Table des matières

Objectifs du module

Bienvenue dans le module de connaissances sur les **infrastructures d'information essentielles et la protection des** infrastructures d'information essentielles dans le cadre du projet GFCE-Afrique.

Ce module de connaissances répondra aux besoins des États membres de l'UA en matière de protection des infrastructures essentielles (IE) et des infrastructures d'information essentielles (IIE). Le module s'adresse (principalement) aux décideurs politiques et aux décideurs impliqués dans divers domaines (affaires étrangères, développement économique, sécurité et criminalité, télécommunications, finances, etc.), et à ceux qui souhaitent se familiariser avec les concepts liés aux risques, aux acteurs et à la protection des infrastructures essentielles et des infrastructures d'information essentielles.

À la fin du module, vous serez en mesure de répondre aux questions et de trouver des ressources supplémentaires dans les domaines d'intérêt suivants :

1. Introduction

Chaque pays dispose d'infrastructures essentielles qui lui permettent de fonctionner. Ces infrastructures essentielles varient d'un pays à l'autre, car elles sont identifiées sur la base de l'évaluation nationale des risques d'un pays. Il s'agit notamment de l'approvisionnement en énergie et en eau, des télécommunications, des systèmes financiers et des services gouvernementaux. En Afrique, ces infrastructures sont de plus en plus surveillées et contrôlées par des réseaux et des systèmes connectés à Internet. Les menaces à la cybersécurité exploitent la complexité et la connectivité accrues de ces infrastructures, mettant en danger la sécurité, l'économie, la sûreté et la santé publique d'un pays.

Ces infrastructures d'information et de communication interconnectées s'appellent infrastructures essentielles (IE) et infrastructures d'information essentielles (IIE). Un incident cybersécuritaire ayant un impact sur les IE et les IIE peut perturber l'ordre social, la fourniture de services essentiels et le bien-être économique d'un pays. Il est donc impératif qu'une nation mette en place des stratégies, des politiques et des activités qui assurent l'identification, la sécurité et la protection des IE et des IIE en utilisant une approche de gestion des risques.

2. Qu'est-ce que les infrastructures essentielles (IE) et les infrastructures d'information essentielles (IIE) ?

Il n'existe pas de définitions universellement reconnues pour les infrastructures essentielles (IE) et les infrastructures d'information essentielles (IIE). Il existe différentes définitions nationales, régionales et internationales des IIE disponibles sur CIpedia. Une définition standard est fournie par l'IETF Request for Comments (RFC): 4949 comme *des systèmes qui sont si vitaux pour une nation que leur incapacité ou leur destruction aurait un effet débilitant sur la sécurité nationale, l'économie ou la santé et la sécurité publiques*. La définition des IE et des IIE est importante pour la classification, l'enregistrement et les ressources.

Recommandation : Comprendre les définitions des secteurs et services relatifs aux IIE d'autres pays

Lors de la définition des infrastructures essentielles d'un pays, il est recommandé de comprendre les définitions des secteurs et des services relatifs aux IIE d'autres pays... « *on peut s'inspirer des ensembles de secteurs et de services relatifs aux IE définis par d'autres pays* ».

La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel définit les infrastructures essentielles de cybersécurité et de TIC comme des « cyber-infrastructures essentielles aux services vitaux pour la sécurité publique, la stabilité économique, la sécurité nationale, la stabilité internationale, ainsi que pour la durabilité et la restauration du cyberespace essentiel ».

Le guide de bonnes pratiques GFCE-MERIDIAN définit les infrastructures d'information essentielles (IIE) comme « les infrastructures d'information et de communication interconnectées qui sont essentielles au maintien des fonctions vitales de la société (santé, sûreté, sécurité, bien-être économique ou social des personnes) - dont la perturbation ou la destruction aurait de graves conséquences ».

Les États-Unis et la Cybersecurity and Infrastructure Security Agency (CISA) définissent les secteurs essentiels de l'économie comme des secteurs d'infrastructure dont les actifs, les systèmes et les réseaux, qu'ils soient physiques ou virtuels, sont considérés comme si vitaux que leur incapacité ou leur destruction aurait un effet débilitant sur la sécurité, la

sécurité économique nationale, la santé ou la sûreté publique nationale, ou toute combinaison de ces éléments.

La Recommandation du Conseil de l'OCDE sur la protection des infrastructures d'information essentielles (anglais, français) définit les infrastructures d'information essentielles (IIE) comme *« des systèmes et réseaux d'information interconnectés dont la perturbation ou la destruction aurait un impact grave sur la santé, la sûreté, la sécurité ou le bien-être économique des citoyens, ou sur le fonctionnement efficace du gouvernement ou de l'économie ».*

La définition britannique des infrastructures nationales essentielles est la suivante : « *les éléments essentiels de l'infrastructure (à savoir les actifs, les installations, les systèmes, les réseaux ou les processus et les travailleurs essentiels qui les exploitent et les facilitent), dont la perte ou la compromission pourrait entraîner : a) un impact préjudiciable majeur sur la disponibilité, l'intégrité ou la fourniture de services essentiels – y compris les services dont l'intégrité, si elle est compromise, pourrait entraîner de nombreux décès ou blessures – compte tenu des répercussions économiques ou sociales importantes ; et/ou b) un impact significatif sur la sécurité nationale, la défense nationale ou le fonctionnement de l'État*. »

Études de cas : Définitions des IE et des IIE selon les pays africains

La loi ghanéenne de 2020 sur la cybersécurité (loi 1038) définit les infrastructures d'information essentielles comme un « *ordinateur ou système informatique identifié comme essentiel à la sécurité nationale ou au bien-être économique et social des citoyens* ».

Au Kenya, la référence à la loi de 2018 sur l'utilisation abusive de l'informatique et la cybercriminalité identifie « *comme infrastructures essentielles celles dont la perturbation du système entraînerait :*

- *L'interruption d'un service vital, notamment l'approvisionnement en eau, en services de santé et en énergie*
- *Un effet négatif sur l'économie de la République*
- *Un incident qui entraînerait un grand nombre de blessures ou de décès*
- *Une défaillance ou une perturbation substantielle du marché monétaire de la République ; et*
- *Un effet négatif et grave sur la sécurité de la République, y compris les services militaires et de renseignement »*

Le Cadre national de cybersécurité pour l'Afrique du Sud définit les infrastructures nationales d'information essentielles comme « *tous les systèmes informatiques, systèmes de données, bases de données, réseaux (y compris les personnes, les bâtiments, les installations et les processus) qui sont fondamentaux pour le fonctionnement efficace de la République ».*

La Stratégie nationale de cybersécurité du Botswana définit les infrastructures d'information essentielles comme « *les infrastructures numériques dont les perturbations ou les dommages affectent négativement le bon fonctionnement de l'économie* ».

