Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de la CEDEAO

SECTION I. INTRODUCTION

La transformation numérique rapide en cours en Afrique de l'Ouest est d'une grande importance pour améliorer le fonctionnement et l'efficacité des administrations, des politiques publiques et des économies, ainsi que le bien-être des populations. Cependant, les menaces et les risques croissants auxquels sont confrontés le cyberespace mondial et les réseaux, les systèmes d'information et les données numériques peuvent considérablement réduire les bénéfices attendus de ces politiques numériques, et porter gravement atteinte aux intérêts des Nations, à leurs économies, leurs institutions et leurs populations.

Face à ces menaces et risques, il convient d'opposer des dispositifs nationaux de cybersécurité et de lutte contre la cybercriminalité robustes, avec une bonne coordination entre les services concernés, des mécanismes de réponse efficaces aux cyberattaques, des experts et des utilisateurs du numérique sensibilisés et formés aux bonnes pratiques, une participation active du secteur privé, une protection renforcée des services numériques et des infrastructures les plus essentiels ou les plus critiques, ainsi qu'une entraide régionale et une coopération internationale.

Force est de constater qu'au sein de la région, ces exigences sont encore loin d'être satisfaites. Si quelques pays ont déjà mis en place les dispositifs nécessaires et atteint un certain degré de préparation, la plupart des autres pays ont encore un niveau insuffisant, constituant une faiblesse qui met en danger leurs Nations autant que le reste de la région. En outre, tous les pays font face à une pénurie d'expertise dans ces domaines. Ils sont donc encouragés à développer les cursus de formation à la cybersécurité et à atteindre un niveau minimal en matière de cybersécurité et de lutte contre la cybercriminalité.

Par ailleurs, l'hétérogénéité des dispositifs en place dans les différents pays limite considérablement toute tentative de coopération régionale. Leur harmonisation doit donc être recherchée : les liens et échanges seraient plus faciles et efficaces entre des institutions ayant des périmètres de responsabilité et des modes de fonctionnement comparables ; des exigences et procédures identiques permettraient d'assurer la protection des infrastructures transnationales de la même manière dans toute la région ; enfin, des dispositions pénales et de procédure pénale harmonisées rendraient possible une véritable entraide judiciaire.

Dans ce domaine, la CEDEAO a mis en place depuis 2010 des dispositions d'harmonisation : l'acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO fixe notamment les obligations de sécurité qui incombent aux responsables du traitement de telles données pour en assurer la confidentialité ; l'acte additionnel A/SA.2/01/10 portant transactions électroniques dans l'espace de la CEDEAO fixe les conditions d'admission de la signature électronique ; enfin, la Directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO adapte le droit pénal et la procédure pénale des États membres au phénomène de la cybercriminalité.

Au niveau du continent, la Convention de l'Union africaine de 2014 sur la cybersécurité et la protection des données à caractère personnel, dite Convention de Malabo, fixe les mesures de cybersécurité et de lutte contre la cybercriminalité à prendre au niveau national. Au niveau mondial, la Convention de 2001 sur la cybercriminalité, dite Convention de Budapest, ouverte à la signature de tous les pays, vise à mener une politique pénale commune par l'adoption d'une législation adaptée, à intensifier la coopération entre les États en matière pénale et à adopter des pouvoirs suffisants pour permettre une lutte efficace contre la cybercriminalité.

La présente Stratégie régionale a pour objectif de tirer le meilleur profit de ces avancées, d'améliorer le niveau des dispositifs nationaux de cybersécurité et de lutte contre la cybercriminalité, et de développer la coopération et l'entraide entre les États Membres de la région. Elle s'appuie sur les meilleures pratiques internationalement reconnues dans ces domaines.

Ces objectifs doivent être atteints sans préjudice des libertés fondamentales et des droits de l'homme et des peuples contenus dans les déclarations, conventions et autres instruments adoptés au niveau régional, continental et international.

