISHUGI,
CEO LOPANGO

Intervenants :

M. Jean-Louis BISSANGILWA,
Conseiller au Collège Socio-culturel au cabinet
du Premier Ministre de la République Démocratique du Congo,
Membre d'Afrik@Cybersécurité

M. Chrysostome NKOUMBI-SAMBA,
Président Afrik@Cybersécurité (France)

M. Olaf OQUEMBA,
Directeur de la logistique au CIRAS
(République du Congo)

M. Gilles CHOULA,
Co-fondateur et Administrateur du CESIA
(Cote d'Ivoire)

M. Francis SECK MANGOUANI, Conseiller à l'économie
numérique du Ministre des Postes, des Télécommunications
et de l'Economie Numérique de la République du Congo

L'Afrique, comme tout autre continent, n'est pas prête à tenir face à une attaque cyber, car ne disposant pas de capacité nécessaire et suffisante, elle devrait entreprendre des actions concrètes à mener afin de se mettre la pointe de la technologie qui évolue de façon exponentielle. Les Etats doivent prendre conscience du retard technologique de l'Afrique et faire de la prospective une priorité pour préparer l'avenir. L'Afrique doit également changer les paradigmes mentaux, comportementaux, économiques sociaux.

et Certains pays d'Afrique, étant plus avancés que d'autres en matière de cybersécurité, les dispositions de formation dans ce domaine diffèrent d'un pays à un autre, à l'exemple de l'Ile Maurice, qui est classé premier dans les formations en cybersécurité. Afin d'anticiper les menaces cyber, il est d'usage de sensibiliser les utilisateurs du cyber espace et les Etats sur le risque que représente la non sécurisation des données et enrichir les compétences des africains dans le secteur du numérique par des formations adéquates selon les avancées de la technologie.

Table-Ronde 07

Thème : La cybersécurité, facteur indispensable pour une transformation numérique durable et efficace

Modération :

Serge Parfait GOMA,
Co-founder Open-source Community 242 (République du Congo)

Panélistes :

Louis Marc SAKALA,
Directeur Général de l'ARPCE
(République du Congo)

Gaëtan SOLTESZ,
Directeur Général de SILICONE CONNECT
(République du Congo)

Vérone MANKOU,
CEO VOX Médias
(République du Congo)

Fulgence FUMUANGANI, Gestionnaire ressources numériques de la Société Congolaise des Postes et Télécommunications (RDC)

Une organisation doit incorporer des technologies dans ses produits, des processus et des stratégies afin qu'elle reste compétitive dans un monde plus en plus numérique. Les secteurs comme l'Energie, les transports, la santé, l'approvisionnement en eau, les infrastructures du numérique et les marchés financiers sont les plus touchés par la transformation numérique et peuvent être source d'aspiration de piratage ou hacking.

Il s'agit de mettre en place un cadre réglementé, des méthodes de protection dès l'installation d'une infrastructure, qui constituerait une première barrière à une attaque cyber.

Les pays partageant le même réseau en fibre optique doivent coopérer et s'assurer d'avoir un niveau semblable en termes de réglementation du numérique voir de la cybersécurité afin de ne pas représenter une menace pour le pays voisin.

Les Etats doivent s'impliquer dans la promotion de la consommation des hébergements de serveurs locaux qui fournirons des services et des exigences de qualité.

Table-Ronde 08

Thème : Cyber diplomatie et échanges stratégiques de l'information dans l'écosystème de la cybersécurité

Modération :

Serge Parfait GOMA,
Co-founder Open-source Community 242 (République du Congo)

Panélistes :

Luc MISSIDIMBAZI,
Conseiller du Premier Ministre aux Télécommunications et Numérique (République du Congo)

Yves Valentin GBEYORO,
Analyste prévention des Conflits, Membre d'Afrik@Cybersécurité (RCA)

Excellence Mohamed EL NOKALY,
Directeur Conseil Egyptien Européen, Membre d'Afrik@Cybersécurité (Egypte)

Les échanges stratégiques de l'information dans l'écosystème de la cybersécurité sont du domaine de la souveraineté de l'Etat.

Les pays doivent coopérer pour élaborer des stratégies de gouvernance commune pour faire face aux dangers communs d'attaques cyber qui déstabilisent les Etats. Les accords de sécurité entre les pays sont de mise. A la coopération entre Etats, se pose le problème de contre-espionnage qui peut constituer un handicap pour l'essor de la cyber diplomatie. Il s'agira de mutualiser les connaissances, les moyens, les informations militaires pour propulser et renforcer la cybersécurité. Il faut organiser le cyber espace africain en identifiant les ressources, dialoguant avec les Etats à travers les communautés de gestion comme la Conférence Internationale sur la Région des Grands Lacs (CIRGL), la Communauté économique et monétaire de l'Afrique centrale (CEMAC) et autres car la problématique de la cybersécurité doit être une priorité. Promouvoir la formation de base en sécurité de l'information afin de protéger l'utilisateur des risques cyber.

