Algerian Journal of Political Economy
EISSN: 2716-8573 ISSN: 2716-7720
Volume: (03) / N°: (01), (2021), p 152-168

La cybersécurité des pays de l'UE et de l'UA : Actions et objectifs

Cyber Security in EU and AU Countries: Actions and Objectives

Abdelmadjid RAMDANE * [1]

[1] Kasdi Merbah University - Ouargla (Algeria), abdelmadjid.ramdane@univ-ouargla.dz

reçu: 13/10/2020 *Accepté : 31/01/2021* *Publié : 01/05/2021*

Résumé:

Cette étude vise à éclairer les politiques suivis dans les pays de l'Union européenne et de l'Union africaine dans le domaine de la cybersécurité collective, où la plupart des pays africains connaissent un retard. Ce qui les pousse à bénéficier de l'expérience européenne, qui mise sur une stratégie unifiée qui a abouti à une loi sur la cybersécurité approuvée par le Parlement européen en mars 2019.

L'étude confirme que l'émergence d'une société mondiale de l'information, ouvre des perspectives nouvelles à tous les pays, grâce aux applications des TIC. Cependant ces TIC posent de nouveaux problèmes liés à la cybersécurité qui touche à la sécurité du patrimoine numérique et culturel des individus, des organisations et des nations. D'où la nécessité d'une coopération entre les pays et les organisations internationales, et entre les secteurs public et privé pour lutter contre les atteintes à la cybersécurité des nations.

Les mots clés: Cybersécurité, actions, Objectifs, Pays de l'UE, Pays de l'UA.

Abstract:

This study aims to shed light on the policies followed in the countries of the European Union and the African Union in the field of collective Cybersecurity, where most African countries are lagging behind. This pushes them to benefit from the European experience, which relies on a unified strategy that resulted in law on Cybersecurity approved by the European Parliament in March 2019.

The study confirms that the emergence of a global information society opens up new perspectives for all countries, thanks to the applications of ICT. However, these ICTs pose new problems related to Cybersecurity which affects the security of the digital and cultural heritage of individuals, organizations and nations. Hence the need for cooperation between countries and international organizations, and between the public and private sectors to combat attacks on the Cybersecurity of nations.

Keywords: Cybersecurity, Actions, Objectives, EU countries, AU countries.

Auteur correspondant.

1. INTRODUCTION

Les cyberattaques occupent une place essentielle dans les discours sur la vulnérabilité de la nation, tenus par les différents acteurs et spécialistes de la sécurité et de la défense nationale partout dans le monde, essentiellement en occident. Cela a incité les pays à nouer des alliances et à prendre des mesures pour contrer ces cyberattaques.

Une citation du dramaturge britannique, Georges Bernard Shaw disait «Si tu as une pomme et que j'ai une pomme, et que nous les échangeons, nous repartons chacun avec une pomme. Si tu as une idée et que j'ai une idée, et que nous les échangeons, nous repartons chacun avec deux idées», cette maxime illustre avec force et précision le besoin actuel de toutes les nations en matière de coopération et de mettre en œuvre une cybersécurité collective.

À l'occasion du 70e anniversaire de l'Organisation internationale de normalisation (ISO), célébré en février 2017, son président en exercice a placé la cybersécurité parmi les défis d'envergure mondiale à relever à l'avenir, au même niveau que le changement climatique ou la rareté de l'eau.

Cette introduction démontre l'importance de la cybersécurité aujourd'hui, d'où la nécessité d'établir une cybersécurité collective impliquant tous les pays, tant au niveau régional qu'au niveau international.

En sachant que les cyberattaques prennent sans cesse de nouvelles formes et il ne s'agit plus de se protéger seulement par des moyens techniques et informatiques ; il convient également de faire intervenir l'humain, de mobiliser l'ensemble des services de l'état et des entreprise et d'impulser de nouvelles collaborations stratégiques.

Les pays de l'Union Européenne (UE) ont franchi des étapes importantes dans ce domaine. Il convient aux pays de l'Union Africaine (UA) de prendre les mêmes mesures, malgré quelques progrès, afin de protéger leurs intérêts économiques et sécuritaires des cybermenaces.

Ceci est l'objet du présent article, en essayant de répondre à la problématique suivante: **Quelles sont les actions prises par l'Union Européenne pour lutter contre les atteintes à la cybersécurité ? , et quelle est la stratégie adoptée par l'Union Africaine dans ce sens?.**

On estime que la réponse aux questions mentionnées ci-dessus, en se basant sur une approche descriptive analytique, exige de donner des définitions aux cybermenaces et cybersécurité dans un premier temps, effectuer ensuite un regard sur la stratégie et le règlement européen sur la cybersécurité, et finir par les actions prises au sein des pays de l'union africaine, et celles qu'elles doivent prendre pour tirer profit des expériences européennes dans ce domaine.

1. Les Cybermenaces et la Cybersécurité : quelles définitions?

De multiples acteurs actifs dans le domaine livrent chacun leur définition de cette notion.

