PLAN NATIONAL DE CYBERSECURITE REALISE A LA DEMANDE DE L'ARCE AVEC L'APPUI DE L'UIT

ARCE Burkina Faso

Autorité de régulation des communications électroniques

Version définitive : 1.0

Réalisé par : AINA Alain Patrick, Consultant

Dernière mise à jour : 20/12/2010

Table des matières

INTRODUCTION

Le cyberespace du Burkina Faso est composé d'un ensemble de systèmes informatiques et télécoms interconnectés servant de centre névralgique au fonctionnement des secteurs vitaux du pays que sont : les finances, la communication, les transports, l'énergie, l'eau, les services d'urgence, les services de santé, les services publics, la défense nationale, etc.

L'Internet joue un rôle de plus en plus important dans ce cyberespace de par son fonctionnement et les services offerts. Ce cyberespace offre des services à une variété d'utilisateurs (novices, avertis, professionnels,...).

Nos investigations sur le terrain ont montré à travers la caractérisation du cyberespace l'existence de nombreuses vulnérabilités, failles de sécurité conduisant à des incidents de sécurité jusqu'alors pas très sérieux. Toutefois il est important d'assurer une meilleure protection et défense de l'infrastructure critique nationale.

Le plan national de cybersécurité doit faire partie d'un effort global de protection de la nation et doit être une composante de la stratégie nationale de protection et de défense du pays.

L'objectif de ce document est d'engager et autoriser chaque burkinabè à sécuriser la portion du cyberespace qu'il contrôle et gère ou avec lequel il interagit. Sécuriser le cyberespace est un exercice difficile qui nécessite un effort coordonné de toute la société (gouvernement, secteur privé, citoyens,...).

Ce plan s'appuie sur la caractérisation du cyberespace (confère rapport de la mission d'élaboration du plan national de cybersécurité) et s'articule autour des principaux axes suivants :

- la réduction de la vulnérabilité du cyberespace,
- la gestion des incidents,
- le renforcement de la culture de cybersécurité.

1. Le cyberespace du Burkina Faso

La caractérisation du cyberespace a montré que le niveau de dépendance par rapport aux TICs des structures des secteurs critiques du pays à savoir les finances, la communication, les transports, l'énergie, l'eau, les services d'urgence, les services de santé, les services publics, la défense nationale… est élevé :

- La plupart de ces structures dépendent pour leur fonctionnement de leur système d'information. Un dysfonctionnement (attaques et autres) aurait de sérieuses conséquences sur les activités de ces dernières.
- La production et la distribution dépendent moins de leur système d'information. Un dysfonctionnement (attaques et autres) n'aurait pas un effet significatif sur les activités de ces dernières. Cette situation va changer dans les années à venir avec tous les projets de modernisation qui sont en cours et à venir qui augmenteront la dépendance.

Malheureusement ce cyberespace n'est pas bien géré et sécurisé sur plusieurs plans. La caractérisation de ce cyberespace a révélé :

1- Une inefficacité des solutions techniques utilisées. Le contrôle de l'efficacité des solutions techniques n'étant pas systématique.

2- Une absence d'information sur les vulnérabilités, failles de sécurité et leurs solutions.

3- Les incidents de sécurité ne sont pas analysés, pour en tirer les leçons et les conséquences, identifier les auteurs et entreprendre des actions légales si nécessaire. Tout le monde semble ignorer l'existence des unités spécialisées de lutte contre la cybercriminalité existantes au niveau de la police et de la gendarmerie et des possibilités d'actions légales auprès des tribunaux. Certains n'étant pas convaincus que ces structures peuvent vraiment aider.

4- Bien que l'analyse et la gestion des risques indiquent un niveau élevé d'impact des incidents de sécurité, le niveau de préparation à faire face aux incidents de sécurité est jugé moyen.

5- Les risques résiduels de cybersécurité ne sont pas dans la plupart des cas couverts par une police d'assurance.

6- La majorité des fonctions de sécurité sont déclarées être gérées en interne alors que les ressources humaines qualifiées n'existent pas.

7- Les pourcentages du budget IT consacré à la sécurité et aux campagnes de sensibilisation et de formation sont très faibles. Ceci explique que la sécurité n'a pas la place qu'il faut dans les stratégies et les budgets.

