LA STRATEGIE AFRICAINE DE LA SECURISATION DES DONNÉES NUMÉRIQUES.

INTRODUCTION.

Le Pétrole croit de manière exponentielle. Les données sont au cœur du modèle économique. Disposer des données numériques permettraient à l'Afrique d'être plus autonome au niveau du développement. De l'individu jusqu'à l'État en passant par les entreprises, nous devons tous apprendre à analyser des données économique. La souveraineté numérique est une obligation pour les États Africains. Nous restons dans une logique ou une donnée renseigne sur autrui. Nous ne faisons pas de l'illusionnisme, nous cherchons juste à préserver l'identité de nos populations et du fruit de leur travail. L'Afrique de 2030 et de 2063 sera une Afrique numérique. La nécessité de penser au fondement et aux piliers d'une Afrique autonome.

Parmi les plus marquantes au niveau mondial, il y a la cyberattaque de SolarWinds qui a visé près de 18 000 entreprises et agences gouvernementales aux États-Unis en 2020. Début 2021, ce sont différents hôpitaux (français) que les hackers ont pris pour cible, mais aussi certains laboratoires médicaux, mettant ainsi la main sur les données de 500 000 patients. La force des pirates informatiques est de réinventer sans cesse leurs modes opératoires et les technologies utilisées, comme le montrent les principales menaces pour 2021.

Comment décider ? Quoi décider ? Quel est l'état actuel de notre cyberespace continental ? Quelles sont les méthodes que nous pouvons déjà appliquer ? Après avoir fait un rappel des définition de cyberattaque et des évènements troublants qui ont marqué le cyberespace mondial, nous verrons pendant cette études les forces et faiblesses de notre continent et proposerons des axes de solutions efficaces.

I- CADRE GÉNÉRAL.

Une des premières formes d'exercice du cyberpouvoir passe par ce que l'on qualifie de cyberattaques (aussi désignées par le terme «attaques informatiques»). De façon générale, les cyberattaques sont caractérisées par une utilisation d'outils ou des technologies afin de perturber, saboter, intercepter, détruire ou encore modifier des données informatisées ou des systèmes électroniques ou matériels présents dans le cyberespace. Les cyberattaques peuvent toucher toutes les sphères d'activité et peuvent être déployées par la grande majorité des acteurs en présence, contrairement aux attaques armées classiques. Un individu peut donc cibler un État, un État peut cibler une entreprise privée et ainsi de suite. Actuellement, une attaque se produit toutes les 39 secondes dans le monde. La numérisation du monde induit logiquement celle de la sécurité, mais cette « technologisation de la sécurité » dissimule d'autres réalités sous-jacentes qui peuvent remettre en cause les fondements des pratiques et des compétences régaliennes dans un État de droit. Car en même temps que la technologie offre de nouveaux outils utiles à la réalisation des missions de prévention ou de répression, on oublie souvent qu'elle produit elle-même sa propre insécurité et qu'elle transforme le cadre de mise en œuvre des missions de sécurité, au risque notamment de brouiller les distinctions essentielles que l'État de droit impose entre les pratiques préventives, y compris privées, et l'action publique garante de la sécurité collective des personnes et des biens.

La technologie produit sa propre insécurité : Il y a plus de trente ans Yves Lasfargues nous prévenait que nous étions « [passés de la] civilisation de la peine à la civilisation de la panne ». À la même époque, Ulrich Beck publiait son ouvrage fameux sur la « société du risque » La fragilité intrinsèque des systèmes numériques Les dernières décennies ont donné raison à ces avertissements que d'aucuns ont sous-estimés sur le moment, les estimant trop alarmistes. Plusieurs cas d'attaques informatiques spectaculaires (notamment contre l'Estonie en 2007, contre la chaîne francophone TV5 Monde en 2015 ou encore la diffusion des virus **WannaCry** et **NotPetya** en 2017) ont, en effet, démontré la vulnérabilité de nos infrastructures numériques face à des actions cyber-malveillantes de grande ampleur. Mais ces menaces en provenance du cyberespace ne sont pas seulement dues au développement (par ailleurs attesté) d'une nouvelle et très impénétrable forme de criminalité globalisée. Elles se traduisent aussi par un risque réel de perturbation, voire d'indisponibilité plus ou moins permanente des nouveaux outils