1.1. Les Cybermenaces et les Cyberattaques :

La cybermenace n'épargne plus personne ni aucune organisation. Ses victimes ne sont en effet plus seulement ces utilisateurs isolés qui courent le risque d'une cyberattaque en raison des sites qu'ils fréquentent sur Internet, de leur naïveté (ouvrir une pièce jointe à un e-mail douteux) ou encore de la protection insuffisante de leur PC ou Smartphone. Aujourd'hui, quelques heures suffisent pour rendre totalement inopérantes des entreprises de la taille d'une multinationale ou des administrations touchant des centaines de millions d'usagers. Quand ce n'est pas la stabilité même d'un État qui est visée (CIRB, 2017).

Le Livre Blanc de la Défense et de la Sécurité Nationale (LBDSN) français de 2013 identifie trois types de cybermenaces (EL OUAZZANI, 2016):

- La cybercriminalité qui ne relève pas spécifiquement de la sécurité nationale: ce type d'attaque vise principalement les particuliers et les entreprises privées. Il consiste à pirater des informations personnelles, de dérober des données bancaires, etc. ;
- Les tentatives de pénétration de réseaux numériques à des fins d'espionnage : ce type d'attaque vise les entreprises et les administrations publiques et principalement conduit par des organisations étrangères. L'objectif recherché est d'espionner les communications et avoir accès à des informations confidentielles ;
- Les attaques visant le sabotage de systèmes d'importance vitale : ce type d'attaque vise à déstabiliser le fonctionnement d'un État. Ils peuvent être considérés comme un acte de guerre. Ainsi, il s'agit d'une atteinte à la souveraineté du pays.

1.2. La Cybersécurité :

En 2010, déjà, l'Union internationale des télécommunication (UIT) a adopté la définition suivante de la cybersécurité : « *L'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs.*

Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement.

La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs soient assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement.

Les objectifs généraux en matière de sécurité sont les suivants : disponibilité, intégrité (qui peut englober l'authenticité et la non-répudiation), confidentialité» (UIT, 2010).

L'Union européenne, pour sa part, a livré une définition dans sa stratégie de cybersécurité, présentée en février 2013 et actualisée en septembre 2017. Pour l'Union européenne, «*la cybersécurité vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues*» (Commission européenne, 2013).

La stratégie vise à ce titre à mettre en œuvre les mesures de sauvegarde et les actions auxquelles il est possible de recourir pour protéger le cyberespace, dans les domaines civil et militaire, des menaces associées à ses réseaux interdépendants et à son infrastructure informatique ou susceptibles de leur porter atteinte.

De plus, la Commission européenne rappelle que les enjeux de Cybersécurité se placent également sur le terrain des droits fondamentaux des citoyens européens en affirmant que « la cybersécurité est essentielle pour protéger la vie privée et les données à caractère personnel des individus conformément aux articles 7 et 8 de la Charte des droits fondamentaux de l'UE» (Commission européenne, 2013).

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au secrétaire général de la défense et de la sécurité nationale qui assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale, définit la cybersécurité comme « *l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles* » (ANSSI, 2019a).

1.3. Les services de premières nécessité comme cibles des Cyberattaques:

Les services publics et, notamment, les fournisseurs d'utilités ne sont évidemment pas épargnés. Les exemples ne manquent pas à ce niveau. Le plus célèbre d'entre eux concerne l'Ukraine où, à la fin décembre 2016, quelque 700.000 foyers furent privés d'électricité suite au premier cas communément admis de cybersabotage réussi du réseau électrique d'un pays tout entier (COLLINS, 2016).

Quelques mois plus tard, en juin 2017, l'Ukraine paya à nouveau un lourd tribut cette fois à l'attaque NotPetya. Ce fut notamment au tour du réseau de métro de Kiev ou de la centrale nucléaire de Tchernobyl d'être mis à l'arrêt.

Le secteur de la santé et les hôpitaux en particulier constituent également une cible des cyberattaques. La diffusion de Wannacry en mai 2017 a par exemple largement déstabilisé les services du National Health Service (NHS - Service national de santé) britannique.

Aux États-Unis, en février 2016, l'attaque subie par le Hollywood Presbyterian Medical Center de Los Angeles a mis en lumière la vulnérabilité globale du secteur. L'hôpital en question s'est trouvé bloqué pendant une dizaine de jours. Non moins de 900 dossiers de patients ont été perdus et, au final, une rançon de quelque 15.000 dollars a été versée pour remettre le système informatique de l'hôpital en fonction.

Ce cas n'est pas isolé : les médias américains ont rapporté à l'époque que quatre autres hôpitaux avaient déjà été victimes de telles attaques.

Selon l'éditeur de solutions de sécurité informatique Symantec, les données médicales représentent un trésor de premier choix pour les pirates informatiques. « *Les dossiers médicaux contiennent la plupart des données qui intéressent les cyberpirates, et sont une cible idéale pour les voleurs d'informations* », analyse Symantec.

Ce risque est d'autant plus avéré que le secteur hospitalier se distingue par la forte dispersion de ses sites, beaucoup de faible taille, le manque de culture de leur personnel en matière de cybersécurité, le faible niveau d'investissement en sécurité informatique ainsi que la forte progression d'équipements connectés, dont le manque de protection constitue une nouvelle porte d'entrée pour les cybercriminels (Symantec, (2016).

