INDICE MONDIAL DE CYBERSÉCURITÉ V4 2019/2020

Les questions qui figurent dans le présent questionnaire ont été élaborées et examinées par les participants à la réunion du Groupe du Rapporteur pour la Question 3/2 (Sécurisation des réseaux d'information et de communication: Bonnes pratiques pour créer une culture de la cybersécurité) de la Commission d'études 2 de l'UIT-D. Cette réunion a servi de cadre pour rechercher l'approbation des Membres en vue de la publication de la quatrième version de l'Indice mondial de cybersécurité (GCI) pour 2019-2020. Le questionnaire se compose de cinq parties, dans lesquelles il faut répondre oui ou non et cocher les cases figurant devant chaque élément, le cas échéant. Il doit être rempli en ligne. Chaque personne interrogée recevra (dans un courriel officiel de l'UIT) une adresse URL unique pour le sauvegarder. Si un coordonnateur choisit une équipe chargée de répondre au questionnaire, le même identifiant peut être utilisé afin de soumettre les réponses.

Le questionnaire en ligne offre la possibilité aux participants de télécharger, pour chaque question, des documents (et des adresses URL) à l'appui. Les informations communiquées par les participants dans le cadre du présent questionnaire ne doivent pas être de nature confidentielle.

MESURES JURIDIQUES

1 Règle juridique de fond en matière de cybercriminalité

Explication: *Une règle juridique de fond englobe toutes les branches du droit public et du droit privé, y compris le droit des contrats, le droit immobilier, la responsabilité délictuelle, le droit patrimonial et le droit pénal et a pour objectif fondamental de créer, définir et régir les droits individuels.*

1.1 Existe-t-il une règle juridique de fond régissant les comportements illicites en ligne?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.1 Existe-t-il une règle juridique de fond relative à l'accès illicite aux dispositifs, aux systèmes informatiques et aux données?

Explication: "**Accès**" – Capacité et manière de communiquer ou d'interagir avec un système, d'utiliser les ressources d'un système pour traiter des informations, de prendre connaissance des informations contenues dans le système ou de contrôler les composantes et les fonctions d'un système (NICCS).

"**Système informatique**" ou "**système**" – Dispositif ou groupe de dispositifs interconnectés ou apparentés, dont un ou plusieurs d'entre eux, conformément à un programme, exécutent un traitement automatisé de données (Convention sur la cybercriminalité).

"**Donnée informatique**" – Toute représentation de faits, d'informations ou de concepts sous une forme adaptée à un traitement dans un système informatique, y compris un programme permettant d'ordonner à un système informatique d'exécuter une fonction (Convention sur la cybercriminalité).

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.2 Existe-t-il une règle juridique de fond relative à l'atteinte à l'intégrité des dispositifs, des données et des systèmes informatiques (par l'introduction, l'altération ou la suppression de données?

Explication: "**Atteinte à l'intégrité d'un système informatique**" – Acte intentionnel et non autorisé visant à perturber gravement le fonctionnement d'un système informatique, consistant par exemple à introduire, transmettre, endommager, effacer, détériorer, altérer ou supprimer des données informatiques.

Atteinte à l'intégrité des données" – Acte intentionnel et non autorisé visant à endommager, effacer, détériorer, altérer ou supprimer des données informatiques.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.3 Existe-t-il une règle juridique de fond relative à l'interception illicite des dispositifs, des systèmes informatiques et des données?

Explication: "**Interception illicite**" – Transmission intentionnelle, non autorisée et non publique de données informatiques vers ou depuis un ordinateur ou un autre système électronique, ou au sein d'un ordinateur ou d'un autre système électronique, effectuée par des moyens techniques.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.4 Existe-t-il une règle juridique de fond relative à l'usurpation d'identité et au vol de données en ligne?

Explication: "**Usurpation d'identité en ligne**" – Vol d'informations personnelles telles que le nom, l'adresse, la date de naissance, les coordonnées ou les données bancaires pouvant être opéré par le biais du hameçonnage, du piratage de comptes en ligne, de la récupération d'informations sur les réseaux sociaux ou de l'accès illicite aux bases de données.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.2 Existe-t-il des dispositions en matière de falsification informatique (piratage/atteinte aux droits d'auteur)?

Explication: introduction, altération ou effacement non autorisé de données informatiques visant à créer des données non authentiques dans l'intention que les données soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, dans un but frauduleux ou malhonnête.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.3 Existe-t-il une règle juridique de fond relative à la sécurité en ligne?