SECTION II. CONSIDERATIONS GENERALES

A. Objectif général

L'objectif général de cette stratégie est d'établir le cadre stratégique communautaire à prendre en compte par les États Membres dans leurs stratégies nationales et à mettre en œuvre dans leurs plans d'action sur la cybersécurité et la lutte contre la cybercriminalité avant fin 2022, avec la pleine participation de la Commission de la CEDEAO au profit des États membres de cette Communauté.

B. Définitions

Au sens de la présente Stratégie régionale, on entend par :

CSIRT (*Computer Security Incident Response Team*) : équipe chargée d'alerter sur les menaces, de prévenir les risques sur les systèmes d'information, de réagir en cas d'incident de sécurité et d'aider à en atténuer les effets ;;

Cybercriminalité : les activités criminelles dont les ordinateurs et systèmes informatiques constituent soit l'arme soit la cible principale. La cybercriminalité recouvre les délits habituels (fraude, contrefaçon, usurpation d'identité ….), les délits liés au contenu (fichiers pédopornographiques, incitation à la haine raciale ...) et les délits spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service, logiciel malveillant …) ;

Cyberespace : le réseau interdépendant des infrastructures utilisant les technologies de l'information, comprenant notamment l'Internet, les réseaux de télécommunications, les systèmes d'information et les objets connectés ;

Cybersécurité : l'ensemble des mesures et des actions destinées à protéger le cyberespace des menaces associées à ses réseaux et à son infrastructure informatique ou susceptibles de leur porter atteinte. 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 ;

Donnée numérique : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;

Hygiène informatique : l'ensemble des bonnes pratiques que chaque acteur du numérique devrait respecter afin de préserver la sécurité du système d'information qu'il utilise ou pour lequel il assure une fonction d'administrateur ;

Infrastructure critique : une infrastructure ou un processus public ou privé dont la destruction, l'arrêt, l'exploitation illégitime ou la perturbation pendant une période de temps définie pourrait entraîner soit des pertes de vies humaines, soit des pertes importantes pour l'économie, ou porter un préjudice considérable à la réputation de l'État ou de ses symboles de gouvernance. Dans cette définition, l'infrastructure comprend les réseaux et systèmes et les données physiques ou numériques indispensables pour fournir ce service. Cette expression peut faire référence à un système ou processus dont le fonctionnement est critique au sein de l'organisation ;

Opérateur d'infrastructure critique : opérateur public ou privé qui opère une infrastructure critique ;

Opérateur de service essentiel : opérateur public ou privé qui fournit un service essentiel ;

Protection des infrastructures critiques : l'ensemble des mesures et des actions destinées à protéger les infrastructures critiques de l'ensemble des risques et menaces susceptibles de provoquer l'interruption totale ou partielle des services essentiels qu'elles fournissent ;

Protection des services essentiels : l'ensemble des mesures et des actions destinées à protéger les services essentiels de l'ensemble des risques et menaces susceptibles de provoquer leur interruption totale ou partielle ;

Service essentiel : un service dont l'interruption totale ou partielle pourrait avoir un impact grave sur le fonctionnement de l'État, sur l'économie du pays ou sur la santé, la sûreté, la sécurité et le bien-être de la population, ou une combinaison d'impacts de cette nature qui, pris individuellement, ne suffiraient pas à classer essentiel le service considéré ;

Réseaux : ensemble des moyens assurant l'alimentation d'une infrastructure en produits ou services nécessaires à son fonctionnement (communications, énergie, logistique, etc.) ;

Système d'information : tout dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou partie, un traitement automatisé de données en exécution d'un programme ;

Technologies de l'Information et de la Communications (TIC): technologies employées pour recueillir, stocker, utiliser et envoyer des informations et incluant celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication y compris de télécommunication.