technologiques dont l'État et ses services les plus régaliens (police, gendarmerie, justice, forces armées) usent pour remplir leurs missions de prévention et de répression. La raison en est simple : même les États disposant d'un écosystème industriel et technologique national sont obligés de recourir pour l'essentiel de leurs infrastructures et de leurs outils numériques à des technologies du marché (qu'il s'agisse de postes de travail, de logiciels standards, de routeurs IP, de messageries électroniques, ou de communications mobiles – y compris la très prochaine.

CAS WANNACRY :

WannaCry, aussi connu sous le nom WannaCrypt est un logiciel malveillant de type rançongiciel auto-répliquant. En mai 2017, il est utilisé lors d'une cyberattaque mondiale massive, touchant plus de 300 000 ordinateurs , dans plus de 150 pays, principalement en Inde, aux États-Unis et en Russie et utilisant le système obsolète Windows XP12 et plus généralement toutes les versions antérieures à Windows 10 n'ayant pas effectué les mises à jour de sécurité, en particulier celle du 14 mars 2017 (bulletin de sécurité MS17-010). Parmi les plus importantes organisations touchées par cette attaque, on retrouve notamment les entreprises Vodafone, FedEx, Renault, Telefónica, le National Health Service, le Centre hospitalier universitaire de Liège, le ministère de l'Intérieur russe ou encore la Deutsche Bahn. La BBC affirme que ce virus serait l'expression d'un mécontentement envers la politique de Donald Trump .

CAS NOTPETYA :

Le 27 juin 2017, une nouvelle vague massive de cyberattaques mondiales « rappelant le mode d'action du virus WannaCry survenu le week-end du 12 au 13 mai 2017 » affecte des centaines de milliers d'ordinateurs du monde entier. Les entreprises touchées par NotPetya simultanément sont :

- *des entreprises majeures et des grandes banques en* Ukraine ; plusieurs grandes entreprises comme Mars ou Nivea (en Allemagne) ; le métro de Kiev indiquait « ne pas pouvoir accepter de paiements en carte bancaire à ses guichets à cause d'une cyberattaque » sur sa page Facebook.

- *la firme de publicité britannique WPP* a déclaré que ses systèmes informatiques avaient également été touchés. Le site de la firme indiquait que des opérations de maintenance étaient en cours sur le site, mais il s'agissait de la cyberattaque.

- *une grande entreprise d'expédition néerlandaise* a confirmé que ses appareils informatiques étaient en panne.

- *l'entreprise danoise Maersk,* de transport et de logistique a annoncé la perte de 300 millions de dollars de perte d'activité5 et la fermeture de plusieurs sites suite à la cyberattaque.

- *le géant pétrolier russe Rosneft* a déclaré que ses serveurs avaient subi une cyberattaque caractérisée comme puissante, mais il a pu passer sur un serveur de secours.

- aux États-Unis, *le laboratoire pharmaceutique américain Merck* a été touché, estimant ses pertes à 870 millions de dollars.

- *la firme Mondelēz International,* qui gère la marque française de biscuiterie LU, a également été touchée, estimant ses pertes à 188 millions de dollars6 ;

- En *Europe, TNT Express, filiale de FedEx,* déclare avoir perdu 400 millions de dollars à la suite de l'attaque.

- la *centrale nucléaire de Tchernobyl* a également été touchée par le virus, et les mesures de la radioactivité ne sont plus suivies informatiquement, mais manuellement, par les techniciens avec des compteurs Geiger.

- *l'entreprise française spécialisée dans la construction de bâtiments Saint-Gobain* a été touchée par le virus, affirmant avoir essuyé des pertes de 384 millions de dollars.

- *l'enseigne de grande distribution française Auchan* a également été touchée via sa filiale ukrainienne mais les magasins français n'ont pas été affectés.

- *la SNCF a également été affectée par le virus,* mais ce dernier a été contenu. Il n'y a eu aucune perturbation sur le réseau.

II- CADRE AFRICAIN.