Le Cyberespace est un espace d'activité commun à l'humanité. L'avenir du cyberespace doit être pris en main par tous les pays. Les différents pays doivent renforcer la communication, élargir le terrain d'entente et approfondir la coopération, afin de bâtir une communauté de destin à partir du cyberespace.

Table-Ronde 09

Thème : Partenariat public-privé pour le financement de la Cybersécurité

Modération :

Babylas BOTON,
Journaliste Africa24

Panélistes :

Dominique MIGISHA,
Conseiller Spécial du Chef de l'Etat en charge du Numérique
(République Démocratique du Congo)

Callixte TUZOLANA,
Directeur de Cabinet Adjoint du Ministre du Numérique
(République Démocratique du Congo)

Jean Claude SAMBA,
Directeur Associé au sein de Prométhée Intelligence Economique et Stratégique, Membre d'Afrik@Cybersécurité (République Démocratique du Congo)

Luc MISSIMDIBAZI,
Conseiller du Premier Ministre aux Télécommunications et Numérique (République du Congo)

Au grand regard du principe de financement des projets de développement qui inclut le numérique, il est important, voir majeur, de préciser la position de l'Etat ainsi que les raisons pour lesquelles celui-ci doit y prendre part, et préciser la part des partenaires techniques financiers.

En effet, le financement de la cybersécurité est de la responsabilité de l'Etat. Toutefois, il s'avère quelques fois que les coûts qu'engendrent ces investissements pèsent sur le Gouvernement seul car les budgets des Etats africains ne permettent pas de couvrir en totalité ces financements, en raison de l'énorme poids financier qu'engendre la construction de l'infrastructure numérique. Le public ne peut seul assurer l'investissement pour le développement de ce dernier. A cet effet, le partenariat entre le secteur public et privé prend tout son sens dans la mesure où tout deux participent ensemble à l'investissement et au développement de la cybersécurité.

Le financement de cybersécurité relève donc de la coopération entre l'Etat et le secteur Privé dans un cadre de confiance mutuelle, qui est impérative dans divers domaines dont celui du numérique.

Seulement, le financement seul ne peut régler entièrement le problème du développement du numérique, il faut aussi y ajouter la mise en œuvre d'outils nécessaire qui assurera son émergence. Créer un cadre dans lequel peut se développer la cybersécurité est une nécessité de plus en plus

urgente, tant dans le secteur public que dans celui du privé. Cette croissance est liée aux multiples facteurs ; mais la digitalisation rapide et la virtualisation due à la pandémie du covid-19, principalement en Afrique, ont joué un rôle déterminant.

Aussi, la pandémie du covid-19, comme la plupart des crises, a impulsé une augmentation des cyberattaques, d'où les partenariats public-privé (PPP) qui jouent un rôle important grâce à leurs coopérations qui renforcent la cybersécurité dans de nombreuses régions d'Afrique.

Atelier 05 : « Les vulnérabilités du cyberespace africain, quelles stratégies ? »

Formateur :

Éric NDOUMBA, Conseiller aux Télécommunications du Ministre des Postes, des Télécommunications et de l'Economie Numérique de la République du Congo

Le cyber espace africain présente des faiblesses permettant à un attaquant de porter atteinte à son intégrité, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Le problème se pose dans la règlementation, en ce qui concerne les conventions de Malabo et de Budapest, il est regrettable de contester les faibles adhésions par la ratification de ces textes. Ce déphasage constitue une vulnérabilité du système de gestion de la donnée en Afrique. Les Etats doivent collaborer en matière de protection de données pour définir des lois à appliquer, respecter.

Le Congo, a pour sa part, mis en place cinq lois :

- La loi sur la protection des données
- La loi sur la cybercriminalité
- La loi sur la cybersécurité
- La loi sur la transaction électronique
- La loi de création de l'Agence Nationale de Sécurité des systèmes d'information

La vulgarisation des lois sur la sécurité des données dans le secteur public, privé, auprès des utilisateurs, est un enjeu majeur pour créer une plateforme de collaboration entre la justice qui fait appliquer ces lois et les corps de répression, dont la Gendarmerie et la Police. La sensibilisation et le renforcement des capacités des corps de répression sur la culture de la cybersécurité est de mise pour son développement.