3. Quelles sont les menaces qui pèsent sur les infrastructures essentielles en Afrique ?

Aujourd'hui, de nombreux pays africains sont confrontés à des défis dans la protection de leurs infrastructures essentielles. Il s'agit notamment de l'absence de politiques et de lois, de l'absence d'un cadre d'échange d'informations et de coordination pour les infrastructures détenues ou gérées par le gouvernement et le secteur privé, des capacités et de ressources insuffisantes, d'actes de terrorisme et de vandalisme.

Ressources : *Exemples d'attaques contre des infrastructures essentielles en Afrique*

Libéria : En 2016, un pirate informatique trop zélé employé par une grande entreprise de télécommunications a saboté le réseau d'un rival, ce qui a privé la moitié du pays de ses transactions bancaires. Coupé de l'accès à Internet, le ministre libérien de l'Information, apparemment chargé de la réponse pays, a demandé de l'aide à la radio française. Malgré les appels à l'aide lancés par le Libéria à l'étranger, les autorités n'ont procédé à des arrestations qu'après que le logiciel utilisé dans l'attaque ait été utilisé pour désactiver Deutsche Telekom.

Nigeria : En août 2012, Boko Haram aurait piraté les bases de données des dossiers personnels des services secrets nigérians, révélant les noms, adresses, informations bancaires et membres de la famille du personnel actuel et ancien de l'agence d'espionnage. La violation a été exécutée au nom de Boko Haram en réponse à la gestion par le Nigeria des interactions avec le groupe. Cette attaque était importante car elle représentait un changement substantiel dans les tactiques du groupe, qui a une position anti-occidentale.

Afrique du Sud : En juin 2020, Life Healthcare, le deuxième plus grand opérateur d'hôpitaux privés en Afrique du Sud, a été frappé par une cyberattaque. Cette attaque,

qui s'est produite pendant la pandémie de COVID-19 et qui aurait coûté à l'organisation plus d'un mois d'indisponibilité, a affecté ses systèmes d'admission, ses systèmes de traitement d'entreprise et ses serveurs de messagerie, certains systèmes étant mis hors ligne.

L'entreprise publique Transnet, qui exploite des chemins de fer, des ports et des pipelines en Afrique du Sud, a fait face à une cyberattaque en juillet 2021. L'attaque a amené Transnet à déclarer le cas de force majeure dans plusieurs terminaux à conteneurs clés, notamment le port de Durban, Ngqura, Port Elizabeth et Cape Town. L'impact de l'attaque a été « sans précédent » selon l'Institut d'études de sécurité (ISS) car il s'agissait de « l'intégrité opérationnelle des infrastructures maritimes essentielles du pays qui avait subi une grave perturbation » pour la première fois, entraînant la fermeture d'une route commerciale essentielle et la perturbation des services commerciaux vitaux au milieu d'une pandémie mondiale.

La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel exige des États qu'ils élaborent une politique nationale et une stratégie de cybersécurité qui définissent les objectifs et les délais de mise en œuvre efficace de la politique. Élaborée en collaboration avec les parties prenantes et fondée sur une approche tous risques, la politique devrait identifier les risques auxquels le pays est confronté et reconnaître l'importance des infrastructures d'information essentielles (IIE). La convention exige des pays qu'ils adoptent les mesures législatives et/ou réglementaires nécessaires pour identifier et protéger les secteurs et les systèmes liés aux technologies de l'information et de la communication qui sont essentiels à la sécurité nationale et au bien-être de l'économie.

La protection des infrastructures essentielles exige l'engagement national énoncé dans la stratégie, la politique et la législation pertinentes.

> « Protéger les infrastructures essentielles et les infrastructures d'information essentielles, c'est comme prédire un tremblement de terre. En géologie, nous savons le lieu de survenance et la magnitude d'un tremblement de terre, mais ce que nous ne savons pas, c'est le moment. »
> Source vidéo : Webinaire de la Strathmore University Business School – Infrastructures d'information essentielles au Kenya : explorer l'efficacité et l'impact du cadre juridique et institutionnel existant

Exercice : Cyberattaques contre les infrastructures

1. Identifiez les cyberattaques contre les infrastructures qui se sont produites dans votre pays.
2. Quel a été l'impact économique et social de la perturbation causée par l'attaque ?
3. Quelles mesures le Gouvernement a-t-il mises en place pour prévenir et atténuer des attaques similaires ?

4. Comment identifier, classer et enregistrer les IE

L'identification des infrastructures essentielles et des secteurs et sous-secteurs qui y sont associés est différente et spécifique à chaque pays.

4.1. Méthodologies d'identification et de classification des infrastructures essentielles

Il existe diverses méthodologies pour identifier les IIE, notamment l'utilisation d'une approche basée sur les services, l'application de critères sectoriels ou fonctionnels, ainsi qu'une évaluation des parties prenantes. Le Guide d'élaboration d'une stratégie nationale de cybersécurité recommande l'évaluation des cyberrisques et la modélisation des menaces pour identifier, désigner et protéger les IE, les IIE ou les services essentiels.

- **Dépendances et interdépendances** : L'examen des dépendances et des interdépendances avec d'autres infrastructures et services est recommandé dans l'identification des I(I)E. Une dépendance se définit comme « la relation entre deux produits ou services dans laquelle un produit ou service est requis pour la génération de l'autre produit ou service »

Recommandation : analyse de la dépendance (nationale et transfrontalière)

Les dépendances peuvent être reconnues au cours du processus d'identification des IE et des évaluations de risque. Ce sont les dépendances des IE au sein d'une nation et celles des nations et régions voisines. Les dépendances peuvent influencer la criticité d'une infrastructure nationale particulière et peuvent être déterminées au moyen de consultations avec les intervenants.

