Présentation du questionnaire relatif à l'Indice de cybersécurité dans le monde (GCI) 2018

Ce document est diffusé à titre indicatif seulement. Le GCI évalue l'engagement des pays en faveur de la cybersécurité au regard des cinq piliers du Programme mondial cybersécurité: cadre juridique, mesures techniques, structures organisationnelles, renforcement des capacités et coopération.

Ce questionnaire regroupe les questions qui permettront de calculer le score GCI 2017/18 et celles requises par la Question 3 de la Commission d'études de l'UIT-D. Il se compose de cinq parties distinctes, dans lesquelles il faut répondre oui ou non et cocher des cases. Le questionnaire doit être rempli en ligne. Chaque personne interrogée recevra (dans un courriel officiel de l'UIT) une adresse Internet unique pour le sauvegarder. Le questionnaire en ligne offre la possibilité aux participants de télécharger pour chaque question des documents (et des adresses Internet) justificatifs.

Les informations communiquées ne doivent pas être de nature confidentielle.

1 Mesures juridiques

1.1 Votre pays dispose-t-il d'une loi relative à la lutte contre la cybercriminalité?

Explication: *La législation anti-cybercriminalité s'entend de toute loi visant à protéger la confidentialité, l'intégrité et la disponibilité des systèmes, réseaux et données informatiques et régissant les infractions informatiques, les infractions se rapportant au contenu et les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes. Elle peut également désigner des dispositions de droit procédural et d'assistance mutuelle.*

☐ *Oui*

☐ *Non*

☐ *Partiellement (**Uniquement** dans le cas de projets de loi avancés et prêts à être adoptés ou vérifiés)*

1.1.1 Votre pays dispose-t-il d'une règle juridique de fond concernant les questions suivantes?

Explication: *Une règle juridique de fond s'entend d'une loi qui crée, définit et régit les droits individuels.* **(Indiquer si votre pays dispose d'(un) article(s) de loi relatif(s) aux questions ci-après en cochant la case correspondante, et préciser les pages et le numéro de l'article/des articles correspondant à votre choix dans vos documents.)**

☐ accès non autorisé aux ordinateurs, aux systèmes et aux données?

☐ atteinte à l'intégrité/interception/modification non autorisée/destruction d'ordinateurs, de systèmes et de données?

☐ protection de la confidentialité/des données?

Ajouter des liens/url

Ajouter des documents

Si vous avez coché la case "Partiellement", présentez la loi ou l'article en fournissant uniquement le projet relatif aux questions cochées.

1.1.2 Votre pays dispose-t-il de droits procéduraux en matière de cybercriminalité sur les aspects suivants?

Explication: *Par droits procéduraux on entend les règles et les formalités qui doivent être respectées dans le cadre d'une procédure légale pour garantir une application juste et cohérente de la loi dans toutes les affaires portées devant les tribunaux.* **(Indiquer si votre pays dispose d'articles de loi relatifs aux questions ci-après en cochant la case correspondante, et préciser les pages et le numéro de l'article correspondant à votre choix dans vos documents.)**

- ☐ *conservation rapide des données informatiques stockées*
- ☐ *ordonnances de production*
- ☐ *recherche et saisie de données informatiques stockées*
- ☐ *collecte en temps réel de données informatiques*
- ☐ *extradition de personnes s'étant rendues coupables de cybercriminalité*
- ☐ *assistance mutuelle*
- ☐ *confidentialité et limitation d'utilisation.*

Ajouter des liens/url

Ajouter des documents

Si vous avez coché la case "Partiellement", présentez la loi ou l'article en fournissant uniquement le projet relatif aux questions cochées.

1.2 Existe-t-il une réglementation relative à la cybersécurité? Dans quels domaines?

Explication: *Une réglementation est une règle qui se fonde sur un texte de loi spécifique et qui vise à l'appliquer. Une* ***autorité de régulation*** *est chargée de veiller au respect des réglementations de façon à mener à bien les dispositions prévues par la loi. On entend donc par réglementation en matière de cybersécurité les principes auxquels sont soumises les parties prenantes, qui émanent et font partie de la mise en oeuvre de la législation couvrant les aspects indiqués ci-après.* **(Indiquer si votre pays dispose d'articles de loi relatifs aux questions ci-après en cochant la case correspondante, et préciser les pages et le numéro de l'article correspondant à votre choix dans vos documents.)** Prière de noter que cette section porte uniquement sur les réglementations, et non sur les lois/législations, qui font l'objet de la question 1.1.1.

- ☐ *Oui*
- ☐ *Non*
- ☐ *Partiellement*
- ☐ *protection des données?*
- ☐ *notification des infractions?*
- ☐ *obligations d'audit et certification/normalisation en matière de cybersécurité*
- ☐ *protection de la vie privée*
- ☐ *signatures numériques et transactions électroniques?*
- ☐ *responsabilité des prestataires de services Internet (PSI)?*
- ☐ *protection des systèmes et des réseaux?*

Ajouter des liens/url

Ajouter des documents

Si vous avez coché la case "Partiellement", présentez la loi ou l'article en fournissant uniquement le projet relatif aux questions cochées.

