PREMIER MINISTERE

Anssi
Agence Nationale de Sécurité des Systèmes d'Information | Burkina Faso

STRATEGIE NATIONALE DE CYBERSECURITE 2019-2023 (SNCS-BF)

JANVIER 2019

Table des matières

Avant-propos

La présente Stratégie nationale de cybersécurité (SNCS) vise à fixer les orientations nationales en matière de cybersécurité au Burkina Faso.

Sur la base des résultats de ce rapport et d'analyse approfondie faite pour déceler les risques et les lacunes des systèmes d'information et de communication présents sur le cyberespace, les axes de la Stratégie nationale de cybersécurité (SNCS) du pays ainsi que les objectifs stratégiques sont définis dans cette stratégie. La vision stratégique a été élaborée dans le souci que la stratégie nationale de sécurité qui en découlera ait les propriétés suivantes :

1. Elle est adaptée à l'état des lieux (à l'échelle nationale) en matière de cybersécurité ;
2. Elle est évolutive par rapport aux tendances mondiales en matière de menaces et de solutions de sécurité ;
3. Elle est conforme aux bonnes pratiques adoptées à l'échelle internationale. Ce dernier point est d'une extrême importance puisqu'il peut conditionner la coopération internationale en la matière.

De ce qui précède il est donc apparu nécessaire, dans un premier temps, de faire l'évaluation de la sécurité du cyberespace du Burkina Faso, dans un second temps de dégager les défis à relever, ensuite de présenter les éléments de la stratégie nationale de cybersécurité dont les fondements, la vision, les principes, les orientations et les objectifs. Ces orientations ont été déclinées en axes stratégiques afin de mieux prendre en compte tous les enjeux de la cybersécurité. Il a été question de définir les différentes sources de financement ainsi que de mettre en place un dispositif de suivi et d'évaluation de la mise en œuvre de la stratégie.

Son Excellence Le Premier ministre

Christophe Marie Joseph DABIRE

Introduction

Dans un contexte d'intenses développements des Technologies de l'information et de la communication (TIC), de nouvelles menaces surgissent pour nos sociétés. Ces menaces présentent des facettes multiples puisqu'elles peuvent se matérialiser sous forme d'attaques visant les infrastructures essentielles, d'activités d'espionnage, de piratages et vols de données des grandes entreprises, de cyberterrorisme, d'actions malveillantes à travers des réseaux criminels transnationaux, de blanchiment d'argent en ligne, voire d'ingérence étrangère dans les élections. La cybersécurité est alors devenue un élément essentiel des systèmes de défense des États et des entreprises privées. Les systèmes d'information et de communication se sont transformés en un terrain fertile pour les réseaux criminels et ont constitué un nouveau terrain d'affrontements dans les conflits.

C'est dans ce sens que la cybersécurité suscite depuis quelques années l'intérêt des Etats pour mettre en place des mécanismes de protection efficace pour protéger les cyberespaces nationaux contre les risques de plus en plus fréquents et dévastateurs.

L'élaboration d'une stratégie nationale de cybersécurité soulève un ensemble de problématiques liées aux points suivants : le périmètre du cyberespace, la diversité de l'expertise, les mécanismes de mise en œuvre, la conformité aux références internationales.

En vue de développer la Stratégie nationale de cybersécurité du Burkina Faso (SNCS-BF) en tenant compte de ces problématiques, la méthodologie adoptée repose sur le cadre de cybersécurité (*cybersecurity framework*) établi par l'Institut américain des standards et des technologies, communément appelé NIST (*National Institute of Standards and Technology*). Ce cadre sera consolidé par des éléments du guide d'élaboration des stratégies nationales de cybersécurité proposé par l'Union Internationale des Télécommunications (GSNC-UIT).

Dans un souci de rigueur et de synthèse, le présent résumé de la SNCS du Burkina Faso est structuré autour de neuf (09) points :

1. Le premier point présente la portée de la présente stratégie.

2. Le deuxième point dresse un état des lieux basé sur une analyse du contexte (national, africain, CEDEAO et international) en matière de cybersécurité et identifie les défis majeurs à relever en la matière.
3. Le troisième point cite les éléments de la SNCS, notamment les fondements internationaux et nationaux ainsi que les principes directeurs.
4. Le quatrième point élabore les orientations de la SNCS.
5. Le cinquième point décortique les orientations stratégiques en sept (07) programmes ainsi que des actions et des sous actions.
6. Le sixième point fournit le détail de chacun des programmes susmentionnés.
7. Le septième point identifie les moyens de financement des sous actions de la stratégie.
8. Le huitième point aborde un modèle de gouvernance permettant d'assurer le bon déroulement des activités de la SNCS et traite de la réduction des risques identifiés qui sont susceptibles d'affecter la mise en œuvre de la stratégie.
9. Le neuvième point présente une analyse des risques affectant la mise en œuvre de la SNCS.

