KM 8 : Culture de la cybersécurité, sensibilisation, main-d'œuvre et compétences

Objectifs du module

Bienvenue dans le module de connaissances 4 sur la culture de la cybersécurité, la sensibilisation, la main-d'œuvre et les compétences dans le cadre du projet GFCE-Africa. Ce module a été **conçu pour répondre à la nécessité d'améliorer les efforts de renforcement des capacités et la culture de la cybersécurité sur le continent africain**. Il vise à guider, soutenir et doter les participants de connaissances sur **le renforcement des capacités de cybersécurité, qui est considéré comme une composante incontournable de la transformation numérique globale dans la région.**

Ce module a pour objectif global de proposer un contexte plus large du renforcement des capacités en matière de cybersécurité en Afrique. Les efforts de renforcement des capacités en matière de cybersécurité doivent être envisagés de manière plus globale, car ils sont liés à une réalité plus large de la politique numérique et ont des retombées directes sur d'autres développements dans la région.

Par leur participation à ce module, **les participants comprendront pourquoi il est vital d'investir dans des projets de renforcement des capacités, en mettant l'accent sur l'importance du renforcement des compétences et de la culture de la cybersécurité.** De même, ce module accorde une attention particulière à une meilleure diversité des genres dans la main-d'œuvre de cybersécurité.

Par ailleurs, ce module présente et aide les participants à comprendre les outils concrets qui contribueront à établir une culture de la cybersécurité mature sur le continent africain.

À la fin de ce module, les participants auront :

1. Des connaissances sur l'impact et la nécessité du renforcement des capacités en matière de cybersécurité dans leurs pays respectifs,

2. Une meilleure compréhension des concepts connexes,
3. Une meilleure connaissance de la façon dont les efforts de renforcement des capacités et les investissements peuvent stimuler la création d'emplois, favoriser le développement socio-économique, renforcer l'engagement des pays africains dans la coopération et les négociations internationales et les aider à promouvoir efficacement leurs intérêts dans les forums internationaux,
4. Élaboré une vision pour une culture renforcée de la cybersécurité et acquis les meilleures pratiques et idées,
5. Envisagé d'impliquer davantage les jeunes générations dans la cybersécurité, en particulier les femmes et les filles dès leur plus jeune âge, afin de réduire l'écart entre les sexes.

En outre, vous serez en mesure de répondre aux questions suivantes et de proposer des actions :

- Dans quelle mesure les défis liés à la cybersécurité dans votre pays s'inscrivent-ils dans un contexte global ?
- Dans quelle mesure les efforts de renforcement des capacités peuvent-ils contribuer à créer une culture de cybersécurité mature ?
- Dans quelle mesure l'éducation précoce à la cybersécurité et le développement des compétences numériques peuvent-ils contribuer au contexte global de la cybersécurité dans votre pays ?
- Comment pouvez-vous procéder pour convaincre vos dirigeants d'adopter une approche à plus long terme de la cybersécurité dans votre pays et votre région ?
- Que peut-on faire pour attirer davantage de femmes vers la cybersécurité et réduire l'écart entre les sexes ?
- Dans quelle mesure le renforcement des cybercapacités peut-il contribuer à stimuler la croissance économique des pays africains ?
- Quelles sont les retombées, pour d'autres secteurs, de la présence dans votre pays de professionnels mieux formés à la cybersécurité ?

Public cible :

Ce module est particulièrement pertinent pour les responsables gouvernementaux de niveau débutant à intermédiaire, qui sont impliqués ou aspirent à travailler dans le domaine de la cybersécurité et/ou travaillent dans la diplomatie numérique. Le module sera utile et pratique

pour les professionnels et les conseillers qui participent activement à différentes fonctions liées à l'élaboration des politiques, ainsi que pour les représentants du secteur privé.

1. Compétences et culture de la cybersécurité en Afrique (contexte)

Déclaration de mission du GFCE

> ***Chaque citoyen du monde devrait pouvoir retirer pleinement les avantages des TIC grâce à un monde numérique libre, ouvert, pacifique et sûr. Le renforcement des cybercapacités fournit les bases nécessaires qui aideront les pays à intensifier leur cyberrésilience par l'acquisition des compétences et des capacités nécessaires pour faire face aux menaces et aux vulnérabilités issues du cyberespace. Nous avons donc pour mission de renforcer les capacités en matière de cybersécurité et l'expertise au niveau mondial par le biais de la collaboration et de la coopération internationales***

La participation active de l'Afrique aux discussions sur la politique numérique et la cybersécurité est bénéfique non seulement pour l'Afrique, mais aussi pour une **politique numérique mondiale plus inclusive, plus percutante et mieux informée**. Il est nécessaire, et urgent, de renforcer les capacités en matière de cybersécurité des parties prenantes africaines. Le renforcement des cybercapacités peut faciliter le processus d'**exploitation des technologies numériques et de l'innovation pour générer une croissance économique inclusive, stimuler la création d'emplois et favoriser le développement socio-économique**. Dans le même temps, le renforcement des capacités apportera une contribution positive à l'**implication des parties prenantes africaines dans les discussions sur la politique numérique** mondiale, par la **promotion efficace des intérêts africains sur la scène internationale**.

Le thème de la culture de la cybersécurité et des compétences a été approuvé par la communauté du GFCE dans le **Communiqué de Delhi** comme l'un des cinq thèmes prioritaires (stratégie et politique en matière de cybersécurité, gestion des incidents et

protection des infrastructures critiques, cybercriminalité, normes de cybersécurité) pour le renforcement des cybercapacités afin de :

1. Sensibiliser toutes les parties prenantes aux menaces et vulnérabilités en matière de cybersécurité et leur permettre d'acquérir les connaissances, les compétences et le sens du partage des responsabilités quant à l'adoption de comportements prudents et avertis dans l'utilisation des TIC.

2. Impliquer toutes les parties prenantes en vue de doter la main-d'œuvre des compétences et des connaissances requises par les employeurs en matière de cybersécurité.

Le groupe de travail D du GFCE (WG D) se concentre sur les sujets suivants :

- Sensibilisation à la cybersécurité

- Éducation et formation, en mettant l'accent sur le développement de la main-d'œuvre en matière de cybersécurité

Pour en savoir plus, consultez le site https://thegfce.org

Principales difficultés à surmonter pour développer une culture de la cybersécurité sur le continent africain

💡 **Point de réflexion**

Selon vous, quels sont les principaux obstacles et défis à relever pour instaurer une culture de la cybersécurité mature dans les pays africains ?

Laissez votre commentaire ci-dessous.

En matière de cybersécurité, la zone Afrique présente plusieurs spécificités liées à des lacunes dans le renforcement des capacités :

➢ **L'adoption des technologies** augmente rapidement en Afrique, notamment grâce à sa population jeune (62 % des Africains auront moins de 25 ans en 2021). **Les jeunes,** en particulier, sont de fervents adeptes de la technologie. En 2019 pourtant, l'IUT a estimé que seulement 28,6 % des Africains utilisaient l'Internet, ce qui est un faible pourcentage faible par rapport au taux moyen mondial de 51,4 %. Néanmoins, à l'avenir, la plupart des nouveaux utilisateurs de l'Internet devraient provenir d'Afrique. Le continent représente un énorme **potentiel d'adoption de l'Internet**. **Le développement d'une culture de la cybersécurité correspondante, tout en veillant à donner à la population les compétences nécessaires en matière de cybersécurité** doit constituer une priorité.

➢ Cette situation est évidemment liée au **coût élevé de l'Internet en Afrique**. La mise à jour des prix des services mobiles par l'Alliance for Affordable Internet (A4AI) indique qu'en moyenne, **le coût de l'Internet est très élevé en Afrique** (A4AI), où il représente près de 6 % du revenu mensuel. D'une façon générale, il est impossible de comparer les pays africains à d'autres pays à revenu faible ou intermédiaire, tels que ceux de la région Asie-Pacifique, d'Amérique latine et des Caraïbes, où le coût moyen de l'Internet mobile correspond à environ 1,5 % du revenu mensuel. La mise à jour des prix mesure le coût d'un Go de données sur un mobile prépayé, en pourcentage du revenu national brut (RNB) par habitant. **Il convient de veiller à comprendre et à atténuer les raisons sous-jacentes des coûts élevés de l'Internet** pour parvenir à **créer la culture de la cybersécurité correspondante** de l'avenir.

