SEPTEMBER 1, 2016

Cybersécurité, Cyber Défense et compétitive en Afrique

Notes : Intelligence Economique, Sécurité Economique et la Compétitivité des Entreprises en Afrique

AZIZ DA SILVA

Sommaire du Document

Introduction

Cybersécurité et Cyberdéfense : Des leviers de l'intelligence économique et comment ils peuvent devenir de redoutables armes de compétitivité dans la guerre économique que l'Afrique doit livrer ? Ma note de ce mois s'organisera autour de 7 parties :

- Partie 1 : Cybersécurité et Cyberdéfense : leviers de l'intelligence économique
- Partie 2 : La culture du risque numérique en Afrique
- Partie 3 : La Cybersurveillance des gouvernements africains
- Partie 4 : Que ce cache-t-il réellement derrière PRISM ?
- Partie 5 : Cartographie de la guerre économique en Afrique
- Partie 6 : Les acteurs de la guerre économique
- Partie 7 : Conclusion et perspectives

En 2013, le coût estimé de la cybercriminalité était de 26 milliards de FCFA (environ 23 millions d'euros) en Côte d'Ivoire, tandis qu'au Sénégal, il était d'environ 15 milliards de FCFA (22 millions d'euros).

Dans un rapport, la firme Kaspersky affirme que plus de 49 millions de cyberattaques ont eu lieu sur le continent au cours du premier trimestre de 2014, la plupart ayant eu pour théâtre l'Algérie, l'Egypte, l'Afrique du Sud et le Kenya.

Dans son Bulletin annuel de Statistiques globales pour 2015, Kaspersky met en évidence une nouvelle tendance : pour la première fois, les menaces financières mobiles se classent parmi les dix premiers programmes malveillants conçus pour voler de l'argent. Deux familles de chevaux de Troie bancaires mobiles - Faketoken et Marcher - ont été inclues dans le top 10 des chevaux de Troie bancaires en 2015. Une autre tendance remarquable et alarmante pour l'année est la propagation rapide de ransomware - rançongiciel. Kaspersky en a détecté dans 200 pays et territoires en 2015.

Le continent africain, qui connaît une explosion du marché de la bancarisation mobile, est particulièrement vulnérable à cette évolution.

Les revenus issus de la téléphonie mobile représentent **3,7% du PIB** sur le continent africain, soit le triple de ceux des économies développées.

Partie 1 : Cybersécurité et Cyberdéfense : leviers de l'intelligence économique

La numérisation de la société africaine s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu continental. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'état, les acteurs économiques et les citoyens.

Cybercriminalité, espionnage, propagande, sabotage ou exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective.

Le second pilier de l'intelligence économique est par définition la sécurité du patrimoine immatériel. Composante indispensable au développement. Le problème est que ce patrimoine est de plus en plus numérisé en Afrique comme partout dans le monde. A cela il faut rajouter le fait que la technologie est injectée à forte dose dans les entreprises pour améliorer la croissance et la compétitivité. Il y va de même pour les états.

Dans ce contexte, l'utilisation, l'accès et l'exploitation de la technologie est en forte croissance. Ce qui a pour implication d'exposer les données stratégiques. Il faut alors disposer de mécanismes efficaces pour protéger ce patrimoine.

« La Cybersécurité est la prévention des risques de sécurité et de sûreté liés à l'emploi des technologies de l'information. Elle est à ce titre un volet de « l'intelligence des risques » elle-même composante de l'intelligence économique. » Bernard Besson

De nouveaux crimes, risques, infractions et menaces sont apparus dans le cyberespace africain : utilisations criminelles d'internet (cybercriminalité), espionnage politique, économique et industrielle, attaques contre les infrastructures critiques de la finance, des transports, de l'énergie et des communications à des fins de spéculation, de sabotage et de terrorisme.

Emanant de groupes étatiques ou non-étatiques, les cyberattaques :

- N'ont aucune contrainte de distances, de frontières et même d'espaces
- Peuvent être complètement anonymes ;
- Ne nécessitent plus de couts et de moyens importants
- Peuvent présenter de très faibles risques pour l'attaquant.

De quoi parlons-nous ?

La cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment sur le réseau Internet. La cybercriminalité désigne à la fois :

- Les atteintes aux biens : fraude à la carte bleue sur Internet, vente d'objets volés ou contrefaits,

- Piratage d'ordinateur, vente de médicaments sans ordonnance, vente de stupéfiants… ;
- Les atteintes aux personnes : diffusion d'images pédophiles, injures à caractère racial, atteintes à La vie privée…
- Le Cyberespionnage et les activités militaires parrainés par des États
- L'utilisation d'Internet par les terroristes

Partie 2 : La culture du risque numérique en Afrique

La culture du risque numérique s'imposera aux managers africains. La numérisation des processus d'industrialisation, de production et de commercialisation est déjà une réalité pour nombre de secteurs d'activités africains. Qui misent sur les technologies de l'information pour accroître leur compétitivité, développer leurs réseaux de clientèle et monter en force dans la chaîne de création de valeur. C'est le visage positif de l'économie numérique. Les dirigeants africains qui se contenteraient de celle-ci hypothèquent l'avenir de leur organisation. Car aujourd'hui quelques minutes de navigation sur Internet permettent d'accéder à des offres de piratage de comptes de messagerie ou à des tutoriels très pédagogiques pour bloquer temporairement l'accès à un site Internet. Ces arsenaux numériques de proximité popularisent l'usage de ces modes d'agression sur la Toile. Les entreprises africaines et leurs dirigeants constituent des cibles privilégiées : l'ère de la communication les incite à ouvrir leurs agendas, les portes de leur société et une partie de leur vie professionnelle. C'est un matériau de premier choix pour conduire des opérations d'ingénierie sociale visant à réaliser de lucratives campagnes de pénétration de leurs systèmes d'Information. S'ils persistent à voir dans la thématique du numérique un simple appareillage technique et technologique sans en comprendre les enjeux stratégiques et les menaces qui y sont reliées, les dirigeants africains d'entreprise exposent leur patrimoine informationnel et leurs finances à toutes les convoitises. Il ne s'agit pas d'en faire des experts de la cybermenace mais bien de leur faire prendre conscience des dégâts pouvant être causés à partir d'une simple connexion à Internet. Cela fait partie intégrante de l'indispensable culture numérique de l'honnête citoyen et citoyenne du XXIème siècle. Une étude publiée par le Nasdaq en avril 2016 et réalisée aux Etats-Unis, au Japon, en Grande-Bretagne, Allemagne et dans les pays nordiques révèle que 91% des dirigeants reconnaissent ne pas être en mesure d'analyser les rapports sur l'état de la Cybersécurité de leur entité qui leurs sont transmis. Quel sera le taux pour le continent africain si une telle étude était réalisée ? A quoi bon être informé si les messages fournis restent illisibles et dénués d'intérêt stratégique ? Ne limitons pas la connaissance des opportunités liées au déploiement du numérique aux seuls périmètres des métiers. Il convient d'y ajouter une information régulière et facilement compréhensible sur les questions de **sécurisation des actifs numériques**. Au risque de voir disparaitre les éléments différenciateurs qui fondent l'existence d'une entreprise et lui assurent un avenir économique. Cette perspective relève pleinement des attributs d'un dirigeant africain. Charge à lui/elle de trouver les moyens de bénéficier de cet éclairage et de l'intégrer avec profit dans les avantages concurrentiels qui participeront à son succès.

Partie 3 : La Cybersurveillance des gouvernements africains

Les gouvernements et les entreprises africains sont cyber surveillés…depuis très longtemps. Nous sommes dans la décennie qui verra la pénétration d'Internet dans le cœur même des compétences régaliennes des états africains.

L'affaire Snowden, bien que datant de 2013 nous révèle encore qu'Internet en réalité et en virtualité est devenu un territoire sans terre, une nouvelle topologie de l'humanité, un espace fertile, une omniprésence et un présent permanents ou la domination des états perd son sens. Internet va concrétiser le lent mouvement d'émancipation des sociétés civiles africaines au point de se trouver à proximité des appareils des états africains.

Pour mémoire, l'Europe n'est pas en reste. La France dispose de moyens ultra performant de renseignements d'origine électromagnétique, et ce hors du contrôle juridique. Le cas du PNIJ français, même s'il ne semble pas répondre aux attentes du gouvernement, en est la plus récente illustration. En Europe les projets FP7, ADABTS et SUBITO, ont permis la mise au point de systèmes très sophistiqués d'anticipations des comportements. Le principe de ces systèmes repose sur la vidéosurveillance intelligente. Un procédé qui consiste à détecter les comportements considérés comme « suspects », permettant ainsi de détecter par exemple, un appel à l'aide ou des coups de feu. Ces technologies d'anticipations des comportements nous renvoient violement vers le film Minority Report de K-Dikien.

PRISM n'est qu'un nom plutôt tendance, un élément infiniment moins important que les moyens réels de surveillance électronique dont disposent les pays industrialisés. PRISM n'est qu'un élément d'un système beaucoup plus complexe. Ce programme beaucoup plus global est composé de plusieurs maillons spécialisés dans des types d'informations spécifiques.