Les agressions dans la cyber sphère se répartissent, généralement, en 12 grandes familles (TENEZE, 2018) :

- les ADS (Attaque par Déni de Services pour neutraliser un système informatique et le rendre inopérant)
- le cyberespionnage
- le cyberharcèlement
- la cyberfraude (triche aux examens, lors de vote, falsification de documents officiels, etc.)
- le cyber-whistleblowing : appelé aussi lanceur d'alerte ; il s'agit généralement d'une personne ou d'un groupe qui estime avoir découvert des éléments qu'il considère comme menaçants pour l'homme, la société, l'économie ou l'environnement et qui décide de les porter à la connaissance d'instances officielles.
- la cybercontrefaçon (musique, livre, jeux-vidéo, logiciels) et le cybermarché noir (achat en ligne de marchandises illégales)

- la cyberfinance criminelle
- la cyberpropagande
- la cyberusurpation d'identité
- le cybercambriolage (vol de données)
- le défaçage (modifier l'apparence d'un site, d'un blog, etc.)

1.4. Les cinq fonctions fondamentales d'un plan de cybersécurité :

Le Cybersecurity Framework (CSF) du National Institute of Standards and Technology (NIST) est un cadre méthodologique permettant aux entreprises d'aborder et traiter les risques de cyberattaques visant leurs infrastructures stratégiques, ainsi que de pouvoir échanger leurs bonnes pratiques sur la base d'un vocabulaire commun. C'est l'un des modèles les plus avancés au niveau pratique et, à ce titre, une référence mondiale en la matière.

Le CSF tire son origine d'une série d'attaques informatiques majeures ayant touché en 2013 des grandes entreprises, des médias et des réseaux sociaux ainsi que des organismes publics des États-Unis.

Révisé en 2017, le CSF définit les cinq fonctions fondamentales d'un plan de cybersécurité : identifier, protéger, détecter, répondre et rétablir (CIRB, 2017) :

- Identifier : développer la compréhension du point de vue organisationnel en vue de gérer la cybersécurité en termes de systèmes, ressources, données et capacités.
- Protéger : concevoir et déployer les mesures de protection adaptées pour assurer la continuité des services délivrés par des infrastructures critiques.
- Détecter : concevoir et déployer les actions adaptées pour détecter, lorsqu'ils surviennent, les événements mettant en péril la cybersécurité.
- Répondre : concevoir et déployer les actions nécessaires pour répondre aux événements mettant en péril la cybersécurité.
- Rétablir : concevoir et déployer les actions nécessaires pour tenir à jour des plans de résilience et pour restaurer des services ou infrastructures affectés par un cyberincident.

2. Les acteurs et politiques de cybersécurité de l'UE :

Tous les États de l'Union européenne ont défini une stratégie de cybersécurité et mis en place des organes et méthodes en vue de la concrétiser.

2.1. La stratégie européenne en Cybersécurité :

Certains pays, cependant, se distinguent par la maturité de leur approche, leurs plans ayant déjà connu diverses évolutions. C'est le cas en particulier de deux pays limitrophes de la Belgique : les Pays-Bas et le Luxembourg.

La comparaison des stratégies de ces différentes sources montre trois objectifs communs (CIRB, 2017) :

- assurer une protection adéquate des administrations publiques et des infrastructures critiques contre les cybermenaces ;
- accroitre la confiance des citoyens dans le cyberespace en luttant contre la cybercriminalité ;
- développer une compétence propre en cybersécurité.

La Stratégie de cybersécurité de l'Union européenne, présentée en 2013 et amendée en 2017, constitue le cœur de l'approche prônée par la Commission européenne pour protéger l'espace numérique, ses entreprises et ses utilisateurs.

En 2013, la Commission et la haute représentante de l'UE pour les affaires étrangères et la politique de sécurité ont présenté conjointement la Stratégie de cybersécurité de l'Union européenne. Cette stratégie visait à offrir un cyberespace ouvert, sûr et sécurisé à ses utilisateurs, tout en attribuant à cet égard un rôle important aux pouvoirs publics.

Dans cette perspective, la Commission a annoncé les mesures suivantes (CIRB, 2017) :

- le renforcement du mandat de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour la transformer en véritable Agence de l'UE pour la cybersécurité;
- l'instauration d'un système de certification de cybersécurité à l'échelle de l'UE;
- la mise en place d'un plan d'action relatif aux modalités de réaction aux crises et incidents de grande ampleur en matière de cybersécurité ;
- la création d'un Centre européen de recherche et de compétences en matière de

cybersécurité ;

- la mise en œuvre rapide de la directive européenne sur la sécurité des réseaux et des systèmes d'informations (ou directive NIS 17).