➢ Les gouvernements africains ont annoncé **des politiques visant à accroître l'accès à l'Internet et à en réduire le coût**. Cependant, ils visent progressivement à imposer l'espace numérique en vue de générer des revenus. Cette situation contribue potentiellement à ralentir l'adoption de l'Internet, car les internautes africains ont souvent d'autres besoins concurrents, comme le montre l'indice d'accessibilité au haut débit mobile. Il s'ensuit donc que pour garantir un Internet vraiment abordable, **les économies africaines doivent se développer et offrir un revenu disponible qui permette d'acheter des données internet.**

➢ L'Afrique est un **leader mondial en matière de services financiers mobiles** (14 % des Africains utilisent l'argent mobile). Selon Matthieu Aucante, le taux d'accès aux services financiers en Afrique a explosé depuis les années 2000, après le lancement des services d'argent mobile. Le rapport GSMA 2021 a estimé que le volume des transactions dans la seule Afrique sub-saharienne s'élevait à 27,4 milliards de dollars US, pour un volume mondial de 41,1 milliards de dollars US. Ce point est important pour l'inclusion financière car « les individus

et les entreprises ont accès à des produits et services financiers utiles et abordables qui répondent à leurs besoins – transactions, paiements, épargne, crédit et assurance – et qui sont fournis de manière durable et responsable » (Groupe de la Banque mondiale). L'ACRC estime que l'avenir de cette « success story dépendra également de **l'attention et des ressources qui seront consacrées à la question de la cybersécurité** ».

➢ On assiste à une augmentation des **logiciels malveillants sur les appareils mobiles**, qui ciblent en particulier les téléphones Android (89 % des smartphones en Afrique fonctionnent sous Android), entraînant le vol de données personnelles et l'extorsion d'argent. Si les Africains veillent à prendre des mesures de sécurité sur leurs ordinateurs portables ou de bureau, il n'en va généralement pas de même sur leurs smartphones. Une étude menée par Peter Elia Mosha (2019) sur les étudiants d'Arusha, en Tanzanie, a conclu qu'ils ne sont qu'une minorité à utiliser les fonctions de sécurité. **Les activités pédagogiques permettront d'améliorer l'utilisation sécurisée des appareils numériques.**

➢ En 2018, McAfee a estimé à 2 milliards de dollars US les **pertes financières imputables à la cybercriminalité en Afrique**. En outre, Interpol, dans son rapport, affirme que **90 % des entreprises africaines fonctionnent sans avoir mis en place les protocoles de cybersécurité nécessaires.** Cela fait courir un risque important au secteur et ouvre la porte aux cybercriminels pour exploiter ces vulnérabilités. Par conséquent, les entreprises subissent d'importantes pertes financières. Le rapport soutient également qu'en 2016, l'économie kényane a perdu près de 36 millions de dollars US, l'économie sud-africaine 573 millions de dollars US et l'économie nigériane 500 millions de dollars US en raison de la cybercriminalité. Par ailleurs, lors du Book Talk organisé par la Commission économique pour l'Afrique (CEA), il a été souligné que la cybercriminalité est l'un des principaux facteurs de risque susceptibles de mettre en péril l'économie africaine**. Cette préoccupation est particulièrement pertinente au moment où le continent est en train de passer au commerce électronique dans le cadre de la zone de libre-échange continentale africaine (AfCFTA).**

➢ L'accès à l'internet n'est pas une connexion insignifiante. **L'aide au développement doit-elle se concentrer sur un accès abordable pour le « prochain milliard » ou le milliard « inférieur » d'utilisateurs ?** Il est plus facile de se connecter au prochain milliard d'utilisateurs, car ils devraient être plus proches des réseaux et posséder des compétences numériques de base, par rapport au milliard inférieur d'utilisateurs, qui va certainement s'enfoncer davantage dans la pauvreté faute d'inclusion numérique. Ainsi, le renforcement des compétences numériques est essentiel et a un impact sur la question de l'accès à l'Internet.

💡 **Point de réflexion**

Comment puis-je faire reconnaître auprès de mes dirigeants l'intérêt de privilégier des programmes efficaces de renforcement des capacités ?

Le contexte et les défis spécifiques de l'Afrique renvoient aux **besoins de concentration des efforts de renforcement des capacités.** L'avancement de la culture de la cybersécurité aura un impact positif sur le continent africain ainsi que sur le reste de la communauté mondiale (en diminuant éventuellement les cyberattaques menées à l'étranger depuis le continent africain). La centralité croissante de la cybersécurité a conduit de nombreux gouvernements et organisations internationales à s'efforcer de renforcer la capacité des nations à résister aux menaces pesant sur le public et ses ressources numériques.

Par conséquent, la sensibilisation à la cybersécurité en Afrique devrait mettre l'accent sur les compétences numériques de base (telles que l'utilisation sans risque des appareils mobiles/smartphones), ainsi que sur une compréhension plus globale de la cybersécurité, parmi tous les groupes de parties prenantes.

Il est essentiel de se concentrer en premier lieu sur les compétences individuelles pour établir en continu une meilleure culture de la cybersécurité. Les décideurs doivent mieux comprendre et connaître les **liens alarmants entre l'absence de cybercapacités et, par exemple, la croissance économique ou la sécurité**. Il est essentiel d'**investir des ressources dans des programmes de renforcement des capacités.**

Une motivation intéressante pour les dirigeants de votre pays peut être de projeter l'image de votre pays en tant que champion du renforcement des capacités en matière de cybersécurité. Comme le fait remarquer le document d'aperçu des *bonnes pratiques mondiales du GFCE*, les pays qui ont déjà bénéficié d'activités de renforcement des capacités, qui ont atteint un certain niveau de maturité et qui ont une expérience à partager peuvent servir de centre régional pour faire part de leur expérience à leurs régions respectives. Le déploiement de capacités dans un pays d'une région pourrait également contribuer à renforcer la capacité des pays voisins.

L'existence d'un centre local et d'un champion dans une région peut faciliter la sensibilisation aux possibilités d'accès à un programme mondial. Le soutien fourni par les centres locaux peut réduire les coûts et accroître la réceptivité aux besoins de ceux qui demandent un soutien et des ressources pour le renforcement des capacités.

2. Renforcement des capacités : aperçu

Explication théorique

Si vous voulez vraiment maîtriser un sujet, vous devez **acquérir une compréhension approfondie des questions en jeu**. Vous devez être capable de percevoir le contexte, de relier les points et d'appliquer vos connaissances dans la pratique. C'est l'idée qui sous-tend le développement des capacités : **permettre aux individus d'appréhender le sujet en question dans toute sa complexité**. Ce point revêt une importance capitale dans le monde de la politique numérique et de la cybersécurité, dans lequel le rythme de développement (tant pour les solutions que pour les problèmes) s'accélère. **Le renforcement des capacités en matière de politique numérique aide les différentes parties prenantes à mieux s'orienter dans les évolutions liées aux TIC et aux implications de politiques associées**.

Renforcement des capacités ou développement des capacités ?

Le développement et le renforcement des capacités sont deux termes qui reviennent souvent dans les discussions relatives au développement. Le terme **renforcement des capacités** était utilisé avant celui de développement des capacités. L'une des raisons principales de ce changement de terminologie est que le renforcement des capacités est désormais considéré par certains comme un point zéro de départ, marqué par le recours à une expertise externe pour créer quelque chose qui n'existait pas auparavant. Ce concept ne reconnaît ou ne respecte pas la capacité inhérente et les processus de développement continu qui existent partout.

Le développement des capacités, en revanche, met l'accent sur l'existence de processus de développement endogènes dans tous les pays et communautés, et répond à la nécessité de soutenir et/ou de faciliter les processus déjà en cours. Bien qu'il n'y ait pas d'accord universel sur le terme le plus approprié et que les deux soient encore couramment utilisés, de nombreuses organisations ont abandonné le renforcement des capacités au profit du développement des capacités.

Le développement des capacités dépasse de loin le cadre de la formation. Le développement des capacités est souvent défini comme l'amélioration des connaissances, des compétences et des institutions en vue d'une utilisation efficace des ressources et des opportunités. Largement répandus dans les stratégies des agences de développement internationales, les programmes de développement des capacités vont du niveau institutionnel et sociétal au niveau individuel, pour inclure un large éventail de stratégies, de la collecte de fonds à la formation ciblée.

Par définition, selon le Centre pour la gouvernance du secteur de la sécurité, Genève (DCAF), le renforcement des cybercapacités renvoie au développement et au renforcement des processus, des compétences, des ressources et des accords visant à renforcer les capacités nationales, à développer les capacités collectives et à faciliter la coopération et les partenariats internationaux afin de répondre efficacement aux défis de l'ère numérique.