Hacking Challenge

Formateurs

Clément DOMINGO, Hacker Ethique (France)

Sanson CHAIGNON, Expert en sécurité informatique (France)

Youssef DESTEFANI, Ingénieur en sécurité informatique (Sénégal)

Adama ASSIONGBON, Analyste et Expert en Cybersécurité (Togo)

Face aux menaces des cyberattaques très rependues de nos jours, les entreprises, en temps de crise, font de plus en plus appel aux hackers chargés de protéger et de trouver les failles des systèmes informatiques qui nuisent à leur fonctionnement. En effet, dans un monde du tout numérique, les experts en hacking sont plus que jamais courtisés par les entreprises.
Le Hacking Challenge **<< Crack me if you can >>**, organisé par le Forum Brazza Cybersecurity, est une compétition ayant pour but de repérer des experts en système informatique dans le milieu estudiantin afin d'en faire des hackeurs éthiques.

Cette compétition a consisté en différentes épreuves et simulations portant entre autres sur le décryptage de messages codés, le déverrouillage de mot de passe, et bien d'autres. La compétition s'est faite en groupe de trois personnes minimums. Les groupes ayant obtenu le plus de points se classent comme suit :

- Spectre Hacker, en première position
- Cyber Expert en deuxième position
- Zombie troisième position

Toutefois un groupe spécialement composé de filles, s'est démarqué, il s'agit du groupe WIN, qui a occupé la cinquième position du classement.

Cérémonie de clôture
Couverture médiatique & visibilité

VI. Cérémonie de clôture

Le Forum Brazza Cybersecurity, pour sa première édition a pris fin le 17 septembre 2021 au Centre International de Conférence de KINTELE. La cérémonie de clôture a été ponctuée par un rappel des objectifs atteints quoi que certaines activités prévues ont été perturbées notamment le premier jour du forum ; et aussi, par la remise des prix aux lauréats du Hacking Challenge, par les allocutions de Monsieur Arnaud AKEN ELION, Manager Général de la Société SKYTECH Congo, qui a exprimé ses vifs remerciements aux personnalités présentes, aux sponsors, aux partenaires ainsi qu'aux participants, de Monsieur Issifou N'DOURO, Ministre d'Etat, ex Ministre de la Défense du Bénin, qui a félicité l'initiative et a fait part de son point de vue sur le développement de l' Afrique face à la menace cyber pour transmettre aux générations futures l'expertise qui est la sienne dans ce domaine.

Pour sa part, Monsieur Patrick MUYAYA, Ministre de la Communication et des Médias, Porte-Parole du Gouvernement de la République Démocratique du Congo, a salué les travaux du Forum qui ont permis aux Etats des pays participants de s'imprégner de la culture de la Cybersécurité qui est la garantie de toute action posée dans le secteur du numérique.

Monsieur Chrysostome NKOUMBI-SAMBA, Président du comité scientifique et Président d'Afrik@Cybersécurité a également remercié l'assistance, souligné que le forum s'inscrit dans une dynamique et a présenté l'équipe d'organisation ainsi que celle de la société SKYTECH CONGO.

Sur une note de contentement et de félicitation pour le travail abattu pendant la tenue du Forum, Madame Horgerie GUEMPIAUT, Coordonnatrice Générale a clos les travaux du Forum Brazza Cybersecurity.