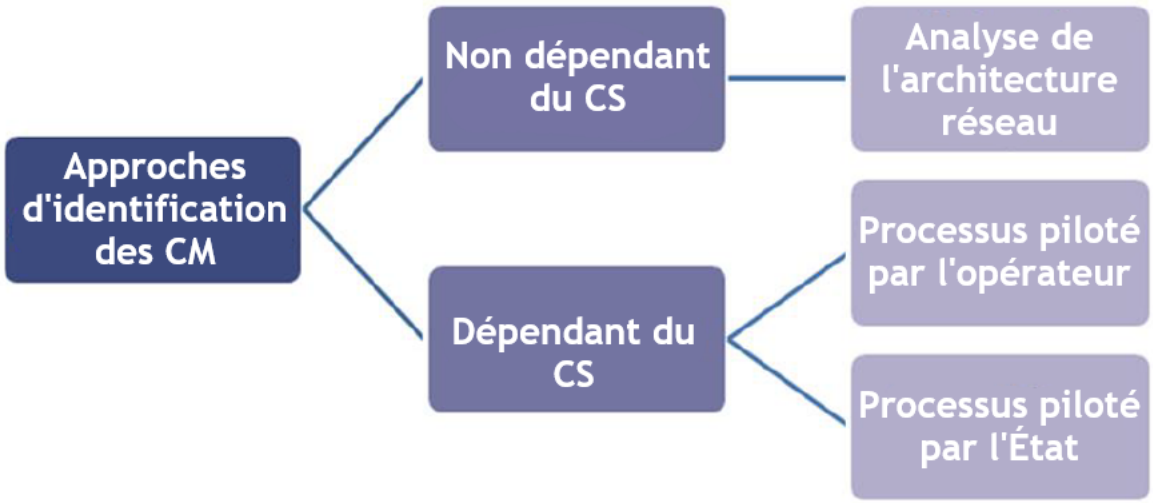

Figure 1 : *Approches méthodologiques pour l'identification des infrastructures d'information essentielles* Source : ENISA

- **Évaluation des risques** : L'identification des IIE nationales devrait être guidée par une évaluation des risques. Une approche fondée sur les risques et les normes internationales est nécessaire pour identifier et hiérarchiser la mise en œuvre de programmes, de politiques et de pratiques de référence communs en matière de sécurité et de résilience des IIE, ainsi que pour assurer leur intégration et leur interopérabilité.

Recommandation : Élaborer un profil de risque national

En élaborant un profil de risque national, les parties prenantes d'un pays acquerraient une compréhension commune des risques, des conséquences et de leur priorité relative. Les pays peuvent utiliser les lignes directrices de l'UE pour l'évaluation des capacités de gestion des risques dans le cadre d'une évaluation des risques.

L'évaluation basée sur un ensemble de 51 questions sur la coordination, l'expertise, la méthodologie, les parties prenantes, l'information et la communication, l'équipement et le financement, aide à identifier et à hiérarchiser les risques, et constitue la base de :

- l'évaluation des risques ;
- la planification de la gestion des risques ;
- la prévention des risques et

- les mesures de préparation.

Le Cadre pour l'amélioration de la cybersécurité des infrastructures essentielles du National Institute of Standards and Technology (NIST) aide les propriétaires et les exploitants d'infrastructures essentielles à identifier, évaluer et gérer les risques cybersécuritaires à l'aide d'une approche hiérarchisée, flexible, reproductible, basée sur les performances et rentable, notamment des mesures et des contrôles de sécurité de l'information.

- **Modélisation des menaces :** il s'agit d'une approche structurée des scénarios de menace ; une technique d'ingénierie pour identifier les menaces, les attaques, les zones vulnérables et les contre-mesures possibles qui pourraient affecter le produit ou l'environnement connexe (réseau, architecture, etc.). À l'aide de méthodes de modélisation des menaces, il est possible de dresser des profils d'attaquants potentiels, y compris leurs objectifs et leurs méthodes, de créer un catalogue de menaces et d'utiliser les informations pour éclairer les mesures défensives.

Recommandation : adopter une méthodologie pour identifier systématiquement les secteurs et les services des IE

Une approche structurée en quatre étapes pour identifier les secteurs et les services des IE est recommandée dans les méthodologies de l'ENISA pour l'identification des actifs et services des infrastructures d'information essentielles pour l'évaluation d'un secteur ou d'un service qui pourraient potentiellement être essentiels :

1. Appliquer des critères sectoriels
2. Évaluer la criticité
3. Évaluer les dépendances
4. Appliquer des critères transversaux.

L'ordre le plus utile de ces étapes dépend des informations dont disposent les décideurs nationaux.

Ressources : *Comment identifier et classer les IE et les IIE*

Vidéo de formation ITU 2021 Global CyberDrill : comment identifier et classer les actifs et services d'infrastructures d'information essentielles

4.2. Identification des secteurs d'infrastructures d'information essentielles

4.2.1. Comment identifie-t-on les infrastructures essentielles ?

Les critères et le processus d'identification des infrastructures comme « essentielles » sont guidés par les dispositions de la stratégie, de la politique ou de la législation nationale. Le rôle de l'identification diffère d'un pays à l'autre et va du président, au ministre en passant par le chef de l'institution responsable de la protection des infrastructures essentielles.

Etude de cas : *comment identifie-t-on les infrastructures essentielles ?*

En Afrique du Sud, la loi 8 de 2019 sur la protection des infrastructures essentielles prévoit que le ministre responsable des services de police peut déclarer les infrastructures comme « essentielles » sur la base de la recommandation du Conseil des infrastructures essentielles, de la demande de déclaration des infrastructures en tant qu'infrastructures essentielles et de toute autre information pertinente.

Dans la loi tanzanienne de 2015 sur la cybercriminalité, le ministre peut désigner un système informatique comme infrastructure d'information essentielle, par ordonnance publiée dans la Gazette. L'ordonnance peut prescrire des lignes directrices ou des procédures pour l'enregistrement, la protection, la gestion des infrastructures d'information essentielles, la gestion et la conservation des données associées, les plans de reprise après sinistre et l'audit.