8- Manque de culture en cybersécurité. Le niveau des employés recrutés est médiocre alors que l'organisation des campagnes de sensibilisation et d'information ainsi que l'évaluation de leur efficacité ne sont pas systématiques. Par ailleurs, les utilisateurs finaux ont jugé non satisfaisant le niveau de sensibilisation et d'information du citoyen.

9- Les structures existantes chargées de l'analyse des cyber incidents et des infractions informatiques ne sont pas outillées pour bien faire leur travail.

10- Le manque de législations spécifiques en matière de procédure et de sanctions des infractions informatiques réduit à néant les efforts de ces structures. Les sanctions appliquées en ce moment à certaines infractions qualifiées sous d'autres titres sont insignifiantes.

11- Les structures chargées d'encadrer et de réguler les communications électroniques, la protection des données à caractère personnel, etc., continuent de se déployer et prendre contrôle de leurs prérogatives. Beaucoup restant à faire pour un meilleur encadrement du cyberespace et sa sécurisation.

12- De nombreux projets IT sont envisagés pour les prochaines années et introduiront de nouveaux risques qui pourraient accentuer les problèmes de sécurité rencontrés aujourd'hui.

2. Cyberstratégie nationale et cybersécurité

Les Technologies de l'Information et de la Communication bouleversent la vie et les habitudes en changeant le mode de fonctionnement du gouvernement, la manière dont les affaires, la sécurité intérieure et la défense nationale sont menées. Ces fonctions dépendent du cyberespace et par conséquent il est de ressort de la stratégie nationale du Burkina Faso de prévenir ou de minimiser les attaques contre les infrastructures d'information critiques et par conséquent protéger les citoyens, l'économie, les services essentiels, les services gouvernementaux et la sécurité nationale.

La stratégie requiert un effort continu pour sécuriser les infrastructures critiques et requiert un partenariat public-privé incluant les sociétés et les organisations non gouvernementales.

En conformité avec les objectifs de la stratégie de sécurité nationale, les objectifs du plan national de cybersécurité doivent être de:

- Prévenir les attaques contre les infrastructures critiques,
- Réduire la vulnérabilité de l'infrastructure nationale aux cyberattaques,
- Minimiser les impacts et le temps de reprise suite aux cyberattaques.

Le développement du cadre d'implémentation de la stratégie de cybersécurité doit tenir compte des principes ci-après :

- ***Un effort national***

Protéger le cyberespace très distribué requiert l'effort de beaucoup de citoyens burkinabè.

Le gouvernement tout seul ne peut pas protéger et défendre ce cyberespace en partie détenu et géré par le secteur privé. Le rôle du gouvernement se concentrera sur la promotion de bonnes pratiques en termes de sécurité, en facilitant les discussions entre les entités non gouvernementales, en identifiant les secteurs les plus vulnérables et en partageant les informations sur les risques, les menaces et vulnérabilités afin que les entités non gouvernementales puissent ajuster leur gestion de risques et leur plan.

Chaque citoyen burkinabè qui peut sécuriser une partie du cyberespace doit être encouragé à le faire. Le gouvernement doit promouvoir dans le cadre du partenariat public-privé des campagnes de formation et de sensibilisation.

- ***Protection de la vie privée et des libertés individuelles***

La cybersécurité et le respect de la vie privée ne doivent pas être des objectifs opposés. Les activités de cybersécurité doivent renforcer et respecter la vie privée et les libertés individuelles.

Les utilisateurs, les opérateurs et autres doivent avoir confiance que les informations confidentielles qu'ils partagent dans le cadre de la cybersécurité sont gérées avec professionnalisme, confidentialité et efficacité et en respectant les lois en vigueur.

La collaboration entre la CIL et l'ARCE dans ce domaine doit être renforcé.

- ***Régulation et force du marché***

La régulation des secteurs des communications électroniques doit s'assurer de la prise en compte des mesures de sécurité dans le développement du cyberespace national, le respect des cahiers de charges, la collaboration entre les acteurs et les entités chargées de la gestion des fonctions de cybersécurité.

La compétition et le dynamisme doivent être encouragés pour améliorer la cybersécurité.