Explication: "**Sécurité en ligne**" – Fait d'accroître au maximum la sécurité sur Internet pour se prémunir contre les différents risques pour les informations privées et personnelles ou les informations liées à la propriété, et d'améliorer la capacité des utilisateurs à se protéger eux-mêmes contre la cybercriminalité.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.3.1 Existe-t-il des dispositions/mesures juridiques relatives aux infractions liées à des données en ligne à caractère raciste ou xénophobe?

Explication: Mesures visant à prévenir différentes formes de discours haineux en ligne et d'autres formes de discrimination fondée sur la race, la couleur, la religion, l'ascendance ou l'origine nationale ou ethnique, l'orientation sexuelle ou l'identité de genre, le handicap, le statut social ou d'autres caractéristiques.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.3.2 Existe-t-il des dispositions/mesures juridiques relatives au harcèlement et aux abus en ligne visant à porter atteinte à la dignité et à l'intégrité des personnes?

Explication: "**Cyberharcèlement**" ou "**cyberintimidation**" – Messages envoyés par courrier électronique, par messagerie instantanée ou via des sites Internet de dénigrement afin d'intimider ou de harceler un individu ou un groupe d'individus par le biais d'attaques personnelles.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.3.3 Existe-t-il des dispositions/mesures juridiques en matière de protection en ligne des enfants?

Explication: *Il s'agit de lois qui établissent clairement que tout crime commis contre un enfant dans le monde réel peut également être commis sur Internet ou par le biais de tout autre réseau électronique. Il est nécessaire d'élaborer de nouvelles lois ou d'adopter des lois visant à interdire certains types de comportements qui ne peuvent exister que sur Internet, par exemple le fait d'inciter les enfants à distance à participer ou à assister à des actes sexuels ou encore de les "préparer" à une rencontre dans le monde réel à des fins sexuelles (Lignes directrices sur la protection en ligne des enfants à l'intention des décideurs, UIT).*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2 Existe-t-il une réglementation relative à la cybersécurité concernant...

Explication: *Une réglementation est une règle qui se fonde sur un texte de loi spécifique et qui vise à l'appliquer. Généralement, une autorité de régulation est chargée de veiller au respect des réglementations, ou a été créée dans ce but, de façon à appliquer les dispositions prévues par la loi.*

On entend par réglementation en matière de cybersécurité les principes auxquels doivent se soumettre diverses parties prenantes, qui émanent et font partie de la mise en oeuvre de la législation régissant: la protection des données, la notification des infractions, les obligations relatives à la certification/normalisation en matière de cybersécurité, la mise en oeuvre des mesures de cybersécurité, les obligations en matière d'audits de cybersécurité, la protection de la vie privée, la protection en ligne des enfants, les signatures numériques et les transactions électroniques, et la responsabilité des fournisseurs de services Internet.

2.1 La protection des données personnelles/de la vie privée?

Explication: *Il s'agit de réglementation se rapportant à la protection des données personnelles contre l'accès, l'altération, la destruction ou l'utilisation non autorisés. La protection de la vie privée sur Internet renvoie au niveau de confidentialité et de sécurité des données personnelles publiées en ligne. C'est un terme général qui désigne une grande diversité de facteurs, techniques et technologies utilisés pour protéger les données, les communications et les préférences à caractère sensible et privé. La loi sur la protection des données est un exemple de législation de ce type.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.2 Le signalement des atteintes aux données/incidents?

Explication: *Les lois ou règlements en matière de signalement des infractions imposent à l'entité victime d'une infraction d'en informer les autorités, les clients et autres parties, et de prendre des mesures en vue de remédier aux dommages causés. Ces lois sont promulguées en réponse au nombre croissant d'infractions perpétrées contre les bases de données de consommateurs, qui contiennent des informations d'identification personnelle.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.3 Les obligations en matière d'audits de cybersécurité?

Explication: *Un audit de sécurité est une évaluation systématique et périodique de la sécurité du système d'information. Généralement, pareil audit comprend une évaluation de la sécurité de la configuration et de l'environnement physiques du système, des logiciels, des processus de traitement de l'information et des pratiques d'utilisation.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.4 La mise en œuvre des normes?