Les logiciels espions et les cyberattaques ont explosé ses dernières années (2020/2021) en période de crise COVID-19. Le Kenya , le Nigéria et l'Afrique du Sud ont enregistré des millions de logiciels malveillants et d'autres attaques selon les données de la société cybersecurité Kapersky. Les applications potentiellement indésirables (graywares) sont des programmes préinstallés sur les téléphones et ordinateurs, qui peuvent présenter des risques pour la sécurité et la confidentialité de nos pays. Ces logiciels malveillants comprennent des logiciels espions, virus , conçus pour causer des dommages. Dans certains pays, ces attaques ont pris une nouvelle dimension, se faisant passer pour des organisations non gouvernementales travaillant sur des questions du COVID-19 disait Verengai Mabika[1] de l'Internet Security. En Afrique du Sud, il y a eu près de 10 millions d'attaques de logiciels malveillants et 43 millions de détections d'applications indésirables[2]. Les Kenyans eux ont été confrontés à environ 14 millions de logiciels malveillants et 41 millions d'apparitions d'applications indésirables[3]. Les cyberattaques sont les causes principales de violations des secrets de sécurité national , vol de données précieuses (économiques, médicales , scolaires , projet de société) , de paralysie des réseaux informatiques aussi. Le groupe cybercriminel dénommé « **Silence** » travaille communément afin d'infiltrer les systèmes les mieux sécurisés, sans que l'institution ne puisse s'en rendre compte. Le mode opératoire est simple. Ils utilisent l'envoi d'email de phishing. L'email de phishing que le groupe « silence » envoie aux boites mails des institutions bancaires contient des logiciels malveillants qui s'installent dans le système de sécurité, une fois l'email ouvert.[4] Les banques africaines aussi sont vulnérables face aux cybercriminels. Une étude publiée par Dataproject, une entreprise marocaine spécialisée dans la cyberdéfense, et conduite auprès de 148 banques dans la zone UEMOA et dans trois pays d'Afrique centrale, révèle que 85% des banques ont déjà été victime d'une ou de plusieurs cyberattaques. Ces attaques représentent pour un tiers, des fraudes sur les cartes bancaires, un autre tiers du phishing et du « **core banking** » (intrusions dans les systèmes d'information pour rançongiciels ou infection virales) dans 24% des cas. Les derniers pourcentages regroupent des fuites d'information (**leaks**) , l'usurpation d'identité, les fraudes pour transfert d'argent ou le retrait des faux chèques. En 2018, NSIA Banque Côte d'Ivoire avait reconnu d'importants dégâts à la suite d'un détournement de fonds par piratage informatique.

[1] Conseiller politique principal pour l'Afrique auprès de l'Organisation à but non lucratif (Internet Security).
[2] KAPERSKY
[3] KAPERSKY
[4] AFRICA CYBER SECURITY MAGAZINE

La banque avait perdu près de 1,2 milliard FCFA. En 2019, ECOBANK Sénégal a déclaré s'être fait soutirer frauduleusement 323 millions de FCFA. En Février 202, la Banque de l'Habitat du Sénégal a déclaré avoir été piratée par des Nigérians qui ont empoché des centaines de millions de dollars[5].

[5] Franck Kié, dans FINANCIAL AFRIK

ETAT DES LIEUX DE LA PROTECTION DU CYBERESPACE AFRICAIN.[6]

PAYS	CRITÈRES DE D'APPRÉCIATIONS						
	1	2	3	4	5	6	7
BENIN							
BURKINA FASO							
BURUNDI							
CAMEROUN							
CÔTE D'IVOIRE							
COMORES							
CONGO RDC							
DJIBOUTI							
ETHIOPIE							
GABON							
GHANA							
GUINÉE							
KENYA							
MADAGASCAR							
MAURITANIE							

[6] CYBERSECURITYMAG / METEO DU JOUR.