La régulation et la force du marché doivent contribuer à l'amélioration de l'infrastructure existante à travers :

- Une meilleure allocation et assignation des adresses IPv4 aux utilisateurs pour réduire les translations d'adresses et faciliter la traçabilité des communications,
- La mise en place de points d'échange Internet,
- L'implémentation de copies de serveurs racines Internet,
- L'introduction et la transition vers IPv6,
- etc.

- ***Rôles et responsabilités***

La stratégie nationale de cybersécurité vise à produire un cyberespace robuste et efficace et doit désigner les structures qui doivent être responsables des initiatives de protection et défense du cyberespace au niveau des secteurs critiques du pays.

Le gouvernement dans son rôle de protection des secteurs critiques du pays devra désigner des départements ministériels qui seront responsables de la coordination, suivi et évaluation des initiatives de protection et de défense des systèmes d'information des secteurs critiques qui leur sont rattachés.

Pour le Burkina Faso les secteurs suivants sont considérés comme critiques : **les finances, la communication, les transports, l'énergie, l'eau, les services d'urgence, les services de santé, les services publics, la défense nationale...**

Des associations professionnelles comme Association Professionnelle des Banques et Etablissements Financiers, Association des Directeurs de Services Informatiques, des associations des consommateurs, les ONG de promotion des TICs... sont des partenaires vitaux.

Pour coordonner toutes les activités de cybersécurité au niveau national une structure nationale (Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)) doit être créée et chargée de la mise en œuvre des objectifs indiqués dans

cette stratégie. Cette structure nationale doit être placée sous la tutelle de l'Etat qui fournira une grande partie de son budget de fonctionnement.

Elle aura pour missions entre autres de :

- *Veiller à l'exécution des orientations nationales et de la stratégie générale en systèmes de sécurité des systèmes informatiques et des réseaux ;*

- *Suivre l'exécution des plans et des programmes relatifs à la sécurité des systèmes d'information et assurer la coordination entre les intervenants dans ce domaine ;*

- *Assurer la veille technologique dans le domaine de la sécurité des systèmes d'information ;*

- *Etablir des normes spécifiques à la sécurité des systèmes d'information et élaborer des guides techniques en l'objet et procéder à leur publication ;*

- *Œuvrer pour encourager le développement de solutions nationales dans le domaine de la sécurité des systèmes d'information et à les promouvoir conformément aux priorités et aux programmes qui seront fixés par l'agence ;*

- *Participer à la consolidation de la formation et du recyclage dans le domaine de la sécurité des systèmes d'information ;*

- *Veiller à l'exécution des réglementations relatives à l'obligation de l'audit périodique de la sécurité des systèmes informatiques et des réseaux.*