En avril 2015, la Commission européenne a communiqué son programme de sécurité pour la période courant jusqu'en 2020. Le programme apporte notamment une réponse à l'inquiétude croissante des citoyens européens face au terrorisme. Le programme pose comme objectif de travailler mieux et plus étroitement entre États membres, en fonction de trois priorités dont la cybercriminalité. Parmi ses actions clés, il prévoit de renforcer les outils de lutte contre ce phénomène en s'attaquant « *aux obstacles à la conduite des enquêtes pénales en ligne, en résolvant notamment la question de la compétence territoriale et en arrêtant des règles pour l'accès aux preuves et aux informations sur l'Internet* » (Commission européenne, 2015a).

En mai 2015, la Commission européenne a lancé sa Stratégie pour un marché unique numérique (ou Digital single market) qui vise à supprimer les obstacles pour exploiter pleinement les possibilités offertes par Internet. Les cybermenaces figurent au rang de ces obstacles (Commission européenne, 2015b).

Pour la Commission, il s'agit à ce niveau de défendre l'économie en ligne et, plus largement, la prospérité.

Les objectifs clés fixés par la Commission sur ce plan sont :

- accroître les capacités et la coopération ;
- faire de l'Union européenne un acteur de poids ;
- intégrer la cybersécurité dans les politiques de l'UE.

Enfin, en juillet 2016, la Commission européenne a annoncé le lancement d'un partenariat public-privé (PPP) axé sur la cybersécurité, dans le cadre de la stratégie pour le marché unique numérique.

L'UE investirait à ce titre 450 millions d'euros dans le PPP puisés dans le budget du programme pour la recherche et l'innovation Horizon 2020. Le secteur privé, représenté dans le PPP par l'Organisation européenne pour la cybersécurité (ECSO : European Cybersecurity Organisation) apporterait pour sa part une contribution trois fois plus élevée au PPP. Celui-ci devrait recruter ses membres parmi les centres de recherches, les universités ainsi que les administrations publiques nationales, régionales et locales. L'objectif du partenariat est de stimuler la coopération à un stade précoce du processus de recherche et d'innovation et de forger des solutions de cybersécurité applicables à différents secteurs tels que l'énergie, la santé, les transports et la finance Commission européenne (Commission européenne, 2016).

2.2. Adoption d'un règlement européen sur la cybersécurité :

Les institutions européennes ont réagi en septembre 2017 lors du premier Sommet européen consacré à l'économie numérique, organisé à Tallinn (Estonie), alors que les cybermenaces ont pris un tournant bien plus politique avec la multiplication d'interférences lors de processus électoraux (aux Etats-Unis et en France). Tandis que de nombreux pays du monde ont été victimes de cyberattaques majeures (WannaCry ou bien NotPetya).

Pourtant, ces mêmes institutions n'ont pas attendu 2017 pour commencer ce travail titanesque : En mars 2004, l'ENISA (l'agence européenne chargée de la sécurité des réseaux et de l'information) est créée à Héraklion, en Grèce. Dès 2013, la Commission a présenté une première stratégie articulée autour de cinq axes (cités ci-dessus). La même année, une proposition de Directive sur la sécurité des réseaux et des informations (Directive SRI) a été mise sur la table. Il s'agissait ni plus ni moins du premier texte législatif européen sur la cybersécurité, censé favoriser la coopération européenne dans le domaine, ainsi que le renforcement des standards de sécurité (Boucart, 2019).

Dans la voie des réformes adoptées par le législateur européen, les députés européens ont adopté, le mois de mars 2019, le règlement européen sur la cybersécurité nommé « Cybersecurity Act ». Le vote s'intègre dans une stratégie

européenne ayant pour objectif de renforcer le cadre juridique européeen relatif à la cybersécurité.

Ce dispositif de certification, premier du genre, s'appliquera aux produits, processus et services vendus dans les pays de l'Union Européenne (UE). Il promet une meilleure protection pour les consommateurs et des procédures plus simples pour les entreprises.

Le Cybersecurity Act est un acte juridique européen, de portée générale, obligatoire dans toutes ses dispositions. Les États membres sont donc tenus d'appliquer ces dernières telles qu'elles sont définies par le règlement.

Il s'agit d'un règlement d'application directe. Les Etats membres disposeront toutefois de deux ans pour se mettre en conformité avec les dispositions impactant leur organisation nationale (ANSSI, 2019b).

3. Cybersécurité en Afrique :

La dernière édition de l'Indice mondial de la cybersécurité établi par l'Union internationale des télécommunications recense pas moins de quinze pays africains parmi la catégorie des nations considérées aujourd'hui comme «matures» dans le domaine de la protection des actifs numériques.

On recense déjà plus de quatre cents millions d'internautes sur le Continent. Le e-commerce y progresse de plus en plus rapidement, avec un revenu de 16,5 milliards de dollars en 2017, selon le cabinet Statista, et les analystes de McKinsey & Company estiment que ce chiffre sera de 75 milliards de dollars en 2025 (Arpagian, 18/04/2019).

La cybermenace est bien réelle. La société de services numérique Serianu, basée à Nairobi au Kenya, a publié la 5e édition de son « Africa Cyber Security Report ». Dans cette étude, elle estime que pour l'année 2017 les cyberattaques dont ont été victimes les entreprises africaines a couté 3,5 milliards de dollars. Rien qu'au Nigeria, au Kenya, en Ouganda et en Tanzanie, ce coût annuel dépasse 1 milliard de dollars, dont 431 millions de dollars de coûts directs et 647 millions indirects.