MALI							
MAROC							
NAMIBIE							
NIGER							
NIGERIA							
OUGANDA							
RWANDA							
SENEGAL							

 SATISFAISANT PEUT MIEUX FAIRE RESTE À FAIRE RIEN N'EST FAIT

CRITÈRES D'APPRECIATIONS

1- Existence d'un document de la stratégie nationale ou régionale de la cybersécurité.
2- Existence d'un cadre règlementaire des communications électroniques.
3- Existence de services ou organismes étatiques pour accompagner en cas d'incidents (CERT,CNIL).
4- Existence d'une agence ou institution étatique dédiée aux questions de sécurité des systèmes d'information (exemple : ANSSI).
5- Adhérence à CERT Africa.
6- Existences de structures pour le développement des compétences locales en expertise cybersécurité
7- Accompagnement et sensibilisation adaptés de la population.

RECAPITULATIF DES DIFFICULTÉS AFRICAINES.

- Les menaces sont grandissantes et la cybercriminalité se banalise et se complexifie. Ces dangers proviennent principalement de pays situés au-delà des rives de l'Afrique. En raison de l'insuffisance des financements et de la sensibilisation, la plupart des pays africains n'ont pas été à même de mettre en place les mesures ou les institutions nécessaires à la sécurité et à la protection des utilisateurs du cyberespace. Une autre difficulté concerne les instances judiciaires chargées de juger les cybercriminels identifiés: la plupart des pays africains manquent de ressources et de compétences pour entreprendre des poursuites judiciaires contre les présumés cybercriminels opérant au-delà de leurs rives.

- Les activités de recherche et de développement sont très limitées dans le domaine de la cyber sécurité en Afrique.

- La compréhension et l'application des lois et des réglementations restent insuffisantes pour la protection de l'information et des données et la sécurité des données.

- Le régime de propriété intellectuelle est fragile, ce qui exerce un effet dissuasif sur l'innovation appliquée en Afrique aux instruments et technologies dédiés à l'instauration de la confiance et à la sécurisation des utilisations de ressources informatiques.

RECOMMANDATIONS ET ORIENTATIONS.

- Veiller à assurer l'équilibre entre la protection des personnes et la protection des TIC, de l'accès à l'Internet et des services de l'Internet pour l'ensemble de la société.

- Accorder un degré de priorité élevé à la cybersécurité dans les programmes africains.

- Encourager les gouvernements à élaborer et mettre en place des mécanismes susceptibles d'améliorer la cybersécurité lors de l'utilisation de l'Internet et des portails informatiques permettant le partage de données personnelles.

- Encourager les organisations internationales et les partenaires de développement à aider les pays africains à concevoir de robustes infrastructures sur la cybersécurité.

- Harmoniser les lois sur la cybersécurité parmi les pays, notamment dans le domaine de la protection des données personnelles, dans le cadre de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel.

- Veiller à ce que la sécurité ne se limite pas à la sécurisation des réseaux contre les attaques et à la protection des données personnelles contre les hackers, mais inclue également des règles contraignantes interdisant aux serveurs d'utiliser ou de partager les données stockées dans leurs centres ou dans des infrastructures nationales, régionales et continentales.

- Encourager la répétition des pratiques exemplaires qui règlent les problèmes posés par la cybersécurité.

- Inviter les gouvernements à transposer la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel dans leurs lois nationales.

- Veiller à la création d'équipes opérationnelles chargées des urgences informatiques à l'échelle nationale et sous régionale et coordonner les efforts déployés contre la cybercriminalité.

- La sensibilisation envers la population de l'importance de la cybersécurité.

- Nous devons d'abord jouer à plein notre rôle d'éclaireur des transformations numériques. Dans ce contexte d'accélération technologique et dans la continuité de la création d'un conseil scientifique, il s'agit de renforcer notre capacité à anticiper les ruptures technologiques et les révolutions d'usages, à discerner les signaux faibles, annonciateurs des mutations profondes pour le monde numérique. Nous devons pouvoir accompagner ces transformations, en acquérant les compétences nécessaires pour toujours mieux

éclairer notre écosystème et les politiques publiques numériques. Nous devons également davantage développer notre vision stratégique de ces défis numériques, en consacrant le temps nécessaire à l'élaboration de cette vision et en diffusant au sein de l'Agence une culture de la mise en perspective.