Explication: *Existence d'un ou plusieurs cadres approuvés (ou ratifiés) par le gouvernement concernant l'application des normes internationalement reconnues en matière de cybersécurité dans le secteur public (administrations publiques) et dans l'infrastructure essentielle (même si elle est gérée par le secteur privé). Les normes concernées sont, entre autres, celles élaborées par les organismes suivants: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.5 L'utilisation de la signature numérique dans les services et les applications de l'administration publique (administration publique en ligne)?

Explication: *Une signature numérique est une technique mathématique qui sert à valider l'authenticité et l'intégrité d'un message, d'un logiciel ou d'un document numérique. Une transaction électronique désigne la vente ou l'achat de biens ou de services entre entreprises, ménages, individus, États et autres organismes publics ou privés, sur des réseaux informatisés. Les lois sur le commerce, les signatures et les transactions électroniques sont autant d'exemples de ce type de législation, qui peut prévoir des réglementations relatives à l'institution d'un contrôleur des autorités de certification.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.6 La réduction des spams?

Explication: *Veuillez fournir des informations sur la législation ou la réglementation visant à lutter contre les spams.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.7 L'identification et la protection des infrastructures essentielles de l'information au niveau national?

Explication: *Les infrastructures essentielles sont des systèmes élémentaires dont dépendent la sûreté, la sécurité en général, la sécurité économique et la santé publique d'un pays. Il s'agit notamment des secteurs de la défense nationale, de la banque et de la finance, des télécommunications et de l'énergie. Veuillez indiquer tout lien ou document définissant les infrastructures essentielles ou tout document/toute nouvelle confirmant la définition de telles infrastructures.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours dans le domaine juridique auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité (Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui)

Ou indiquez les documents pertinents contenant des liens à l'appui.

MESURES TECHNIQUES

1 Équipe CIRT/CSIRT/CERT nationale/gouvernementale

Explication: "***CIRT-CSIRT-CERT***": *Équipes d'intervention en cas d'incident informatique, entités organisationnelles doté d'un personnel chargé de coordonner et d'appuyer les interventions en réponse à des évènements ou des incidents en matière de sécurité informatique au niveau national ou gouvernemental.*

NOTE: *Une distinction est parfois opérée entre les équipes CIRT gouvernementales et nationales: les équipes CIRT gouvernementales sont au service des parties prenantes gouvernementales tandis que les équipes CIRT nationales sont au service des parties prenantes nationales, y compris le secteur privé et les particuliers. Elles sont parfois considérées comme une seule et même entité.*

1.1 Existe-t-il une équipe CIRT/CSIRT/CERT nationale/gouvernementale?

Explication: *Appuyée par une décision gouvernementale ou intégrée dans les structures publiques ou nationales.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.2 L'équipe CIRT/CSIRT/CERT nationale/gouvernementale de votre pays effectue-t-elle est activités suivantes:

1.2.1 Conception et mise en œuvre d'activités de sensibilisation en matière de cybersécurité?

Explication: Il s'agit d'efforts visant à promouvoir des campagnes publicitaires à grande échelle pour sensibiliser la population aux comportements sécurisés en ligne.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.2.2 Réalisation d'exercices de cybersécurité réguliers tels que des cyberexercices?

Explication: *Il s'agit d'une activité planifiée au cours de laquelle une organisation simule une cyberperturbation afin de renforcer ou de tester ses capacités de prévention, de détection, d'atténuation ou de traitement des perturbations, ou de rétablissement après une perturbation. Cet exercice est-il périodique ou régulier?*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.2.3 Publication d'orientations à l'intention du public?

Explication: *Orientations des équipes CIRT: informations communiquées au grand public au sujet des nouvelles cybermenaces et des mesures recommandées.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.2.4 Contribution aux questions liées à la protection en ligne des enfants?

Explication: *Les équipes CIRT/CSIRT/CERT fournissent des services d'appui, par exemple en organisant des campagnes de sensibilisation, en signalant les incidents liés aux enfants, en fournissant des supports éducatifs sur la protection en ligne des enfants, etc.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.3 Les équipes CIRT (CSIRT ou CERT) susmentionnées sont-elles affiliées au Forum des équipes d'intervention et de sécurité en cas d'incident (FIRST)?

Explication: *Membre titulaire ou agent de liaison du FIRST (www.first.org).*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.4 Les équipes CIRT (CSIRT ou CERT) susmentionnées sont-elles affiliées à une équipe CERT régionale?