1. Mainway et Marina pour les métadonnées...
2. Nucleon et PRISM pour le contenu
3. XKeyscore pour l'espionnage massif des Etats-Unis sur Internet

Partie 4 : Que ce cache-t-il réellement derrière PRISM ?

PRISM a des émanations françaises, anglaises, canadiennes, allemandes et…chinoises
Selon le Guardian, la NSA consacre 250 millions de dollars par an pour influer sur les choix des technologies de cryptages des entreprises, sur la définition des standards mondiaux et la conception de leurs produits. Cette simple affirmation aura des implications importantes sur la crédibilité et les choix des technologies de cryptage des gouvernements africains.

Les grandes puissances on par essence besoin de protéger leurs intérêts et de maintenir un niveau de renseignement qui leur donne un avantage et une longueur d'avance en permanence. Il n'est donc pas surprenant que des programmes comme PRISM existent, mais ce qui l'est

vraiment c'est qu'aucun gouvernement africain, ne semble avoir mis en place des programmes ou dispositifs anti-PRISM.

Au moment où j'écris cet article, la NSA s'est fixé comme objectif de décrypter TOR, l'un des mécanismes permettant de surfer sur Internet anonymement.

Comment les gouvernements africains peuvent-ils se protéger contre ces programmes de cyber surveillances ?

Sans être paranoïaques, les gouvernants africains peuvent toutefois légitimement tenter d'échapper à l'éventualité d'un espionnage de leurs données par les services de surveillance étrangers. Il faut complètement repenser la notion d'infrastructure numérique en Afrique et y intégrer la sécurité comme axe principal qui déterminera tous les choix y afférents.

Pourquoi les économies et les gouvernements africaines sont en dangers ? La notion de sécurité économique

Si les états africains ne traitent pas ces questions, ils prennent le risque de mettre en danger leurs indépendances politique, stratégique, économique et militaire.

Les africains doivent-ils développer un système de cryptographie indépendant ?

Les africains doivent-ils penser à développer leur propre système de navigation ? Les américains ont le GPS, les russes GLONASS, les chinois ont Beidou depuis 2012 et les européens Galileo, pas encore totalement opérationnel.

Les africains doivent-ils stocker les données dans les clouds américains, européens ou créer un Cloud Africain ?

Et à propos des moyens de communications par satellites, indispensables aujourd'hui ?

Ces questions ne sont pas seulement liées à la Cybersécurité mais aussi aux notions d'indépendance, de protection du patrimoine informationnel, de protection des états africains, et de la sécurité de leurs économies. L'Afrique doit se doter d'instruments stratégiques de protection de son espace numérique en urgence.

En début du mois de juin 2016, le directeur de la CIA, John Brennan, affirmait que les systèmes de cryptographies n'étaient pas du tout développés sur le plan pratique en dehors des USA. Ce qui selon lui leur procurait une avance technologique et un avantage stratégique.

C'est une contre vérité, soit par mensonge pour induire en erreur, soit par ignorance. Nous sommes bien là dans les méandres de la guerre informationnelle.

Une étude datant de février 2016, bien qu'incomplète, prouve le contraire. En effet il existe aujourd'hui 865 produits, logiciels ou matériels, offrant des solutions très performantes. Environ 546 sont issus des pays hors USA. Dans cette liste 56% sont des produits commerciaux, 44% sont gratuit, 66% sont propriétaires et and 34% sont open source. Les détails de cette étude sont ici. Ces produits sont offerts par 55 pays en dehors des USA. Le Royaume-Uni, le Canada, la France,

et la Suisse sont des puissants fournisseurs de solutions cryptographiques. A cette liste il faut ajouter l'Allemagne qui est l'un des pays offrant des solutions ultra performantes et open source dans certains cas, près de 112 sur les 855. A cette liste il faut ajouter des pays comme l'Algérie, l'Argentine, le Belize, Les Iles Britanniques, le Chili, Chypre, l'Estonie, l'Irak, la Malaisie, la Tanzanie et la Thaïlande qui ont au moins un produit cryptographique performant. Nous voyons bien deux pays africains dans la liste. Très intéressant pour les pays africains qui souhaitent s'affranchir des produits américains.

Dans cet élan d'indépendance technologique, la Chine vient de mettre en place son premier super ordinateur sans aucune composante ou pièce étrangère. Elle a aussi lancé en aout 2016 le premier système de communication par satellite doté d'un système de cryptage quantique théoriquement inviolable. Remettant en cause les moyens utilisés par les nations qui cherchent à intercepter leurs communications en les rendant obsolètes malgré les millions de dollars investis pour les concevoir.