SECTION III. OBJECTIF STRATEGIQUE 1 : FORMULER UNE POLITIQUE NATIONALE ET UNE STRATEGIE NATIONALE DE CYBERSECURITE ET DE LUTTE CONTRE LA CYBERCRIMINALITE

Chaque État Membre devrait adopter et mettre à jour au moins tous les cinq ans une politique nationale et une stratégie nationale de cybersécurité et de lutte contre la cybercriminalité[1], prenant en compte la présente Stratégie régionale et fixant pour chacun de ces deux domaines :

- la situation du pays et les défis auxquels il fait face ;
- la vision politique du pays ;
- les objectifs stratégiques à atteindre, les délais et les priorités ;
- la gouvernance, les rôles et les responsabilités ;
- les objectifs en matière de :
    - renforcement des dispositions législatives et règlementaires ;
    - normes, standards et référentiels d'exigences ;
    - sécurité des infrastructures critiques et des services essentiels ;
    - renforcement du cadre institutionnel ;
    - capacités techniques et ressources humaines qualifiées à acquérir ;
    - sensibilisation, de communication, d'éducation et de formation ;
    - prévention des menaces et gestion des risques ;
    - signalement des incidents de sécurité ;
    - détection et attribution des attaques ;
    - réaction en cas d'attaque ;
    - développement d'un écosystème de cybersécurité et de lutte contre la cybercriminalité ;
    - synergie des actions à l'échelle nationale, concertation et coordination nationale ;
    - coopération régionale et internationale ;
- les actions à mener pour atteindre ces objectifs, les acteurs concernés, les échéances et les budgets estimatifs ;
- les moyens destinés à renforcer les institutions et les capacités et à en garantir la pérennité.

Chaque État Membre devrait définir un mécanisme de suivi et d'évaluation au moins annuel des actions prévues par sa stratégie nationale de cybersécurité et de lutte contre la cybercriminalité.

[1] La politique nationale et la stratégie nationale peuvent faire l'objet de documents séparés, ou d'un unique document de stratégie nationale qui indique la vision et les objectifs politiques du pays.

SECTION IV. OBJECTIF STRATEGIQUE 2 : RENFORCER LA CYBERSÉCURITÉ AVEC UN CYBERESPACE SÛR ET SÉCURISÉ

Sous-objectif 2.1. Établir une Autorité nationale de cybersécurité

Chaque État Membre devrait établir et désigner une autorité nationale de cybersécurité, disposant des pouvoirs et des moyens nécessaires pour assurer les fonctions suivantes, soit directement, soit par délégation d'une autorité gouvernementale (si possible interministérielle[2]) :

- la gouvernance globale du dispositif national de cybersécurité (définition de la politique nationale et des politiques sectorielles de cybersécurité, élaboration de la stratégie nationale et des stratégies sectorielles, suivi des plans d'action, élaboration des textes législatifs et règlementaires, coordination des tâches liées à la cybersécurité, pilotage des dispositifs de prévention et de réaction, animation des échanges avec les parties prenantes publiques et privées, etc.) ;
- l'animation du dispositif national de cybersécurité, notamment au travers du CSIRT national ;
- la coordination avec les autorités en charge de la lutte contre la cybercriminalité ;
- la transposition des actes communautaires en matière de cybersécurité dans les textes nationaux ;
- le contrôle de la bonne application des Conventions internationales, des actes communautaires, de la présente Stratégie régionale et des dispositions législatives et réglementaires nationales en matière de cybersécurité ;
- le rôle de point de contact principal pour la coopération régionale et internationale.

L'autorité nationale de cybersécurité devrait pouvoir exercer sa mission sur l'ensemble des secteurs d'activité (services de l'État Membre, télécommunications, énergie, santé, transports, banques …), en liaison avec les autorités sectorielles compétentes et sans préjudice des pouvoirs dévolus à ces autorités.

Sous-objectif 2.2. Établir des capacités d'alerte et de réaction en cas d'incident (CSIRT)

Chaque État Membre devrait disposer d'un CSIRT national :