Explication: *Relation, officielle ou non, avec n'importe quelle autre équipe CERT, au sein du pays ou non, dans le cadre d'un groupe régional de CERT. Parmi les équipes CERT régionales, on peut citer APCERT, AFRICACERT, EGC, OIC et OAS.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.5 Quel est le niveau de maturité des services CIRT, CSIRT ou CERT susmentionnés bénéficiant d'une certification TI dans le cadre du Modèle SIM3 du Groupe TF-CSIRT (Groupe de travail des Équipes d'intervention sur les incidents de sécurité informatique)?

Explication: *Le modèle SIM3 (Security incident management maturity model) est un critère de base de la certification pour les équipes CIRT.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2 Équipes CIRT/CSIRT/CERT sectorielles

Explication: *Une équipe CIRT/CSIRT/CERT sectorielle est une entité qui intervient en cas d'incident relatif à la sécurité informatique ou à la cybersécurité affectant un secteur d'activité spécifique. Les équipes CERT sectorielles sont généralement créées pour des secteurs essentiels, tels que la santé, les services publics, l'enseignement supérieur, les services d'urgence et le secteur financier. Une équipe CERT sectorielle fournit ses services aux parties prenantes d'un seul secteur d'activité.*

2.1 Existe-t-il des équipes CIRT/CSIRT/CERT sectorielles dans votre pays?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.2 Dans votre pays, les équipes CIRT/CSIRT/CERT sectorielles effectuent-elles les activités suivantes:

2.2.1 Conception et mise en œuvre d'activités de sensibilisation en matière de cybersécurité à l'intention d'un secteur?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.2.2 Participation active aux cyberexercices nationaux?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.2.3 Signalement des incidents liés au secteur auprès des parties prenantes concernées?

Explication: *Communication d'informations au sujet des nouvelles cybermenaces et des mesures recommandées.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3 Cadre national pour la mise en oeuvre des normes en matière de cybersécurité?

Explication: *Adoption d'un ou de plusieurs cadres visant à appliquer des normes internationalement reconnues en matière de cybersécurité dans le secteur public (administrations) et dans l'infrastructure essentielle (même si elle est gérée par le secteur privé). Les normes concernées sont, entre autres, celles élaborées par les organismes suivants: ISO, UIT IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.*

3.1 Existe-t-il un cadre pour la mise en œuvre/l'adoption de normes en matière de cybersécurité?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.2 Ce cadre porte-t-il sur des normes internationales ou d'autres normes connexes?

Explication: *UIT-T, ISO/CEI, NIST, ANSI/ISA et d'autres organismes.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4 Protection en ligne des enfants

Explication: *Cet indicateur vise à déterminer l'existence d'un organisme national consacré à la protection en ligne des enfants, la mise à disposition d'un numéro de téléphone national permettant de signaler les problèmes liés à la protection en ligne des enfants et l'existence de dispositifs et de fonctionnalités techniques contribuant à la protection en ligne des enfants et d'activités mises en œuvre par des organisations gouvernementales ou non pour aider et informer les parties prenantes sur la façon de protéger les enfants en ligne (numéro de téléphone, adresse électronique et site web au moyen desquels les parties prenantes peuvent rendre compte d'incidents ou d'inquiétudes liés à la protection en ligne des enfants).*

4.1 Des dispositifs et des fonctionnalités en matière de signalement sont-ils mis en œuvre pour contribuer à la protection en ligne des enfants?

Explication: *Services téléphoniques d'urgence, lignes d'assistance téléphonique, etc.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours dans le domaine technique auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité (Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui)

Ou indiquez les documents pertinents contenant des liens à l'appui.

MESURES ORGANISATIONNELLES

1 Stratégie nationale en matière de cybersécurité

Explication: *L'élaboration d'une politique visant à promouvoir la cybersécurité devrait figurer parmi les priorités absolues des pays. Une stratégie nationale en matière de cybersécurité devrait assurer la résilience et la fiabilité de l'infrastructure informatique essentielle du pays et garantir la sécurité de la population; protéger les biens matériels et intellectuels des citoyens, des organisations et de l'État; prévenir les cyberattaques contre les infrastructures essentielles et lutter contre ces cyberattaques; et limiter au maximum les dégâts dus aux cyberattaques et raccourcir les délais nécessaires pour le rétablissement.*

1.1 Existe-t-il une stratégie/politique nationale en matière de cybersécurité dans votre pays?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.1 Cette stratégie ou politique porte-t-elle sur la protection des infrastructures informatiques essentielles du pays, y compris dans le secteur des télécommunications?