VII. Couverture médiatique et Visibilité

Avant		Pendant		Après	
		Couverture Médiatique : Presse TV/Radio, Webmag			
Communication Institutionnelle (Audiences & autres activités)	Communication Marketing	Ouverture	Clôture	Communication Marketing	Actions Médias
Participation au Cyber Afrik Tour 2021	Diffusion spot tv teaser "La menace est réelle"	Télé Congo	Télé Congo	Campagne de l'événement	Article sur le site courconsitutionnelle.cd
Audience avec Léon Juste IBOMBO, Ministère des Postes, Télécommunications, et de l'Economie numérique	Déploiement de la campagne de teasing "La menace est réélle" sur panneaux 4/3	VOX TV VOX TV	VOX Africa VOX Africa		Article sur le site courconsitutionnelle.cd Article sur le site de ICIBRAZZA
Audience avec Thierry Lézin MOUNGALLA, Ministre de la Communication, des Médias, et Porte-parole du Gouvernement	Communication digitale : Website, réseaux sociaux. o Count-down de l'événement Relais des audiences o Parlons cybersécurité (Contenu de sensibilisation) o Astuces de sécurité (Contenu de sensibilisation)	DRTV Radio Congo	DRTV Radio Congo	Campagne de l'événement	Article sur le site de ICIBRAZZA Article sur le webmag LSI Africa
Audience avec le Consul de l'Ambassade de la Fédération de Russie au Congo	Diffusion spot/TV Hackaton	Radio Congo Pause-Café (Magazine)	Radio Congo Pause-Café (Magazine)		Article sur le webmag LSI Africa Article sur le webmag Yabiladi.com
Audience avec Luc Joseph OKIO, Ministre délégué auprès du Premier Ministre, chargé de la réforme de l'Etat		Pause-Café (Magazine) ACI	Pause-Café (Magazine) ACI		Article sur le webmag Yabiladi.com Article sur le webmag Ciberobs
Audience avec Séraphin BHALAT, Directeur Général du Port Autonome de Pointe-Noire	Diffusion spot/TV Hackaton	ACI Webtv R10	ACI Webtv R11		Article sur le webmag Ciberobs Article de Presse sur le webmag Financial Afrika
Audience avec Séraphin BHALAT, Directeur Général du Port Autonome de Pointe-Noire	Diffusion spot Tv annonce du Forum Brazza Cybersecurity	Webtv R10 TSIELEKA MEDIA	Webtv R11 TSIELEKA MEDIA		Article de Presse sur le webmag Financial Afrika
Audience avec Michel DZOMBALA Directeur National de la BEAC	Déploiement national de la campagne de l'évènement sur panneaux 4/3	TSIELEKA MEDIA Focus Médias (Web TV)	TSIELEKA MEDIA Focus Médias (Web TV)		

Audience avec Brice ETOU **Directeur Général de CACOGES**	Passage de Clément Domingo, hacker éthique pour annoncer l'évènement au JT de TV5 Monde Afrique	Focus Médias (Web TV) Le pari africain	Focus Médias (Web TV) Equinoxe TV		
Audience avec Raymond MBOULOU Ministre de la Sécurité et de l'Ordre public	Interview du Promoteur du forum dans le webmag LSI Africa	Le pari africain GéoAfrique Médias	Equinoxe TV GéoAfrique Médias		
Audience avec Roger KWAMA Directeur Général de ENCO	Passage du promoteur du l'événement au JT de TV CONGO	GéoAfrique Médias Kongo Lissolo	GéoAfrique Médias Kongo Lissolo		
Audience avec William MASSEMBO Directeur Général de l'ARC	Passage du Président du comité scientifique au programme matinal -Matin Bonheur – de DRTV	Kongo Lissolo Lux TV	Kongo Lissolo Echos du Congo (Webmag)		
Audience avec Jean-Pierre NONAULT Directeur Général des Institutions financières		Lux TV Panoramik actu	Echos du Congo (Webmag) Panoramik actu		
Audience avec Hughes NGOUENLONDELE Ministre de la Jeunesse, des sports, de l'Education civique et de la Formation qualifiante		Panoramik actu Le républicain	Panoramik actu Le républicain		
Audience avec Guy Georges MBAKA Ministre de l'administration du térritoire		Le républicain Les dépêches de Brazzaville	Le républicain Les dépêches de Brazzaville		
Audience avec Stella MENSAH SASSOU NGUESSO **Maire de Kintélé**		Les dépêches de Brazzaville C-direct	Les dépêches de Brazzaville C-direct		
Audience avec Dieudonné BANTSIMBA Maire de Brazzaville		Equipe de communication Min. Postes et télécommunications	Equipe de communication Min. Postes et télécommunications		
Audience avec le Colonel OLLANGUE Commandant de la Gendarmerie		Radio Brazza	Radio Brazza		
Audience avec Tedi Christel SASSOU NGUESSO Directeur Général de la SNPC-D		Yango TV (Webtv)	Yango TV (Webtv)		
Audience avec Patrick MUYAYA KANAMBWE Ministre de la communication et des médias, porte-parole du gouvernement : RDC		Yango TV (Webtv)	Yango TV (Webtv)		
Audience avec Didier MUSETE Directeur Général de la Société congolaises des postes et télécommunications : RDC					
Audience avec Bruno Jean-Richard ITOUA Ministre des hydrocarbures					

Bilan, Vision du Forum, Recommandations & Les Chiffres

VIII. Bilan et Vision du Forum

Le **Forum Brazza Cybersecurity** s'est inscrit dans une dynamique nouvelle en Afrique centrale en favorisant le partage entre les différents acteurs et décideurs, aptes à mener la réflexion sur les enjeux stratégiques qu'engendre la cybersécurité pour les Etats, les entreprises et institutions en Afrique.