Les activités de renforcement des cybercapacités sont particulièrement importantes lorsqu'il s'agit de la prévention des cyberrisques et des activités malveillantes dans le cyberespace, comme la protection des systèmes, des infrastructures et, surtout, des citoyens. Globalement, il s'agit à la fois de **renforcer les capacités institutionnelles** (en particulier pour le déploiement technique, l'élaboration et la mise en œuvre des politiques) et de **développer les compétences individuelles** (aptitudes et capacités relatives à la société de l'information, notamment les connaissances en informatique, la protection de la vie privée, etc.) L'efficacité et la légitimité de la politique numérique et de la cybersécurité dépendent de la capacité des nations, des organisations et des individus à participer utilement aux processus politiques. Une capacité suffisante en matière de politique numérique se traduit par des décisions politiques plus éclairées.

💡 Point de réflexion

Pouvez-vous expliquer dans vos propres mots ce qu'est le renforcement des capacités et le renforcement des cybercapacités ?

Laissez votre commentaire ci-dessous.

📚 Ressources

*Consultez l'**article de Robert Collet** pour en savoir plus sur la relation entre le renforcement des capacités en matière de cybersécurité, les normes et les mesures de rétablissement de la confiance. Selon lui, le renforcement des capacités internationales en matière de cybersécurité est apparu au milieu des années 2000, sous la forme d'un mécanisme permettant aux pays et aux organisations de s'entraider, par-delà les frontières, pour protéger l'utilisation sûre, sécurisée et ouverte de l'environnement numérique. Parallèlement à cette coopération pratique, la communauté internationale a négocié des normes et des mesures de rétablissement de la confiance pour soutenir la paix et la stabilité dans le cyberespace. Le cadre proposé déplace le renforcement des capacités au-delà des relations entre pays développés et pays en développement et souligne les nombreux objectifs qu'il sert. Le document explore la relation entre le renforcement des capacités en matière de cybersécurité, les normes et les mesures de rétablissement de la confiance. Il soutient que le renforcement des capacités ne se contente pas de soutenir les normes et les mesures de rétablissement de la confiance, mais qu'il en est également une instance et bénéficie de normes qui lui sont propres.*

Pourquoi le renforcement des capacités est-il important dans le contexte mondial ?

Le renforcement des capacités est intrinsèquement lié aux débats actuels qui se déroulent dans les forums internationaux en rapport avec la stabilité et la paix dans le cyberespace.

Dans les documents finaux du Sommet mondial sur la société de l'information (SMSI) (2003/2005), **le renforcement des capacités est souligné comme une priorité pour les pays en développement**. De même, le document final de la réunion de haut niveau de l'Assemblée générale des Nations unies (AGNU) sur l'examen global de la mise en œuvre des résultats du SMSI appelle à de nouveaux investissements dans le développement des capacités. Plus récemment, l'importance du développement des capacités a été soulevée dans le rapport du Groupe de haut niveau des Nations unies sur la coopération numérique.

Le renforcement des capacités dans le domaine des TIC a également figuré en bonne place dans l'ordre du jour de l'AGNU. Lors de la 74e session de l'AGNU, le renforcement des capacités en matière de TIC a été abordé principalement par les délégués nationaux de pays en développement, qui ont souligné l'importance du soutien et des partenariats internationaux, de l'investissement dans le capital humain et d'une formation adéquate.

Le groupe de travail à composition non limitée des Nations unies et le groupe d'experts gouvernementaux des Nations unies ont également des principes utiles sur le renforcement des capacités. Voir plus.

Le passage à une phase plus mature de la politique numérique nécessiterait de mettre davantage l'accent sur le développement organisationnel en assurant une participation soutenue aux processus politiques. Il s'agit notamment de **développer les capacités organisationnelles des gouvernements, de la société civile, des entreprises et des universités**. Le développement des capacités au niveau des organisations et des systèmes revêt une importance particulière lors du traitement de questions telles que la cybersécurité.

Les recherches sur le développement des capacités en général et les expériences passées mettent en évidence les points suivants :

- Si l'Internet est un système mondial, la politique de l'Internet, elle, est souvent très locale. Elle est façonnée par les spécificités culturelles et sociales locales (par exemple, la sensibilité culturelle au contenu, la pertinence de la protection de la vie privée). Par conséquent, **le renforcement des capacités se devrait de suivre la dynamique locale**, en prenant en considération les conditions locales spécifiques (politiques, sociales, culturelles et autres) dans l'élaboration et la mise en œuvre des programmes et activités de renforcement des capacités.

- Un **apprentissage juste à temps dans le cadre des processus politiques** pourrait permettre de répondre à l'urgence du développement des capacités.

- ➢ Le besoin croissant de capacités dans le domaine de la politique numérique doit être traité à un niveau plus systémique, en **incluant la gouvernance de l'Internet, la cybersécurité et les sujets connexes dans le programme des études universitaires de troisième cycle**.

Un **développement global des capacités aux niveaux individuel, organisationnel, systémique et réseau** pourrait permettre de parvenir à une autonomisation véritable et durable, comme le montre le papillon de développement des capacités ci-dessous.

D'une manière générale, le **manque de ressources suffisantes, de volonté politique et la durabilité limitée des initiatives demeurent les principaux obstacles au renforcement des capacités**.

Une autre difficulté réside dans la **délicate distinction entre le développement neutre des capacités et le plaidoyer**, car les activités de développement des capacités ne visent pas à influencer les décisions politiques.

❗ Lien entre les problèmes urgents de l'Afrique et la cybersécurité

Il arrive souvent que d'autres problèmes auxquels la région est confrontée semblent plus urgents (la construction d'une école, par exemple). Pourtant, ces difficultés ne sont pas déconnectées de la cybersécurité. Par exemple, l'accès à l'éducation est une priorité, mais le manque de compétences numériques suffisantes peut exacerber le problème que nous avons connu lors de la pandémie de COVID-19, lorsque le monde entier s'est soudainement tourné vers l'apprentissage en ligne.

En Afrique, le manque de compétences numériques de base et la culture de la cybersécurité peu favorable ont bien souvent découragé les enfants de poursuivre leur scolarité.

3. Le renforcement des capacités en matière de cybersécurité dans le contexte plus large de l'Afrique

Le continent africain a été la cible de cyberactivités malveillantes au cours des deux dernières années. De nombreux pays ont enregistré une augmentation significative des sabotages d'infrastructures publiques, des flux financiers illicites, des attaques par ransomware ou même des atteintes à la sécurité nationale, comme l'espionnage ou le vol de renseignements, pour n'en citer que quelques-uns.

🌍 **Étude de cas**

Selon l'indice mondial de cybersécurité (GCI), que l'UIT a publié en 2021 après avoir mesuré et combiné le score de chaque pays sur les 5 piliers de la cybersécurité : juridique ; technique ; organisationnel ; **mesures de développement des capacités** ; et mesures de coopération, tous les pays d'Afrique, sauf six, manquent d'incitations au développement des capacités en matière de cybersécurité.

Selon le classement effectué en 2020, l'île Maurice est la mieux placée au niveau mondial (17e), suivie de l'Égypte (23e), la Tanzanie étant le troisième meilleur pays africain (35e). Sur les dix pays les moins bien classés, six sont des pays d'Afrique.

L'inconvénient majeur en Afrique est la sensibilisation et la connaissance limitées du public quant au risque potentiel que représente le cyberespace. Le problème est encore exacerbé par le faible développement de l'infrastructure numérique et la capacité institutionnelle limitée à mettre en œuvre et élaborer des lois et des politiques en matière de cybersécurité, en raison du manque de professionnels de la cybersécurité parfaitement équipés.

Le manque de ressources financières limite souvent les pays du Sud dans leur volonté d'investir dans des infrastructures et des mesures de cybersécurité plus solides. Un document récemment publié par l'université d'Oxford analyse les résultats que devraient viser les bonnes approches de la cybersécurité nationale fondées sur le risque, en particulier dans les environnements offrant des ressources limitées, et fournit des conseils sur la hiérarchisation des investissements dans la cybersécurité.

En outre, les **responsables gouvernementaux ne comprennent pas non plus l'interconnexion substantielle entre la cybersécurité et la sécurité nationale, ni ce qu'elle implique.**

Le renforcement des capacités en matière de cybersécurité vise à remédier explicitement à ces lacunes et à combler le déficit de compétences en cybersécurité dont les pays africains ont besoin pour répondre de manière adéquate aux risques liés à la cybersécurité. Il vise à combler la fracture numérique, à développer les connaissances

institutionnelles ou à remédier aux limites de la sensibilisation aux politiques et aux déficits de compétences en matière de cyberprotection.