Les premiers secteurs victimes sont les banques et services financiers, le gouvernement et l'administration publique, le commerce électronique, suivis par les transactions à partir de mobile, les télécommunications et les autres secteurs industriels. Globalement, 90 % des entreprises africaines se situent en dessous d'un *« seuil de pauvreté »* de la cybersécurité (security poverty line) (De Laubier, 2018).

3.1. Vulnérabilité de l'Afrique aux cybermenaces :

De nouveaux défis se posent en Afrique parallèlement à cette croissance, et l'augmentation de l'utilisation des technologies présente ses propres vulnérabilités et risques. L'un de ces risques, qui découle de l'augmentation de l'utilisation des

technologies et nécessite une attention et des mesures urgentes, est la cybercriminalité.

La cybercriminalité est un phénomène mondial en pleine croissance qui, selon un rapport publié par Symantec Corporation en 2013, augmente plus rapidement en Afrique que dans toute autre région du monde (Symantec Corporation, 2013).

En effet, les experts de la cybersécurité estiment que, sur le continent africain, 80% des ordinateurs personnels sont infectés par des virus et autres logiciels malveillants (Gacy, 2010).

Les cybercriminels ont longtemps considéré l'Afrique comme un lieu providentiel pour commettre leurs actes criminels. Les statistiques provenant de diverses sources indiquent que l'Afrique est très vulnérable aux cybermenaces en raison du nombre élevé de domaines à faible sécurité des réseaux et de l'information. Par exemple, selon la Rapport Norton sur la cybercriminalité, chaque seconde, 18 adultes sont victimes de la cybercriminalité, soit plus de 1,5 million de victimes dans le monde par jour.

La récente utilisation des technologies de l'information et des communications (TIC) pour faciliter les attaques terroristes en Afrique ajoute une dimension supplémentaire à la question de la cybersécurité. Les données recueillies lors de l'enquête sur l'attaque récente du centre commercial Westgate au Kenya, et les activités de Boko Haram au Nigéria et d'Al-Qaida au Maghreb islamique (AQMI) en Afrique du Nord mettent en évidence l'utilisation des TIC dans la planification, la coordination et la mise en œuvre de ces attaques ainsi que dans leur retentissement médiatique. Ces attaques ont déstabilisé et entravé la récente croissance économique des pays africains.

3.2. Les défis de la cybersécurité en Afrique :

L'Afrique est face à plusieurs défis liés à Internet: risque pour la sécurité, viol de la propriété intellectuelle et protection des données personnelles. Les cybercriminels ciblent des particuliers à l'intérieur et à l'extérieur de leurs frontières nationales et les gouvernements africains n'ont pas les moyens techniques et financiers de cibler et de suivre les échanges électroniques jugés sensibles pour la sécurité nationale. Ces défis sont les suivants (CEA, 2014):

- Faiblesse du niveau des dispositions de sécurité nécessaires pour prévenir et maîtriser les risques technologiques et informationnels.
- Manque de savoir-faire technique en matière de cybersécurité et incapacité de surveiller et de défendre les réseaux nationaux, rendant les pays africains vulnérables au cyberespionnage ainsi qu'au cyberterrorisme.
- Incapacité à mettre en place les cadres juridiques nécessaires pour lutter contre la cybercriminalité. Une enquête menée par la CEA19 auprès de 21 pays a permis de constater que si de nombreux pays ont proposé des

législations, peu de systèmes de sécurité permettant de lutter contre la cybercriminalité ont été installés, tant dans le secteur privé que dans le secteur public.

- Les enjeux de la cybersécurité ont une portée plus large que ceux de la sécurité nationale. Pourtant, peu d'initiatives majeures ont été mises en œuvre en Afrique dans le domaine de la cybersécurité. Alors que les TIC sont saluées comme la panacée aux nombreux problèmes de l'Afrique, la cybersécurité est une question cruciale qui doit être abordée plus en profondeur.
- Il est nécessaire de mettre en place une société de l'information qui respecte les valeurs, les droits et les libertés et qui garantit l'égalité d'accès à l'information tout en encourageant la création de connaissances authentiques et en renforçant la confiance dans l'utilisation des TIC en Afrique.
- D'une manière générale, les parties prenantes, comme les organes de réglementation des TIC, les organismes chargés de l'application des lois, la justice, les professionnels de la technologie de l'information et les utilisateurs sont peu conscients des problèmes de sécurité liés aux TIC.

3.3. La Convention de l'Union africaine sur la cybersécurité :

La Commission de l'Union africaine (CUA) et la Commission Economique pour l'Afrique (CEA) ont chapeauté les efforts de développement de la Convention de l'Union africaine sur la cybersécurité, qui a fait l'objet d'une série d'examens par les communautés économiques régionales puis a été entérinée par la Conférence ordinaire de l'Union africaine en charge des technologies de l'information et des communications en septembre 2012 à Khartoum, et enfin adoptée par le Sommet des chefs d'État et de gouvernement de l'Union africaine du 27 juin 2014 à Malabo (Guinée Equatoriale). Il est attendu, par conséquent, à ce que les pays dotés d'une législation sur la cybersécurité la transposent dans le cadre de la Convention et que ceux qui n'en n'ont pas encore doivent s'en doter.