Portée de la stratégie

La portée de la SNCS est définie selon trois (03) dimensions principales :

1. Périmètre documentaire : les documents stratégiques des systèmes d'information et de communication faisant partie du cyberespace burkinabè qui supportent la provision de services numériques au Burkina Faso et ne sont pas nécessairement hébergés sur le territoire burkinabè.
2. Tiers considérés : définis par le standard NIST800-39, ces tiers, illustrés sont : les aspects organisationnels, les aspects informationnels et les aspects techniques
3. Besoins de sécurité : les besoins de sécurité considérés sont la confidentialité, l'intégrité et la disponibilité (définis dans le standard FIPS 199).

Contexte

1. Contexte international

La première réglementation internationale, contribuant à appréhender la dimension internationale de la cybercriminalité est la Convention sur la cybercriminalité du Conseil de l'Europe, adoptée à Budapest le 23 novembre 2001.

2. Contexte africain

Les Etats Africains sont à différents niveaux d'avancement en matière d'établissement d'instruments politiques, de cadres législatifs, et de mécanismes techniques pour la protection des cyberespaces nationaux. Cette situation est corroborée par l'Indice global de cybersécurité (IGC), élaboré en 2017 par l'UIT, qui révèle que le classement des pays africains est en dessous de la moyenne des classements des autres régions.

Tableau 1 : Scores relatifs aux piliers du IGC .

Région	Juridique	Technique	Organisationnel	Renforcement des capacités	Coopération
AFRIQUE	0.29	0.18	0.16	0.17	0.25
AMERIQUE	0.40	0.30	0.24	0.28	0.26
PAYS ARABES	0.44	0.33	0.27	0.34	0.29
ASIE	0.43	0.38	0.31	0.34	0.39
COMMONWEALTH	0.58	0.42	0.37	0.38	0.40
EUROPE	0.61	0.60	0.45	0.49	0.46

Pour réagir aux difficultés posées par les activités criminelles commises sur le cyberespace et en réponse à la nécessité d'harmoniser les législations dans le domaine de la cybersécurité et la protection des données à caractère personnel, la 23e Assemblée des chefs d'Etat et des gouvernements de l'Union africaine (UA), tenue à Malabo les 26-27

Juin 2014 a adopté la "Convention sur la cybersécurité et la protection des données à caractère personnel" aussi appelée la "Convention de Malabo".

3. Contexte CEDEAO

Une conférence régionale organisée conjointement entre la CEDEAO et le Conseil de l'Europe ayant pour thème «Harmonisation de la législation sur la cybercriminalité et les preuves électroniques, avec des garanties pour l'état de droit et les droits de l'homme » s'est tenue en septembre 2017 au Nigeria. Cette conférence visait à faire le point sur l'état des législations sur la cybercriminalité et les preuves électroniques des Etats membres de la CEDEAO vis-à-vis de la Convention de Budapest sur la cybercriminalité. Selon les scores IGC 2017, le Nigeria occupe la première place avec un score 0.596 sur 1 et le Burkina Faso la sixième place avec un score 0.208 sur 1.

4. Contexte national

Le nombre croissant de cyber-incidents signalés exige que les gouvernements procurent des réponses stratégiques pour contrer les cybermenaces. Le contexte national est analysé suivant quatre (04) points que sont :

1. Contexte politique : les attaques visant les composantes du cyberespace peuvent aussi avoir une connotation politique. Les informations publiées sur la toile par des entités de confiance dans la diffusion de l'information sont supposées vrai d'office. Dès lors ces entités et les réseaux sociaux peuvent être utilisés pour manipuler l'opinion publique. Les réseaux sociaux comme tous les lieux de socialisation offrent une bonne image de l'opinion d'un peuple à un moment donné. Il n'est dès lors pas inenvisageable d'imaginer que les services de renseignement d'un pays puissent accéder à de précieuses informations sur ces espaces.
2. Contexte socio-économique : l'évolution du secteur des Technologies de l'information et de la communication (TIC) a un impact direct et positif sur le développement social et économique des pays africains. Il existe également un lien étroit entre les mécanismes mis en place pour la protection du cyberespace et le développement des indicateurs relatifs à la société de l'information. Contexte technique.