Il a permis aux institutions nationales et internationales, aux entreprises, aux centres de recherches et universitaires, aux personnalités et à la société civile, de mettre au cœur du développement de l'Afrique centrale, un meilleur usage de la cybersécurité.

Cependant, compte tenu du retard du Ministre des Postes, des Télécommunications et de l'Economie Numérique, appelé à prendre part au départ de SEM Denis SASSOU NGUESSO, Président de République du Congo à l'aéroport international de Maya-Maya, et, à prendre également part au conseil de cabinet de la Primature prévu ce même jour, aussi, suite à l'indisponibilité de certains panélistes, le comité scientifique a jugé bon, d'ajuster le programme selon les convenances.

Ainsi, certains ateliers et table-rondes n'ont pu se tenir. Tels que:

- Atelier 01 : La cybersécurité et la géopolitique
- Table-ronde 02 : Cyber finance, quels défis ?
- Atelier 02 : L'intelligence collective et les Cyber menaces : mesures stratégiques et Opérationnelles
- Table-ronde 03 : Protéger les administrations publiques des risques cyber
- Atelier 07 : Cybersécurité et souveraineté numérique de l'Etat
- Atelier 08 : Cyber approvisionnement, quels défis ?

La non-exécution de ces activités représente un défi à relever pour la bonne réalisation des prochaines éditions. Le comité d'organisation se met à pied d'œuvre pour faire appliquer, dans la mesure du possible, les recommandations issues du forum.

IX. Recommandations

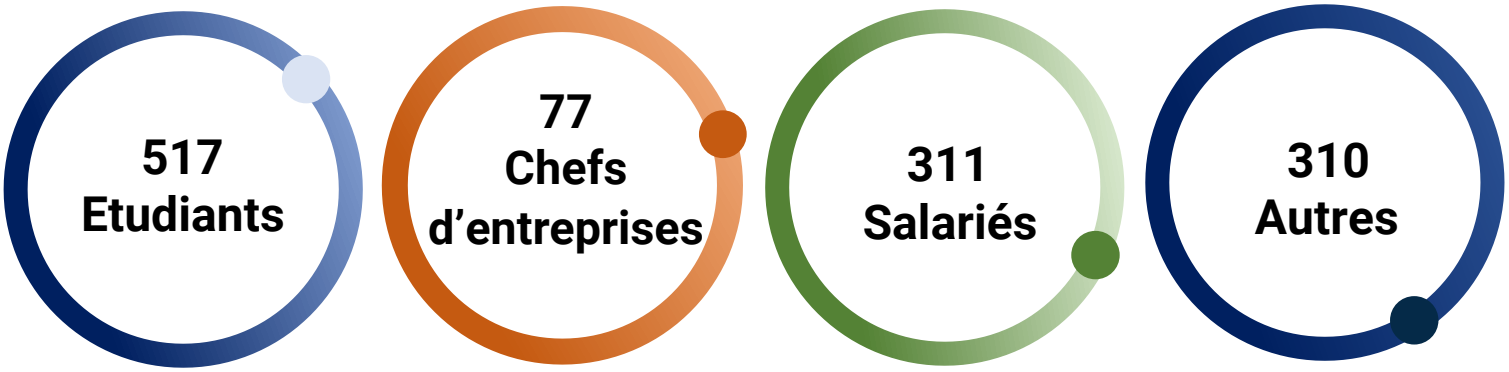
Des différents table-rondes et partages de connaissances sont ressorties des recommandations suivantes qui seront applicables selon les besoins :

- Sensibiliser les dirigeants des Etats, des institutions et des entreprises aux enjeux de la cybersécurité afin de définir des stratégies sectorielles, au niveau des Etats, et mener des compagnes pour sensibiliser les utilisateurs finaux des outils du numérique sur les risques de cybersécurité ;
- Réguler le sous-secteur de cybersécurité avec un cadre légal et des moyens d'action ;
- Mettre en place une coopération internationale au niveau de la sous-région sur les questions de la cybersécurité ;
- Mettre en place des outils collaboratifs entre Etats pour la bonne gestion des données produites en Afrique ;
- Les Etats africains doivent prendre au sérieux les menaces cybernétiques et se préparer en conséquence ;
- Mettre en place un institut africain de la cybersécurité sous le contrôle de l'Union Africaine ;
- Les Etats africains doivent envisager une souveraineté numérique nationale ;
- Le Etats africains se doivent d'anticiper les besoins en ressources humaines et disposer des formations de qualités pour la jeune génération afin de promouvoir les compétences locales ;
- Pérenniser la sensibilisation sur la culture de la cybersécurité et favoriser son inclusion en Afrique ;
- Mettre en commun des efforts et des compétences des Etat africains pour faire face à la menace cyber ;
- Mettre en place des cyber diplomates, des référents qui traiteront les questions de cybersécurité en cas d'attaque ;
- Les entreprises doivent désigner un référent pour la gestion de la cybersécurité ;
- Les Etats africains doivent tous ensemble rejoindre et ratifier la convention de Malabo ;
- Mettre en place des cyber partenariats public-privés.