Explication: *Tout système informatique physique ou virtuel qui contrôle, traite, transmet, reçoit ou stocke des informations électroniques sous quelque forme que ce soit (données, voix ou vidéo) dont l'importance est cruciale pour le fonctionnement de l'infrastructure essentielle, à tel point que le dysfonctionnement ou la destruction de ce système aurait un effet dévastateur sur la sécurité, la sécurité économique ou la santé et la sécurité publiques au niveau national.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.2 Cette stratégie ou politique renvoie-t-elle à un plan national de résilience en matière de cybersécurité?

Explication: *Un plan national de résilience en matière de cybersécurité permet au pays de résister aux conséquences d'une catastrophe, de les atténuer, de s'y adapter et de se rétablir rapidement et efficacement des conséquences d'une catastrophe (d'origine naturelle ou anthropique), notamment grâce à la préservation et à la restauration de ses fonctions et services essentiels en s'appuyant sur des services extérieurs.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.3 La stratégie nationale en matière de cybersécurité est-elle révisée et actualisées de manière continue?

Explication: *La gestion du cycle de vie de la stratégie est définie et la stratégie est actualisée au regard des évolutions nationales, technologiques, sociales, économiques et politiques susceptibles d'avoir de conséquences pour la situation nationale en matière de cybersécurité.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.4 La stratégie en matière de cybersécurité fait-elle l'objet de consultations auprès des spécialistes de la cybersécurité au niveau national?

Explication: *La stratégie peut faire l'objet de consultations auprès de toutes les parties prenantes concernées, y compris les opérateurs d'infrastructures essentielles, les fournisseurs de services Internet, les universitaires, etc.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.2 Existe-t-il un plan d'action/une feuille de route pour la mise en œuvre de la gouvernance en matière de cybersécurité?

Explication: *Il s'agit d'un plan stratégique qui définit les objectifs nationaux en matière de cybersécurité ainsi que les étapes nécessaires pour les atteindre.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.3 Existe-t-il une stratégie nationale en matière de protection en ligne des enfants?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2 Organisme responsable

Explication: *L'organisme responsable de la mise en oeuvre de la stratégie/politique nationale en matière de cybersécurité peut être un comité permanent, un groupe de travail officiel, un conseil consultatif ou un centre interdisciplinaire. Cet organisme peut aussi être directement responsable d'une équipe CIRT nationale. Il peut appartenir au gouvernement et avoir le pouvoir d'obliger d'autres agences et organismes nationaux à mettre en oeuvre les politiques et à adopter des normes.*

2.1 Existe-t-il un organisme responsable de la coordination en matière de cybersécurité au niveau national?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.1.1 Cet organisme gère-t-il la protection de l'infrastructure informatique essentielle au niveau du pays?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.2 Existe-t-il un organisme national chargé du renforcement des capacités en matière de cybersécurité dans le pays?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.3 Existe-t-il un organisme chargé des initiatives en matière de protection en ligne des enfants au niveau national?

Explication: *Existence d'un organisme national chargé de superviser et de promouvoir la protection en ligne des enfants.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3 Indicateurs relatifs à la cybersécurité

Explication: *Existence d'exercices d'évaluation comparative, nationaux ou sectoriels, reconnus officiellement ou d'un référentiel servant à mesurer le développement de la cybersécurité, de stratégies d'évaluation des risques, d'audits de cybersécurité et d'autres outils et activités permettant de noter ou d'évaluer la qualité de fonctionnement à des fins d'amélioration. Par exemple, des exercices basés sur la norme ISO/CEI 27004, qui définit les* mesures relatives à la gestion de la sécurité des informations*.*

3.1 Des audits sont-ils effectués dans le domaine de la cybersécurité au niveau national?

Explication: *Un audit de sécurité consiste à évaluer méthodiquement la sécurité d'un système d'information en mesurant dans quelle mesure il respecte un ensemble de critères prédéfinis. Un audit minutieux comprend généralement une évaluation de la sécurité de la configuration et de l'environnement physiques du système, des logiciels, des processus de traitement de l'information et des pratiques d'utilisation. L'accès à des infrastructures essentielles gérées par des entités privées peut être demandé par les organismes de régulation afin de procéder à des évaluations périodiques des conditions de sécurité et de rendre compte des résultats.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.2 Existe-t-il des indicateurs visant à évaluer les risques liés au cyberespace au niveau national?

Explication: *Il s'agit d'un processus comprenant l'identification, l'analyse et l'évaluation des risques.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.3 Existe-t-il des mesures visant à évaluer le niveau de développement de la cybersécurité au niveau national?