Les membres du Forum mondial sur la cyber-expertise (GFCE) collaborent sur plusieurs initiatives pratiques de renforcement des cybercapacités. En 2017, différentes **bonnes pratiques mondiales des membres du GFCE** ont été cartographiées. Elles constituent un riche ensemble d'expériences et de connaissances. La collecte et le partage des bonnes pratiques mondiales, sous forme de catalogue, garantissent que d'autres initiatives de renforcement des cybercapacités peuvent bénéficier de cette expérience et de cette expertise dans leurs propres efforts.

📚 **Ressources**

***Le portail Cybil** du GFCE est un référentiel en ligne pour les projets internationaux de renforcement des capacités de cybersécurité. Il héberge une vaste bibliothèque de ressources à utiliser pour les projets. Ce portail contribue à améliorer l'efficacité du renforcement des capacités, sa coordination et sa transparence.*

***L'étude et le rapport de Diplo intitulés Renforcement durable des capacités : Gouvernance de l'Internet en Afrique**, avec enregistrement en anglais et en français*

https://africacenter.org/spotlight/africa-evolving-cyber-threat

Pourquoi est-il important pour les pays africains d'améliorer le renforcement des capacités en matière de cybersécurité et par quels moyens ?

A) Renforcement des compétences et de la culture

Les pays africains ne sont pas bien préparés à une cyberattaque. De manière générale, **l'Afrique est mal classée en matière de législation sur la cybersécurité**. Selon un rapport de la Commission de l'Union africaine (CUA) et de Symantec établi en 2016, seuls 20% des pays africains ont élaboré des cadres juridiques pour lutter contre la cybercriminalité, qui devrait croître en raison de l'essor rapide du marché du commerce électronique en Afrique, pour atteindre 75 milliards de dollars US d'ici 2025.

L'une des raisons expliquant le **faible niveau d'adoption de lois sur la cybersécurité,** en général, est le **manque de sensibilisation globale à la cybersécurité**. En conséquence, certains gouvernements traitent uniquement la cybersécurité dans le cadre de la cybercriminalité ; le terme « cybercriminalité » est utilisé dans différents types de lois, ou les lois existantes sont employées pour poursuivre les cybercrimes.

💡 **Point de réflexion**

Vous ou les responsables de la sécurité de votre pays êtes-vous pleinement conscients de l'intersection entre la sécurité numérique et la sécurité nationale ? Comment le manque de professionnels de la cybersécurité peut-il entraver la croissance économique ? Quelles retombées l'accroissement du nombre de professionnels de la cybersécurité pourrait-il entraîner sur la prospérité économique globale des pays africains ?

Laissez votre commentaire ci-dessous.

SCÉNARIO : CYBERSÉCURITÉ ET MANQUE DE COMPÉTENCES NUMÉRIQUES

Avez-vous, vous ou vos collègues, déjà rencontré une situation dans laquelle le manque de compétences numériques a entravé des discussions politiques plus avancées sur la cybersécurité dans votre pays ?

⬇

RÉSULTAT : Les cyberattaques ont explosé au cours des dernières années. De même, l'Afrique a connu une augmentation spectaculaire des cyberattaques pendant la pandémie de COVID-19.

Premièrement, le manque de compétences numériques a un impact direct, et significatif, sur les organisations ou les organismes publics et entraîne une plus grande exposition aux risques potentiels et aux cyberactivités malveillantes.

Deuxièmement, la pénurie de professionnels adéquatement formés entrave la prospérité économique globale d'une nation. Le manque de personnel qualifié en matière de cybersécurité peut menacer le succès d'une entreprise : les cyberattaques peuvent causer d'énormes pertes financières, perturber les opérations, les services et les chaînes d'approvisionnement, et compromettre la vie privée et les données personnelles. Dans l'ensemble, les cyberattaques ont de graves répercussions, qui peuvent compromettre la réussite des entreprises à tous les niveaux. Par exemple, on estime **que le** milieu des affaires africain a perdu près de 3,5 milliards de dollars US en 2017 du fait de la cyberfraude et du vol. De plus, la cybercriminalité est régulièrement classée parmi les principales menaces auxquelles il est confronté.

Troisièmement, la pénurie de main-d'œuvre sensibilisée à la cybersécurité empêche toute participation significative des pays africains dans les forums internationaux. Comme ils ne peuvent pas exprimer leurs besoins, ils brillent souvent par leur absence pendant le déroulement des discussions et l'élaboration des politiques. Cette situation est notamment imputable aux déficits de capacités et au manque de sensibilisation de base qui sont, entre autres, associés à des politiques de cybersécurité dépassées.

Quatrièmement, au niveau national, les administrations publiques ont désespérément besoin de personnel spécialisé dans la cybersécurité pour protéger leurs systèmes, leurs données et leurs informations confidentielles, afin d'accroître la capacité du pays à répondre aux menaces provenant du cyberespace. Autrement dit, les professionnels de la cybersécurité sont indispensables pour la sécurité nationale et la prévention des menaces numériques, qu'il s'agisse d'espionnage, de sabotage d'infrastructures critiques ou de crime organisé. En outre, par suite de ce manque d'expertise, les gouvernements ne parviennent pas à surveiller les incidents ni, en fin de compte, à poursuivre les cybercriminels.

ACTION : L'industrie et le secteur public devraient investir du temps et de l'argent **dans l'éducation à la cybersécurité, la formation à long terme, la sensibilisation et les programmes de mentorat. L'accent devrait être mis sur de multiples groupes de parties prenantes. Il convient toutefois de tenir compte du fait que le renforcement des compétences** et de la culture est un processus à long terme. La situation s'améliorera progressivement par le biais d'investissements dans des programmes de développement des capacités allant des compétences numériques de base pour les enfants et les jeunes à l'apprentissage continu, en passant par un soutien ciblé au renforcement des capacités des professionnels, notamment les décideurs.

RETOMBÉES : L'amélioration des compétences et de la culture en matière de cybersécurité assurera une meilleure préparation au travail et devrait permettre de lutter contre le chômage des jeunes en Afrique.

L'OCDE s'est penchée sur la cybercompétence des travailleurs en Afrique et sur la réalité des travailleurs indépendants en Afrique. Selon l'OCDE, les travailleurs indépendants et les travailleurs familiaux en Afrique représenteront 65 % de l'emploi d'ici 2040, sur la base des tendances actuelles. Leur nombre pourrait augmenter de 163 %, pour atteindre 529 millions de personnes en 2040, contre 325 millions de personnes estimées en 2020. Même dans le meilleur des cas, avec un développement substantiel des secteurs de la fabrication et du numérique, le travail indépendant restera probablement le pilier de la plupart des jeunes Africains. Une proportion importante de la main-d'œuvre que représentent les jeunes du continent ne fréquente pas les systèmes d'éducation et de formation, est sans emploi ou travaille dans le secteur informel. Les politiques doivent les aider à adopter la transformation numérique. Pour que la numérisation profite aux travailleurs informels et indépendants, il faut multiplier les possibilités d'apprentissage et de développement des compétences tout au long de la vie.

L'étude de l'OCDE attire l'attention sur l'émergence de nouvelles formes de travail indépendant par le biais de plateformes électroniques et d'applications numériques, prônant l'amélioration des cadres réglementaires et des régimes de protection sociale pour prévenir les conditions de travail précaires. En Afrique du Sud, par exemple, le nombre de travailleurs

de plateformes augmente de plus de 10 % chaque année et pourrait atteindre des millions au cours des prochaines décennies.

💡**Point de réflexion**

Selon une étude de la Société financière internationale (IFC), membre du Groupe de la Banque mondiale qui est la principale institution de développement international axée sur le secteur privé dans les marchés émergents, près de 230 millions d'emplois sur le continent nécessiteront des compétences numériques d'ici 2030. En d'autres termes, il existe un potentiel de 650 millions de possibilités de formation et un marché estimé à 130 milliards de dollars US.

L'étude a examiné les marchés de la Côte d'Ivoire, du Kenya, du Mozambique, du Nigeria et du Rwanda. Ses conclusions préliminaires révèlent que d'ici 2030, **des compétences numériques seront nécessaires pour 50 à 55 % des emplois au Kenya, 35 à 45 % en Côte d'Ivoire, au Nigeria et au Rwanda, et 20 à 25 % au Mozambique.**

Pouvez-vous penser au niveau de compétences numériques qui sera requis dans votre propre pays ? Pourquoi ?

Laissez votre commentaire ci-dessous.

L'offre et la demande pour les compétences les plus importantes de la main-d'œuvre

Source : FEM

❗ **LES SOFT SKILLS SONT IMPORTANTS**

En plus des compétences techniques, les **professionnels de la cybersécurité doivent posséder des soft skills pour la suite de leur carrière dans la cybersécurité**.

