Laboratoire Africain de
Recherches en Cyberstratégie

Guide pratique d'une analyse de cyber-risques pour les Etats africains

Par DJIMGOU NGAMENI

Mai 2021

Extrait du livre ***« Souveraineté numérique et cyberdéfense : un enjeu de taille pour l'Afrique »****, du même auteur.*

Résumé :

Face aux cybermenaces qui sont de plus en plus présentes, à la multiplication de cyberattaque s de plus en plus sophistiquées, ainsi qu'à la multitude d'acteurs de plus en plus performante et qui souhaitent acquérir ou conserver des intérêts sur le continent africain par tous les moyens y compris des moyens cybers, l'analyse des risques est une étape cruciale pour les états africains dans la démarche de protection de leur cyberespace. Toutes les grandes puissances l'ont compris et le pratiquent avec rigueur. En s'appuyant sur la méthode EBIOS, nous proposons un guide pratique d'analyse de risque numérique à l'échelle du cyberespace d'un pays africain, avec d'en inspirer certains pour développer efficacement leur propre stratégie de cyberdéfense.

Introduction

En cyber comme dans d'autres domaines, afin de pouvoir cartographier les menaces et déterminer les mesures efficaces de sécurité à mettre en œuvre, il est nécessaire de mener au préalable une évaluation rigoureuse des risques. Face aux cybermenaces qui sont à la fois de plus en plus présentes et de plus en plus sophistiquées, face à la multitude d'acteurs[1] de plus en plus performante et qui souhaitent acquérir ou conserver des intérêts sur le continent africain par tous les moyens y compris des moyens cybers, l'analyse des risques est une étape cruciale pour les états africains dans la démarche de protection de leur cyberespace. Toutes les grandes puissances l'ont compris et le pratiquent avec rigueur. Ces extraits du prologue de la stratégie nationale des Etats-Unis pour les opérations du cyberespace, rendu publique par le ministère de la Défense (*U.S Department of Defense*), l'illustrent très justement :

"*... Through the process of risk management, leaders must consider risk to U.S. interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations...*"

"... For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and de conflict all cyberspace operations..."

"... Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain..."

Ces courts extraits nous révèlent que dans leur stratégie de sécurité nationale, les États-Unis considèrent la gestion des cyber-risques comme étant le processus par lequel les dirigeants identifient les acteurs hostiles et évaluent les menaces que ces derniers font peser sur leurs intérêts dans le cyberespace, mais aussi comme un moyen d'évaluer leurs propres capacités à exploiter la nature même du cyberespace pour réaliser des objectifs stratégiques.

Ainsi, comme le recommande le guide pratique de la cybersécurité et de la cyberdéfense publié par l'OIF en 2016 (Organisation Internationale de la Francophonie)[2], tous les dirigeants africains devraient (au moins pour ces mêmes raisons) avoir une bonne maîtrise de leur écosystème numérique, de son évolution planifiée, et donc des risques y afférent.

[1]Qualifié à juste titre de « scandale géologique » en raison de son énorme potentiel économique et démographique, le continent noir apparaît comme le terrain privilégié de compétitions entre Etats et de rivalités entre grandes puissances (telles la chine, la France, les Etats-Unis, la Russie, etc.), y compris par les moyens cybers.

[2]Guide pratique de la cybersécurité et de la cyberdéfense, publié par l'OIF en 2016