Explication: *Il s'agit d'une approche visant à mesure le niveau de développement de la cybersécurité dans un pays.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours concernant les mesures organisationnelles auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité (Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui)

Ou indiquez les documents pertinents contenant des liens à l'appui.

RENFORCEMENT DES CAPACITÉS

1 Campagnes de sensibilisation du public à la cybersécurité

Explication: *La sensibilisation du public comprend les efforts déployés pour promouvoir des campagnes visant à toucher autant de personnes que possible, mais aussi à recourir à des ONG, des institutions, des organisations, des fournisseurs de services Internet, des bibliothèques, des organisations du commerce locales, des centres communautaires, des lycées, des programmes de formation pour adultes, des écoles et des organisations parents-enseignants, afin de faire passer les messages relatifs à un comportement sécurisé en ligne. Il peut s'agir de la création de portails et de sites Internet de sensibilisation, de la distribution de matériel pédagogique et d'autres activités pertinentes.*

1.1 Existe-t-il des campagnes de sensibilisation du public destinées à un secteur en particulier, comme les PME, les entreprises du secteur privé ou les organismes publics?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.2 Existe-t-il des campagnes de sensibilisation du public destinées à la société civile?

Explication: *ONG, organisations communautaires, etc.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.3 Existe-t-il des campagnes de sensibilisation du public destinées aux particuliers?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.4 Existe-t-il des campagnes de sensibilisation du public destinées aux personnes âgées?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.5 Existe-t-il des campagnes de sensibilisation du public destinées aux personnes ayant des besoins particuliers?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.6 Existe-t-il des campagnes de sensibilisation du public organisées avec la participation des parents, des enseignants et des enfants (en lien avec la protection en ligne des enfants)?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2 Formation à l'intention des professionnels de la cybersécurité

Explication: *Existence de programmes de formation professionnelle sectoriels visant à sensibiliser le grand public (journée, semaine ou mois de sensibilisation nationale à la cybersécurité, par exemple), promotion de l'éducation en matière de cybersécurité pour les ressources humaines dans différents domaines (technique, sciences sociales, etc.) et promotion de la certification des professionnels dans le secteur public ou privé.*

Ces programmes comprennent la formation sur la cybersécurité à l'intention des membres des forces de l'ordre, du personnel judiciaire ou d'autres acteurs de la scène juridique et désignent des formations professionnelles et techniques pouvant être organisées de manière récurrente à l'intention des agents de police ou agents des forces de l'ordre, des juges, avocats, conseillers juridiques, magistrats, auxiliaires juridiques ainsi que de toute autre professionnel dans le domaine juridique ou dans le domaine de l'application de la loi.

Cet indicateur tient également compte de l'existence d'un ou plusieurs cadres approuvés (ou ratifiés) par le gouvernement concernant la certification et l'accréditation de professionnels sur la base de normes internationalement reconnues en matière de cybersécurité. Ces certifications, accréditations et normes sont notamment les suivantes: Connaissance de la sécurité dans le nuage informatique (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK et Cybersecurity Forensic Analyst (ISC²).

2.1 Votre gouvernement élabore-t-il des cours de formation professionnelle dans le domaine de la cybersécurité ou encourage-t-il leur tenue?

Explication: *Promotion de cours sur la cybersécurité au sein des ressources humaines (domaine technique, sciences sociales, etc.) et promotion de la certification des professionnels dans le secteur public ou privé.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.2 Existe-t-il un programme d'accréditation des professionnels de la cybersécurité dans votre pays?

Explication: *Instituts délivrant une accréditation aux professionnels de la cybersécurité ou autres mécanismes apparentés.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.3 Existe-t-il des programmes pédagogiques/formations/cours nationaux à l'intention des professionnels de la cybersécurité dans un secteur donné?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.3.1 Existe-t-il des programmes pédagogiques/formations/cours nationaux à l'intention des autorités chargées de l'application de la loi dans un secteur donné?

Explication: *Processus formel en matière de cybersécurité visant à former les acteurs juridiques (agents de police et agents des forces de l'ordre) à la sécurité informatique*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.3.2 Existe-t-il des programmes pédagogiques/formations/cours nationaux à l'intention du personnel judiciaire ou d'autres acteurs juridiques dans un secteur donné?