Dans la loi kényane de 2018 sur l'utilisation abusive de l'informatique et la cybercriminalité, le directeur, qui est le secrétaire du Comité national de coordination de l'informatique et de la cybercriminalité (NC4), identifie un système comme étant une infrastructure essentielle si elle répond à la définition des infrastructures essentielles et est conforme à un cadre d'infrastructures essentielles.

Dans la loi nigériane de 2015 sur la cybercriminalité (interdiction, prévention, etc.), le président peut, sur recommandation du conseiller à la sécurité nationale, par ordonnance publiée dans la Gazette fédérale, identifier certains systèmes informatiques et/ou réseaux comme constituant des infrastructures d'information nationales essentielles s'il le souhaite, lorsqu'ils sont inopérants ou détruits, lorsqu'ils affaiblissent la sécurité nationale ou économique, la santé publique et la sûreté.

4.2.2. Quels sont les secteurs d'IIE identifiés ?

En ce qui concerne la définition, l'identification et la classification des IIE, un pays peut élaborer un registre national des infrastructures d'information essentielles. Un registre précis et à jour de tous les actifs et emplacements déclarés comme infrastructures essentielles devrait être tenu par l'entité chargée de la gestion et de la protection des infrastructures essentielles.

Étude de cas : Secteurs désignés de IIE

La loi ghanéenne de 2020 sur la cybersécurité (articles 35) a identifié 13 secteurs relatifs aux IIE : sécurité nationale et renseignement, technologies de l'information et de la communication (TIC), banque et finances, énergie, eau, transports, santé, services d'urgence, services administratifs, alimentation et agriculture, fabrication, mines et éducation.

La Stratégie nationale de cybersécurité du Botswana a identifié les secteurs suivants comme secteurs nationaux d'infrastructures essentielles en ce qui concerne la cybersécurité : finances, communications, énergie, eau, services d'urgence, alimentation, sécurité publique, santé, services publics et administration en ligne.

Le directeur du Comité national de coordination de l'informatique et de la cybercriminalité (NC4) du Kenya, dans un avis publié dans la Gazette (en vigueur le 20 janvier 2022), a identifié comme infrastructures essentielles les secteurs suivants : télécommunications, élection, justice, éducation, santé, alimentation, eau, terre, énergie, transports et industrie, banque, finance, défense, sécurité et sûreté publique

La Stratégie nationale de cybersécurité de Maurice identifie les secteurs essentiels tels que les services financiers, le tourisme, l'électricité, l'eau, les TIC et la radiodiffusion, la santé, les services administratifs, la fabrication, les transports et la logistique, le sucre et les douanes.

Ressource : **Cybersécurité sous forme** vidéo *et protection des infrastructures essentielles*

Discussions lors du webinaire de l'Université de Fairfax :

- Plan américain de protection des infrastructures nationales (NIPP),
- Secteurs relatifs aux infrastructures essentielles,
- Cyber-risques communs partagés par tous les éléments des infrastructures essentielles,
- Comment la directive de politique présidentielle/PPD 21 - Sécurité et résilience des infrastructures essentielles soutient le besoin de résilience aux cyber-risques,
- Aperçu du cadre du National Institute of Standards and Technology (NIST) pour l'amélioration de la cybersécurité des infrastructures essentielles,
- Méthodologie de prise en charge de la protection des infrastructures essentielles et suggestions d'amélioration de la résilience aux cyber-risques.

Ressource : Secteurs relatifs aux IIE dans d'autres pays

Les États-Unis d'Amérique comptent 16 secteurs d'IE : chimie ; installations commerciales ; communications ; fabrication essentielle ; barrages ; base industrielle de défense ; services d'urgence ; énergie ; services financiers ; alimentation et agriculture ; établissements administratifs ; soins de santé et santé publique ; technologie de l'information ; réacteurs, matières et déchets nucléaires ; systèmes de transport ; et systèmes d'approvisionnement en eau et de gestion des eaux usées.

La directive de l'Union européenne (UE) sur la sécurité des réseaux et des systèmes d'information (directive SRI) exige que les États membres adoptent une stratégie nationale sur la sécurité des réseaux et des systèmes d'information définissant les objectifs stratégiques et les mesures politiques et réglementaires appropriées couvrant au moins les sept secteurs relatifs aux IE : énergie, transports, banque, marché financier, santé, approvisionnement et distribution d'eau potable, et infrastructures numériques.

Le rapport de la Commission au Parlement européen et au Conseil évalue la cohérence des approches adoptées par les États membres pour identifier les opérateurs de services essentiels (OES) conformément à l'article 23, paragraphe 1, de la directive 2016/1148/UE relative à la sécurité des réseaux et des systèmes d'information.

La loi PCII en France adoptée en décembre 2013 et le cadre pour la « sécurité des activités d'importance vitale » établi en 1998 identifient plus de 200 opérateurs essentiels (appelés « opérateurs d'importance vitale ») dans 12 secteurs dont : l'alimentation, la santé, l'eau, les télécommunications et la radiodiffusion, l'espace et la

recherche, l'industrie, l'énergie, les transports, les finances, l'administration civile, les activités militaires et la justice. En vertu de la loi, ces opérateurs sont tenus d'identifier leurs « systèmes d'information essentielles », c'est-à-dire les systèmes « dont l'indisponibilité pourrait fortement menacer le potentiel économique ou militaire, la sécurité ou la résilience de la nation ».

Le Centre for the Protection of National Infrastructure (CPNI) du Royaume-Uni a identifié 13 secteurs d'infrastructures nationales : produits chimiques, nucléaire civil, communications, défense, services d'urgence, énergie, finances, alimentation, administration, santé, espace, transports et eau. Plusieurs secteurs ont défini des « sous-secteurs » ; les services d'urgence, par exemple, peuvent être scindés en police, ambulance, services d'incendie et garde côtière.

***Exercice** :*

Sur la base des exemples nationaux, régionaux et internationaux de définition, d'identification et de classification des infrastructures essentielles évoqués, en prenant exemple sur votre pays :

- Définir les infrastructures essentielles et les infrastructures d'information essentielles I(I)E
- Identifier les I(I)E
- Classer les I(I)E
- Quels principes/critères avez-vous utilisés ?