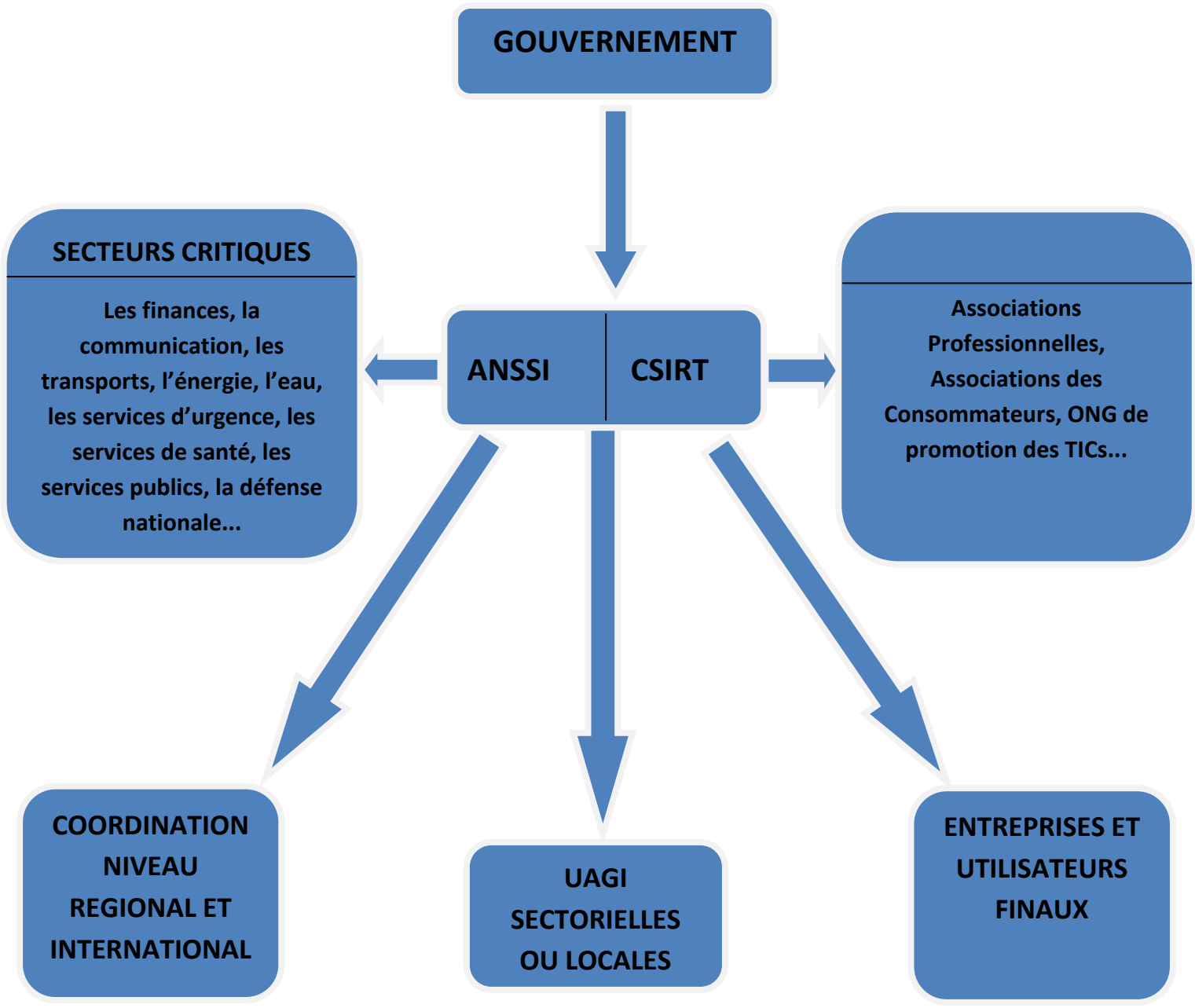

Figure n°1 : Entités et interactions

- ***Flexibilité***

Les nouvelles formes d'attaques apparaissent régulièrement et donnent des avances aux pirates dans leurs actions contre les systèmes, la stratégie nationale doit être suffisamment flexible pour permettre aux structures de réadapter facilement leurs

techniques de réduction de vulnérabilités et de réponse à ces nouvelles formes d'attaques.

- ***Révision continuelle***

La sécurisation du cyberespace est un effort dynamique et permanent puisque de nouvelles technologies apparaissent ainsi que de nouvelles vulnérabilités. La stratégie nationale de cybersécurité fournit un cadre de départ pour atteindre les objectifs de sécurité mais les départements et les structures doivent réviser régulièrement leur plan.

3. Priorités pour une meilleure gestion de la sécurité du cyberespace

La sécurisation du cyberespace s'articule autour des trois priorités suivantes :

- Réduction de la vulnérabilité du cyberespace,
- Gestion des incidents,
- Renforcement de la culture de cybersécurité.

3.1. Priorité n°1 : Réduction de la vulnérabilité du cyberespace

Les ennemis du cyberespace peuvent prendre plusieurs formes : individus, groupes organisés, terroristes, nations... Tous cherchent à exploiter des vulnérabilités créées dans la conception ou l'implémentation des logiciels, du matériel, des réseaux, des protocoles. Plus notre dépendance du cyberespace augmente, plus l'impact de ces ennemis augmente. Attendre de réagir à des tentatives d'exploitation de vulnérabilités peut être dangereux. Il vaut mieux identifier et corriger les vulnérabilités dans les infrastructures critiques avant que les menaces ne se présentent. Les vulnérabilités les plus dangereuses doivent être en priorité réduites de façon systématique.
La technologie évolue, de nouveaux systèmes sont introduits créant souvent de nouvelles vulnérabilités et menaces.