Explication: *Formations à la cybersécurité ou formations techniques pouvant être organisées de manière récurrente à l'intention des agents de police ou agents des forces de l'ordre, des juges, avocats, conseillers juridiques, magistrats, auxiliaires juridiques ainsi que de toute autre professionnel dans le domaine juridique ou dans le domaine de l'application de la loi.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.3.3 Existe-t-il des programmes pédagogiques/formations/cours nationaux à l'intention de PME/d'entreprises privées dans un secteur donné?

Explication: *Formation aux bonnes pratiques/ renforcement des capacités en matière de sécurité en vue de protéger les entreprises en utilisant les services en ligne de manière adaptée.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.3.4 Existe-t-il des programmes pédagogiques/formations/cours nationaux à l'intention d'autres responsables publics ou gouvernementaux dans un secteur donné?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3 Votre gouvernement/organisation élabore-t-il/elle des programmes pédagogiques ou universitaires ayant trait à la cybersécurité ou encourage-t-il/elle leur élaboration…

Explication: *Existence et promotion de cours et programmes nationaux de formation au sein des écoles, lycées, universités et autres établissements d'enseignement, afin d'enseigner à la nouvelle génération des compétences ou un métier ayant trait à la cybersécurité. Les métiers de la cybersécurité sont, entre autres: cryptanalyste, spécialiste de la criminalistique numérique, intervenant en cas d'incident, architecte de sécurité et expert des tests d'intrusion.*

3.1 Dans l'enseignement primaire?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.2 Dans l'enseignement secondaire?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.3 Dans l'enseignement supérieur?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4 Programmes de recherche-développement en matière de cybersécurité

Explication: *Cet indicateur vise à mesurer les investissements dans les programmes nationaux de recherche-développement en matière de cybersécurité à l'intention d'institutions pouvant être privées, publiques, universitaires, non gouvernementales ou internationales. Il tient également compte de la présence d'un organisme institutionnel responsable du programme et reconnu au niveau national. Les programmes de recherche en matière de cybersécurité comportent, entre autres, des analyses de logiciels malveillants, des études cryptographiques, des recherches concernant les failles des systèmes ainsi que des modèles et concepts de sécurité. Les programmes de développement en matière de cybersécurité concernent l'élaboration de solutions matérielles et logicielles, telles que les pare-feu, les systèmes de prévention d'intrusion, les leurres informatiques et les modules matériels de sécurité. La présence d'un organisme national de supervision est nécessaire pour faciliter la coordination entre les institutions ainsi que le partage des ressources.*

4.1 Existe-t-il des activités de recherche-développement en matière de cybersécurité au niveau national?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4.1.1 Existe-t-il des programmes de recherche-développement en matière de cybersécurité dans le secteur privé?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4.1.2 Existe-t-il des programmes de recherche-développement en matière de cybersécurité dans le secteur public?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4.1.3 Les établissements d'enseignement supérieur tels que les établissements universitaires et les universités participent-ils aux activités de recherche-développement?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

5 Secteur de la cybersécurité à l'échelle nationale

Explication: *Un environnement économique, politique et social favorable au développement de la cybersécurité facilite la croissance du secteur privé autour de cette activité. L'existence de campagnes de sensibilisation du public, le développement de la main-d'oeuvre, le renforcement des capacités et les mesures incitatives du gouvernement soutiennent le marché des produits et services liés à la cybersécurité. L'existence d'un secteur de la cybersécurité au niveau local atteste d'un tel environnement et encourage la croissance de startups dans le domaine de la cybersécurité et de marchés de la cyberassurance associés.*

5.1 Existe-t-il un secteur de la cybersécurité à l'échelle nationale?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

6 Existe-t-il des mécanismes incitatifs du gouvernement visant à...

Explication: *Cet indicateur concerne toute mesure incitative à l'initiative du gouvernement visant à encourager le renforcement des capacités en matière de cybersécurité (exonérations fiscales, subventions, financements, prêts, mise à disposition d'infrastructures et autres incitations d'ordre économique et financier, ou encore organisme institutionnel dédié, reconnu au niveau national et chargé de superviser les activités de renforcement des capacités dans ce domaine). Les mesures incitatives stimulent la demande de services et produits liés à la cybersécurité, améliorant ainsi la lutte contre les cybermenaces.*

6.1 Encourager le renforcement des capacités dans le domaine de la cybersécurité?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

6.2 Créer un secteur de la cybersécurité?

Explication: *Appui fourni aux startups, services de cybersécurité dans les établissements universitaires, etc.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours concernant les mesures de renforcement des capacités auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité (Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui)

Ou indiquez les documents pertinents contenant des liens à l'appui.