5. Directives en matière de politique, de législation et de réglementation

Lors de l'élaboration des politiques, des lois et des directives nationales pour la protection des IE et des IIE, un examen des dispositions des conventions, lois et structures internationales existantes devrait être envisagé.

La résolution 58/199 (2003) de l'Assemblée générale des Nations Unies intitulée « Création d'une culture mondiale de la cybersécurité et de la protection des infrastructures d'information essentielles » reconnaît que chaque pays déterminera ses propres infrastructures d'information essentielles et invite les États membres à prendre en considération les éléments de protection des infrastructures d'information essentielles dans l'élaboration des stratégies visant à réduire les risques pour les infrastructures d'information essentielles, conformément aux lois et réglementations nationales ;

La stratégie antiterroriste mondiale des Nations unies dans le cadre du deuxième pilier « Mesures de lutte et de prévention du terrorisme », les États membres ont décidé « d'intensifier tous les efforts visant à améliorer la sécurité et la protection des cibles particulièrement vulnérables, telles que les infrastructures et les lieux publics, ainsi que la réponse aux attaques terroristes et autres problèmes, en particulier dans le domaine de la protection civile ».

Le Rapport de 2015 du Groupe d'experts gouvernementaux des Nations Unies sur l'évolution de la situation dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale (paragraphe 13g) recommande d'examiner des normes volontaires et non contraignantes pour un comportement responsable des États dans le cyberespace, notamment en prenant des mesures appropriées pour protéger leurs infrastructures essentielles contre les menaces liées aux TIC, compte tenu de la résolution 58/199 de l'Assemblée générale sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures d'information essentielles, et d'autres résolutions pertinentes.

L'article 24 de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel exige des signataires qu'ils élaborent, en collaboration avec les parties prenantes, une politique nationale de *cybersécurité* qui reconnaisse l'importance des infrastructures d'information essentielles (IIE) pour la nation afin d'identifier les risques auxquels la nation est confrontée en utilisant l'approche tous risques et de décrire comment les objectifs de cette politique doivent être atteints.

En vertu de l'article 25 de la convention, les États sont tenus d'adopter les mesures législatives et/ou réglementaires qu'ils jugent nécessaires pour identifier les secteurs considérés comme sensibles pour leur sécurité nationale et le bien-être de l'économie, ainsi que les systèmes de technologies de l'information et de la communication conçus pour fonctionner dans ces secteurs en tant qu'éléments des infrastructures d'information essentielles ; et, à cet égard, proposer des sanctions plus sévères pour les activités criminelles sur les systèmes TIC dans ces secteurs, ainsi que des mesures visant à améliorer la vigilance, la sécurité et la gestion.

En outre, il existe des exigences dans les accords signés dans le cadre des Communautés économiques régionales en Afrique, tels que le Protocole de coopération en matière de politique, de défense et de sécurité de la SADC, 2001, qui visent à établir un cadre institutionnel par lequel les États membres pourraient coordonner les politiques et les activités dans les domaines de la politique, de la défense et de la sécurité.

L'Organe pour la politique, la défense et la sécurité créé en vertu de ce protocole appuie la réalisation et le maintien de la sécurité et de l'état de droit dans la région de la SADC. Les objectifs de l'Organe portent sur les domaines de l'armée/défense, de la prévention du crime, du renseignement, de l'application et du maintien de la paix, de la politique étrangère, de la gestion des conflits, de la prévention et de la résolution, et des droits de l'homme. Les activités spécifiques visant à atteindre ces objectifs sont définies dans le Plan indicatif stratégique de l'Organe de coopération politique, de défense et de sécurité (SIPO I). Il s'agit notamment d'évaluations régulières de la situation régionale en matière de sécurité publique et de renforcement des capacités de lutte contre la cybercriminalité et le terrorisme.

Point de réflexion :
Quelles conventions internationales, régionales et exigences législatives et réglementaires nationales votre pays a-t-il utilisées pour mettre en œuvre des politiques, des stratégies et des structures de protection des infrastructures essentielles ?

Exercice

Sur la base des exemples donnés, votre pays devrait-il envisager d'élaborer un plan national de gestion des cybercrises ?

Préparer une justification ou une note conceptuelle faisant référence aux dispositions pertinentes en matière de stratégie, de politique et de législation à présenter au président ou au ministre concerné.

6. Comment élaborer une politique de protection des infrastructures essentielles et des infrastructures d'information essentielles

Le guide de bonnes pratiques GFCE-MERIDIAN définit la protection des infrastructures d'information essentielles (PCII) comme suit : « Toutes les activités visant à assurer la fonctionnalité, la continuité et l'intégrité des IIE afin de dissuader, d'atténuer et de neutraliser une menace, un risque ou une vulnérabilité ou de minimiser l'impact d'un incident ».

La PCII est un élément essentiel de la cybersécurité et fait partie intégrante de la stratégie nationale de cybersécurité. Un pays peut envisager d'élaborer une politique de PCII pour établir la cohérence et la coordination des activités, des ressources et des initiatives nécessaires afin de protéger les infrastructures essentielles contre les catastrophes naturelles et les incidents cybernétiques.

Une politique nationale de protection des IE et des IIE est guidée par un ensemble de principes déterminés par le gouvernement et est influencée par les conventions, les normes et les meilleures pratiques internationales et régionales. L'objectif de cette politique est d'établir un cadre national pour l'harmonisation et la coordination de la protection des infrastructures essentielles.

Les Lignes directrices sur les infrastructures Internet pour l'Afrique recommandent aux décideurs d'utiliser quatre principes essentiels comme guide dans l'élaboration de stratégies et de politiques pour la sécurité des infrastructures Internet. Ces principes sont les suivants :

1. Sensibilisation : une compréhension des risques de sécurité, de leur impact sur l'écosystème des infrastructures Internet.
2. Responsabilité : responsabilisation des intervenants et compréhension des répercussions potentielles de leurs actions ou de leur inaction.
3. Coopération : dialogue pour encourager la coopération et la responsabilité collective entre toutes les parties prenantes.
4. Droits fondamentaux et propriétés de l'Internet : respect de la transparence et non-violation des propriétés fondamentales de l'internet : collaboration volontaire, normes ouvertes, blocs de construction technologiques réutilisables, intégrité, innovation sans autorisation et portée mondiale.