Cette convention a été adoptée par les chefs d'états africains, étant convaincus de la nécessité de mobiliser l'ensemble des acteurs publics et privés (États, collectivités locales, entreprises du secteur privé, organisations de la société civile, médias, institutions de formation et de recherche etc.) en faveur de la cybersécurité. Elle détermine les règles de sécurité essentielles à la mise en place d'un espace numérique de confiance pour les transactions électroniques, la protection des données à caractère personnel et la lutte contre la cybercriminalité.

La convention comporte quatre chapitres :

- Les transactions électroniques,
- La protection des données à caractère personnel,
- Promotion de la cybersécurité et lutte contre la cybercriminalité,

- Dispositions finales.

Concernant la promotion de la cybersécurité et lutte contre la cybercriminalité, et au sujet de **la Politique nationale,** chaque État Partie s'engage en collaboration avec les parties prenantes, à se doter d'une politique nationale de cyber sécurité qui reconnaisse l'importance de l'infrastructure essentielle de l'information (IEI) pour la nation, qui identifie les risques auxquels elle est confrontée en utilisant une approche tous risques et qui définit dans les grandes lignes la façon dont les objectifs seront mis en œuvre.

Quant à la **Stratégie nationale**, les États Parties s'engagent à adopter les stratégies qu'ils jugent appropriées et suffisantes pour mettre en œuvre la politique nationale de cyber sécurité, spécifiquement dans le domaine de la réforme législative et du développement, de la sensibilisation et du développement des capacités, du partenariat public privé et de la coopération internationale, pour ne citer que ceux-ci. Les stratégies devront établir des structures organisationnelles et se fixer des objectifs ainsi que des délais pour mener à bien tous les aspects de la politique de cyber sécurité, tout en posant les bases d'une gestion effective des incidents et de la coopération internationale (Union Africaine, 2014).

En ce qui concerne **la coopération internationale**, la convention stipule que (Union Africaine, 2014) :

- Les États Parties s'engagent à garantir que les mesures législatives et/ou réglementaires adoptées pour lutter contre la cybercriminalité renforcent la possibilité d'harmonisation régionale de ces mesures et respectent le principe de la double incrimination.
- Les États Parties qui n'ont pas de conventions d'assistance mutuelle en matière de cybercriminalité s'engagent à encourager la signature des conventions d'entraide judiciaire en conformité avec le principe de la double incrimination tout en favorisant les échanges d'informations ainsi que le partage efficient des données entre les organisations des États membres sur une base bilatérale et multilatérale.
- Les États Parties s'engagent à encourager la mise en place des institutions qui échangent des informations sur les cybermenaces et sur l'évaluation de la vulnérabilité telles que les équipes de réaction d'urgence en informatique (CERT: Computer Emergency Response Teams) ou les équipes de réaction aux incidents de sécurité informatique (CSIRTS: Computer Security Incident Response Teams).
- Les États Parties s'engagent à se prévaloir de moyens existants pour la coopération internationale aux fins de répondre aux cybermenaces, à améliorer la cybersécurité et à stimuler le dialogue entre les parties prenantes. Ces moyens pourraient être internationaux, intergouvernementaux ou régionaux, ou basés sur des partenariats privés et publics.

4. Une stratégie continentale en Afrique fait défaut:

Partons du constat selon lequel les technologies de l'information et de la communication (TIC) se développent, aux pays de l'Afrique, non seulement à un rythme infiniment plus rapide que les réformes juridiques, mais qu'elles évoluent également dans un environnement marqué par un vide juridique, car les lois existantes ne sont plus pertinentes.

Cela nous conduit à une situation paradoxale dans la mesure où les règles afférentes au fonctionnement des TIC sont définies et imposées, non pas par l'Etat, mais par des acteurs nationaux et étrangers dominant le secteur, ainsi que par les cybercriminels.

Depuis l'adoption de la Convention de Malabo sur la cybersécurité, une toute petite minorité d'Etats africains l'ont ratifiée. Or la seule souveraineté numérique d'un pays ne suffira pas à le protéger contre les cyberattaques qui, en 2017, ont fait perdre au Continent 3,5 milliards de dollars. Et le fléau n'ira qu'en empirant si la défense ne s'organise pas mieux.

La Convention de l'Union africaine (UA) sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo), fut élaborée sur le modèle de celle du Conseil de l'Europe. L'échéance des dernières signatures était fixée au 14 mars 2018. Or, force est constater que seuls 10 pays sur les 55 de l'Afrique ont signé cette convention (18 % seulement) : Bénin, Tchad, Comores, Congo, Ghana, Guinée-Bissau, Mauritanie, Sierra Leone, São Tomé-et-Príncipe et Zambie (De Laubier, 2018).

Nous notons ici l'absence totale des pays nord-africains qui n'ont pas adopté une stratégie unifiée en matière de cybersécurité au niveau régional ni continental, ce qui les rend vulnérables, d'une façon permanente, aux cyberattaques.