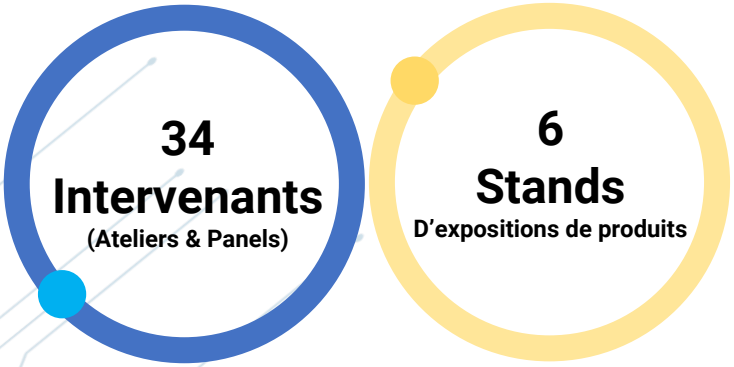
X. FORUM BRAZZA CYBERSECURITY, les Chiffres

Le Forum Brazza Cybersecurity a suscité un grand intérêt des utilisateurs du numérique, des étudiants dans le domaine de la tech, des institutions et des entreprises privés, soit :

1215 inscrits en ligne via le site internet du Forum avec :



159 participants se sont inscrits surplace et **218 personnes** ont répondu à l'invitation émise par le comité d'organisation dont **50 étudiants** du CFI-CIRAS et **50 gendarmes**.



13 pays ont pris part au **Forum Brazza Cybersecurity**, entre autres

- République Démocratique du Congo
- République Centrafricaine
- République du Gabon
- République du Mali
- République du Tchad
- République d'Angola
- Egypte
- République du Togo
- Madagascar
- République du Benin
- République du Sénégal
- France
- Suisse

Nos Sponsors

XI. Nos sponsors

Le Forum Brazza Cybersecurity a été soutenu par de diverses institutions et organismes, nationaux et internationaux, qui ont bien voulu accompagner cette initiative pionnière de la Cybersécurité en Afrique centrale, il s'agit de :

Sponsor Officiel

Fondée en 2020, SILICONE CONNECT est un opérateur Télécoms en République du Congo. Concessionnaire du réseau national de fibre optique construit par la société Energie Electrique du Congo (E^2C). Il déploie des solutions sur mesure pour répondre aux besoins spécifiques des entreprises au Congo, SILICONE CONNECT s'appuie sur un réseau de fibre optique de première qualité et une expertise solide et pluridisciplinaire pour proposer en tant qu'opérateur de gros et opérateur B2B les services suivants : l'interconnectivité, l'accès internet & vente de capacité pour les entreprises. Plus qu'un opérateur de télécommunications, SILICONE CONNECT se veut être un acteur impliqué dans l'ensemble des domaines qui touchent le public : l'éducation, les finances, le culturel et le divertissement, la cybersécurité, la santé ou encore les objets connectés.

Autres Sponsors

L'ARPCE, Agence de Régulation des Postes et des Communications Électroniques, est l'Autorité congolaise de contrôle, de suivi et de régulation des secteurs des Postes et Communications Électroniques. Elle garantit le service aux usagers, œuvre pour l'intérêt national, encadre l'activité des Opérateurs, gère le domaine des fréquences radioélectriques. Elle est placée sous la tutelle du Ministère en charge des Postes, des Télécommunications et de l'Economie Numérique. Structure opérationnelle et technique de l'État dans le domaine des Postes et Communications Électroniques, l'ARPCE est née de la volonté commune du Gouvernement congolais, de la Banque Mondiale et du Fonds Monétaire International, sur les cendres de la Direction Générale de l'Administration Centrale des Postes et Télécommunications.