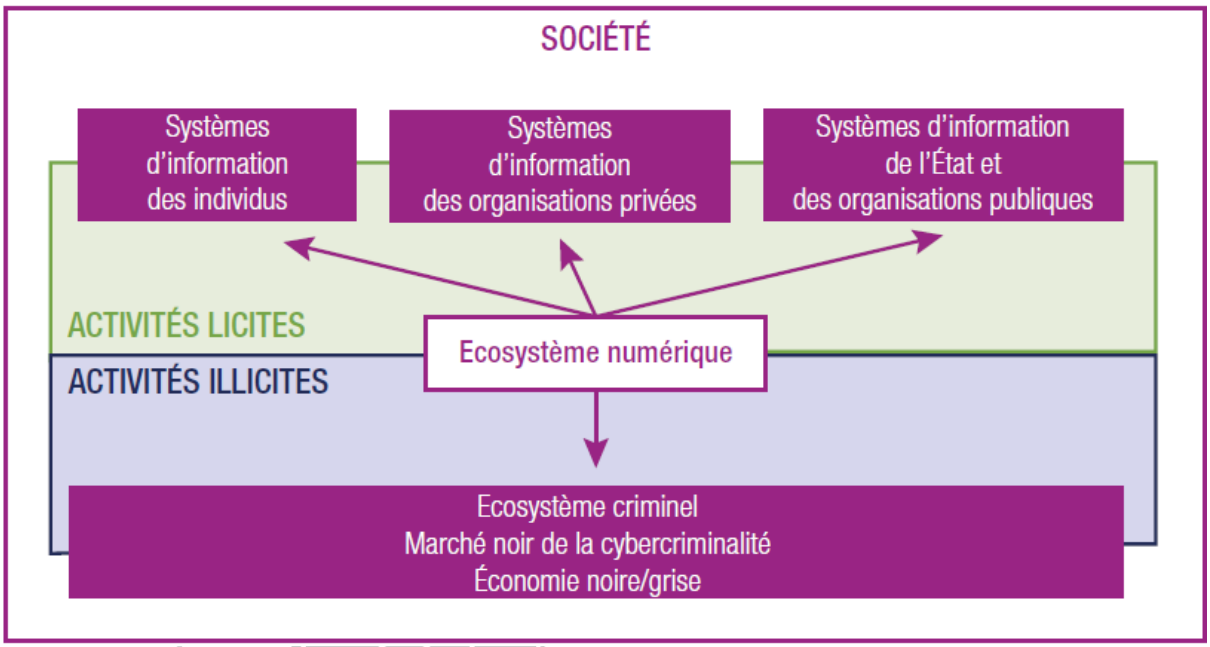
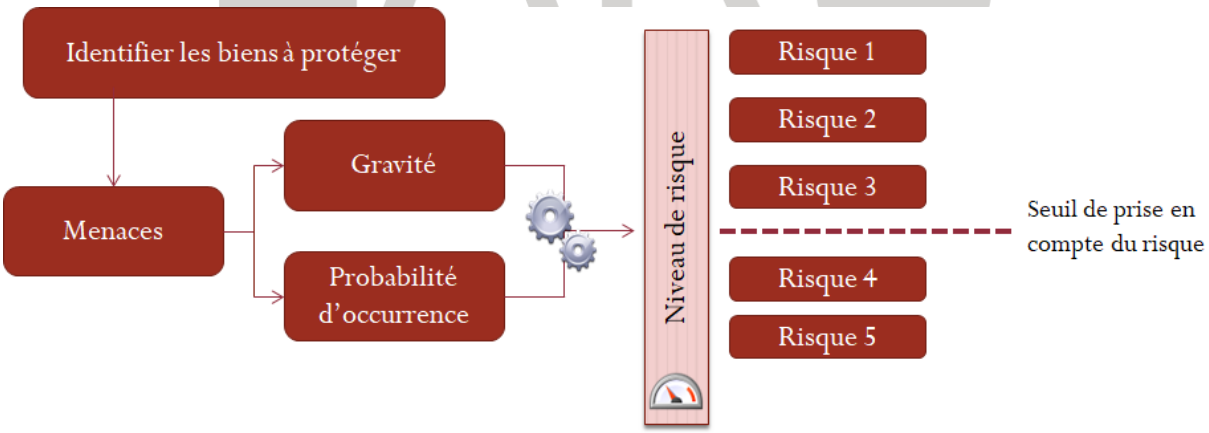


Figure 1 : Représentation de l'écosystème numérique d'un pays (Source : extrait du guide pratique de la cybersécurité et de la cyberdéfense, publié par l'OIF en 2016)

Comprendre le risque cyber

Un *risque numérique* est la possibilité qu'une *menace* donnée exploite les *vulnérabilités* d'un actif ou d'un groupe d'actifs et nuise donc à une organisation ou à un pays. Le risque est mesuré en termes de combinaison entre la *vraisemblance* d'un événement (probabilité qu'il se réalise) et ses *conséquences* (son impact concret s'il se réalisait).

La *menace* est la source de risque associée à sa méthode d'attaque, tandis que la *vulnérabilité* représente la faille existante dans le système et identifiable par la source de risque. L'exploitation de cette faille revient donc à compromettre le système. Ainsi, une démarche d'analyse de risque peut être schématisée ci-dessous :



Trouvez ci-dessous quelques formules simplifiant la compréhension du lien existant entre ces différents concepts, qui sont déterminants pour bien appréhender la notion de cyber-risque :

R *= M x V (Risque = Menace x Vulnérabilité)*

M *= S x A (Menace = Source/Origine x Méthode attaque)*

nR *= R x P x I (Niveau de risque = Risque x Probabilité x Impact)*

Maintenant que nous avons posés ces fondamentaux, je vous invite à démarrer l'analyse proprement dite. Pour y parvenir, il existe plusieurs normes qui détaillent les raisons pour lesquelles une analyse de risque est importante et les éléments clés qu'il faut prendre en compte. La plus connue, largement utilisée par les spécialistes du monde entier, c'est la norme ISO 27005. Cependant, si cette norme vous indique bien « pourquoi » il vous faut mener une analyse de risque, elle ne vous dit pas « comment » le faire. Une méthode est donc ici nécessaire pour implémenter la norme. Là encore, il en existe plusieurs dont les plus utilisées sont OCTAVE aux Etats-Unis, puis MEHARI et EBIOS en Europe.

Dans cet article, nous utiliserons la méthode EBIOS[3] pour proposer un schéma d'analyse de risque à l'échelle d'un pays africain (ou une organisation d'importance vitale dans ces pays), afin que ceux qui le souhaitent puissent s'en inspirer pour développer efficacement leur propre stratégie de cyberdéfense.

