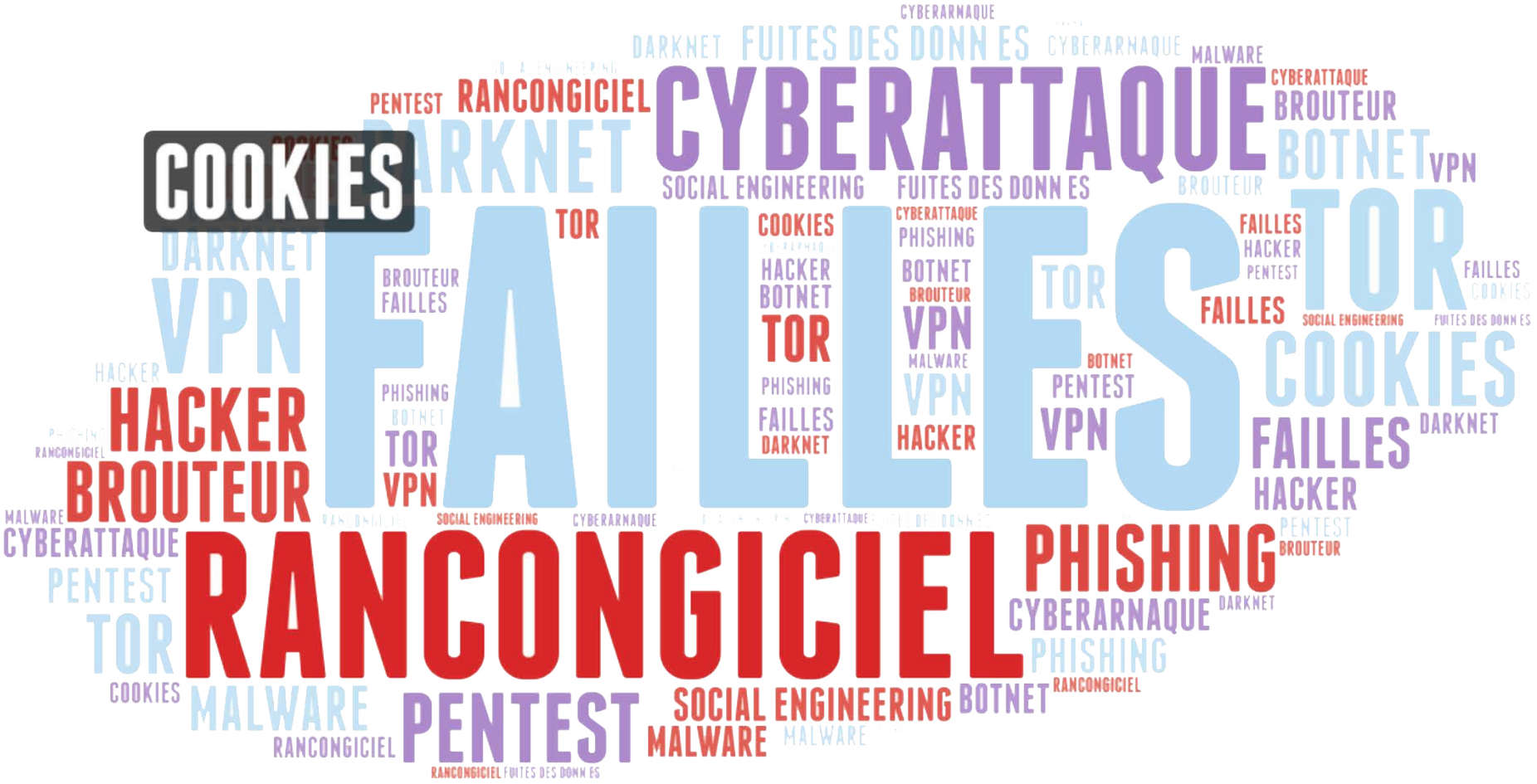
DÉFIS ET ENJEUX DE LA CYBERSÉCURITÉ

Il est temps d’ouvrir les yeux !