Les objectifs de ce plan ne sont pas d'éliminer toutes les vulnérabilités ou de décourager toutes les menaces, il devra au contraire aider à :

1- **Identifier et corriger les vulnérabilités existantes qui peuvent créer des dommages aux infrastructures critiques si elles sont exploitées ;**

2- **Développer les nouveaux systèmes avec moins de vulnérabilités et évaluer les technologies émergentes pour les vulnérabilités ;**

3- **Réduire les menaces et décourager les pirates à travers un programme d'identification et de sanctions.**

De nombreuses vulnérabilités ont été relevées par la caractérisation du cyberespace menée dans l'étude pour l'élaboration du plan national de cybersécurité (confère rapport d'étude pour l'élaboration du plan national de cybersécurité).

3.1.1. Identification et correction des vulnérabilités existantes

Il faut en urgence prendre les mesures sous le contrôle de l'ANSSI et en coordination avec les acteurs pour remédier aux vulnérabilités présentées par le cyberespace à travers :

- *Une meilleure gestion de l'accès aux informations sur les vulnérabilités présentées par les logiciels, matériels, systèmes et solutions ainsi que les correctifs (les contournements, patches, mises à jour). Le cyberespace de Burkina Faso dépend en grande partie des logiciels propriétaires.*

    - *Ceci nécessite un système de veille et de diffusion précoce d'informations ;*
    - *Un accès facile aux correctifs : mise à disposition de dépôts locaux (repository), des patches, mises à jour, des logiciels propriétaires les plus utilisés (les produits Microsoft, les anti-virus...).*

- *L'Amélioration des techniques d'analyse et de gestion des risques au niveau des infrastructures critiques.*

    - *Identifier et recenser les infrastructures critiques ;*
    - *Développer et renforcer les capacités en termes d'analyse et gestion des risques des systèmes d'information ;*
    - *Rendre obligatoire l'analyse et la gestion des risques à périodicité déterminée pour les infrastructures critiques ;*
    - *Rendre obligatoire les audits des systèmes d'information pour évaluer les résultats de l'analyse et gestion des risques ainsi que les solutions techniques et procédures mises en place ;*
    - *Elaborer et mettre à disposition des guides sur la protection des systèmes d'information.*

- *Tirer les leçons qui s'imposent des incidents de sécurité pour améliorer le programme de réduction des vulnérabilités.*

3.1.2. Développer les nouveaux systèmes avec moins de vulnérabilités et évaluer les technologies émergentes pour les vulnérabilités

3.1.2.1. Développer les nouveaux systèmes avec moins de vulnérabilités

De nombreux projets sont envisagés pour les cinq (5) prochaines années pour améliorer la capacité du cyberespace avec pour conséquence l'augmentation du niveau du pays par rapport à ce dernier.

La nation tout entière sous l'impulsion de l'ANSSI va s'assurer que les futures composantes du cyberespace sont construites de façon sécurisée.

L'objectif du développement et de déploiement des systèmes sécurisés, fiables et robustes doit être poursuivi, en tenant compte des contraintes budgétaires et des règles claires définies par les structures compétentes.

- La priorité doit être donnée aux logiciels, systèmes... qui ont fait leur preuve et ont une bonne historique en termes de sécurité et gestion des vulnérabilités pour les infrastructures critiques.

- L'ANSSI facilitera un effort national de promulgation de bonnes pratiques et de méthodologies qui :

    - *garantissent l'intégrité, la sécurité, la fiabilité dans le développement des logiciels ainsi que dans les processus et procédures qui réduisent la probabilité que des codes erronés, des codes malveillants... puissent être introduits pendant les développements ;*

    - *garantissent un choix judicieux des équipements et systèmes de sécurité.*

- *Les nouveaux services et solutions comme la virtualisation des postes et serveurs, les Cloud-computing, etc. envahissent de plus en plus les systèmes*

d'information. Ils devront être déployés en suivant les bonnes pratiques et recommandations de l'ANSSI.

- *Les nouveaux protocoles comme IPv6, DNSSEC, etc. doivent être déployés en suivant les bonnes pratiques et recommandations de l'ANSSI.*

- *La migration des réseaux opérateurs vers les NGN IP doivent se faire suivant les bonnes pratiques et recommandations de l'ANSSI.*

3.1.2.2. Evaluer les technologies émergentes pour les vulnérabilités

Quand les nouvelles technologies sont déployées, elles introduisent des nouvelles vulnérabilités et menaces. Certaines de ces nouvelles technologies introduisent des problèmes de sécurité qui sont seulement corrigés avec le temps et avec grande difficulté ou pas du tout. Par exemple les téléphones, les équipements mobiles intègrent de plus en plus des systèmes d'exploitation et des moyens de connectivité très sophistiqués créant le besoin des mesures de sécurité pour prévenir de leur exploitation pour leurs attaques distribuées sur les réseaux mobiles et sur le cyberespace en général.