- Devant couvrir en priorité les services de l'État Membre, les infrastructures critiques et les services essentiels (les "bénéficiaires prioritaires") ;
- Chargé d'animer et de coordonner le réseau de CSIRT sectoriels, s'il en existe, en recherchant toutes les synergies et subsidiarités possibles ;
- Capable d'assurer au moins les fonctions suivantes :
  - rechercher et diffuser les alertes (vulnérabilités, risques, incidents), les mesures de contournement des menaces, des guides et des bonnes pratiques ;
  - Suivre les incidents au niveau national ;
  - Traiter les incidents affectant les bénéficiaires prioritaires ;
  - Participer aux réseaux régionaux et mondiaux des CSIRT ;
  - Coordonner les réactions et la gestion de crise, en liaison avec les autorités, en cas d'attaque majeure ;
  - Recueillir les flux de renseignements pertinents ;
  - Incorporer les systèmes et technologies pertinents pour collecter et analyser rapidement les données pertinentes ;
  - Établir un centre d'appel pour signaler les cyberattaques.
- doté des moyens nécessaires (financiers, locaux et système d'information sécurisés, effectif suffisant pour assurer une disponibilité permanente, personnel compétent, capacités de forensic, procédures, site Internet …).

Chaque État Membre devrait encourager la constitution de CSIRT sectoriels, destinés à assurer notamment, de manière mutualisée au profit des opérateurs de certains secteurs d'activité, la recherche et la diffusion des

[2] Cependant, en raison du manque de ressources, des changements rapides et du besoin d'être rapidement à niveau, il est recommandé que les États petits et moyens établissent une autorité centrale, qui travaillera avec tous les autres ministères, plutôt que de créer de grands comités interministériels qui peuvent parfois retarder la progression.

alertes sur les systèmes et applications numériques propres à ces secteurs d'activité, et le traitement des incidents. Il est recommandé de colocaliser les CSIRT pour assurer un dialogue ouvert et un enrichissement intersectoriel.

Sous-objectif 2.3. Mettre en œuvre une approche de gestion des risques

Chaque État Membre devrait adopter et faire adopter par chaque opérateur concerné une approche de gestion des risques, tant au niveau stratégique qu'au sein des organismes publics et privés, afin d'assurer au juste niveau nécessaire la sécurité des réseaux, systèmes d'information et données numériques.

Chaque État Membre devrait veiller à ce que les responsables de la cybersécurité, quel qu'en soit le niveau, bénéficient du soutien hiérarchique nécessaire pour que leurs analyses et recommandations soient prises en considération par les décideurs.

Sous-objectif 2.4. Renforcer la cybersécurité des infrastructures critiques et des services essentiels

Chaque État Membre devrait prioriser ses efforts en matière de cybersécurité sur ses infrastructures critiques et sur les services essentiels.

Chaque État Membre devrait se doter d'une procédure d'identification des réseaux, systèmes d'information et données numériques essentiels pour le fonctionnement des infrastructures critiques et la fourniture des services essentiels.

Chaque État Membre devrait imposer aux opérateurs publics et privés qui ont la responsabilité des infrastructures critiques et des services essentiels des mesures concrètes pour assurer la sécurité de ces réseaux, systèmes d'information et données numériques, parmi lesquelles notamment les mesures minimales suivantes :

- le respect des mesures d'hygiène informatique reconnues internationalement ;
- un audit de sécurité des systèmes d'information par un organisme qualifié, à une périodicité n'excédant pas deux ans ;
- la notification des incidents de sécurité à l'autorité nationale de cybersécurité ou au CSIRT national (via son éventuel CSIRT sectoriel).

Sous-objectif 2.5. Adopter des politiques de sécurité des systèmes d'information

Chaque État Membre devrait imposer aux services de l'État et aux opérateurs d'infrastructures critiques et de services essentiels, et recommander aux autres opérateurs, d'élaborer et d'appliquer des politiques de sécurité décrivant les dispositions qu'ils prévoient pour assurer la sécurité de leurs systèmes d'information (responsabilités, organisation, ressources humaines dédiées, équipement de cybersécurité, procédures de protection, de détection et de réaction aux attaques, etc.).

Sous-objectif 2.6. Établir un référentiel général de sécurité

Chaque État Membre devrait établir un référentiel général de sécurité fixant les exigences minimales en matière de sécurité des systèmes d'information (gouvernance, organisation, politique de sécurité des systèmes d'information, cartographie des systèmes, exigences techniques, etc.) et désigner dans un document ayant force juridique les organismes qui y sont soumis.