Développée par l'ANSSI (*Agence Nationale de Sécurité des Systèmes d'Information en France*), la méthode EBIOS que nous mobilisons ici s'appuie sur une démarche comprenant les cinq étapes suivantes :

- L'étude du contexte et du socle existant
- L'identification des sources de risque
- L'identification des événements redoutés et des objectifs visés
- L'étude des scénarios de menaces (stratégiques et opérationnels)
- Le traitement des risques (réduire, accepter, éviter, etc.).

Dans un premier temps, commençons par définir le périmètre de l'analyse.

[3]EBIOS signifie *Expression des Besoins et Identification des Objectifs de sécurité* | Guide de la méthode EBIOS -

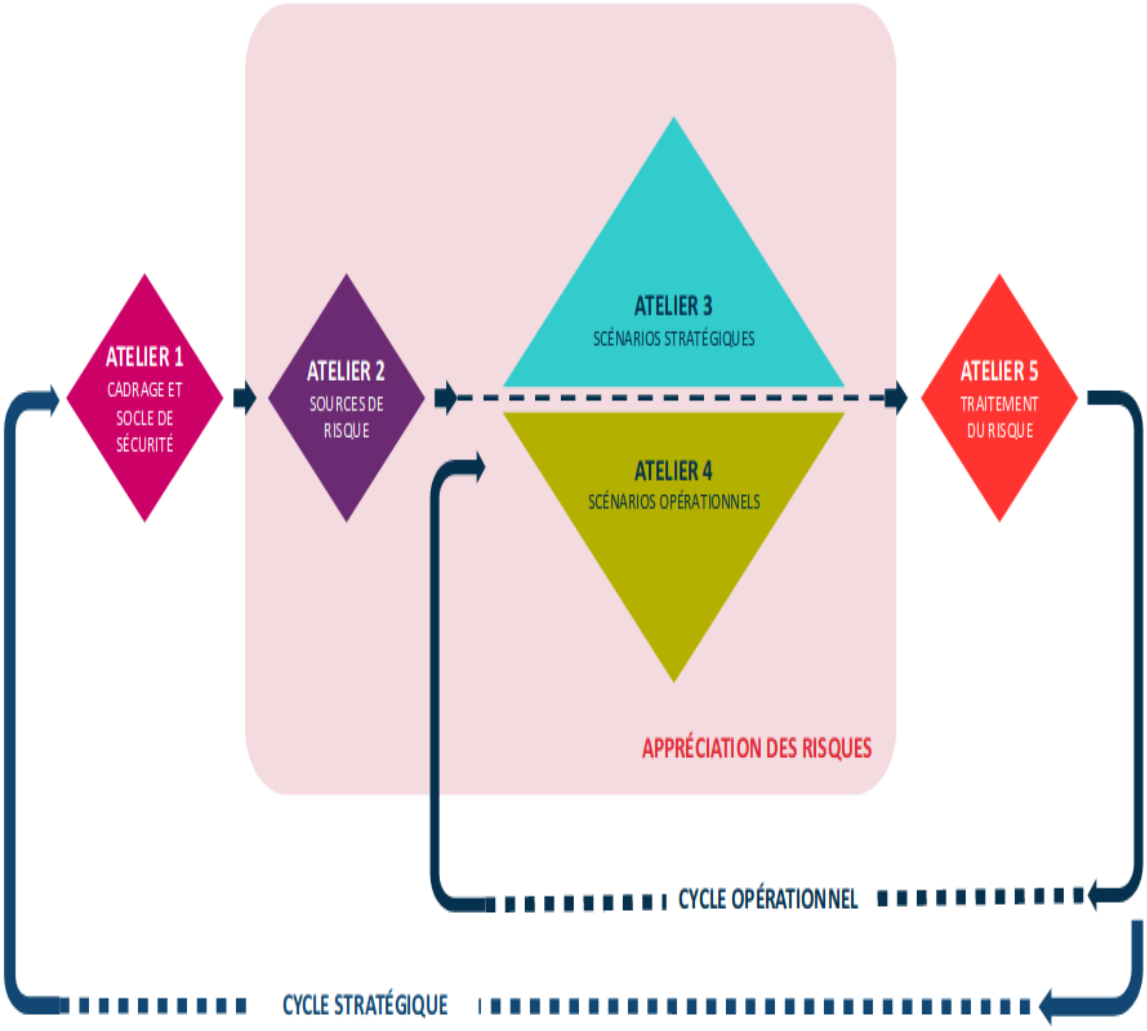


Figure 2 : Les étapes de la méthode EBIOS (Source : Extrait du Guide la méthode EBIOS publié par l'ANSSI)