Une grande partie du matériel informatique et des logiciels développés à l'origine n'ont pas toujours intégré la dimension sécurité dès le départ. Or, des acteurs malveillants peuvent exploiter cet écart entre commodité et sécurité ; le réduire constitue donc une priorité nationale. C'est dans ce sens que des décisions stratégiques doivent être conçues dans un premier temps pour faciliter la mise en place des solutions de sécurité.

Défis à relever

Les défis majeurs à relever dans le cadre de la sécurisation du cyberespace burkinabè sont les suivants :

1. Disposer d'un cadre juridique adéquat permettant de garantir la confiance dans le cyberespace burkinabè et de combattre efficacement la cybercriminalité ;
2. Accroitre les capacités techniques d'intervention pour la surveillance et la défense des infrastructures critiques et des systèmes d'information sensibles de l'Etat et des entreprises ;
3. Garantir la recevabilité de la preuve numérique ;
4. Disposer de ressources humaines qualifiées pour garantir l'expertise nationale dans le domaine de la cybersécurité ;
5. Assurer une culture de la cybersécurité.

Eléments de la stratégie nationale de cybersécurité

1) Les fondements

1.1. Les fondements à l'échelle régionale et internationale

Au niveau international la Stratégie nationale de cybersécurité trouve ses fondements dans :

a) La Convention de Budapest ;

b) La Convention de l'Union africaine sur la cybersécurité et les données personnelles de Malabo adoptée en 2014, qui prévoit le développement d'une SNCS en tant que priorité.

1.2. Les fondements à l'échelle nationale

Au niveau national, la stratégie de cybersécurité s'adosse sur les lois et référentiels suivants :

a) la loi N°010/2004/AN du 20 Avril 2004 portant protection des données à caractère personnelle ;

b) la loi N° 061/2008/AN portant réglementation général des réseaux et services des communications électronique au Burkina Faso ;

c) la loi N°045/2009/AN portant réglementation des services et des transactions électroniques au Burkina Faso ;

d) l'Etude nationale prospective 2025 (ENP 2025) fait aussi allusion à la sécurité nationale au niveau de l'objectif stratégique 3.3.4 : "La lutte contre l'insécurité par le renforcement du dispositif de sécurité nationale afin de rendre effective la sécurité des personnes et des biens, le renforcement d'une armée effectivement républicaine, c'est-à-dire, au service exclusif de la nation, politiquement neutre et professionnellement opérationnelle, au service de la paix et de la justice pour tous, la lutte contre le grand banditisme en recrudescence, l'adoption d'une attitude créatrice d'entente entre le Burkina Faso et les pays voisins." ;

a) le Plan national de développement économique et Social (PNDES 2016 - 2020) dont l'axe 1 « reformer les institutions et moderniser l'administration » ;

b) la Stratégie nationale de développement de l'économie numérique 2018-2027 qui consacre son programme 2 à l'instauration d'un environnement de confiance numérique au Burkina Faso.

2) Vision

L'ambition du Burkina Faso en matière de sécurisation de son espace cybernétique se décline comme suit : « A l'horizon 2023, le Burkina Faso dispose d'un cyberespace de confiance favorable au développement économique et social. »

3) Orientations stratégiques

Les orientations fondamentales qui doivent être considérées dans le cadre de la mise en œuvre de la SNCS sont :

1. Faire de la lutte contre la cybercriminalité et du renforcement des capacités de cybersécurité une priorité ;
2. Renforcer la coordination entre les différents acteurs du cyberespace et avec les homologues internationaux ;
3. Respecter les droits fondamentaux des personnes ;
4. Mettre en œuvre des mesures appropriées et proportionnées aux menaces ;
5. Mobiliser, fédérer et engager les différents acteurs privés du cyberespace et de la société civile autour des actions prévues dans la SNCS en vue de lutter contre la cybercriminalité.

4) Objectifs

1.1. Objectif général

L'objectif général de la Stratégie nationale de cybersécurité est de garantir un cyberespace sûr qui contribue d'une manière efficace aux objectifs de transformation numérique du Burkina Faso.

1.2. Objectifs spécifiques

Les objectifs spécifiques de la SNCS sont :

a) Objectif 1 : instaurer une synergie à l'échelle nationale.

b) Objectif 2 : renforcer la coopération internationale.

c) Objectif 3 : informer, former et sensibiliser les acteurs du cyberespace sur les risques encourus.

d) Objectif 4 : instaurer une coopération avec le tissu universitaire et de recherche.

e) Objectif 5 : mettre en place des normes, des standards et des référentiels d'exigence.

f) Objectif 6 : améliorer la sécurité et la résilience des infrastructures sensibles et critiques.

g) Objectif 7 : combattre la cybercriminalité.