A noter aussi que les outils de cybersécurité utilisés pour protéger les réseaux dans les pays africains tel l'Algérie sont étrangers, il faut savoir qu'il n'y a de sécurité réelle que si l'origine des outils et des solutions de sécurité est nationale.

Selon des experts de la criminalité, le problème est que les lois existantes se sont figées alors que les crimes en ligne connaissent une constante évolution et adaptation aux mesures de sécurité. La loi algérienne d'août 2009 sur la cybercriminalité dont les points saillants sont la création d'un organe national de coordination, l'usage des données électroniques par la justice, la surveillance des communications électroniques à des fins préventives et la coopération internationale nécessite une adaptation à la «vitesse des crimes électroniques».

L'Algérie connaît un retard certain dans la production de solutions nationales de cybersécurité et surtout dans la mise en place de son cadre juridique et organisationnel (DERDOURI, 2015).

Mais signalons, néanmoins, que l'Algérie entretient des relations de coopération bilatérale, multilatérale en matière des TIC d'une manière générale y compris la cybersécurité. En effet, elle a signé la convention des Nations Unies

contre la criminalité transnationale organisée le 12 décembre 2000 et elle l'a ratifié le 7 octobre 2002. Elle a ratifié la convention arabe de de lutte contre les crimes liées aux technologies d'information faite au Caire le 21 décembre 2010. La cybercriminalité a aussi été l'objet de coopération bilatérale avec la France, et ce, notamment, par le Décret n° 2008-373 du 18 avril 2008 portant publication de l'accord entre la France et l'Algérie relatif à la coopération en matière de sécurité et de lutte contre la criminalité organisée, signé à Alger le 25 octobre 2003.

Depuis la promulgation de la loi 09-04 du 5 août 2009, portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, l'Algérie n'a cessé d'investir dans la cyberdéfense et les nouveaux systèmes d'information, notamment à travers le durcissement des crimes et délits commis par les moyens des technologies de l'information et de la communication, incluant même les actes malveillants commis au moyen de la téléphonie mobile **(BELGACEM,** 2017).

5. CONCLUSION:

Le fait que les européens aient voté la directive sur la sécurité des réseaux et des informations (SRI) et le règlement européen sur la cybersécurité (Cybersecurity Act), montre bien que le principe même d'une coordination européenne dans un domaine aussi sensible et stratégique ne fait pas vraiment débat, l'ensemble des pays européens semblent avoir compris que la cybersécurité est un pilier fondamental du développement d'un marché unique numérique, véritable nouvelle impulsion du projet européen dans les prochaines années.

En Afrique, le dispositif de lutte contre la criminalité liée aux technologies de l'information et de la communication (TIC) reste incomplet, comparé aux standards internationaux ou aux expériences étrangères pionnières en la matière. Ceci, notamment, sur le plan de l'actualisation des textes législatifs et réglementaires et sur le plan de la coopération internationale. Il est donc de la responsabilité des autorités publiques des pays africains d'entreprendre les actions nécessaires pour assurer une sécurité des outils et réseaux numériques. Il s'agit d'instaurer un climat de confiance propice à faire profiter chacun du meilleur des technologies aujourd'hui à sa disposition.

En conclusion finale, la cybersécurité ne connait pas de frontières et, compte tenu de sa dimension mondiale, il est difficile de prendre des mesures au seul niveau national. La lutte contre les atteintes à la cybersécurité nécessite une coopération à tous les niveaux, entre les pays et les organisations internationales, et entre les secteurs public et privé. Par conséquent, un cadre global de coopération et de sensibilisation internationales doit être mis en place, et la lutte contre la cybercriminalité exige des stratégies coordonnées et ciblées.

6. Références bibliographiques

Ouvrages et thèses :

EL OUAZZANI S., (2016). « *Analyse des politiques publiques en matière d'adoption du Cloud Computing et du Big data. Une Approche comparative des modèles français et marocain* ». Université Paris-Saclay, p.49.

TENEZE N. , (2018). « *Combattre les cyberagressions* ». Nuvis Editions, Paris.

Articles :

ARPAGIAN N. (2019). *« Faire de la cybersécurité un atout de l'économie africaine* ». La tribune Afrique. (consulté le 23/01/2020). Disponible sur https://afrique.latribune.fr/think-tank/tribunes/2019-04-18/faire-de-la-cybersecurite-un-atout-de-l-economie-africaine-tribune-814365.html

BELGACEM F. (12 juillet 2017). « *Cybersécurité : l'Algérie gagne 36 places* ». Liberté (quotidien indépendant). (consulté le 26/01/2020). Disponible à l'adresse https://www.liberte-algerie.com/actualite/cybersecurite-lalgerie-gagne-36-places-273422

BOUCART T. , (2019). « *L'émergence d'une politique européenne de cybersécurité* ». Magazine Le Taurillon, Disponible sur https://www.taurillon.org/l-emergence-d-une-politique-europeenne-de-cybersecurite . (consulté le 23/01/2020).