Sous-objectif 2.7. Assurer le développement des compétences en matière de cybersécurité

Chaque État Membre devrait veiller à la constitution d'une ressource humaine qualifiée suffisante formée aux différents aspects de la cybersécurité :

- en introduisant des cursus de formation dans les différents domaines relatifs à la cybersécurité (technique, juridique, etc.) dans ses programmes d'enseignement, notamment universitaire et professionnel ;
- en promouvant le renforcement des compétences en cybersécurité chez tous les professionnels des technologies de l'information et de la communication ;
- en encourageant la recherche et l'innovation dans le domaine de la cybersécurité ;
- en intégrant des exigences de connaissances éprouvées en matière de cybersécurité dans les appels d'offres de services des gouvernements.

Sous-objectif 2.8. Assurer le développement de l'écosystème de cybersécurité

Chaque État Membre devrait veiller à favoriser la création d'organismes publics et privés aptes à apporter une assistance aux opérateurs en matière de cybersécurité (fourniture de solutions sécurisées, sécurisation des systèmes d'information, conseil, audit, traitement d'incidents, etc.).

SECTION V. OBJECTIF STRATEGIQUE 3 : REDUIRE LA CYBERCRIMINALITE PAR UN ENVIRONNEMENT ADAPTE ET LA CAPACITE DE TRADUIRE LES DELINQUANTS EN JUSTICE

Sous-objectif 3.1. Adopter des dispositions pénales et de procédures pénales

Chaque État Membre devrait adopter les dispositions pénales et de procédure pénale prescrites ou recommandées au niveau régional, continental et mondial.

Chaque État Membre devrait adopter des sanctions proportionnées pour les infractions pénales ayant affecté ou tenté d'affecter les systèmes d'information et données nécessaires au bon fonctionnement d'infrastructures critiques et de services essentiels.

Sous-objectif 3.2. Mettre en place des capacités de lutte contre la cybercriminalité

Chaque État Membre devrait se doter des capacités minimales suivantes de lutte contre la cybercriminalité :
- Une unité opérationnelle de lutte contre la cybercriminalité au moins ;
- Une autorité de coordination s'il dispose de plusieurs unités de lutte contre la cybercriminalité ;
- Un laboratoire d'investigation numérique au moins ;
- Des capacités de recueil de preuves numériques ;
- Des procédures d'investigation et de recueil et de traitement des preuves numériques ;
- Des enquêteurs de l'État Membre (officiers et agents de police judiciaire, experts judiciaires, etc.) formés aux investigations numériques et au recueil et au traitement des preuves numériques ;
- Des magistrats formés à l'instruction et au jugement des affaires relevant de la cybercriminalité.

SECTION VI. OBJECTIF STRATEGIQUE 4 : PROMOUVOIR LA COORDINATION ET LA COOPERATIONDANS LE RENFORCEMENT DE LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMALITE

Sous-objectif 4.1. Promouvoir la ratification de conventions

Chaque État Membre devrait ratifier les conventions régionales, continentales et internationales nécessaires sur la cybersécurité et la lutte contre la cybercriminalité.

Sous-objectif 4.2. **Assurer la promotion de la culture de cybersécurité**

Chaque État Membre devrait promouvoir une culture de la cybersécurité, en utilisant tous les moyens possibles (communication gouvernementale, séminaires, médias, formation scolaire, universitaire et continue, etc.) pour atteindre les objectifs suivants :

- La sensibilisation de tous aux cybermenaces ;
- La promotion de l'hygiène informatique et des autres bonnes pratiques numériques auprès du grand public ;
- La sensibilisation des décideurs publics et privés à leurs rôles et responsabilités ;
- La mise en garde des citoyens sur les peines encourues en cas de commission d'actes de cybercriminalité.

Sous-objectif 4.3. **Assurer la coordination nationale**

Chaque État Membre devrait mobiliser l'ensemble des acteurs publics et privés pour promouvoir et développer la concertation, la coordination et les synergies entre toutes les parties prenantes, notamment :

- les autorités et les institutions chargées de la cybersécurité ou de la lutte contre la cybercriminalité ;
- les opérateurs des infrastructures critiques ;
- les fournisseurs de produits de cybersécurité ou sécurisés ;
- les prestataires de services de cybersécurité ;
- les institutions de formation et de recherche ;
- les organisations de la société civile ;
- les médias.