Recommandation : principes du G8 pour la protection des infrastructures d'information essentielles

Les Principes du G8 pour la protection des infrastructures d'information essentielles comprennent la coordination et la collaboration nationales, régionales et internationales, l'échange d'information, l'identification des interdépendances, la détermination des rôles et des responsabilités des intervenants, l'amélioration des capacités, la fourniture juridique adéquate, la recherche et le développement, et l'application de normes certifiées à l'échelle internationale.

Les étapes de base de l'élaboration et du maintien d'une politique actuelle de la PCII sont les suivantes :

Étape 1. Faire de la PCII une priorité nationale : une politique de PCII est plus efficace si elle est intégrée au Profil national des risques (PNR) et à la Stratégie nationale de cybersécurité et mise en œuvre par un comité composé d'une représentation multisectorielle des intervenants de haut niveau.

Étape 2. Identification des infrastructures d'information essentielles : les infrastructures essentielles peuvent être identifiées à l'aide des quatre piliers méthodologiques inspirés de la directive européenne sur les infrastructures essentielles (EC2008). Les quatre piliers sont les suivants :

1. appliquer des critères sectoriels
2. évaluer la criticité
3. évaluer les dépendances
4. appliquer des critères transversaux.

Étape 3. Élaboration d'une politique de protection des infrastructures d'information essentielles, notamment :

3a. une approche fondée sur les risques (par rapport à une approche ad hoc)
Consulter la section 4

3b. l'intégration d'une PCII dans la gestion nationale des crises
Consulter la section 7

3c. le soutien à la mise en réseau et au partage des informations
La protection des infrastructures essentielles repose sur une communication fiable, sécurisée et efficace entre les différentes parties prenantes.

Recommandation : adopter une approche multi-agences et commencer à partager les informations

Les gouvernements devraient adopter une approche multi-organismes pour faire face aux risques et à la complexité associés à la PCII aux niveaux stratégique, tactique, opérationnel et technique.

Il faudrait envisager de réunir régulièrement les intervenants sélectionnés en fonction de leur mandat légal, de la propriété et de

l'exploitation des infrastructures essentielles. Ces intervenants comprennent les ministères et organismes gouvernementaux, la sécurité nationale, la défense et la police, l'équipe nationale d'intervention d'urgence en matière de sécurité informatique ainsi que les propriétaires et exploitants d'infrastructures essentielles du secteur privé.

D'autres recommandations en matière de réseautage et de partage d'information sont les suivantes :

1. Stimuler le partage d'informations liées à la cybersécurité
2. Établir des rôles clairs au sein de la PCII dans le cadre du partage des initiatives
3. Être informé des normes d'échange d'informations
4. Prenez note du guide de partage d'informations sur les cybermenaces
5. Le système de jumelage
6. Diverses formes d'organisation des partenariats public-privé pour la PCI/PCII
7. Conseil de la cybersécurité au niveau national
8. Protocole des feux de signalisation (TLP)

Source : Chapitre 7 Guide de bonnes pratiques GFCE-MERIDIAN sur la protection des infrastructures d'information essentielles à l'intention des décideurs

Étape 4. Suivi et amélioration continue

La mise en œuvre réussie de la politique dépend du suivi et de l'évaluation périodiques (S&E). La surveillance comprend le suivi des interventions, des initiatives et des ressources proposées par rapport aux résultats escomptés des politiques, tandis que l'évaluation implique la détermination de la valeur de la mise en œuvre et des réalisations de la politique. Les résultats du S&E sont mis à la disposition des parties prenantes et des commentaires sont fournis pour améliorer les initiatives futures.

7. Plan national de gestion des cybercrises

Le Guide d'élaboration d'une stratégie nationale de cybersécurité recommande aux pays d'envisager d'élaborer un plan national d'urgence en matière de cybersécurité dans le cadre du plan national global de gestion des situations d'urgence ou des crises ou de l'harmonisation avec celui-ci. Ce plan devrait tenir compte des conclusions des évaluations nationales des risques, prévoir des mécanismes de reprise après sinistre et d'intervention en cas d'incident. Le plan d'urgence en matière de cybersécurité devrait déterminer les dépendances intersectorielles qui pourraient affecter les infrastructures

essentielles et classer les cyberincidents en fonction de leur impact sur les actifs et services essentiels.

Plusieurs pays africains ont des plans ou des politiques de gestion des catastrophes qui traitent de la gestion des catastrophes naturelles. Basés sur une approche systématique, ces plans, qui peuvent faire référence à la convention de Tampere, fournissent des lignes directrices, des principes et un code de conduite aux parties prenantes, ainsi que la promulgation d'une législation qui soutient la mise en place d'un cadre institutionnel. Les plans de gestion des catastrophes prévoient également divers moyens de mobilisation des ressources ainsi qu'un cadre de suivi et d'évaluation. Ces plans doivent être mis à jour pour inclure la gestion des cyberincidents et la protection des infrastructures essentielles.

Un plan national de gestion des cybercrises peut être défini comme un cadre stratégique qui énonce les rôles et les responsabilités, les capacités et les structures de coordination qui soutiennent la façon dont une nation réagit aux cyberincidents importants qui présentent des risques pour les infrastructures essentielles et s'en remet.

Il peut également être défini comme un plan stratégique qui recommande et développe les actions et les responsabilités d'une approche coordonnée et multidisciplinaire pour répondre aux incidents de cybersécurité d'importance nationale ayant une incidence sur les systèmes essentiels et l'économie.

Les objectifs du Plan national de gestion des cybercrises sont les suivants :

- Recommander et préciser les mesures et les responsabilités en matière d'approche coordonnée et multidisciplinaire pour répondre aux incidents de cybersécurité d'importance nationale ayant une incidence sur les systèmes essentiels et l'économie et s'en remettre.
- Minimiser les interruptions de services ou la perte/le vol d'informations causées par des incidents.
- Utiliser les informations obtenues pour une meilleure préparation au traitement futur des incidents.

Ressources : plans nationaux de gestion des cybercrises

Le National Cyber Incident Response Plan (NCIRP), États-Unis, fournit des conseils pour permettre une approche coordonnée à l'échelle du pays en matière d'activités d'intervention et de coordination avec les parties prenantes lors d'un cyberincident important ayant un impact sur les infrastructures essentielles.