Guy Germain **MBAKI**

- Spécialiste en **Cybersécurité**
- Breveté du Collège des Hautes Etudes de Stratégie et de Défense
- Co-rédacteur de la Première Stratégie Nationale de Cybersécurité de la RD Congo
- Conférencier et formateur : Parle de Cybersécurité, de Cybercriminalité, de Cyberespace, de Cyberdéfense, de Cyberstratégie et de Cyberconflictualité
- Consultant Pentester - Hacker Éthique
- Enseignant-Expert à l'Université Protestante au Congo (Cybersécurité)
- Membre de Droit-Numérique.cd
- Certifié : CEH Master, CEH Practical, CEH, ESCA, CNDA, ISO 27001 LI, CSCU

NUAGES DE MOTS.



Pour les Etats

La cybersécurité, c'est la capacité d'un pays à protéger ses institutions, ses infrastructures essentielles et ses citoyens contre les menaces et attaques venues du cyberspace.

Pour les **entreprises**

La cybersécurité, c'est l'ensemble des moyens humains, organisationnels et technologiques et juridiques mis en place pour protéger les données et systèmes d'information, en garantissant leur confidentialité (protéger l'accès), leur intégrité (éviter les altérations) et leur disponibilité (assurer leur accès en continu).

Sommaire - Exécutif

- La cybersécurité : un facteur indispensable pour la réussite de toute transformation numérique durable des organisations...
- Une révolution numérique qui expose les organisations aux risque de cybersécurité...
- La Cybersécurité doit donc impérativement accompagner la transformation digitale dans une optique «secure by design», c'est-à-dire dès le développement initial de nouveaux produits et services.
- D'où la nécessité de la présentation sur les enjeux et les défis de la cybersécurité

Les principaux **enseignements**

- L’importance de la cybersécurité commence à être reconnue, mais...
- La responsabilité en matière de cybersécurité est encore attribuée au personnel technique

- Une stratégie de gestion des risques pas toujours adaptée au contexte de l’entreprise
- La gestion des incidents de cybersécurité n’est pas encore maîtrisée

- Le facteur humain est identifié comme une lacune importante liée aux cyber risques

Les actions à mener par le **Gouvernement**, par les **organisations** et par les **citoyens**

- L'implication effective des autorités politiques, de la Direction Générale et du Conseil d'Administration
- La gestion effective des risques et cyber menaces, tant au niveau national qu'au niveau des organisations
- La mise en place d'une stratégie cyber efficace et optimisée adaptée au spécificités locales
- Un programme efficace de cyber résilience au niveau national avec une déclinaison au niveau des organisations
- La prise en compte du facteur humain comme élément clé du dispositif de cybersécurité

Sommaire

Introduction

L’Afrique et la RD Congo face à la cybercriminalité

Importance de la cybersécurité

- La cybercriminalité représente la « plus grande menace pour chaque profession, chaque secteur, chaque entreprise du monde », déclarait Ginni Rometty, CEO d'IBM en 2015 à l'occasion d'un Forum économique mondial (WEF). Une prédiction qui s'est confirmée, au regard du nombre sans cesse croissant des cyberattaques déclarées en Afrique.
- Cette situation est favorisée par l'essor de la technologie et le boom numérique, mais également par la faiblesse d'une stratégie globale incluant les infrastructures de sécurité adéquates, le développement d'un personnel qualifié et la mise en place d'un cadre légal et réglementaire. S'il est vrai que nous avons vu émerger des initiatives pour adresser la plupart des problématiques suscitées, il est important de reconnaître malheureusement que les actions entreprises restent isolées, à l'heure où des actions coordonnées entre tous les acteurs de la société, aideraient à une meilleure prise en charge des menaces cyber.

Quelques chiffres sur la cybersécurité en Afrique

- “A l'échelle du Continent, le coût des cybercrimes est estimé à 1,37 milliard d'euros pour une population globale connectée à 23%.” Source www.afrique.latribune.fr (Par Mounir El Figuigui)

- Au cours des deux dernières années, une dizaine de pays africains ont adopté ou ont entamé un processus visant à adopter une nouvelle législation en matière de cybersécurité. - - RAPPORT INTERPOL DE 2024 SUR L’ÉVALUATION DES CYBERMENACES EN AFRIQUE