Définition du périmètre

Objet d'étude	**Cyberespace d'un pays africain**		
Mission	**Acquérir et préserver l'autonomie stratégique (évaluation, décision, action) dans le cyberespace.**		
Intérêts de souveraineté	Traitement (échange, utilisation et stockage) sécurisé du patrimoine informationnel		
Nature	Processus		
Description	Toutes activités relatives au traitement d'information jugée stratégique (Information politique, économique, diplomatique, militaire, Information à caractère personnel), notamment: la communication intra et inter gouvernementale (différents ministères, et présidence), la communication avec les représentations diplomatiques, la communication intra et inter états-majors, la communication inter et intra administrations publiques.		
Entité /Personne responsable	Agences / Services de l'Etat / État-major		
Biens supports associés	SI des Administrations publiques critiques	SI des Opérateurs d'Importance Vitale	Infrastructures des centres d'hébergement de données
Description	Système d'information du gouvernement, des administrations et des entreprises publiques.	Infrastructure des systèmes industriels, des opérateurs de télécommunications, des opérateurs de réseau électrique, etc.	Infrastructure permettant le traitement (stockage, utilisation) des informations stratégiques
Entité /Personne responsable	DSI / RSSI	DSI / RSSI / Fabricant matériel industriel	DSI / RSSI

Tableau 1 : Contexte de l'étude (ceci est un échantillon, qui doit être adapte au contexte particulier du pays)

PS : Nous entendons par « Cyberespace d'un État », l'ensemble constitué des réseaux (interconnectés ou non) et de l'espace informationnel sous la juridiction de l'Etat en question. Cette étude est circonscrite aux réseaux et systèmes d'information (gouvernementaux, militaires, opérateurs économiques vitaux, administrations publiques) à partir desquels sont générées, utilisées, échangées ou stockées les informations jugées stratégiques, et dont la compromission porterait atteinte à la souveraine numérique de cet Etat.

Evaluation du socle de sécurité des systèmes d'information au niveau étatique

Dans la plupart des pays africains, la réglementation en matière de sécurité des systèmes d'information gouvernementaux et d'administrations publiques tourne autour des éléments suivants :

- Loi sur la cybersécurité et la cybercriminalité
- Loi sur la protection des données personnelles et la protection de l'enfance en ligne
- Loi sur les transactions électroniques
- Existence d'une Stratégie ou d'une Politique nationale de sécurité des SI
- Loi portant sur la création de CERT ou d'agence nationale de cybersécurité.

Certains Etats essayent de mettre en œuvre les recommandations de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, par eux adoptée en 2014 à Malabo. Même si d'un point de vue formel, il est à noter que cette convention n'est à date (Janvier 2021) signée que par 16 pays et ratifiée uniquement par 8 des 55 Etats membres.

De toute façon, à l'exception des pays africains les mieux classés dans l'étude GCI[4] (*Global Cybersecurity Index*) tels que l'Ile Maurice, le Rwanda, l'Egypte, le Kenya et quelques autres, très rares sont les pays qui ont mis en place un arsenal complet et équilibré, ou même qui respectent simplement les normes internationales (normes ISO 2700x par exemple) et les bonnes pratiques en matière de cybersécurité et de lutte contre la cybercriminalité.

Ainsi, sur les 44 pays africains qui ont participé à cette étude en 2018, il ressort du rapport que 38 d'entre eux ont mis en place une loi pour lutter contre la cybercriminalité, 19 pays ont légiféré sur la protection de l'enfance en ligne, 17 pays ont des programmes conformes de formation des professionnels en cybersécurité, rien que 14 de ces 44 pays ont élaboré et rendu publique une stratégie nationale de cybersécurité, et seulement 13 ont un CERT (*Computer Emergency Response Team*) reconnu et fonctionnel. Plus récemment, 33 pays africains ont voté une loi sur la protection des données personnelles, parmi lesquels 14 ont même créé une autorité chargée de son application rigoureuse. Cet intérêt pour la protection des données personnelles

[4]L'Union Internationale des Télécommunications (UIT) réalise chaque année une étude appelée Indice Globale de Cybersécurité (ou ***GCI*** mis pour *Global Cybersecurity Index*), qui mesure le niveau de développement de chaque pays dans le monde en matière de cybersécurité.

est certainement le résultat du retentissement mondial du RGPD[5], devenu d'ailleurs un outil d'influence normatif de l'Europe dans le cyberespace.

Plus grave, la quasi-totalité des pays n'a toujours pas abordé la question de protection de son cyberespace sous l'angle de la « cyberdéfense », c'est-à-dire sous l'angle de la conflictualité qui s'y déroule. Plusieurs études soulignent pourtant que les menaces et les risques vont au-delà des seules pertes financières. Elles démontrent la présence accrue de piratage diplomatique parrainé par les États. Même si la Chine est très souvent désignée comme le principal acteur menaçant dans cette région, il en ressort clairement que d'autres puissances se livrent aux mêmes activités d'espionnage / de piratage, et profitent allègrement des « largesses[6] » de leurs partenaires africains.