MESURES DE COOPÉRATION

1 Accords bilatéraux de coopération avec d'autres pays en matière de cybersécurité

Explication: *Les accords bilatéraux (ou accords entre deux parties) désignent toute forme de partenariat officiellement reconnu, national ou sectoriel, visant à partager des informations ou des ressources relatives à la cybersécurité avec un autre État ou une entité régionale (coopération ou échange d'informations, d'expertise, de technologies et d'autres ressources). L'indicateur mesure également l'échange d'informations sur les menaces. Le renforcement des capacités désigne l'échange d'outils professionnels, le perfectionnement des compétences spécialisées, etc.*

1.1 Existe-t-il des accords bilatéraux de coopération avec d'autres pays en matière de cybersécurité?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.1 L'échange d'informations fait-il partie de cet accord ou de ces accords?

Explication: *L'échange d'informations désigne les pratiques liées à l'échange d'informations à caractère non sensible.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.2 Le renforcement des capacités fait-il partie de cet accord ou de ces accords?

Explication: *Promouvoir des formations visant à renforcer les capacités et les compétences des professionnels de la cybersécurité au niveau national dans le cadre d'une coopération pour lutter collectivement contre les cybermenaces.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

1.1.3 L'assistance juridique mutuelle fait-elle partie de cet accord ou de ces accords?

Explication: *Assistance mutuelle entre deux pays ou plus visant à recueillir et à échanger des informations en vue de faire respecter le droit public et pénal.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2 Participation du gouvernement à des mécanismes internationaux liés aux activités dans le domaine de la cybersécurité

Explication: *Peut aussi désigner la ratification d'accords internationaux relatifs à la cybersécurité, tels que la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, la Convention de Budapest sur la cybercriminalité, etc.*

2.1 Votre gouvernement ou votre organisation participent-ils à des mécanismes internationaux liés aux activités dans le domaine de la cybersécurité?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3 Accords multilatéraux en matière de cybersécurité

Explication: *Les accords multilatéraux (accords entre au moins trois parties) désignent toute forme de programme officiellement reconnu, national ou sectoriel, visant à partager des informations ou des ressources relatives à la cybersécurité avec plusieurs autres États ou organisations internationales (coopération ou échange d'informations, d'expertise, de technologies et d'autres ressources).*

3.1 Votre gouvernement a-t-il conclu des accords multilatéraux en matière de cybersécurité?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.1.1 L'échange d'informations fait-il partie de cet accord ou de ces accords?

Explication: *L'échange d'informations désigne les pratiques liées à l'échange d'informations à caractère non sensible.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.1.2 Le renforcement des capacités fait-il partie de cet accord ou de ces accords?

Explication: *Promouvoir des formations visant à renforcer les capacités et les compétences des professionnels de la cybersécurité au niveau national dans le cadre d'une coopération pour lutter collectivement contre les cybermenaces.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4 Partenariats avec le secteur privé

Explication: *On entend par partenariats public-privé les initiatives associant le secteur public et le secteur privé. Cet indicateur de performance mesure le nombre de partenariats public-privé nationaux ou sectoriels officiellement reconnus, visant à partager des informations et des ressources relatives à la cybersécurité (personnel, processus, outils) entre le secteur public et le secteur privé (partenariats officiels pour la coopération ou l'échange d'informations, d'expertise, de technologie et/ou de ressources), qu'ils soient nationaux ou internationaux.*

4.1 Votre gouvernement a-t-il conclu des partenariats public-privé avec des entreprises locales?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4.2 Votre gouvernement a-t-il conclu des partenariats public-privé avec des entreprises étrangères dans votre pays?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

5 Partenariats interorganismes

Explication: *Cet indicateur de performance désigne toute forme de partenariat officiel entre les différents organismes publics d'un pays (il n'inclut donc pas les partenariats internationaux). Il peut s'agir de partenariats en faveur du partage d'informations ou de ressources entre les ministères, les départements, les programmes et d'autres institutions du secteur public.*

5.1 Existe-t-il des partenariats/accords interorganismes entre différents organismes publics dans le domaine de la cybersécurité?

Explication: *Coopération entre les ministères ou les organismes spécialisés.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours concernant les mesures de coopération auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité (Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui)

Ou indiquez les documents pertinents contenant des liens à l'appui.