LA BANQUE DES ETATS DE L'AFRIQUE CENTRALE : INSTITUT D'EMISSION EN AFRIQUE CENTRALE

Créée en 1972, la Banque des Etats de l'Afrique Centrale (BEAC) est la banque centrale commune aux six Etats qui constituent la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC). Il s'agit respectivement du Cameroun, de la République Centrafricaine, du Congo, du Gabon, de la Guinée Equatoriale et du Tchad. La BEAC a pour missions de : définir et conduire la politique monétaire de la CEMAC ; émettre la monnaie fiduciaire (billets de banque et pièces qui ont cours légal et pouvoir libératoire dans la CEMAC) ; conduire la politique de change de la CEMAC ; détenir et gérer les réserves officielles de change des Etats-membres ; promouvoir le bon fonctionnement des systèmes de paiement et de règlement ; promouvoir la stabilité financière.

La Banque Centrale met à la disposition de la Commission Bancaire des Etats de l'Afrique Centrale (COBAC), les moyens financiers, matériels et humains nécessaires à l'exécution de sa mission de supervision bancaire ; mission indispensable pour garantir la stabilité économique de la CEMAC. Elle entretient aussi des relations régulières et efficaces avec des partenaires internationaux faisant d'elle une Institution monétaire et financière de référence.

Créée le 23 avril 1998, la Société Nationale des pétroles du Congo (SNPC), par ses attributions, est un pilier énergétique et économique de la République du Congo. Elle est une société de droit public congolais. C'est un établissement à caractère industriel et commercial doté de la personnalité morale et de l'autonomie financière. Son rôle est de rechercher, exploiter, valoriser et distribuer les hydrocarbures au Congo.

La SNPC assure cette mission seule ou en partenariat avec de nombreuses compagnies internationales installées au Congo, tout en dynamisant la coopération sud-sud dans ce secteur. L'ambition de la SNPC est d'asseoir une expertise nationale de haut potentiel dans l'industrie pétrolière, à travers une stratégie de croissance.

Le Guichet Unique des Opérations Transfrontalières, en sigle GUOT, est un Etablissement Public à caractère Industriel et Commercial (EPIC), Il est placé sous tutelle du ministère des transports, de l'aviation civile et de la marine. Depuis le 3 NOVEMBRE 2014 en effet, le GUOT a débuté ses activités. Il est chargé de simplifier les procédures et faciliter les formalités administratives, commerciales et douanières, tout en réduisant les coûts et délais de passage des marchandises aux frontières.

Le GUOT se caractérise par un point d'entrée unique électronique pour la soumission et le traitement de toutes les données, et de tous les documents nécessaires aux opérations d'importation ou d'exportation de marchandises.

Autorité de certification (primaire) des échanges électroniques en République du Congo, le GUOT délivre les agréments aux fournisseurs des prestations de services de certification comme autorité secondaire, émet et délivre les certificats. Le guichet unique soutient de ce fait l'interconnexion de tous les acteurs participant au commerce extérieur congolais, afin de garantir l'interopérabilité de leurs systèmes d'information.

La Banque Postale du Congo, banque de l'émergence, a débuté ses activités le 25 janvier 2013. Elle a pour vocation d'être avant tout une banque de proximité. A cet effet, son objectif, à moyen terme, est de s'étendre dans tous les départements du Congo. Elle met à la disposition de sa clientèle une gamme de produits et services bancaires classiques tels que les comptes bancaires, les crédits, les virements nationaux et internationaux ainsi que les transferts d'argent, et une banque digitale.

La Banque Postale du Congo c'est :

- Créer des produits et services pour répondre à vos attentes ;
- Proposer des conditions tarifaires compétitives et attractives ;
- Un réseau de plus en plus dense ;
- Plus de 70 000 clients en huit ans d'activité ;
- Des partenaires nationaux et internationaux ;

Un personnel jeune, qualifié, disponible et à l'écoute avec une parité homme/femme respectée.

Le Port Autonome de Pointe-Noire (PAPN), principal port en eaux profondes d'Afrique centrale, est une infrastructure stratégique pour le Congo. C'est un établissement public à caractère industriel et commercial, doté de la personnalité civile et l'autonomie financière et de gestion créé par l'ordonnance n°2-2000 du 16 février 2020.

Le port autonome de Pointe-Noire, dans la limite de leur circonscription territoriale, est chargé de :

- Gérer le domaine mobilier et immobilier du port ;
- Exploiter, dans les meilleures conditions de sécurité et d'accessibilité toutes activités portuaires et maritimes sur son domaine ;
- Assurer la maintenance, la police, le gardiennage et l'exploitation du port ;
- Etudier et réaliser les travaux portuaires ;
- Créer et aménager les zones industrialo-portuaires ;
- Assurer les prestations de remorquage, de lamanage, de pilotage et autres services aux navires et aux tiers ;
- Offrir, dans les conditions normales de coûts et de compétitivité, des prestations complémentaires liées aux activités portuaires nécessaires à la satisfaction des besoins des usagers.