Ce constat dénote d'une mauvaise connaissance du panorama des cybermenaces qui pèsent sur le continent, de leurs évolutions, ainsi que des différents acteurs / agents et leurs modes opératoires. Le déficit ainsi décrit est la conséquence de l'absence d'un processus clair de gestion des risques cyber au sein de nos Etats. On peut également y voir le manque d'une cyberstratégie, d'une stratégie de cyberdéfense ou de doctrine connue en la matière au sein des pays africains, qui pour la plupart n'envisage pas encore la question des risques numériques au-delà de la cybercriminalité. Or, d'après les experts, dans la classification des types de menaces numériques en fonction de leur gravité, la criminalité sur internet est tout en bas de l'échelle derrière le cyberespionnage, le cyberterrorisme, voire la cyberguerre. Il est donc urgent pour ces derniers de mieux protéger leur patrimoine informationnel et autres actifs numériques (politiques, diplomatiques, industriels, énergétiques, télécoms et financiers).

Mais quels sont les types d'évènements qu'un Etat africain devrait redouter dans le cyberespace et surtout quel serait leur gravité ? Examinons maintenant cette question.

[5] Règlement General pour la Protection des Données.

[6] Entendez ici la naïveté et l'impréparation des états africains, ce qui facilite la tâche de ceux qui les prend pour cible.

Identification des événements redoutés

Intérêts de souveraineté	Evénements redoutés	Impact / Conséquences	Gravité
Création, utilisation, échange et stockage sécurisé de l'information stratégique.	Cyberespionnage / surveillance (interception, vol d'information).	Impact sur l'avantage stratégique avec une perte du patrimoine intellectuel, perte économique, perte de compétitivité, perte de la confidentialité de l'information, limitation des marges de négociation.	**3 (Grave)**
	Sabotage (perturbation, destruction, prise de contrôle) des infrastructures.	Indisponibilité des infrastructures de services critiques (donc indisponibilité de l'information stratégique hébergée) avec un impact majeur sur la sécurité nationale et les missions régaliennes de l'état (santé, finances, transports, énergie, etc.).	**4 (Critique)**
	Subversion (propagande, manipulation) de l'information	Dégradation de la réputation et de la crédibilité publique, désinformation, humiliation, démobilisation, encerclement cognitif, etc.	**2 (Significatif)**

Tableau 2 : Classification des événements redoutés par rapport à la gravité

ÉCHELLE	DÉFINITION
G4 – CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée)
G3 – GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé)
G2 – SIGNIFICATIVE	Dégradation des performances de l'activité sans impacts sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé)
G1 – MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges)

Figure 3 : Echelle de gravité des risques
(Source :Extrait du Guide la méthode EBIOS publié par l'ANSSI)

Évaluation du rapport entre les sources de risque et les objectifs visés

			RESSOURCES			
			Incluant les ressources financières, le niveau de compétences cyber, l'ouillage, le temps dont l'attaquant dispose pour réaliser l'attaque, etc.			
			Ressources limitées	Ressources significatives	Ressources importantes	Ressources illimitées
MOTIVATION	Intérêts, éléments qui poussent la source de risque à atteindre son objectif	Fortement motivé	Moyennement pertinent	Plutôt pertinent	Très pertinent	Très pertinent
		Assez motivé	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent	Très pertinent
		Peu motivé	Peu pertinent	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent
		Très peu motivé	Peu pertinent	Peu pertinent	Moyennement pertinent	Moyennement pertinent

DEGRÉ DE PERTINENCE D'UN COUPLE SR/OV

Figure 4 : Évaluation de la pertinence entre les sources de risque et les objectifs visés (Source : Extrait du Guide la méthode EBIOS publié par l'ANSSI)

Il s'agit ici d'identifier de façon exhaustive les motivations qui poussent une source de risque à vouloir s'attaquer aux intérêt du pays en question. Aussi, il faut évaluer le niveau de ces motivations, et surtout bien déterminer si la source de risque en question détient les moyens suffisant pour atteindre son objectif. Par exemple, la motivation idéologique d'un terroriste qui s'attaquent à une cible est largement différente de celle d'un mercenaire qui lui agit pour des raisons pécuniaires. Ce croisement entre motivation et moyen permet d'évaluer la pertinence d'un risque, ce qui va orienter les mesures à prendre pour traiter.

Sources de risque	Objectifs visés	Motivation	Ressources	Pertinence
Etats / Agences de renseignement étrangères	Espionner, Voler des informations, Saboter les infrastructures critiques (services publics régaliens), réduire l'autonomie de décision et d'action, domination économique et stratégique	Fortement motivé	Ressources importantes	Très pertinent
Cyber terroristes	Sabotage (Déstabilisation), subversion (modification des perceptions, dégradation de l'image de l'État et destruction de sa réputation).	Fortement motivé	Ressources significatives	Très pertinent
Hacktivistes (cyber activistes idéologique)	Divulguer des informations classifiées (secrets économique, secrets d'Etat, etc.), Voler des informations, etc.	Assez motivé	Ressources significatives	Plutôt pertinent
Catastrophes naturelles	Destruction des infrastructures	Assez motivé	Ressources significatives	Plutôt pertinent