L'évolution des protocoles et des systèmes va continuer à offrir de nouvelles technologies et de nouvelles solutions qui se grefferont sur le cyberespace, il est donc important sous la coordination de l'ANSSI et avec la collaboration de tous les acteurs :

- *De faire de la veille technologique en suivant l'évolution des protocoles et solutions à travers les groupes de travail de normalisation de l'UIT, de l'IETF...*

- *De faire l'évaluation des technologies émergentes et des recommandations quant à leur déploiement et mise en service.*

3.1.3. Réduire les menaces et décourager les pirates à travers un programme d'identification et de sanctions

La dernière action dans le programme national de réduction de la vulnérabilité est de réduire les menaces et de décourager les pirates à travers :

- *Le renforcement des capacités du système légal à prévenir et à punir les cybercrimes :*

  - *Adopter les lois qualifiant et punissant les cybercrimes ainsi que les réformes nécessaires au code de procédure pénale,*

  - *Renforcer les capacités des cyberdivisions de la Justice, de la Police, de la Gendarmerie ainsi que de l'Armée.*

- *Identifier et mettre hors d'état de nuire des individus ou groupes qui peuvent créer des dommages à la nation à travers le cyberespace ;*

- *Beaucoup de cyberattaques sont des crimes. Les cyberdivisions de la Police et de la Gendarmerie doivent travailler avec la Justice ainsi qu'avec l'ANSSI et les autres acteurs pour appréhender et traduire les responsables devant la Justice.*

- *La Justice, la Police, la Gendarmerie et l'ANSSI doivent travailler en étroite collaboration pour s'assurer que les informations obtenues à travers les poursuites et les investigations sont sérieusement analysées et partagées avec les autres structures non gouvernementales pour améliorer la gestion des risques sur les infrastructures critiques.*

3.2. Priorité n°2 : Gestion des incidents

Malgré les mesures préventives et correctives prises pour protéger le cyberespace, les attaques et incidents pourraient toujours survenir et avoir de sérieuses conséquences pour le pays. Il est donc vital que le Burkina Faso mette en place un système national de gestion des incidents pour détecter, analyser, alerter les victimes, coordonner la réponse aux incidents et restaurer les services essentiels qui ont été atteints.

Mettre en place un système de gestion des incidents sur le cyberespace national très distribué et géré par plusieurs entités, présente quelques challenges.

Les attaques sur ce cyberespace peuvent venir de n'importe où et se propager partout ; les informations sur les attaques peuvent aussi venir à travers différentes organisations et canaux rendant difficile leur évaluation et dissémination. Or pour réduire l'impact des incidents, les informations les concernant doivent être distribuées très rapidement et à grande échelle.

Le système national de gestion des incidents doit être une architecture multi-acteurs (public, privé,...) coordonnée par l'ANSSI pour analyser et alerter, gérer des incidents d'ampleur nationale, promouvoir la continuité dans les services gouvernementaux ainsi que du secteur privé et faciliter les échanges d'informations entre tous les acteurs pour améliorer la sécurité du cyberespace.

Il s'agira entre autres de :

- *Encourager la mise en place d'Unités d'Analyse et de Gestion des Incidents (UAGI) au niveau des organisations, des groupes sectoriels et industriels, et encourager la collaboration et le partage d'informations entre elles ;*
- *Mettre en place un centre de coordination de la gestion des incidents qui :*
    - *Doit fournir une assistance de gestion de crise en réponse aux menaces ou attaques sur les infrastructures critiques ;*
    - *Doit coordonner avec les UAGI sectorielles et autres organisations du public, du privé et les citoyens pour fournir les informations d'alerte spécifiques et des mesures de protection appropriées à mettre en place ;*

- *Doit coordonner les actions de réponse avec les organisations sœurs au niveau régional et international.*

Les principales missions de ce centre sont :