En s'inspirant de ces bonnes pratiques, et en considérant l'état des lieux en matière de cybersécurité au Burkina Faso, les objectifs stratégiques suivants sont définis pour la SNCS :

1. **Orientation 1 : amélioration de la gouvernance de la cybersécurité**
    1. Objectif 1 : instaurer une synergie à l'échelle nationale.
    2. Objectif 2 : renforcer la coopération internationale.
2. **Orientation 2 : renforcement de la culture de la cybersécurité**
    1. Objectif 3 : informer, former et sensibiliser les acteurs du cyberespace sur les risques encourus.
    2. Objectif 4 : instaurer une coopération avec le tissu universitaire et de recherche.
3. **Orientation 3 : protection contre les risques de sécurité**
    1. Objectif 5 : mettre en place des normes, des standards et des référentiels d'exigence.
    2. Objectif 6 : améliorer la sécurité et la résilience des infrastructures sensibles et critiques.
    3. Objectif 7 : combattre la cybercriminalité.

DISPOSITIF DE MISE EN ŒUVRE ET DE SUIVI-ÉVALUATION DE LA SNCS

1) Dispositif de mise en œuvre

1.1. Instruments de mise en œuvre

La SNCS sera mise en œuvre à travers des Plans d'actions triennaux glissants élaborés suivant l'approche programme et des plans de travail annuels.

1.2. Les acteurs

Ils regroupent l'ensemble des intervenants dans les domaines de la cybersécurité notamment les structures étatiques, les Partenaires techniques et financiers (PTF), les acteurs privés et les organisations de la société civile.

2) Dispositifs de mise en œuvre et de supervision

Le dispositif de mise en œuvre et de supervision comprend les organes et les instances suivants :

1.1. Dispositifs de mise en œuvre

Les organes de mise en œuvre et de suivi évaluation sont, le Conseil d'administration des secteurs ministériels (CASEM), les Conseils d'administration des structures rattachées et des structures de mission, les Comités de revue des projets et programmes de développement, les Conseils de direction.

1.2. Dispositifs de suivi-évaluation de la stratégie

Pour garantir une bonne mise en œuvre et l'atteinte des résultats escomptés, la présente stratégie fera l'objet d'un suivi et d'une évaluation réguliers en vue d'apporter au besoin les actions nouvelles ou correctives nécessaires.

Dans le cadre de la coordination, l'ANSSI se chargera de :

a) élaborer le Programme de travail budgétisé annuel (PTBA) ;
b) suivre la mise en œuvre des PTBA ;
c) Élaborer les rapports annuels et à mi-parcours ;
d) Préparer les sessions de suivi-évaluation.

Financement

La mise en œuvre effective des programmes de la Stratégie nationale de cybersécurité ne pourrait se faire qu'avec les financements nécessaires. Cette stratégie et son plan d'actions triennal glissant doivent donc être capitalisés pour inciter les partenaires financiers (publics, privés, associations, …) à supporter les actions prévues. Les partenaires potentiels pour le financement de la stratégie sont principalement :

Tableau 3 : Les partenaires potentiels pour le financement de la stratégie

Partenaires	Mécanismes de mobilisation
Ministères et institutions	Au travers du budget de l'Etat, le financement sera mobilisé via les dotations aux différents ministères et institutions
Sociétés d'état et EPE	Au travers de leurs investissements propres
Opérateurs télécoms	Au travers de leurs investissements et de leur soutien à des programmes d'appui et de diffusion des usages numériques
Secteur privé	Au travers de leurs investissements propres et de partenariats publics et privés en faveur de la cybersécurité
Coopération africaine	Au travers des instruments de soutien aux TIC des organismes africain
Coopération avec les institutions financières	Au travers des instruments de soutien aux TIC des institutions financières et organismes africains, entre autres la BAD, la BOAD, la BM, la BID.
Coopération internationale	Au travers des instruments de soutien aux TIC des institutions financières et organismes internationaux, entre autres UE, UIT, INTERPOL et de la coopération bilatérale et multilatérale
Multinationales	Au travers d'accords de partenariats stratégiques avec les équipementiers, éditeurs de logiciels…
Organisations de la société civile (ONG, associations, …)	Au travers d'accords de partenariats spécifiques

Analyse des risques

Le plan d'action opérationnel de la Stratégie nationale de cybersécurité peut être affecté par quatre (04) risques majeurs suivants : instabilité politique et institutionnel, dispersion des responsabilités, l'inertie légale et réglementaire, incertitude du financement.