Partie 5 : Cartographie de la guerre économique en Afrique

Comment la Cybersécurité peut-elle devenir une redoutable arme de compétitivité dans la guerre économique que l'Afrique doit livrer ?

L'action militaire unilatérale à des fins de puissance est peu concevable de nos jours car moins acceptable par la communauté internationale. Les puissances mondiales ont dû se montrer plus créatives et trouver des moyens plus inventifs et complexes pour développer leur puissance. Aujourd'hui la puissance d'un État s'évalue principalement sur son économie. Ces derniers tentent d'accroitre en priorité leur rayonnement économique au sein d'une concurrence mondiale redoutable. Nous sommes passés d'une logique géopolitique à une logique géoéconomique.

Nous avons connu le pétrole comme la principale matière première du vingtième siècle. Elle a façonné l'économie, la finance, la géopolitique ainsi que les rapports de forces entre les états. Le vingt-et-unième siècle a vu l'émergence d'une nouvelle matière première : l'information, que dis-je, l'information stratégique. Qui la détient, détient le pouvoir. Pour bâtir, protéger et affirmer son influence, le continent africain va devoir être en mesure de l'identifier et de la protéger farouchement. L'espionnage dit économique est devenu une véritable industrie. La guerre militaire n'est plus la seule guerre à mener pour se protéger. La guerre est, aussi, désormais informationnelle et économique. La concurrence s'est fortement intensifiée à l'échelle mondiale, la montée en puissance des pays émergents, la révolution des TIC, la déréglementation et la globalisation financière en ont été de puissants accélérateurs sur le continent africain. Même si ces deux concepts n'ont pas de définitions précises, et que C. Schmidt [Schmidt, 1991] n'a pas

hésité à qualifier la guerre économique de pseudo-concept, force est de constater leur manifestation depuis une vingtaine d'années. Ne pas l'accepter, c'est fausser toute la perception de la réalité du monde d'aujourd'hui. Et donc de rendre difficile voire impossible la résolution des problèmes et la capacité à anticiper. Sur le plan militaire, on cherche systématiquement à réduire les capacités de l'adversaire en éliminant ses principaux éléments. La fuite des cerveaux ne réduit-elle pas la capacité de l'Afrique à se battre ? Même si cet état de fait n'est pas le résultat d'un vaste complot, le résultat au final est le même : la fragilisation de la force de travail et de savoir-faire du continent africain. Donc le ralentissement de la croissance et de la compétitivité de son économie.

Partie 6 : Les acteurs de la guerre économique

La débauche concurrentielle, le lobbying, la normalisation, l'influence socioculturelle, les actions humanitaires et les ONG, la contrefaçon concurrentielle et la guerre de l'information sont en train de devenir les principaux leviers de la guerre informationnelle et économique.

Aujourd'hui, Il n'y plus de doute possible que la crise que traverse le capitalisme mondial a ouvert un cycle d'incertitudes fondamental. Si la voie sur laquelle est engagé celui-ci ne s'infléchit pas, il n'est pas à exclure que les prochaines décennies soient marquées par la coexistence de la guerre économique et de la guerre militaire de manière encore plus prononcée.

Il est important de rappeler que la fuite des données n'est pas seulement liée aux cyberattaques donc à la Cybersécurité. Il existe des moyens légaux de détourner de l'information stratégique. L'achat de filiale ou de sous-traitant est un des exemples les plus utilisés aujourd'hui. Il existe aussi l'instrumentalisation des procédures administratives ou judiciaires pour accéder à des informations stratégiques. D'où l'importance de développer le volet légal et juridique créant ainsi un véritable bouclier que nous pouvons appeler la sécurité des affaires.

Comme il faut une armée militaire, il faudra également une armée économique. Comme il faut des armes militaires, il faudra également des armes économiques. La compétitivité et la Cybersécurité peuvent en être les précurseurs avec l'état comme arbitre de la stratégie de puissance et les entreprises comme joueurs.

Compétitivité, Cybersécurité et Cyberdéfense

D'après AlixPartners, le marché de la Cybersécurité représentera 120 milliard de dollars américain en 2017.

La compétitivité, ce terme savant désigne la capacité d'un secteur économique, d'un territoire (pays, bassin économique...), d'une entreprise, à vendre et fournir durablement un ou plusieurs biens ou services marchands sur un marché donné en situation de concurrence.