- Entre 2019 et 2022, plus de 160 millions de personnes en Afrique ont eu un accès régulier à Internet. Plus de 650 millions d'Africains utilisent leur téléphone mobile comme principal moyen d'accès à Internet. - - RAPPORT INTERPOL DE 2024 SUR L’ÉVALUATION DES CYBERMENACES EN AFRIQUE

Quelques chiffres sur la cybersécurité en Afrique –Suite

- D’après l’entreprise de cybersécurité Chainalysis, les paiements de rançon dans le cadre de ces attaques s’élevaient à plus de 1 milliard d’USD dans le monde en 2023 - RAPPORT INTERPOL DE 2024 SUR L’ÉVALUATION DES CYBERMENACES EN AFRIQUE
- “Chez Visa Afrique de l'ouest et Afrique centrale, chaque attaque coûte en moyenne 1,2 million de dollars US, notamment en perte de revenus.” Source www.afrique.latribune.fr (Par Mounir El Figuigui)
- 2020 Vol des données chez Bolloré Transport & Logistics République Démocratique du Congo (RDC) à travers le ransomware Net Walker avec menace de publication d’informations confidentielles. Source: lemondeinformatique.fr

Les enjeux

L’importance de la cybersécurité ne fait pas encore l’unanimité

“Les pirates informatiques ou les cyber-mercenaires n’ont pas nécessairement des motivations monétaires comme la cybercriminalité traditionnelle. Ils volent plutôt des données privées pour les monétiser d’une autre manière – généralement dans le but de fournir des conseils ou des informations, sur la base des données, afin de partager la valeur d’un avantage concurrentiel.”

– Kaspersky

La cybersécurité: un sujet prioritaire pour États, les entreprises et les citoyens ? - Rapport: PWC

- 56% : La plupart des entreprises reconnaissent que la cybersécurité est un sujet prioritaire ayant un impact considérable sur la politique commerciale et l'image de marque de l'entreprise. Toutefois, un pourcentage important d'entreprises considère encore qu'il s'agit d'un sujet important mais pas prioritaire.
- Seuls 29% des institutions publiques estiment la cybersécurité prioritaire. Malgré quelques lois et stratégies nationales, les actions restent fragmentées et tardives face aux menaces croissantes. Les États peinent à considérer la cybersécurité comme un pilier de souveraineté, ce qui fragilise la protection des infrastructures critiques.
- Les citoyens, de plus en plus connectés, restent vulnérables aux fraudes et vols de données. La sensibilisation et la formation à la sécurité numérique demeurent insuffisantes, ce qui réduit la conscience des risques liés aux usages quotidiens. Beaucoup considèrent encore la cybersécurité comme secondaire, exposant ainsi la société à des menaces persistantes.

Des considérations différentes selon les secteurs d'activité

- Rapport: PWC

- La majorité des entreprises du secteur financier reconnaît que la cybersécurité est d'une importance capitale. Toutefois, certains secteurs d'activité notamment le secteur public, le gouvernement et le marché de consommation semblent moins concernés par la cybersécurité. Ceci dénote d'un manque de maturité dans ces secteurs d'activité et pose le problème de la gestion des risques cyber émanant des tiers, compte tenu de l'interconnexion qui pourrait exister entre les différents secteurs d'activité. D'autre part, le faible niveau de maturité des uns peut mettre tout l'écosystème à risque.

  – **72%** Secteur financier
  – **65%** Technologie, médias et télécommunications
  – **29%** Gouvernement et secteur public
  – etc…

Les Gouvernements et les institutions publiques ne sont pas toujours en avant garde

- Seuls 29% des répondants des institutions publiques interrogés pensent que la cybersécurité est un sujet prioritaire pour leur institutions.

- **Le rôle des gouvernement et des institutions publiques face à la cybersécurité.**
  Face à la cybersécurité, les Gouvernements ont une double responsabilité : celle de se protéger en tant qu'Institution et celle de mettre en place un cadre nécessaire pour la protection des organisations, des personnes et des infrastructures publiques

- **La cybersécurité: une importance mitigée pour les gouvernements et institutions publiques**
  Au sein des pays de l'Afrique francophone sub-saharienne, nous notons sur le plan législatif la mise en place des instruments de régulation de la cybersécurité. Mais beaucoup reste encore à faire…

Les stratégies

Les programmes de gestion des risques et des menaces cyber sont quasi absents

Stratégie pour les **Gouvernements**

- Une bonne stratégie nationale de cybersécurité doit être alignée sur les priorités de développement et de sécurité nationale afin de protéger les infrastructures critiques, gérer efficacement les risques, encadrer les ressources humaines et technologiques, et garantir la souveraineté numérique face aux menaces cyber.