Sous-objectif 4.4. **Promouvoir la coopération régionale et internationale**

Les États Membres et la Commission de la CEDEAO devraient promouvoir et développer la coopération régionale et internationale entre les autorités et institutions chargées de la cybersécurité et de la lutte contre la cybercriminalité :

- Dans le domaine du développement des capacités : par le partage des bonnes pratiques et par la recherche de synergies et de mutualisations intrarégionales, dans le domaine de la formation notamment ;
- Dans le domaine institutionnel : pour harmoniser les stratégies, les organisations et les procédures des pays de la région, notamment pour ce qui concerne la sécurité des infrastructures critiques transnationales et la lutte contre la cybercriminalité ;
- Dans le domaine opérationnel : pour partager les alertes et les informations de cybersécurité entre les CSIRT nationaux, et pour organiser des réponses communes, voire mettre en commun des moyens d'intervention afin de lutter le plus efficacement possible contre les cybermenaces potentielles ou avérées et contre la cybercriminalité ;
- Dans le domaine judiciaire : pour assurer l'entraide judiciaire en matière de cybercriminalité et l'accès transnational aux preuves numériques ;
- Par l'établissement d'un centre régional de simulation et de formation à la cybersécurité pour réduire les coûts et promouvoir l'interopérabilité ;
- En encourageant la création de structures conjointes de partage d'informations dans les infrastructures critiques et les services essentiels (énergie, finance, santé, etc.) ;
- En créant des mécanismes et des mémorandums d'accord communs avec d'autres organisations de partage d'informations.

SECTION VII. OBJECTIF STRATEGIQUE 5 : ETABLIR DES MECANIMES REGIONAUX

Sous-objectif 5.1. Établir un plan régional d'assistance à la mise en œuvre de la Stratégie régionale

Afin d'aider les États Membres à décliner la présente Stratégie régionale, la Commission de la CEDEAO mettra en œuvre, avec les moyens à sa disposition, le plan d'action régional figurant en annexe.

Sous-objectif 5.2. Établir un dispositif de suivi de la Stratégie régionale

La Commission de la CEDEAO étudiera avec les États Membres la possibilité de mettre en place un Comité technique régional (CTR/RTC, *Regional technical Committee*) pérenne, composé d'un représentant de haut niveau fourni par chaque État, placé sous la coordination de la Commission de la CEDEAO et qui se réunit au moins une fois par an, pour assurer dans le temps le suivi des dispositions de la présente Stratégie et proposer les nouvelles actions nécessaires.

Sous-objectif 5.3. Établir un centre de coordination de la cybersécurité

La Commission de la CEDEAO étudiera avec les États Membres l'opportunité de créer, à court ou moyen terme, un centre de coordination de la cybersécurité pour la CEDEAO, chargé notamment de coordonner les diverses démarches de renforcement des capacités conduites dans les différents pays en matière de cybersécurité et de lutte contre la cybercriminalité, et d'organiser, quand cela est possible, les mutualisations et le partage des résultats entre les pays.

Elle pourra envisager à plus long terme la mise en place d'une agence régionale chargée de promouvoir et d'animer la coopération régionale en matière de cybersécurité et de lutte contre la cybercriminalité.

Sous-objectif 5.4. Identifier et rechercher des financements pour les dispositifs nationaux de cybersécurité et de lutte contre la cybercriminalité

La Commission de la CEDEAO, en liaison avec les États membres, étudiera les possibilités d'harmonisation, au sein de la CEDEAO, des mécanismes de financement des dispositifs nationaux de cybersécurité et de lutte contre la cybercriminalité, notamment en ce qui concerne les partenariats public-privé.

La Commission de la CEDEAO, en liaison avec les États membres, recherchera des financements auprès des bailleurs de fonds pour répondre aux besoins prioritaires non satisfaits de ces États.