Serfin SA est un acteur de l'écosystème financier du Congo, spécialiste du transfert d'argent, du change et des cartes prépayées, créé en 2011. Il dispose de 16 Agences en République du Congo où effectuent des transactions de change et des transferts d'argent via Western Union Ria Transfert ou MoneyGram.

RAWBANK est une banque commerciale de la République démocratique du Congo, qui occupe une place significative dans le secteur bancaire congolais par son total actif, son total des dépôts et son total des crédits. Elle a été créée en 2002 et a son siège social à Kinshasa. La banque offre des services bancaires à la clientèle de détail et aux entreprises (Corporate, PME). Elle offre des services bancaires par internet (online banking). RAWBANK a créé avec des banques présentes en RDC (Equity Bank Congo, BCDC, FBN Bank RDC), un réseau monétique interbancaire (interswitch bancaire), permettant aux clients en RDC d'utiliser leurs cartes privatives sur les distributeurs automatiques des banques membres du réseau Multipay.

Le forum numérique Congo est un évènement pensé et conçu par monsieur Eugène Rufin BOUYA, Directeur Général du Guichet Unique des Opérations Transfrontalières (GUOT), dans la perspective de contribuer à enrichir la réflexion sur le rôle et la place du numérique dans le développement socio-économique de la république du Congo.

C'est un évènement biannuel qui s'articule autour de 10 grandes sessions d'une heure chacune, pilotée par un modérateur. Chaque session laisse libre cours à l'expression de quatre intervenants de profils variés (professeurs, docteurs, ingénieurs, juristes, économistes, praticiens…), parmi les plus grosses pointures de l'industrie des TIC et du Numérique, exposer leur point de vue et interagir avec le public.

ENCO est une entreprise de taille humaine fondée en 2009 au Congo et exerçant dans le secteur de l'Energie qui propose des solutions variées pour les Entreprises et les Particuliers ou toutes formes d'organisations. Spécialiste dans les domaines de l'Energie (Réseaux d'énergie Moyenne Tension et Basse Tension, Éclairage Public, Feux tricolores, Électricité Générale (tertiaire et industriel, Poste de Transformation, Groupe Électrogène, Onduleur), et de l'Hydraulique (Réseaux d'adduction d'eau, Station de traitement des eaux). ENCO opère aussi dans les domaines de la Climatisation, Plomberie, courants faibles et détection incendie, Télécommunications.

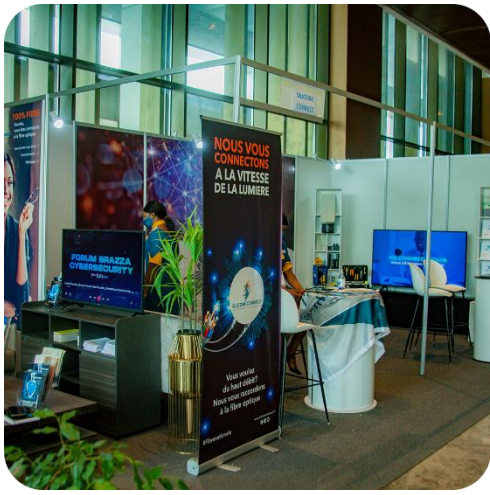
DigiPay est une entreprise qui ambitionne de révolutionner le transfert d'argent au Congo. Il s'agit d'une plateforme de transfert de fonds accessible à distance et en physique. Le principe repose sur un service de transfert dématérialisé le « DigiTranfer ». DigiPay propose à la clientèle congolaise de transférer de l'argent sur des comptes bancaires et mobiles partout dans le monde.

SNPC DISTRIBUTION

Créée en 2011, la SNPC Distribution est une des cinq filiales de la Holding SNPC. Elle est le dernier maillon de la chaine de services pétroliers, faisant d'elle le premier contact avec le consommateur final. En effet, la SNPC D est un acteur majeur dans la réussite des activités de la société nationale des pétroles du Congo, tel que le transport ou la distribution des produits pétroliers.

Ainsi la SNPC Distribution:

- Procède à la distribution des produits blancs sur l'étendue du territoire congolais ;
- Constitue les stocks stratégiques et de sécurité ;
- Commercialise les produits pétroliers ;
- Construit, développe et exploite des dépôts d'hydrocarbures ;
- Acquiert, installe et exploite des pipelines.



Nos Partenaires

XII. Nos partenaires

EDITION 2021