Tableau 3 Rapport entre les potentiels sources de risque et les objectifs visés

Analyse de l'écosystème et cartographie des menaces

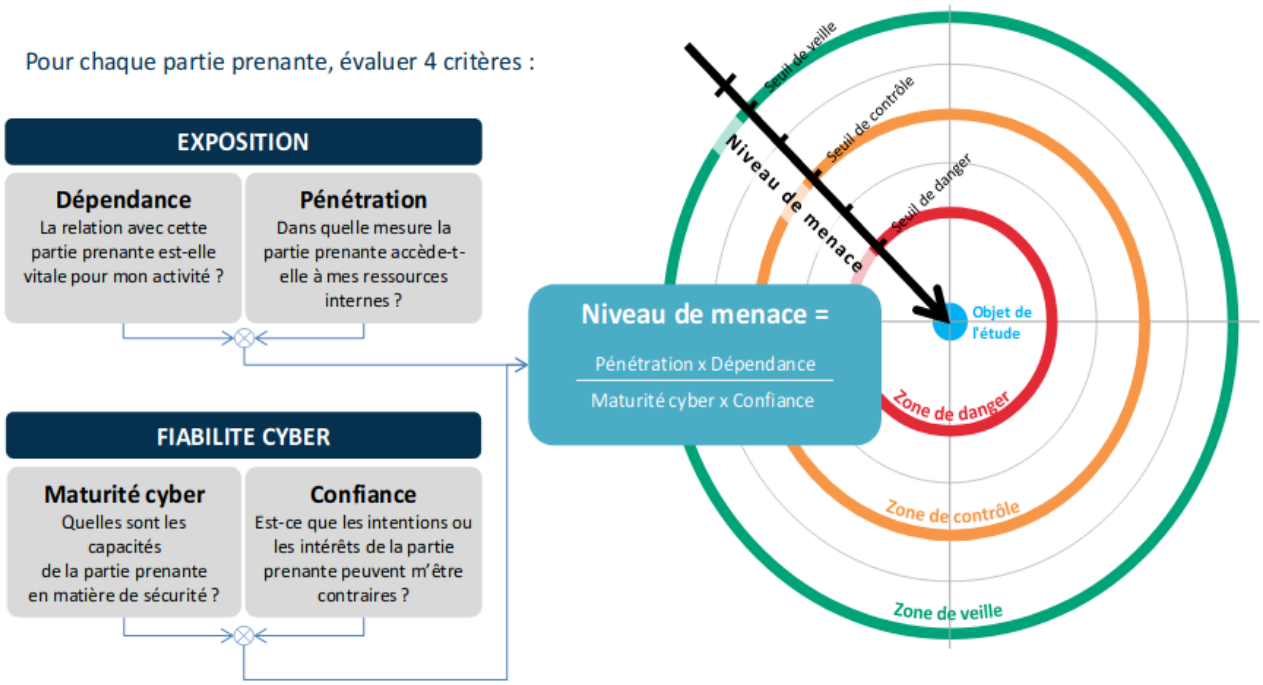


Figure 5 : Schéma de cartographie des menaces
(Source : Extrait du Guide la méthode EBIOS publié par l'ANSSI)

L'idée est d'identifier tous les acteurs qui font partie de l'écosystème du cyberespace du pays (donc qui sont parties prenantes dans son fonctionnement), et de déterminer leur niveau de fiabilité cyber par rapport à la mission initiale de protection des informations stratégiques, afin de prendre les mesures de sécurité qui s'imposent. Le tableau ci-dessous est donné à titre indicatif, mais reflète mon appréciation de l'état des lieux dans la plupart des pays africains.

Parties prenantes	Dépendance	Pénétration	Maturité cyber	Confiance
Fournisseurs Informatique d'équipements et logiciels (Microsoft, Cisco, Huawei, etc.)	Lien client / fournisseur du matériel et logiciel, utile pour la mission	Accès probable via des portes dérobées.	Bonnes pratiques, normes et réglementation respectées.	Intentions considérées comme neutres pour les locaux et hostiles pour les multinationales.
Prestataires de services informatiques (hébergement, support, etc.)	Lien utile pour la réussite de la mission	Accès physique aux équipements, accès privilégié aux systèmes.	Bonne pratiques, normes et réglementation peu respectées.	Intentions considérées comme neutres pour les locaux et hostiles pour les multinationales.
Opérateurs Internet / Telecom / Satellite	Lien utile pour la réussite de la mission	Accès physique aux équipements, accès privilégié aux systèmes.	Bonne pratiques, normes et réglementation passablement respectée.	Intentions considérées comme neutres pour les locaux et hostiles pour les multinationales.
Fournisseurs de téléphones et logiciels mobiles (Apple, Google, Samsung, Huawei, etc.)	Lien client / fournisseur du matériel et logiciel, utile pour la mission	Accès probable via des portes dérobées.	Bonne pratiques, normes et réglementation passablement respectée.	Intentions considérées comme neutres pour les locaux et hostiles pour les multinationales.
Représentations diplomatiques	Lien utile pour la réussite de la mission	Accès physique ou via des connexions distantes autorisées.	Bonne pratiques, normes et réglementation passablement respectée.	Intentions considérées comme bienveillantes.