- ✓ *Mise en place d'un centre d'appel opérationnel 24H/24 pour l'assistance en cybersécurité et recueil des incidents de sécurité survenus sur les systèmes d'information ;*
- ✓ *Analyser les incidents, donner les alertes, faciliter les échanges et discussions entre les acteurs pour une gestion efficace des incidents ;*
- ✓ *Promouvoir et aider dans les mises en œuvre des plans de continuité et de contingence ;*
- ✓ *Former et recycler les différents acteurs dans les différentes branches de sécurité des systèmes d'information ;*
- ✓ *Sensibiliser les internautes sur les problèmes de sécurité et les aider à une utilisation rationnelle du cyberespace pour une bonne protection de celui-ci ;*
- ✓ *Permettre un travail communautaire des experts et des professionnels pour une meilleure sécurité des systèmes d'information ;*
- ✓ *Mettre en place une veille technologique en matière de la sécurité des systèmes d'information ;*
- ✓ *Adhérer à des organisations comme le FIRST, IMPACT et autres pour une meilleure coordination de réponse au niveau régional et international.*

3.3. Priorité n°3 : Renforcement de la culture de cybersécurité

La sécurisation du cyberespace doit être l'affaire de tous les citoyens quel que soit leur niveau. Tous les utilisateurs ont des responsabilités non seulement par rapport à leur propre sécurité mais par rapport à la sécurité globale du cyberespace.

En plus des vulnérabilités, le cyberespace de Burkina présente deux insuffisances majeures que sont :

- un manque de familiarité et connaissance sur la cybersécurité : le niveau de sensibilisation et d'information du citoyen est jugé non satisfaisant et l'organisation des campagnes de formation et de sensibilisation n'est pas systématique.

- une insuffisance de ressources humaines qualifiées pour assurer la sécurité des systèmes d'information : le niveau en cybersécurité des employés recrutés est médiocre.

Pour assurer la sécurisation du cyberespace, tout citoyen doit avoir accès aux informations de base pour contribuer à la prévention contre les intrusions, les attaques ou tout autre incident de sécurité.

Les objectifs de cette priorité sont entre autres de:

- Promouvoir un programme national de sensibilisation de tous les citoyens burkinabè, le monde des affaires, la force de travail et la population en général pour sécuriser la partie du cyberespace sous leur contrôle ;
- Adopter des programmes de formation et d'éducation adéquats pour supporter les besoins en cybersécurité de la nation ;
- Promouvoir avec le secteur privé des programmes de certification professionnelle en cybersécurité ;

3.3.1. Sensibilisation

L'ANSSI travaillera en coordination avec le secteur public et le secteur privé pour faciliter des campagnes de sensibilisation spécifiques pour chaque audience, des campagnes de « vivre en sécurité sur le cyberespace » et le développement de programmes de récompense et de distinction pour les citoyens ou les organisations qui apportent une importance significative à la sécurité.

- Encourager les utilisateurs finaux et les petites structures à aider à la sécurisation du cyberespace en protégeant leur propre connexion à ce dernier par :

- *L'installation et la mise à jour régulière des pare-feu,*
- *L'installation et la mise à jour régulière des anti-virus,*
- *La mise à jour régulière de leurs systèmes d'exploitation et applications importantes avec l'amélioration de sécurité.*

Pour ce faire, il faudra rapprocher ces derniers aux utilisateurs par la mise en place des dépôts locaux (repository).

- Encourager les grandes structures à évaluer la sécurité de leur système d'information qui peut avoir un impact sur les infrastructures critiques de la nation. De telles évaluations peuvent inclure :

- *Conduire des audits réguliers pour vérifier l'efficacité des mesures, solutions et procédures déployées ;*
- *Développer des plans de continuité qui prennent en compte des personnels et des équipements hors site ;*
- *Participer aux initiatives de partage d'information et de bonnes pratiques au niveau de leurs secteurs respectifs ainsi qu'avec les institutions nationales.*

- Encourager le partenariat public-privé pour la dissémination des bonnes pratiques de cybersécurité aussi bien dans les structures gouvernementales que non gouvernementales.

3.3.2. Formation

En plus des campagnes de sensibilisation, le Burkina Faso doit dédier des ressources à la formation des citoyens compétents, spécialisés dans la sécurisation du cyberespace. Les réseaux et les infrastructures se sont développés très rapidement alors que les programmes de formation n'ont pas suivi.