Stratégie pour les **entreprises**

- Une bonne stratégie de cybersécurité doit être alignée sur la stratégie d'entreprise pour soutenir la croissance par la gestion efficace des risques, des ressources et de la gouvernance et pour faire face aux menaces cyber

La responsabilité en matière de cybersécurité : une perception à changer

- Nombreux sont ceux là qui estiment que la cybersécurité est de la responsabilité du personnel technique : Directeur informatique, Ingénieur informatique, RSSI. La responsabilité de la mise en place de la stratégie de cybersécurité n’est pas attribuée à la Direction Générale. Ceci dénote un réel besoin de sensibilisation et de formation du Top Management des entreprises

“La sécurité ne doit pas être une affaire de spécialiste, mais un nouveau paradigme commun. Cela passe avant tout par la sensibilisation des populations.”

– Mes libres pensées

La sensibilisation à la cybersécurité : une pratique pas encore maîtrisée ni systématisée

- Très peu d'entreprises disposent d'un programme de sensibilisation à la cybersécurité ou estiment que le programme de sensibilisation à la cybersécurité existant ne répond pas complètement aux besoins de l'entreprise en matière de cybersécurité

Les scénarios d’attaques sont illimités, avec pour seules limites l’imagination des Cybercriminels et la naïveté des victimes…

Les défis

Réponses de la RD Congo face à la cybercriminalité.

- L'enjeu de la numérisation en RD Congo

- La RDC connaît une numérisation accélérée, perçue comme un moteur de développement économique et social. Mais, cette numérisation se fait en silo sans stratégie globale et cela est porteuse de plusieurs risques.

- Le gouvernement congolais a une volonté politique de transformation numérique. Cela se manifeste avec la création du Ministère de l'Economie Numérique.

Le Cyberespace congolais - Couche physique

- Cette couche regroupe les éléments matériels et les infrastructures de base du cyberespace.

- Câbles sous-marins (2Africa à Moanda), centres de données de pointe et déploiement de 38 000 km de fibre optique, Datacenters des entreprises (Banques, Télécoms). Même nos smartphones permettent l'extension du Cyberspace congolais…

- Ces investissements massifs dans l'infrastructure physique, bien que capital pour le développement, augmentent la surface d'attaque potentielle de la RD Congo.

Le Cyberespace Congolais - Couche logicielle

- Couche immatérielle composée des applications, logiciels, codes et protocoles

- Plateformes gouvernementales (Passeports, eVISA, Impôts - DGI, DGRA - LOGIRAD etc…)

- La dépendance aux systèmes logiciels peut rendre la RDC vulnérable. Une faille dans cette couche peut avoir des conséquences en cascade sur la sécurité nationale.

Le Cyberespace Congolais - Couche informationnelle - sémantique - cognitive

- La couche la plus intangible, incluant les utilisateurs, les informations, les réseaux sociaux et les échanges en temps réel.

- Des millions d'utilisateurs congolais sur Facebook, TikTok, Instagram, LinkedIn, X etc…

- L'utilisation massive des réseaux sociaux crée un terrain propice à la désinformation, à la confusion et à la cybercriminalité (arnaques, sextorsion, etc.), impactant directement les forces armées, les décideurs politiques, les citoyens et la stabilité sociale.

Guerre de l'information mène le Rwanda contre la RD Congo

Définition des infrastructures critiques

- **Opérateurs d'Importance Vitale (OIV)** sont des entités, publiques ou privées, dont l'activité est jugée essentielle au fonctionnement de la nation et à sa sécurité. Les OIV sont responsables des infrastructures critiques.
- **Qu'est-ce qu'une Infrastructure Critique (IC)?** Ce sont des infrastructures vitales pour des fonctions sociales essentielles, dont la défaillance aurait de graves conséquences sur la population, l'économie et les institutions.
- **Adaptation au contexte de la RDC** étant donné que la nature des IC varie selon le niveau de développement et le contexte d'un pays. La RDC doit donc identifier ses propres actifs vitaux.