Le **NICE Cybersecurity Workforce Framework** a dressé une liste des connaissances, compétences et aptitudes (KSA) nécessaires pour accomplir des tâches susceptibles de renforcer la position de cybersécurité d'une organisation.

***NICE** est un partenariat entre le gouvernement, le monde universitaire et le secteur privé, dirigé par le National Institute of Standards and Technology (NIST) du ministère américain du commerce. Depuis sa création, il a pour mission de développer la main-d'œuvre dans le domaine de la cybersécurité en accélérant l'apprentissage et le développement des compétences, en encourageant une communauté d'apprentissage diversifiée et en guidant le développement de carrière et la planification des effectifs. L'une des initiatives mises en place par NICE est le **NICE Cybersecurity Workforce Framework** (lancé en 2017). Cette initiative s'efforce de fournir aux employeurs des orientations supplémentaires sur la manière de préparer une main-d'œuvre de cybersécurité apte et compétente.*

Suite à une demande de commentaires, le GFCE a soumis quelques suggestions pour améliorer le NICE Cybersecurity Workforce Framework. Le GFCE a suggéré **d'ajouter des soft skills à la formation des futurs professionnels de la cybersécurité, telles que la pensée critique, les compétences en communication, le travail d'équipe, etc.**

Les employeurs recherchent d'autres soft skills lorsqu'ils recrutent des professionnels de la cybersécurité : leadership, communication (traduction de sujets techniques en termes commerciaux), pensée critique/analytique, travail d'équipe et créativité. De même, le rapport sur le développement des soft skills recherchés par les employeurs en matière de cybersécurité présente les soft skills nécessaires aux professionnels de la cybersécurité.

Un nouveau projet sur le **développement de la cybersécurité dans le cadre professionnel** a été lancé par le **groupe de travail du GFCE sur la culture et les compétences en matière de cybersécurité**. L'équipe en charge du projet a fait circuler une

enquête en vue de recueillir des avis internationaux. Cette enquête est en cours d'évaluation.

B) Les femmes dans la cybersécurité

💡 **Point de réflexion**

Pouvez-vous estimer le pourcentage de femmes travaillant dans le domaine de la cybersécurité sur le continent africain ?

Laissez votre commentaire ci-dessous.

Plusieurs spécificités de l'Afrique sont liées à des lacunes concernant l'inclusion des femmes et des filles dans la transformation numérique :

- Les femmes sont encore largement sous-représentées dans les effectifs de la cybersécurité à travers le monde. En Afrique, **les femmes représentent 9 % des professionnels de la cybersécurité.**

- En outre, les femmes et les filles africaines ont une culture numérique plus faible et un accès à l'Internet plus limité que les hommes africains. Il est essentiel de s'attaquer à la fracture numérique entre les sexes pour que les femmes aient la possibilité de créer des entreprises, de s'instruire, de trouver un emploi, de recevoir des soins de santé, de trouver des services bancaires et d'autres services financiers, ou de s'engager dans un large éventail d'activités dans le cadre de la reprise numérique post-Covid-19.

- Selon Amnesty International, les femmes de couleur sont 34 % plus susceptibles d'être la cible de discours haineux en ligne que leurs homologues blanches.

Contribuer et s'engager

Parmi les initiatives de l'UIT visant à faire participer davantage de femmes et de filles à la transformation numérique des économies et des sociétés, citons :

L'**espace d'apprentissage CISCO EQUALS** : formation en ligne gratuite aux compétences numériques sur des sujets tels que la cybersécurité, l'entrepreneuriat et l'internet des objets ;

Le Défi de l'innovation : les femmes dans la technologie : concours destiné à soutenir les innovateurs les plus brillants dans le secteur de la technologie, dont les solutions font la différence pour les femmes et qui aident les femmes en leur donnant les moyens d'exceller dans l'accès et l'utilisation des TIC en vue d'améliorer leur capacité productive et économique dans différents secteurs ;

Le volet spécial du **Sommet mondial sur la société de l'information** (SMSI), consacré aux TIC et à la parité hommes-femmes ;

La **Coalition d'action sur les technologies et l'innovation de Génération égalité** : en 2020, l'UIT est devenue l'un des chefs de file de la Coalition d'action et, avec d'autres partenaires, elle s'est engagée à ne rien négliger pour tirer parti des partenariats, mais aussi de la puissance et de l'étendue de ses membres, afin de faire de Génération égalité un forum concret, ciblé et, surtout, efficace.

Girls and Women in Talking Tech: Girls in ICT : série d'entretiens au cours desquels des jeunes filles et des jeunes femmes, qui aspirent à une carrière dans le secteur des technologies, ont la possibilité d'interviewer des femmes de premier plan et des modèles dans ce domaine.

Le GFCE[1] [2] continue de sensibiliser la communauté mondiale au rôle des femmes dans le renforcement des capacités en matière de cybersécurité. Il contribue à célébrer les femmes dans ce secteur, en partageant leurs réalisations et leurs expériences, ainsi qu'en présentant les opportunités qui encourageront les communautés de femmes à s'impliquer davantage dans les processus CCB et l'aide que le GFCE peut apporter dans ce cadre.

💡 **Point de réflexion**

Quel type de personnes travaille dans la cybersécurité ? Vos collègues ou consœurs envisagent-elles une carrière dans la cybersécurité ?

Laissez votre commentaire ci-dessous.

SCÉNARIO : METTRE FIN À LA DISPARITÉ ENTRE LES SEXES DANS LE DOMAINE DE LA CYBERSÉCURITÉ

Avez-vous déjà entendu vos collègues ou consœurs dire que les tâches dans le domaine de la cybersécurité sont purement techniques et que les hommes sont plus à même de s'en acquitter avec succès ?

⬇

RÉSULTAT : En général, les filles ont le sentiment, dès leur plus jeune âge, qu'une carrière dans la cybersécurité est excessivement axée sur la technique. Même si cette conception peut être correcte dans une certaine mesure, il y a bien d'autres postes qui exigent davantage de compétences interpersonnelles et de soft skills (comme le travail en équipe, le leadership et les compétences en communication, etc.) que les femmes possèdent.

En outre, les femmes sont généralement moins enclines à percevoir la cybersécurité comme un parcours professionnel viable en raison du jugement erroné selon lequel il s'agit d'une profession masculine.

⬇

ACTION : Compte tenu du fait que près de 60 % de la population africaine a moins de 25 ans, ce qui fait de l'Afrique le continent le plus jeune du monde, et que les femmes représentent plus de 50 % de la population africaine combinée, il est essentiel de se concentrer sur les jeunes filles et les femmes pour les encourager à choisir le secteur de la cybersécurité et y faire carrière. En fin de compte, cela ouvrirait une multitude d'options à la population féminine africaine sans emploi, avec des revenus élevés à la clé, et contribuerait à réduire le déficit de main-d'œuvre dans le domaine de la cybersécurité qui est particulièrement préoccupant et bouleverse l'avancée numérique et technologique dans la région.

Comme pour tout autre environnement professionnel, plus la diversité est grande (origines, pensées, perceptions, idées), plus le succès d'une entreprise l'est également. La même règle s'applique au domaine de la cybersécurité : la présence d'un plus grand nombre de femmes garantit et apporte davantage de perspectives et de points de vue.

Il faut commencer par trouver des mentors et des modèles féminins qui parleront ouvertement de leurs succès et de leurs capacités et, en fin de compte, de l'énorme potentiel de ces domaines. Les femmes qui occupent des postes de direction dans le secteur de l'informatique devraient commencer à tirer parti de la sensibilisation, par exemple en créant un réseau de femmes travaillant dans les domaines de la technologie ou de la cybersécurité. Les organisations qui sont déjà parvenues à une certaine maturité en matière de cybersécurité devraient commencer à former leurs employées ou à recruter des femmes et leur proposer des programmes de formation ou de mentorat.

Contribuer et s'engager

Le Programme de mentorat Women in Cyber, géré par l'UIT, est ouvert aux femmes d'Afrique et des régions arabes qui travaillent dans le domaine de la cybersécurité à des niveaux subalternes, ainsi qu'aux femmes dans le domaine des TIC/STEM qui souhaitent entrer dans le monde du travail de la cybersécurité.

Women in Africa et Deloitte ont développé un programme de mentorat dont l'objectif principal est de développer le leadership des femmes en Afrique et d'aider chaque mentor et mentorée à atteindre leurs objectifs professionnels.