COLLINS K., (2016). « *Ukraine blackout is a cyberattack milestone. CNET – Security, CNET, CBS Interactive* ». Disponible sur https://www.cnet.com/news/cyberattack-causes-widespread-powerblackout-in-ukraine/ .(consulté le 23/01/2020).

DE LAUBIER C. (2018). « *L'Afrique se met en ordre de bataille contre la cybermalveillance et la cybercriminalité* ». CIO-mag (magazine). (consulté le 23/01/2020). Disponible à l'adresse https://cio-mag.com/lafrique-se-met-en-ordre-de-bataille-contre-la-cybermalveillance-et-la-cybercriminalite/

DERDOURI A., (28 avril 2015). « *Une loi pour la cybersécurité en Algérie* ». Le soir d'Algérie (quotidien indépendant), pp.6-7.

Gacy F., (2010). «*Foreign policy: Africa's internet threat*». National Public Radio. (consulté le 25/01/2020). Disponible à l'adresse www.npr.org/templates/story/story.php?storyId=125297426 .

Documents divers :

Agence nationale de la sécurité des systèmes d'information (ANSSI) , (2019a). « *Glossaire »*. Secrétariat général de la défense et de la sécurité nationale, République française. Site Internet de l'ANSSI, (consulté le 22/01/2020). Disponible sur https://www.ssi.gouv.fr/entreprise/glossaire/c/ .

Agence nationale de la sécurité des systèmes d'informatique (ANSSI), (2019b). « *Adoption définitive du Cybersecurity Act : un succès pour l'autonomie stratégique européenne* ». Disponible sur https://www.ssi.gouv.fr/actualite/adoption-definitive-du-cybersecurity-act-un-succes-pour-lautonomie-strategique-europeenne/ .(consulté le 22/01/2020).

Commission européenne, (2013). « *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé* ». Haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité. Bruxelles, en ligne Disponible sur http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_fr.pdf . (consulté le 22/01/2020).

Commission européenne, (2015a). « *La Commission prend des mesures pour renforcer la coopération au sein de l'UE contre le terrorisme, la criminalité organisée et la cybercriminalité* ». Communiqué de presse. Strasbourg, en ligne Disponible sur http://europa.eu/rapid/pressrelease_IP-15-4865_fr.htm . (consulté le 23/01/2020).

Commission européenne, (2015b). « *Digital skills for the Digital Single Market* ». Site Internet de la Commission européenne, en ligne Disponible sur https://ec.europa.eu/digital-single-market/en/opening-workshop-digital-skills-digital-single-market . (consulté le 23/01/2020).

Commission européenne, (2016). « *La Commission signe un accord avec le secteur de la cybersécurité et redouble d'efforts pour lutter contre les cybermenaces* ». Communiqué de presse. Bruxelles, en ligne Disponible sur http://europa.eu/rapid/press-release_IP-16-2321_fr.htm . (consulté le 23/01/2020).

Commission européenne, (2017). « *Proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité)* ». Direction générale des réseaux de communication, du contenu et des technologies. Cybersecurity Package, site internet de la Commission européenne, en ligne Disponible sur https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en . (consulté le 22/01/2020).

Les cahiers du CIRB, (2017). « *Vers un plan régional de cybersécurité, Centre d'Informatique pour la Région Bruxelloise* ». P.11. Disponible sur https://cirb.brussels/fr/quoi-de-neuf/publications/cahiers/vers-un-plan-regional-de-cybersecurite-septembre-2018 . (consulté le 20/01/2020).

Nations Unies, Commission Economique pour l'Afrique (CEA), (2014). « *Les défis de cybersécurité en Afrique* ». Note d'orientation. Disponible à l'adresse :

https://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1_fr.pdf . (consulté le 28/01/2020).

Symantec Corporation, (2013). «*Internet Security Threat Report 2013*». Volume 18. Disponible à l'adresse https://www.insight.com/content/dam/insight/en_US/pdfs/symantec/symantec-corp-internet-security-threat-report-volume-18.pdf . (consulté le 24/01/2020).

Symantec Corporation, (2016). «*Cybersecurity in Healthcare : Why It's Not Enough, Why It Can't Wait* » . (Infographie). Symantec – Healthcare Symante. Disponible sur https://www.symantec.com/content/dam/. (consulté le 22/01/2020). symantec/docs/infographics/symantec-healthcare-it-security-risk-management-study-en.pdf .

Union Africaine, (2014). « *Convention de l'Union Africaine sur la cyber sécurité et la protection des données à caractère personnel* ». Article 24 : Cadre de la cyber sécurité nationale, p.27. Disponible à l'adresse : https://www.afapdp.org/wp-content/uploads/2018/06/CONV-UA-CYBER-PDP-2014.pdf . (consulté le 28/01/2020).

Union internationale des télécommunications (UIT) , (2010). « *Les décisions phares de Guadalajara : cybersécurité* ». Compte-rendu en ligne de la Conférence de plénipotentiaires de l'UIT 2010 à Guadalajara, Nouvelles de l'UIT, UIT. Disponible sur http://www.itu.int/net/itunews/issues/2010/09/20-fr.aspx. (consulté le 22/01/2020).