Il s'agira donc d'adopter en coordination avec le Ministère de l'Enseignement Supérieur et de la Recherche et le Ministère de l'Enseignement Technique et de la Formation Professionnelle, des programmes de formation et d'éducation appropriés pour les besoins de cybersécurité de la nation :

- *Former des spécialistes :*

  - opérationnels (sécurité des systèmes informatiques et réseaux, exploitation et gestion de la sécurité,...) ;

  - recherche et investigation (audits, investigations numériques, espionnages et contre espionnages numériques, etc.) ;

- *Intégrer la sécurité dans la formation des administrateurs réseaux et systèmes, des ingénieurs systèmes et même des développeurs ;*

- *Encourager des projets de recherche sur la cybersécurité.*

3.3.3. Certification

Au-delà de l'éducation et de la formation, la certification peut fournir aux employés, les aptitudes techniques et les connaissances nécessaires pour mieux gérer les solutions et infrastructures qu'ils ont sous leur contrôle.

- Aller au-delà des certifications proposées de façon systématique par les vendeurs de solutions ;

- *Proposer des programmes de certification en sécurité qui tiennent compte du background et des aptitudes des candidats ainsi que des enjeux de la sécurisation du cyberespace qui soient acceptés par la communauté locale.*

- *Proposer des programmes de certification des auditeurs qui seront utilisés pour auditer les infrastructures critiques.*

CONCLUSION

La dépendance du Burkina sur son cyberespace va continuer au fil des années. Cette dépendance doit être gérée dans un effort continuel pour sécuriser les cybersystèmes qui contrôlent l'infrastructure nationale.

Sécuriser le cyberespace est un exercice complexe et évolutif. Ce plan est développé en étroite collaboration avec les acteurs importants de l'économie qui dépendent de ce cyberespace.

Un partenariat public-privé et un effort national sont nécessaires pour la mise en œuvre de ce plan national.

Le plan national a identifié trois grandes priorités qui aideront à atteindre les objectifs fixés :

Priorité n°1 : **Réduction de la vulnérabilité du cyberespace**

Priorité n°2 : Gestion des incidents

Priorité n°3 : Renforcement de la culture de cybersécurité

Ces trois priorités vont aider à prévenir, décourager et protéger contre les attaques. Elles créent aussi un processus et les moyens pour minimiser les dommages et accélérer la reprise en cas d'attaques.

Le plan national de cybersécurité n'est que la première étape d'un effort pour sécuriser l'infrastructure d'information nationale.

Le gouvernement utilisera plusieurs moyens pour implémenter cette stratégie. Il faudra doter les départements ministériels responsables de la coordination des initiatives de sécurité au niveau des secteurs critiques ainsi que l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), le centre de coordination de la gestion des incidents, les cyberdivisions... de moyens adéquats pour exécuter leurs responsabilités.

Ces derniers doivent se doter de programmes et plans pour exécuter les initiatives qui leur sont assignées par ce plan national.

Les citoyens burkinabè à tous les niveaux doivent être sensibilisés et encouragés à participer à cet effort national. Des prix de récompense doivent être attribués à ceux qui apportent des contributions significatives à la sécurité de ce cyberespace.

Cybersécurité et vie privée ne doivent pas être des objectifs opposés. Les initiatives de cybersécurité doivent renforcer et non fragiliser la vie privée et les libertés individuelles.

Pour des raisons pratiques et de budget, l'ANSSI et le CSIRT pourraient être fusionnés sous une entité unique qui prenne en compte les différentes missions des deux entités dans une première phase de mise en œuvre.

Ce plan national doit être révisé régulièrement pour prendre en compte les changements technologiques, les réalités du terrain et l'évolution du cyberespace.

GLOSSAIRE

ANSSI : Agence Nationale de Sécurité des Systèmes d'Information

CSIRT: Computer Security Incident Response Team

DNSSEC: Domain Name System Security Extension

FIRST: Forum Incident Response and Security Teams

IMPACT: International Multilateral Partnership Against Cyber Threats

IPv6 : Internet Protocol version 6

NGN: Next Generation Network

IETF: Internet Engineering Task Force

IP: Internet Protocol

UAGI: Unité d'Analyse et de Gestion des Incidents

UIT: Union Internationale des Télécommunications