CyberGirls est un programme de bourses d'un an qui permet aux jeunes filles d'acquérir des compétences en cybersécurité recherchées mondialement, ce qui les aide à saisir des opportunités professionnelles en Afrique et dans le monde entier.

Women in Cybersecurity (WiCyS) propose différents programmes de formation pour les femmes à l'échelle du globe.

💡 **Point de réflexion**

Pouvez-vous expliquer dans quelle mesure la société bénéficiera du recrutement d'un plus grand nombre de femmes hautement qualifiées dans le domaine de la cybersécurité ?

Pouvez-vous penser à un modèle féminin dans le domaine de la cybersécurité dans votre pays ?

Laissez votre commentaire ci-dessous.

Katherine Getao, *directrice générale de l'Autorité des TIC au Kenya, a expliqué les raisons pour lesquelles peu de femmes choisissent de s'impliquer dans le domaine de la cybersécurité et du renforcement des cybercapacités au Kenya. Tout d'abord, les jeunes filles ne sont pas suffisamment sensibilisées à ce domaine lorsqu'elles choisissent la carrière qu'elles souhaitent embrasser. Deuxièmement, étant donné que la cybersécurité est une priorité au Kenya, les femmes qui optent pour ce domaine ne sont pas pleinement conscientes des différents parcours professionnels qui s'offrent à elles, et quelques-unes seulement choisissent le secteur CCB. Troisièmement, les jeunes femmes cadres manquent d'assurance dans le cadre du travail et elles ne sont pas encouragées à défendre leurs intérêts et leurs réalisations professionnelles. Katherine Getao a non seulement souligné la nécessité de célébrer les réalisations et les contributions des femmes, notamment dans le cadre du Groupe d'experts gouvernementaux des Nations unies, en faveur de la sécurité mondiale dans le domaine des TIC et du renforcement des cybercapacités, mais elle a également souligné l'importance de former les femmes au plus haut niveau, pour leur permettre de prendre confiance en elles et de les pousser à accomplir davantage sur le terrain, à obtenir des postes stratégiques et à acquérir la visibilité dont elles ont besoin pour progresser et montrer leur contribution réelle à la cybersécurité et au renforcement des capacités.*

📚 **Ressources**

Communiqué de Delhi du GFCE : programme global du GFCE pour le renforcement des cybercapacités, approuvé par tous les membres du GFCE et réaffirmant leur engagement commun à renforcer les cybercapacités et l'expertise au niveau mondial.

Portail Cybil du GFCE : référentiel en ligne pour les projets internationaux de renforcement des capacités de cybersécurité. Il héberge une vaste bibliothèque de ressources à utiliser pour les projets. Ce portail contribue à améliorer l'efficacité du renforcement des capacités, sa coordination et sa transparence.

Rapport : Sustainable Capacity Building: Internet Governance in Africa : commandé par l'Union africaine, ce rapport s'inscrit dans le volet IG de l'initiative de politique et de régulation pour l'Afrique numérique (PRIDA).

Rapport : Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities : publication de l'Institut norvégien des affaires internationales.

https://dig.watch/topics/capacity-development à l'observatoire Geneva Internet Platform Digital Watch.

Base de données des Nations unies sur les possibilités de cyberformation : effort des Nations unies en réponse à la feuille de route sur la coopération numérique.

Courte vidéo présentant les avantages de l'apprentissage en ligne et le développement des capacités

Courte vidéo sur la méthodologie et le développement des cours en ligne

Le rapport d'évaluation des cybermenaces en Afrique 2021

4. Outils concrets pour la création d'une culture de cybersécurité mature : meilleures pratiques de la communauté du GFCE

A) Campagnes de sensibilisation

Les **campagnes de sensibilisation** constituent l'un des outils permettant de créer une culture de cybersécurité plus mature. Votre campagne de sensibilisation n'est probablement pas la seule, d'autres campagnes sont menées au niveau local, national et/ou international. Il est conseillé de les aligner pour optimiser l'impact et utiliser les ressources plus efficacement. L'alignement des campagnes soutient l'objectif ultime de sensibilisation aux cybermenaces par un comportement en ligne sûr. (GGP)

Voici quelques exemples :

- ➔ Les expériences tirées de huit campagnes de sensibilisation différentes menées en Afrique (Tips for running public awareness campaigns in Africa [Conseils pour l'organisation de campagnes de sensibilisation du public en Afrique]) identifient quelques conseils pour garantir le succès des campagnes de sensibilisation, par exemple : comprendre le problème et les résultats que vous souhaitez atteindre, confirmer que le sujet concerne des personnes extérieures à votre organisation, impliquer le groupe cible dans la planification de la campagne, utiliser le langage et les médias de votre groupe cible, faciliter la participation du groupe cible,

utiliser les médias et les réseaux grand public pour amplifier votre message, veiller à la précision, être flexible en ce qui concerne le plan de la campagne et vérifier que vous pouvez maintenir l'élan de la campagne sur la période prévue.

➔ La campagne de cyberhygiène « CyberSmartBW » a été menée au Botswana en 2020. Elle avait pour objectif de contrer le problème lié à l'augmentation des escroqueries en ligne ciblant les jeunes.

➔ Afin de sensibiliser à la cybercriminalité et à d'autres méfaits en ligne, Get Safe Online (qui travaille avec 25 pays, dont le Rwanda) a compilé un rapport présentant des exemples de meilleures pratiques de sensibilisation, accessible ici.

➔ Le fait de déclarer un mois dédié à la sensibilisation à la cybersécurité peut contribuer à concentrer les efforts de nombreuses parties prenantes et à améliorer leur collaboration, tout en délivrant un message fort auprès du public et en augmentant l'efficacité des efforts de renforcement des capacités. (GGP) Exemple : Le Mois européen de la cybersécurité (ECSM) en octobre 2019 et d'autres années, sous l'égide de l'ENISA. Voir également l'aperçu de cette bonne pratique mondiale du GFCE.

Conseils pratiques pour préparer une campagne de cybersécurité efficace (GGP) :

- Rassemblez les parties prenantes pour engager le dialogue et faites des efforts pour coordonner les événements et les activités. Alignez la vision, les messages et les thèmes de la campagne entre les partenaires.
- Confirmez qu'il existe une vision commune.
- Si le fond et les informations sont les mêmes pour tous, veillez à conceptualiser les campagnes pour une base constitutive spécifique. Dans la plupart des cas, vous ne pourrez pas vous contenter d'un copier-coller.
- Coopérez et alignez-vous sur les parties prenantes à différents niveaux : au niveau national entre les communautés de parties prenantes, au niveau bilatéral et/ou régional, et au niveau international.
- Coordonnez des cyberévénements, en personne ou via les médias sociaux, tout en avançant le concept de la participation de plusieurs parties prenantes à la mise en œuvre d'initiatives nationales de sensibilisation.
- Travaillez au partage de supports et de boîtes à outils, et faites activement la promotion des ressources existantes disponibles. Réutilisez le matériel existant afin de réduire le coût des campagnes et d'éviter de réinventer la roue. Cette procédure permet d'employer les matériels contextualisés et réutilisés pour d'autres campagnes nationales et/ou internationales. Elle contribue également à réduire les coûts.
- Envisagez de partager gratuitement les documents.
- Préparez un dossier pour votre partenaire, comportant les instructions de base, et indiquez à votre partenaire les ressources disponibles. Veillez à ne pas partager une quantité excessive d'informations avec vos partenaires. Choisissez plutôt de les orienter vers des sections spécifiques.
- Essayez d'adapter les ressources à la région des partenaires (par exemple, les téléphones portables sont très répandus en Afrique. Adaptez le format de vos ressources en conséquence).
- Adaptez votre message et votre style de campagne au contexte dans lequel il s'inscrit. D'autres partenaires peuvent vouloir partager leur message d'une manière différente. Vous devez vous préparer à cette possibilité.
- Tenez compte des spécificités locales, notamment la culture de l'organisation avec laquelle vous travaillez.
- Utilisez les plateformes de partage existantes, par exemple, la Coalition pour la cybersensibilisation Stop.Think.Connect.™
- Mesurez votre campagne en termes de succès déclarés et de participation.
- Vous devez avoir conscience des obstacles, tels que la langue de la campagne. D'autres obstacles relèvent des marques déposées et des droits d'auteur, qui peuvent présenter des difficultés lorsque vous cherchez à réutiliser et à contextualiser les supports d'autres organisations.

💡 **Point de réflexion**

Avez-vous connaissance de campagnes de sensibilisation liées à la cybersécurité dans votre propre pays ? Dans l'affirmative, pouvez-vous partager leurs principaux objectifs et caractéristiques ?