Identification des Infrastructures Numériques Critiques (INC) en RDC

- **Communications** : Réseaux de télécommunications (fixe, mobile, 5G, IoT), câbles sous-marins (2Africa), stations satellites et projets de 38 000 km de fibre optique.
- **Énergie** : Centrales INGA, réseaux de distribution, et projets transfrontaliers (ligne électrique Angola-RDC).
- **Services financiers** : Banques, systèmes de paiement et plateformes financières numériques.
- **Eau** : Infrastructures d'approvisionnement et de traitement. Regidéso
- **Mines** : Mines et raffineries de minerais stratégiques (cobalt, lithium, coltan) en raison de leur importance économique et de leur impact sur la chaîne d'approvisionnement numérique mondiale.
- **Transports et logistique** : Aviation, chemins de fer, routes et systèmes maritimes. Cfr. OGEFREM

Le cadre stratégique et légal de la RD Congo

Stratégie Nationale de Cybersécurité 2022-2025

- Vise à rendre la RDC sécurisée et résiliente d'ici 2025
- S'appuie sur une approche basée sur les risques et la coopération nationale/internationale.

Législation :

- L'Ordonnance n°87-243 du 22 juillet 1987 portant réglementation de l'activité informatique au Zaïre. L'article 9 de cette Ordonnance stipule que: « Tout acte accompli à l'occasion d'une application informatique et qui porte atteinte à la sécurité de l'Etat, à l'ordre public ou aux bonnes mœurs, est punissable conformément aux lois en vigueur ».
- Loi n°20/017 du 25 novembre 2020 sur les Télécommunications
- Ordonnance Loi No. 23/010 du 13 mars 2023 portant code du numérique

Acteurs institutionnels clés

L'Agence Nationale de Cybersécurité (ANCy) - Prévue par le Code du numérique et par la Stratégie Nationale de Cybersécurité mais pas toujours créee

- **Rôle** : Organe de gouvernance central et de régulation, chargé de piloter la SNCS et la réglementation.
- **Missions** : Prévention, protection des données et des INC, gestion des risques et des crises cyber, développement des capacités et mise en place d'un Centre Opérationnel de Sécurité (SOC).

Le Conseil National de Cyberdéfense (CNC)

- **Rôle :** Créé en août 2023 pour renforcer la sécurité numérique avec une vision d’une coordination inter-entités dans la cyberdéfense et le cyber-renseignement.
- **Missions :** Protection des infrastructures critiques (Cfr. OIV), Améliorer la préparation face aux attaques cybernétiques.

Piliers de la protection des infrastructures numérique critique en RDC

- Nomination des répondants cyber dans tous les OIV comme interfaces entre les OIV et les entités en charge de la cybersécurité
- Utilisation de l'expertise du secteur privé dans un partenariat Public-Privé
- Investir massivement dans l'éducation et la formation pour combler le déficit de compétences.
- Programmes de sensibilisation (ANCy), formations spécialisées, et intégration de la cybersécurité dans les cursus universitaires pour favoriser le développement des Compétences

Recommandations et perspectives d'avenir

- Opérationnaliser rapidement l'ANCy et le CNC.
- Développer des réglementations sectorielles adaptées aux particularités de l'énergie, des mines et des télécommunications.
- Établir un Plan National de Réponse aux Incidents Cyber (PNRIC) .
- Investir massivement dans l'éducation et la formation pour combler le déficit de compétences.
- Promouvoir la souveraineté numérique par un contrôle national renforcé et le développement de produits "Made in DRC".
- Adopter une approche proactive de cyber-résilience, en intégrant la sécurité dès la conception des infrastructures numériques, plutôt que comme une réflexion après-coup.

Ce que je **pense…**

“Et donc comme on ne peut pas envisager une transformation numérique sans aborder les enjeux liés à la cybersécurité et la lutte contre la cybercriminalité, le modèle congolais(africain) de cybersécurité doit être le résultat d’une succession de choix politiques ambitieux issus d’une prise de conscience: la transformation numérique de la société, de l’économie et de l’action publique devra se faire en confiance et en sécurité, ou elle ne se fera pas.”

QUESTIONS

Merci !