Le Plan de gestion des incidents de cybersécurité du Canada fournit un cadre opérationnel pour la gestion des incidents de cybersécurité qui ont une incidence sur la capacité du gouvernement canadien à offrir des programmes et des services aux citoyens ou qui menacent de l'avoir. Le plan décrit les intervenants et les mesures à prendre pour s'assurer que les incidents de cybersécurité sont traités de manière cohérente, coordonnée et opportune.

Les accords de gestion des cyberincidents pour le gouvernement australien décrivent les arrangements de coordination interjuridictionnelle, les rôles et responsabilités, ainsi que les principes de coopération des gouvernements australiens en réponse aux cyberincidents nationaux.

.

8. Audits de sécurité des infrastructures et évaluations des vulnérabilités

Les audits des infrastructures et les évaluations de vulnérabilité, effectués périodiquement selon des normes minimales, sont essentiels pour la protection de la sécurité nationale. Les résultats des audits comprendraient un profil national des risques (PNR). La stratégie nationale de cybersécurité devrait définir les référentiels minimaux en matière de cybersécurité axés sur les résultats qui sont pertinents pour les opérateurs des IE et des IIE, sur la base des normes internationales et des meilleures pratiques répondant aux priorités de gestion des risques de haut niveau et à la conformité à des pratiques interopérables et cohérentes.

Recommandation : *définition de référentiels de sécurité minimaux*

Le **Guide d'élaboration d'une stratégie nationale de cybersécurité** recommande aux pays d'identifier et de suivre les bonnes pratiques qui soutiennent la vision et les objectifs de la Stratégie nationale de cybersécurité. La définition d'une stratégie minimale de cybersécurité figure parmi ces bonnes pratiques.

La législation ou la réglementation devrait définir les référentiels minimaux en matière de cybersécurité pour les opérateurs des IE et des IIE. Pour assurer l'uniformité, de meilleurs résultats, une plus grande efficacité et une plus grande interopérabilité, les référentiels de sécurité devraient être axés sur les résultats et faire référence à des normes et à des pratiques exemplaires reconnues à l'échelle internationale.

Les référentiels de sécurité portent sur :

- les priorités élevées en matière de gestion des risques
- les pratiques spécifiques en matière de cybersécurité
- l'identification des cyberrisques
- la mise en place de structures de gouvernance de gestion des risques
- les mesures de protection des données et des systèmes
- la surveillance de l'environnement numérique et la détection d'anomalies/événements
- l'intervention et la récupération après des incidents
- les exigences en matière d'approvisionnement

Etude de cas : audits des IIE par pays

La directive du Ghana pour la protection des infrastructures d'information essentielles (IIE) établit des mesures et des procédures d'audit pour assurer la conformité conformément à l'article 38 de la loi de 2020 sur la cybersécurité. L'audit des IIE identifiées est effectué par l'Autorité de cybersécurité (CSA) ou sa référence d'auditeur autorisé pour soumettre des rapports, un registre des risques et toute activité de cybersécurité menée. Les changements importants prévus dans la conception, la configuration, la sécurité ou le fonctionnement des IIE doivent être approuvés par l'Autorité.

Ressource : agence nationale de la sécurité des systèmes d'information (ANSSI) transsectorielle, règles de sécurité pour les opérateurs d'IIE et d'IE

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a défini des règles de sécurité transversales pour les opérateurs d'IIE et d'IE, basées sur l'expérience opérationnelle et les normes internationales existantes qui incluent principalement des mesures d'hygiène et appartiennent à 20 catégories :

- les politiques d'assurance de l'information
- l'accréditation de sécurité
- le mappage réseau
- la maintenance de la sécurité
- la consignation des bonnes pratiques

- la corrélation et l'analyse des journaux
- la détection
- la gestion des incidents de sécurité
- la gestion des alertes de sécurité
- la gestion de crise
- l'identification
- l'authentification
- le contrôle d'accès et la gestion des privilèges
- le contrôle des accès administratifs
- les systèmes d'administration
- la ségrégation dans les systèmes et les réseaux
- la surveillance et filtrage du trafic
- l'accès à distance
- les systèmes mis en place
- les indicateurs

9. Cadre de gouvernance

Le cadre de gouvernance décrit les rôles, les responsabilités en matière de protection des propriétaires d'IE/IIE et des exploitants à l'échelle nationale. Le cadre de gouvernance est guidé par la stratégie, la politique, la législation, les directives, les règlements, les bonnes pratiques et/ou les lignes directrices en matière de cybersécurité.

Étant donné que les IE/IIE ne sont pas souvent détenus ou contrôlés par le gouvernement et que la PCII dépasse généralement les capacités et le mandat d'une seule entité, l'établissement d'une structure de gouvernance interagences telle qu'un comité ou un organisme est important.

Le modèle de gouvernance devrait comprendre :

- l'identification des entités publiques et privées en charge de secteurs verticaux spécifiques
- les responsabilités et la responsabilisation des exploitants d'IE et d'IIE
- les référentiels de cybersécurité intersectoriels et sectoriels
- les processus et protocoles d'échange d'information
- les canaux de communication et mécanismes de coopération
- les structures de coordination et d'harmonisation entre les entités gouvernementales dont les mandats se chevauchent

Étude de cas : Gouvernance des IE et des IIE

L'Autorité ghanéenne de cybersécurité (CSA) fournit un soutien et des conseils à des IIE identifiées conformément aux dispositions de la loi de 2020 sur la cybersécurité (loi 1038).

Le Comité national de coordination de l'informatique et de la cybercriminalité (NC4) est le point de contact central pour les questions de cybersécurité au Kenya et coordonne les cyberactivités en référence aux dispositions de la loi de 2018 sur l'utilisation abusive de l'informatique et la cybercriminalité**.**

10. Participation des intervenants aux IE et IIE

Il est important de faire participer un éventail diversifié d'intervenants dès le début de l'élaboration d'un profil de risque national, car leur acceptation de l'identification, de la classification et de la protection des infrastructures essentielles est indispensable. Divers outils et méthodes peuvent être utilisés pour l'analyse des parties prenantes. Cependant, une simple catégorisation des parties prenantes comme publiques, semi-publiques ou privées, et comme opérant au niveau régional, national ou international, suffirait.