Tableau 4 : Ecosystème et cartographie des menaces

Définition des Scénarios Stratégiques

Description du Scénario : Un pays étranger à travers ses agents de renseignement veut voler des informations stratégiques en espionnant toutes les entités du pays africain cible susceptible de traiter ce type d'information. Il s'agit ici d'un scénario de cyberespionnage.

Gravité de ce scénario : **3 (Grave)**

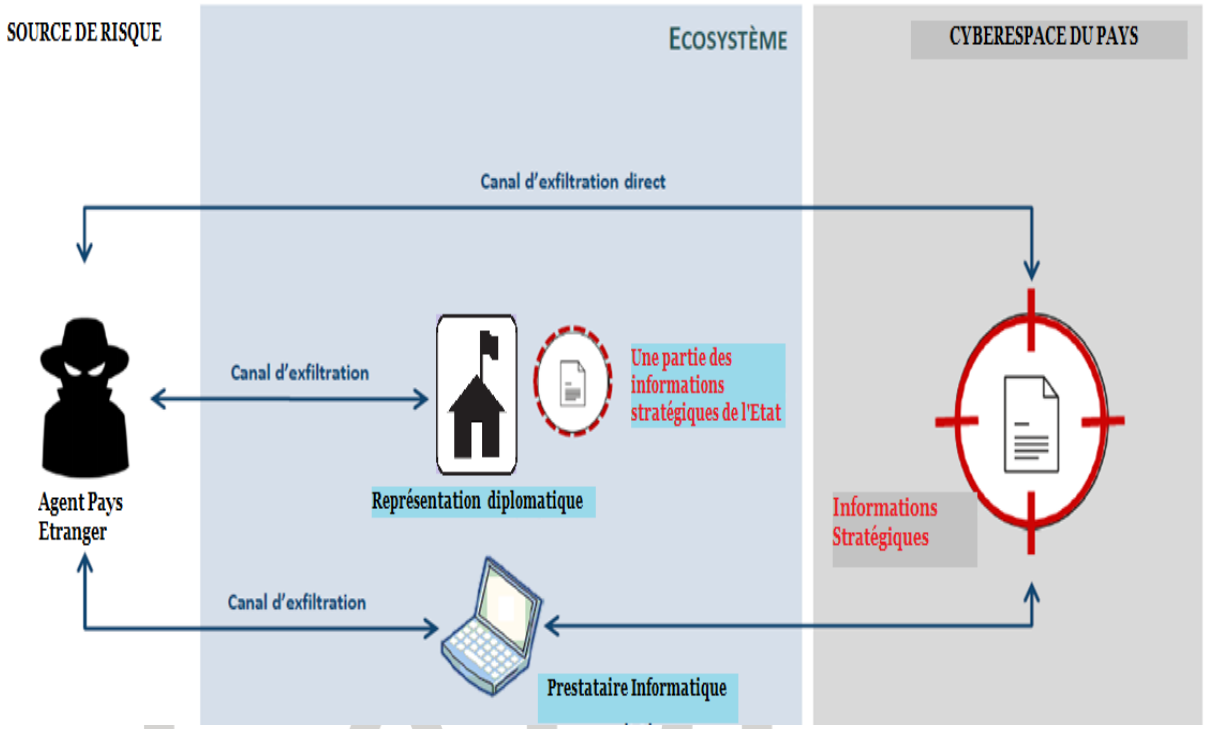


Figure 7 : Représentation schématique d'un scénario stratégique
(Source : Extrait adapté du Guide la méthode EBIOS publié par l'ANSSI)

Plusieurs autres scénarios stratégiques peuvent être schématisés selon la même approche, afin de représenter clairement et même de façon plus spécifique quelle est la source de risque, le chemin d'attaque (canal d'exfiltration) et l'objectif visé en fonction des entités qui ont accès aux informations sensibles, sont responsables d'infrastructures critiques, ou qui peuvent influencer la perception des citoyens vis à vis de l'État. Cela peut aller du sabotage de la tenue des élections à la destruction d'un objectif militaire, en passant par le vol d'information pour une négociation économique ou un plan de développement, etc.

L'analyse du volet technique du rapport *CTA-2018-0816*[7]en est une illustration éclairante. En effet, on y apprend qu'au début du mois de juin 2018 la Chine a mené une opération de cyberespionnage contre des entreprises du Kenya (la société d'État *Kenya Ports Authority* par exemple, chargée de l'entretien et de l'exploitation de tous les ports du Kenya). Cette opération chinoise coïncide avec l'annonce faite par le gouvernement de Nairobi selon lequel il ne signerait pas l'accord de libre- échange alors en cours de négociation entre la Chine et les Etats de la communauté Est africaine. De plus, dans la même période, plusieurs officiels kenyans et américains faisaient état d'un accord de libre-échange en préparation entre les deux pays. Au regard de ce contexte et des rivalités Chine-USA connues, cette opération de cyberespionnage semble avoir été menée pour des raisons économiques (contrat pour la route de la soie) et stratégiques (démonstration de puissance et d'influence).