- Nous devons sans cesse renforcer notre efficacité opérationnelle face à des menaces profondément changeantes, notamment face à la recrudescence des menaces de masse. Il y a là une responsabilité importante, mais aussi une grande opportunité de renforcer notre capacité à détecter et répondre aux attaques. Pour cela, nous devons être en mesure de faire fructifier cette donnée pour renforcer la cybersécurité d'aujourd'hui et inventer les moyens de la cybersécurité de demain.

- Nous devons davantage mettre cette compétence au service de la formation en cybersécurité. Dans un contexte de compétition internationale acharnée sur les talents, nous devons renforcer notre engagement dans la formation initiale et continue pour intégrer plus avant ces thématiques dans les formations en informatique. Dans un monde où les compétences numériques deviennent des fondamentaux, la cybersécurité doit également être renforcée dans les enseignements scolaires, notamment pour susciter les vocations dès le plus jeune âge. Mise en place des structures capable de former des élites en cybersécurité.

- Nous devons également renforcer notre culture interne de l'expérimentation et amplifier notre capacité d'innovation. Nous devons nous donner la possibilité de pivoter et d'expérimenter dans un contexte profondément changeant et incertain, où les cycles d'innovation ne cessent de se raccourcir. Cela passera notamment par le lancement d'une démarche d'innovation et un accompagnement plus resserré des projets de cybersécurité, y compris d'éventuels projets entrepreneuriaux.

- La cybersécurité dans le secteur de la santé doit beaucoup s'améliorer, et les gouvernements et les établissements médicaux doivent davantage fournir des efforts et de ressources pour prévenir les cybermenaces dans le secteur de la santé, mais il faudra

continuer de sensibiliser le personnel aux risques et de protéger davantage les robots médicaux.

- Les Cyberassurances : En raison de la menace croissante des cyberattaques, il sera essentiel pour les organisations de souscrire des polices d'assurance pour atténuer les risques financiers liés aux cyberattaques. Certaines entreprises aux États-Unis ont déjà la possibilité de souscrire des assurances contre les cyber-risques et les pays africains devraient rapidement leur emboîter le pas.

Conclusion. L'Afrique a de nombreux progrès à faire en matière de cybersécurité. S'il faut saluer les efforts de certains pays et remarquer les avancés notoires, il n'en demeure pas moins que d'autres traînent toujours les pas et peine à bouger pour multiples raisons. En accélérant l'adoption des outils digitaux et en modifiant les organisations, la sécurité des infrastructures numériques est devenue très complexe face un timide résultat de recherche empirique sur les sujets de cybersécurité en Afrique. Quatre axes[7] doivent être observés et développés à savoir :

- Connaissances de la sécurité et de la cybersécurité : entre regard ancien et perspectives nouvelles sur la sécurité ;
- Environnement socio-psychologique, économique de la cybersécurité ;
- Environnement juridique et politique de la cybersécurité ;
- Environnement technique de la cybersécurité

[7] Le Professeur Guy Nvelle de l'Université de Dschang au Cameroun, à proposer une réflexion sous forme de colloque pluridisciplinaire sur le thème : Cybercriminalité et cybersécurité au Cameroun et en Afrique : représentations, manifestations, financements & traitements des menaces qui se tiendra du 06 au 07 Mai 2021 au Palais des Congrès de Yaoundé au Cameroun sous la patronage du ministre d'état de l'enseignement supérieur et du Ministère des Postes et Télécommunications.

ANNEXE 1 : MATÉRIEL DE CYBERSÉCURITÉ HORIZON 2022.

Trustway Proteccio™ NetHSM[8]

Trustway Proteccio NetHSM est un module matériel de sécurité (Hardware Security Module – HSM) mettant à disposition des solutions logicielles dans un environnement performant et hautement sécurisé pour la réalisation de leurs opérations cryptographiques les plus sensibles. Une sécurité optimale requiert une variété de solutions de chiffrement. La gamme de produits Trustway Proteccio certifiée propose de multiples produits pour répondre à vos exigences cryptographiques.

ANNEXE 2 : **LISTE DES LOGICIELS MALVEILLANTS OU ESPIONS RECONNUES.**

- RANSOMWARE.
- BACKDOOR
- SPYWARE
- SCAREWARE
- ADWARE
- CHEVAL DE TROIE

8