Laissez votre commentaire ci-dessous.

B) Éducation à la cybersécurité

La création d'une culture de cybersécurité mature est un processus à long terme. C'est un changement. Il est absolument essentiel que les gouvernements des pays africains intègrent l'éducation à la cybersécurité, ainsi que les compétences numériques **nécessaires pour naviguer en toute sécurité dans le cyberespace, dans les programmes scolaires nationaux, dès l'école primaire**.

Les cybercompétences sont des compétences numériques spécialisées, mais dans de nombreux pays, le système éducatif n'est pas totalement équipé pour permettre aux élèves d'acquérir les compétences numériques nécessaires de manière suffisamment approfondie et étendue. Certains pays visent à financer des initiatives qui créent et développent un vivier durable de talents en matière de cybersécurité, aujourd'hui et à l'avenir, afin de répondre au besoin croissant en cybercompétences à l'échelle du globe. De nombreux pays s'efforcent de développer les cybercompétences chez les jeunes. Toutefois, ils ne savent pas ce que font les autres pays dans ce domaine et ne sont pas en mesure de s'inspirer des meilleures pratiques. En savoir plus sur ces déficits de connaissances identifiés.

Le GFCE a pleinement conscience qu'il est nécessaire d'examiner les bonnes pratiques en matière d'éducation des jeunes à la cybersécurité. Le GT D a commandé à l'Université du Kent un projet de recherche sur **l'éducation préuniversitaire à la cybersécurité : rapport sur le développement des cybercompétences chez les enfants et les jeunes.** Le rapport résume les résultats des recherches menées pour cartographier l'enseignement préuniversitaire de la cybersécurité dans un contexte mondial. Les résultats de la recherche

ont conduit aux principales conclusions et recommandations suivantes, qui, nous l'espérons, pourront aider les parties prenantes du monde entier à améliorer l'enseignement de la cybersécurité dans un cadre préuniversitaire. L'Afrique du Sud figure parmi les pays cartographiés.

Le Programme de recherche est un nouvel outil développé pour et par la communauté du GFCE. L'objectif principal du Programme de recherche est d'**aider la communauté du renforcement des capacités à concevoir et à mener des projets plus efficaces en identifiant les lacunes dans les connaissances et en les comblant par la recherche.**

Ces compétences sont d'autant plus nécessaires aujourd'hui que la pandémie de Covid-19 a obligé un plus grand nombre d'**enfants à aller en ligne pour suivre un enseignement à distance.** Les enfants utilisent de plus en plus le web à des fins éducatives. Si la ludification présente certains avantages, l'augmentation rapide de l'exposition aux TIC entraîne de nombreux inconvénients et risques liés au cyberespace, en raison du manque de sensibilisation des enfants à l'utilisation sûre et appropriée du cyberespace.

Le Norton Group a dressé la liste des principales cybermenaces auxquelles les enfants sont confrontés lorsqu'ils sont en ligne : **contenus inappropriés, « amis » dans les salons de discussion, cyberharcèlement et escroqueries en ligne.** En outre, Kaspersky cite d'autres menaces telles que la **publication d'informations privées, l'hameçonnage (phishing), le téléchargement accidentel de logiciels malveillants et les messages qui reviendront hanter l'enfant au cours de sa vie**. Il est donc essentiel d'introduire dans les programmes scolaires des compétences spécifiques en matière de cybersécurité afin de contrer ces menaces et d'assurer la cybersécurité des enfants.

En ce qui concerne la méthodologie d'enseignement, les enfants sont plus motivés et se concentrent davantage sur l'activité d'apprentissage lorsque le matériel pédagogique utilisé est interactif et stimulant. Cela peut passer par la conception d'un jeu éducatif sur la cybersécurité, comme l'a noté Kritzinger A (2017). Il est toutefois important de créer des jeux adaptés, qui permettent aux apprenants d'atteindre les résultats d'apprentissage souhaités, et de combiner les jeux avec d'autres supports.

Voici quelques exemples :

- ➔ L'initiative CyberPatriot Elementary School Cyber Education Initiative (ESCEI) propose trois modules d'apprentissage sur la cybersécurité, distrayants et interactifs, destinés aux élèves de la maternelle à la 6e.

- ➔ Webrangers est une initiative sud-africaine menée par Media Monitoring Africa. Ce programme de culture numérique doit permettre aux jeunes d'acquérir des compétences et des connaissances essentielles en matière de sécurité en ligne, qu'ils utiliseront pour créer des campagnes innovantes visant à promouvoir une utilisation en toute sécurité d'Internet et à défendre leurs droits dans le monde numérique.

- ➔ *Enfants avertis* est le programme interactif d'éducation à la sécurité du Centre canadien de protection de l'enfance, conçu pour les élèves de la maternelle à la 3e. Ce programme est également disponible en français.

L'internet pouvant être lent dans certaines régions d'Afrique, les jeux et les programmes éducatifs doivent comporter des éléments hors ligne en plus des éléments en ligne.

Pour garantir une mise en œuvre réussie de la formation à la cybersécurité dans les écoles, il faut souligner l'importance de la formation des enseignants. Par exemple, une initiative du Département de la sécurité intérieure des États-Unis équipe les enseignants de la maternelle à la terminale de programmes et d'outils pédagogiques en matière de cybersécurité (Cybersecurity Education Training Assistance Program). Kids for Cyber est un kit prêt à l'emploi permettant aux éducateurs de créer un atelier et d'explorer le cyberespace avec les générations futures.

Les parents doivent être impliqués dans le processus d'éducation à la cybersécurité de leurs enfants. En sa qualité de parent, Corbin Roof partage quelques conseils et bonnes pratiques

sur la manière d'enseigner les bases de la cybersécurité aux enfants. D'après son expérience personnelle, les parents devraient souligner qu'il est important de protéger leur identité, évaluer régulièrement les progrès réalisés par l'enfant, entamer les conversations sans attendre, s'impliquer régulièrement auprès de leurs enfants, encourager leur curiosité, être l'administrateur de leur foyer, apprendre aux enfants qu'ils sont responsables de leurs actes.

Le GFCE a conscience de ce besoin et, dans le cadre de son programme de recherche, a fourni un espace et un financement pour un projet de cartographie de l'éducation à la cybersécurité destiné aux jeunes dans plusieurs pays/régions.

Voir le rapport sur le portail Cybil.

Si les éléments interactifs dans l'apprentissage et la formation sont importants pour les enfants, ils ne doivent pas être éludés par les professionnels. Par exemple, Kaspersky a préparé un **jeu de simulation en ligne à l'intention des diplomates et des professionnels, pour les amener à mieux comprendre les aspects techniques du comment et du pourquoi des cyberattaques, sans pour autant survivre à une telle attaque.**

Conseils pratiques pour développer les capacités nationales en matière de cybersécurité, par le renforcement des compétences

Les activités malveillantes sont en augmentation dans le cyberespace. Il est donc **nécessaire de pouvoir compter sur des professionnels qualifiés** pour pouvoir faire face à cette situation. Selon le livre blanc de l'Organisation des États américains intitulé *Cybersecurity Education: Planning for the Future Through Workforce Development*, les compétences requises pour ces professionnels comprennent, entre autres, la capacité « de concevoir et d'exploiter de manière optimale des applications et des systèmes, avec la capacité d'identifier les cybermenaces et d'y répondre ».

Le déficit de compétences en matière de cybersécurité en Afrique et au Moyen-Orient est estimé à 142 000 personnes, selon le rapport *Addressing the cybersecurity skills gap through cooperation, education and emerging technologies*. Un rapport produit par l'équipe Serianu Cyber Intelligence *2018 Africa Cyber Security Report - Kenya* indique que 60 % des entreprises surveillées sont confrontées à une pénurie de professionnels de la cybersécurité. Cette pénurie existe aussi bien dans le secteur public que dans le secteur des entreprises.

En plus de la pénurie, **les professionnels formés doivent continuer à se perfectionner et à se recycler afin de s'adapter aux menaces émergentes**, et cette exigence a un coût. Malheureusement, les entreprises considèrent souvent que cette dépense n'offre aucun retour sur investissement évident, comme l'indique le rapport Serianu ci-dessus.

Différents gouvernements africains s'efforcent de mettre en place des services d'administration en ligne, et les institutions financières africaines ont déployé des services financiers mobiles. Malheureusement, la pénurie de personnel qualifié en matière de cybersécurité en Afrique expose ces projets à un risque élevé de cyberattaques.