Tout en tirant parti de leurs perspectives, responsabilités et expertises complémentaires, la collaboration entre les intervenants des secteurs public et privé est la pierre angulaire de la protection efficace des infrastructures et des services essentiels.

11. Financement

Les infrastructures essentielles nécessitent des ressources financières, humaines et matérielles qui devraient être identifiées dans la stratégie ou la politique. Les ressources peuvent provenir du gouvernement, des partenaires au développement ou du partenariat public-privé (PPP).

Les propriétaires et les exploitants d'infrastructures essentielles doivent investir considérablement dans leur sécurité et adopter les meilleures pratiques en matière de cybersécurité. Étant donné que ces mesures peuvent ne pas produire immédiatement d'avantages mesurables, le secteur privé peut être à juste titre préoccupé par le rendement des investissements en matière de sécurité. Le gouvernement peut donc

mettre en œuvre des normes et des pratiques pour inciter les propriétaires et les exploitants du secteur privé à s'acquitter de leurs responsabilités individuelles en matière de cybersécurité, en fonction du risque auquel ils sont confrontés et qui justifient les coûts d'investissement dans la cybersécurité.

Ressource : incitations pour les propriétaires et les exploitants d'IE

Le rapport d'analyse de l'étude sur les incitations du décret présidentiel américain 13636: Improving Critical Infrastructure Cybersecurity, Incentives Study définit une incitation comme un coût ou un avantage qui motive une décision ou une action des propriétaires et des exploitants d'actifs d'infrastructures essentielles à adopter le cadre de cybersécurité en cours d'élaboration par le NIST. Il s'agit notamment d'incitations fondées sur le marché telles que l'assurance. Cependant, pour accélérer le rythme de l'amélioration nécessaire de la cybersécurité, l'action gouvernementale peut donner un élan supplémentaire au marché. Aux États-Unis, les incitations contenues dans la législation, les politiques et d'autres sources comprennent des subventions accélérées, le partage d'informations, l'assurance, une nouvelle réglementation/législation, une assistance technique prioritaire, des considérations d'approvisionnement, une reconnaissance publique, des subventions et des incitations fiscales.

12. Renforcement des capacités

La Division de la sécurité des infrastructures de la Cybersecurity and Infrastructure Security Agency (CISA) offre des programmes de formation gratuits aux partenaires du gouvernement et du secteur privé.

Les programmes de formation comprennent des cours fondamentaux sur la protection nationale des infrastructures, tels que l'introduction au Plan national de protection des infrastructures, l'obtention de résultats grâce au partenariat et à la collaboration en matière d'infrastructures essentielles, ainsi que des formations sur la sensibilisation à la sécurité en milieu professionnel, Tireur actif : ce que vous pouvez faire et Protection des infrastructures essentielles contre les menaces internes. Une formation sectorielle spécifique est proposée pour les secteurs de la chimie, des installations commerciales, des barrages, des services d'urgence, des réacteurs, des matériaux et des déchets nucléaires.

13. Facteurs (géo)politiques et sociaux

Les infrastructures essentielles se trouvent généralement à cheval entre les frontières nationales et juridictionnelles. La sûreté et la sécurité de ces infrastructures nécessitent une collaboration entre les partenaires des secteurs public et privé aux niveaux régional et mondial. La coopération internationale, en particulier la volonté et la capacité de partager des informations, un cadre juridique contre la cybercriminalité et une forte culture de la sécurité face à la croissance technologique rapide et aux changements sociaux qui en découlent, renforcent les capacités de sécurité des infrastructures opérationnelles nationales.

Les États-Unis collaborent avec des partenaires internationaux pour améliorer et promouvoir la sécurité et la résilience des infrastructures essentielles transfrontalières et mondiales grâce au partage d'informations. En 2012, les Critical Five (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis) ont été créés pour améliorer l'échange d'informations et le travail sur des questions d'intérêt mutuel. La collaboration entre les communautés économiques régionales devrait donc être envisagée pour renforcer la protection des infrastructures essentielles en Afrique.

Les infrastructures de communication sont considérées comme des IE. Par conséquent, la 5G est une infrastructure nationale essentielle et gérera d'autres secteurs relatifs aux infrastructures essentielles. Avec l'inquiétude croissante suscitée par la domination technologique de la Chine à l'échelle mondiale et en particulier en Afrique, les décisions des opérateurs de s'associer à des fournisseurs particuliers dépendront du goût pour le risque d'un pays.

Les normes permettent l'interopérabilité des systèmes et des réseaux et font donc partie intégrante de la protection des infrastructures essentielles. Par conséquent, les propositions faites par la Chine à l'Union internationale des télécommunications (UIT) en vue de l'élaboration des normes pour un nouveau protocole Internet (« New IP ») et de systèmes de reconnaissance faciale dans la surveillance visuelle pourraient avoir un impact significatif sur la sécurité et la protection des infrastructures essentielles, en particulier la prise en compte des villes et des communautés intelligentes en Afrique.

14. Conclusion

Félicitations, vous avez atteint la fin du module. Dans la partie finale, nous réfléchirons aux principaux points à retenir de ce module, en vous laissant un espace supplémentaire pour noter les points qui vous semblent importants et qui ne sont pas inclus ci-dessus.

Alors que de plus en plus d'infrastructures gérées par le gouvernement et le secteur privé sont mises en ligne pour améliorer l'efficacité et l'intégration, il est impératif de prendre en compte la protection de ces infrastructures, intégrées dans la stratégie, la politique et la législation.

Dans ce module, grâce à l'exploration des définitions et des méthodologies d'identification des infrastructures essentielles (IE) et des infrastructures d'information essentielles (IIE), nous avons apprécié les différences entre les perspectives internationales, régionales et nationales. Nous avons considéré que les lignes directrices politiques, législatives et réglementaires sont nécessaires pour l'identification des ressources et la création de cadres de gouvernance pour la protection des IE et des IIE. Enfin, nous avons brièvement discuté des questions géopolitiques que les pays africains doivent garder à l'esprit lors de l'élaboration et de la mise en œuvre des politiques de protection des IE et des IIE.

Réflexion : les points importants

Notez 5 points essentiels qui vous semblent importants et qui ne sont pas inclus dans ce module.