Inéluctable et onéreuse, la Cybersécurité et la Cyberdéfense ont longtemps été considérées par les africains comme de « simples » exigences liées aux risques et aux usages. Ce n'est plus vrai. La Cybersécurité et la Cyberdéfense deviennent de fait deux réponses nécessaires aux nouvelles

menaces et plongent désormais au cœur des stratégies de défenses de l'état ainsi que des produits ou des processus de l'entreprise : un changement que l'état et l'entreprise africain peut et doit transformer en avantage compétitif.

En apportant plus de confiance numérique, cela réduira fortement les risques, engendrera moins de coûts, et développera ainsi de nouveaux avantages compétitifs.

Comment positionner la confiance numérique dans le business model de l'entreprise africaine pour en faire un avantage concurrentiel ?

Quatre vecteurs de valeur s'imposent alors pour atteindre cet objectif de compétitivité grâce à la Cybersécurité :

1) En développant la confiance numérique à l'échelle du continent
2) En identifiant les nouveaux vecteurs de valeurs qui sont liés à la Cybersécurité
    a. Introduire la sécurité dans les produits et services
    b. Introduire plus de sécurité dans les processus
3) En développer les compétences spécifiques à ce secteur et créer l'embryon d'une véritable industrie
4) En formant le grand public

Partie 7 : Conclusion et perspectives

Face à ces enjeux, les gouvernements et les entreprises africains doivent rester déterminés. Il faudra que la politique en Afrique dépasse ses contradictions pour se concentrer sur les problèmes structurels du continent. Les dirigeants africains doivent comprendre et intégrer les défis à relever en changeant de paradigme de gouvernance, en adoptant un véritable leadership, en modifiant les perceptions des problèmes et en accélérant leur résolution.

Il existe un véritable marché de la Cybersécurité, donc de nombreuses opportunités pour ce secteur, même si embryonnaire pour le moment, avec des acteurs compétents offrant des conseils, produits, services et solutions pertinents, efficaces et adaptés à toutes les situations.

En prenant le control de leur Cybersécurité et de leur Cyberdéfense, les gouvernements et entreprises africains apprendront à maitriser de nouveaux risques tels que :

1. Le risque lié au vol de données
2. Le risque lié à l'image et a la réputation
3. Le risque lié au secret des affaires
4. Le risque lié à la désinformation
5. Le risque lié à la fraude
6. Le risque lié aux crimes économiques
7. Le risque lié à la déstabilisation des économies

Même si la Cybersécurité et la Cyberdéfense ne sont pas des fins en soit, ils demeurent deux leviers déterminants d'une véritable stratégie d'intelligence économique. Chaque gouvernement doit l'ériger au plan de levier de compétitivité.

Les états africains doivent penser à une stratégie qui devra reposer sur cinq axes et deux leviers juridique et technologique :

- Axe 1 : Défense et sécurité des systèmes d'information de l'État et des infrastructures critiques
- Axe 2 : Confiance numérique, vie privée, données personnelles, cybermalveillance
- Axe 3 : Sensibilisation, formations initiales, formations continues
- Axe 4 : Environnement des entreprises du numérique, politique industrielle
- Axe 5 : Afrique, souveraineté numérique, stabilité du cyberespace

Je developperai chaque axe dans mes prochaines notes.

L'intelligence économique est un outil indispensable en mesure d'aider les différents acteurs du continent dans cette guerre informationnelle et économique. Elle permet la maitrise de l'information, matière première immatérielle. Elle permet d'identifier les opportunités et les conditions du succès, d'anticiper les menaces, de prévenir les risques, de se sécuriser économiquement, d'agir et d'influencer sur son environnement intérieur et extérieur dans une logique de compétitivité continentale et internationale.

L'intelligence économique permet de mieux connaître le contexte concurrentiel, les donneurs d'ordre, les règles du jeu de la compétitivité et les normes qui peuvent influencer l'activité et donc d'agir sur son espace au lieu de le subir.

Si l'on croise les trois principales branches de l'intelligence économique, la veille stratégique, la sécurité économique et l'influence, aux formes de la guerre informationnelle et économique, il apparait clairement que l'intelligence économique représente une véritable arme offensive et défensive pour les entreprises et les États.

L'Afrique est en guerre, une guerre non déclarée, une guerre silencieuse, sans victimes apparentes, sans dégâts visibles. Une guerre aux implications stratégiques déterminantes pour l'avenir du continent. Une guerre pour la survie et la vie….

Aziz Da Silva

Consultant Senior en Stratégies et Innovations Technologiques (CSSIT)

Consultant en Sécurité Economique et Protection du Patrimoine (CSEPP)

http://azizdasilva.cloudaccess.host