Les mesures concrètes suivantes peuvent être envisagées :

- ➔ Les secteurs public et privé disposent déjà de personnel informatique. Ce **personnel peut recevoir une formation ponctuelle supplémentaire sur la cybersécurité.**
- ➔ **Les établissements d'enseignement supérieur doivent mettre en place des sections de cybersécurité** au sein de leurs départements d'informatique, en vue de combler l'écart entre les besoins et la main-d'œuvre de demain.
- ➔ **La création de partenariats, qu'il s'agisse de partenariats public-privé ou d'autres types de partenariats**, afin de surmonter les différents obstacles à la formation d'une main-d'œuvre en matière de cybersécurité. À cet égard, l'Afrique peut s'inspirer d'autres initiatives telles que :

    a) NICE (National Initiative for Cybersecurity Education) - voir ci-dessus.

    b) Le Royaume d'Arabie saoudite a mis en place une initiative gouvernementale résultant d'une collaboration entre différents ministères/départements. Il s'agit de l'Autorité nationale de cybersécurité (NCA). Entre autres missions, la NCA vise à

développer la main-d'œuvre nationale en matière de cybersécurité. Pour cette tâche spécifique, la NCA a mis en place une initiative appelée The Saudi Cybersecurity Higher Education Framework (SCyber-Edu), fruit de la collaboration et de la coordination entre la NCA, le ministère de l'éducation et la commission d'évaluation de l'éducation et de la formation. Les objectifs de l'initiative SCyber-Edu sont : l'élaboration de programmes d'éducation et de formation, la préparation de normes et de cadres professionnels et de tests d'évaluation professionnelle liés à la cybersécurité.

c) L'École Nationale à Vocation Régionale a été créée à Dakar grâce à la coopération entre la France et le Sénégal. Elle devrait constituer un pôle régional dans lequel les apprenants d'autres pays africains peuvent s'inscrire pour renforcer leurs capacités.

💡 **Point de réflexion**

Pouvez-vous penser à un exemple, dans votre propre pays, d'un lien public-privé en matière de cybersécurité qui a mené à une solution gagnant-gagnant ?

Laissez votre commentaire ci-dessous.

Étude de cas : Comment développer un programme d'enseignement de la cybersécurité à l'intention des professionnels ?

Plusieurs membres du GFCE ont élaboré des cours de formation en matière de cybersécurité et nous les encourageons à explorer la fonction de centre d'échange d'informations du GFCE pour trouver la bonne solution.

Plusieurs parties prenantes africaines ont élaboré et dispensé des programmes de développement des capacités. La communauté technique africaine est remarquablement active dans le domaine du renforcement des capacités à l'échelle régionale. Ce groupe de parties prenantes présente également un degré de coordination élevé par rapport aux autres groupes. Le renforcement des capacités ne relève pas du mandat principal de la plupart des organisations de la société civile, mais bon nombre d'entre elles présentent des activités

dans le cadre de leurs projets, visant à renforcer les capacités. Les publics ciblés par les initiatives de la société civile varient.

Les recherches documentaires ne permettent guère d'identifier les initiatives de renforcement des capacités proposées par les universités, mais il existe plusieurs programmes comportant des éléments de cybersécurité. Certaines universités tentent d'établir un lien solide avec le marché du travail en diversifiant les types de cours qu'elles proposent. C'est le cas, par exemple, de l'Université du Witwatersrand Johannesburg, qui propose des cours sanctionnés par un certificat, des cours abrégés, d'une durée d'environ une semaine, destinés aux professionnels.

Le secteur privé contribue au renforcement des capacités principalement selon deux axes : a) indirectement, en soutenant les efforts d'autres groupes de parties prenantes ; b) directement, en tant que principal fournisseur de renforcement des capacités. Dans le premier cas, le soutien du secteur privé aux initiatives visant à renforcer les capacités dans le domaine spécifique de la GI est clair. Dans le second cas, la motivation principale semble être le renforcement des compétences recherchées sur le marché du travail et la valorisation des talents locaux. La relation avec la GI est donc moins claire. Cette section a pour but de fournir quelques exemples choisis des deux modalités de soutien fournies par le secteur privé.

Rapport : « Sustainable Capacity Building : Internet Governance in Africa » (2021)

Développement durable des compétences : Gouvernance de l'internet en Afrique

Pourtant, il n'existe pas de guide universel sur la marche à suivre pour élaborer un programme de cybersécurité. Un programme de formation réussi doit prendre en compte les objectifs du programme, le groupe cible, la durée, ainsi que les ressources disponibles et le mode de prestation (en ligne, hybride, en personne). En termes d'approche méthodologique, les initiatives en face-à-face étaient largement prédominantes en Afrique avant la pandémie de COVID-19.

C) Recherche et développement

Les centres de recherche doivent aider les décideurs du secteur public ou du secteur privé en proposant des solutions innovantes qui visent à relever les défis actuels et futurs de la cybersécurité. Ces centres peuvent prendre la forme de laboratoires de cybersécurité nationaux, voire régionaux, dont le rôle est de résoudre les problèmes les plus urgents en matière de cybersécurité.

Différentes expériences semblent montrer que les initiatives de recherche et développement en matière de cybersécurité fonctionnent mieux lorsqu'elles impliquent plusieurs parties prenantes. Il est donc souhaitable d'inclure les établissements d'enseignement supérieur dans les efforts globaux de renforcement des capacités en matière de cybersécurité.

Principaux enseignements

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.

- Le renforcement des cybercapacités peut faciliter le processus d'**exploitation des technologies numériques et de l'innovation pour générer une croissance économique inclusive, stimuler la création d'emplois et favoriser le développement socio-économique**. De même, le renforcement des capacités apportera une contribution positive à l'**implication des parties prenantes africaines dans les discussions sur la politique numérique** mondiale, par la **promotion efficace des intérêts africains sur la scène internationale**.

- La différence majeure entre le renforcement des capacités et le développement des capacités s'explique par le fait que le renforcement des capacités englobe le départ à un point zéro, marqué par le recours à une expertise externe pour créer quelque chose qui n'existait pas auparavant ; le développement des capacités,

en revanche, met l'accent sur l'existence de processus de développement endogènes, et soutient les processus déjà en cours.

- Le renforcement des cybercapacités est axé sur le développement des capacités collectives et la facilitation de la coopération et des partenariats internationaux dans le but de répondre efficacement aux cyberdéfis.

- Selon l'indice mondial de cybersécurité (GCI), qui a mesuré et combiné le score de chaque pays sur les 5 piliers de la cybersécurité (juridique, technique, organisationnel, mesures de développement des capacités et mesures de coopération), tous les pays d'Afrique, sauf six, manquent d'incitations au développement des capacités en matière de cybersécurité.

- La sensibilisation et la connaissance limitées du public quant au risque potentiel que représente le cyberespace, associées au manque de compréhension par les responsables gouvernementaux de l'interconnexion entre la cybersécurité et la sécurité nationale, constituent le principal obstacle pour les pays africains en matière de cybersécurité.

- Une pénurie de professionnels adéquatement formés entrave la prospérité économique globale d'une nation. Le manque de personnel qualifié en matière de cybersécurité peut menacer le succès d'une entreprise : les cyberattaques peuvent causer d'énormes pertes financières, perturber les opérations, les services et les chaînes d'approvisionnement, et compromettre ainsi la vie privée et les données personnelles. En outre, il empêche toute participation significative des pays africains dans les forums internationaux. Comme ils ne peuvent pas exprimer leurs besoins, ils brillent souvent par leur absence pendant le déroulement des discussions et l'élaboration des politiques.

- Outre les compétences techniques, les professionnels de la cybersécurité ont besoin de soft skills pour mener à bien leur carrière dans ce domaine, telles que des compétences en matière de leadership, communication (traduction de sujets techniques en termes commerciaux), pensée critique/analytique, travail en équipe et créativité.

- Les efforts de renforcement des capacités devraient cibler les femmes, qui sont encore largement sous-représentées dans la main-d'œuvre de la cybersécurité. En Afrique, les femmes représentent 9 % des professionnels de la cybersécurité.

Compte tenu du fait que près de 60 % de la population africaine a moins de 25 ans, ce qui fait de l'Afrique le continent le plus jeune du monde, et que les femmes représentent plus de 50 % de la population africaine combinée, il est important de se concentrer sur les jeunes filles et les femmes pour les encourager à choisir le secteur de la cybersécurité et y faire carrière. En fin de compte, cela ouvrirait une multitude d'options pour la création d'emplois bien rémunérés, et contribuerait à réduire le déficit de main-d'œuvre dans le domaine de la cybersécurité qui est particulièrement préoccupant et bouleverse l'avancée numérique et technologique dans la région.