Définition des Scénarios Opérationnels

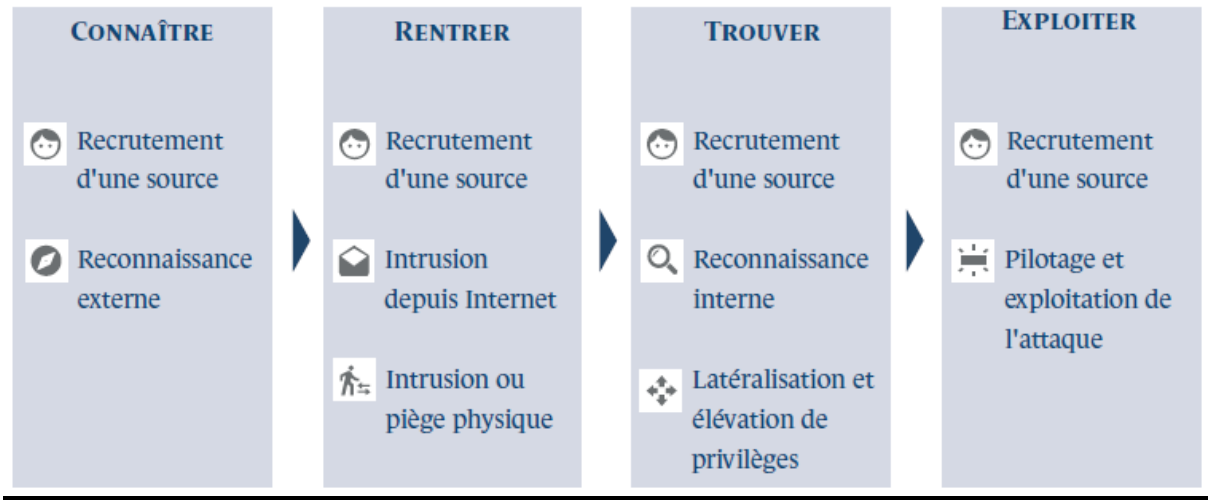


Figure 8 : Séquence d'attaque type dans un scénario opérationnel
(Source : Extrait du Guide la méthode EBIOS publié par l'ANSSI)

[7]Rapport CTA-2018-0816 de l'entreprise américaine *Reported Future* portant sur des opérations de cyberespionnage de la chine en rapport avec la nouvelle route de la soie.

L'idée du scenario opérationnel est d'appliquer la séquence d'attaque aux différents scénarios stratégiques, afin de déterminer de façon précise quelles seront les étapes opérationnelles pour atteindre l'objectif visé. C'est donc dans ce scenario qu'on voit concrètement comment l'attaquant procède pour atteindre son but. Il identifie les chemins d'attaques spécifiques qu'il peut emprunter en fonction du contexte et de l'environnement. Dans le cas des Etats africains par exemple, le niveau de corruption des agents publics peut représenter une voie d'intrusion plus vraisemblable qu'ailleurs.

Une fois toutes les étapes précédentes menées à bien, du cadrage et socle de sécurité en passant par l'identification des sources de risque et objectifs visés, l'énumération des scenarios stratégiques jusqu'à la détermination des chemins d'attaque (et la probabilité qu'ils se réalisent), il est temps de conclure l'analyse au travers d'une dernière étape : il s'agit du traitement des risques. Cette étape consiste à déterminer la façon dont les risques identifiés seront pris en charge, et permet de nous projeter la manière dont on souhaite effectuer le suivi de l'analyse et gérer les risques à l'avenir. En général il y a 4 façons de traiter un risque : le réduire, l'accepter, le refuser ou le transférer.

Que vous soyez en charge du réseau de la présidence, du gouvernement, d'une grande entreprise ou même de l'armée d'un pays africain, si vous avez pu mener les étapes précédentes et souhaitez être accompagné pour clôturer votre analyse avec les étapes de scenarios opérationnels, la cartographie finale et le plan de traitement des risques, n'hésitez pas à nous contacter ! Nous pouvons aussi vous accompagner dès le début de l'analyse si vous le souhaitez.

A propos de l'Auteur :

DJIMGOU NAGMENI est Entrepreneur, Conférencier, Consultant international en cybersécurité / cyberdéfense, Enseignant à l'École Politique Africaine de Paris, Spécialiste de cyberstratégie et Fondateur du LARC.

A propos du LARC :

Le LARC (Laboratoire Africain de Recherches en Cyberstratégie) est un cadre de réflexion créé par votre serviteur et regroupant des chercheurs pluridisciplinaires, avec pour mission de décrypter, d'analyser et d'anticiper les enjeux de demain dans le cyberespace africain.

Pour soutenir les activités du LARC ou y contribuer par vos propres publications, visitez notre site web : https://www.larc.africa

Pour citer cet article :

DJIMGOU NGAMENI, « Guide pratique d'une analyse de cyber-risques pour les Etats africains », Note n°06 - LARC, Mai 2021.