1.3 Existe-t-il une législation ou une réglementation relative au filtrage ou à la réduction des spams?

***Explication**: Il s'agit d'une loi/réglementation relative à la protection contre les courriels indésirables liés à l'utilisation d'Internet. (Veuillez indiquer la réglementation et/ou la législation (loi).)*

☐ *Oui*

☐ *Non*

☐ *Partiellement*

Ajouter des liens/url

Ajouter des documents

Si vous avez coché la case "Partiellement", présentez la loi ou l'article en fournissant uniquement le projet relatif à la question traitée.

1.4 Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées dans le domaine juridique auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité (N.B.: Seuls les pays disposant d'une loi ou d'une réglementation en matière de cybersécurité peuvent indiquer des bonnes pratiques)

Ajouter des liens/url

Ajouter des documents

Veuillez énumérer ici les bonnes pratiques si aucun lien ou document n'a été fourni.

2 Mesures techniques

2.1 Existe-t-il un CIRT/CSIRT/CERT?

Explication: *Un CIRT est une équipe d'intervention en cas d'incident informatique. Un CSIRT est une équipe d'intervention en cas d'incident relatif à la sécurité informatique. Quant au CERT, il s'agit d'une équipe d'intervention d'urgence en cas d'incident informatique. Ces termes désignent, de façon interchangeable, une entité à laquelle sont signalés les cas de violation de la sécurité, qu'elle analyse et traite.*

☐ *Oui*

☐ *Non*

2.1.1 Veuillez indiquer la nature du CIRT/CSIRT/CERT dans votre pays.

Explication: *Un CSIRT/CIRT/CERT national désigne une entité chargée de surveiller, gérer et traiter les incidents relatifs à la cybersécurité en collaboration avec ses partenaires locaux: universitaires, forces de l'ordre, société civile, secteur privé (au sein de groupes économiques ou techniques, infrastructures informatiques essentielles (énergie, santé, transport, finance, etc.) et Etats. Ce dispositif collabore également avec les CIRT d'autres pays, ainsi qu'avec des intervenants régionaux et internationaux, afin d'assurer une coordination ciblée et efficace en cas d'attaque.*

☐ *CIRT, CSIRT ou CERT national*

☐ *CIRT, CSIRT ou CERT gouvernemental*

☐ *CIRT, CSIRT ou CERT sectoriel*

Ajouter des liens/url

Ajouter des documents

2.2 Le CIRT/CSIRT/CERT réalise-t-il des exercices de cybersécurité de façon continue?

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 à prévenir, détecter, atténuer, traiter un incident ou à s'en rétablir. Cet exercice est-il périodique ou régulier?*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.3 Le CIRT/CSIRT/CERT indiqué ci-dessus est-il affilié/associé:

☐ *au Forum of Incident Response Security Teams (FIRST)?*

☐ *à un CERT régional (APCERT, ICCERT, AFRICACERT, TFCCERT)?*

☐ *à toute autre association CERT?*

Ajouter des liens/url

Ajouter des documents

2.4 Existe-t-il un cadre pour la mise en oeuvre des normes en matière de cybersécurité dans:

Explication: *Existence d'un ou plusieurs cadres approuvés (ou ratifiés) par le gouvernement concernant l'application des normes internationales en matière de cybersécurité dans le secteur public (administrations) et dans l'infrastructure vitale (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.*

☐ *le secteur public?*

☐ *le secteur privé?*

Ajouter des liens/url

Ajouter des documents

2.5 Votre pays dispose-t-il d'un organisme de normalisation qui:

☐ *a ses propres normes en matière de cybersécurité?*

☐ *adopte les normes internationales?*

Ajouter des liens/url

Ajouter des documents

2.6 Existe-t-il des dispositifs et fonctionnalités techniques visant à combattre les spams?

Explication: *Existe-t-il des mesures et outils techniques destinés à garantir la cybersécurité, tels que des logiciels antivirus ou antispam?*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.7 Votre gouvernement/organisation utilise-t-il/elle le nuage pour assurer la cybersécurité dans le secteur public?

Explication: *Il peut s'agir d'un logiciel assurant la sauvegarde des données en cas d'atteinte à l'intégrité du réseau Internet ou d'un ordinateur, qui s'ajoute à l'utilisation d'un logiciel anti-virus, de suites de logiciels de sécurité Internet et d'outils de lutte contre les logiciels malveillants ou de chiffrement visant à améliorer les systèmes du gouvernement en matière de cybersécurité. Le système du nuage permet à chacun d'avoir accès, en tout lieu et à tout moment, à ses documents/données ou à tout élément sauvegardé, et de les utiliser, en évitant le risque d'atteinte à l'intégrité d'un ordinateur à une extrémité. (Ici encore, le but de la question est de mieux comprendre l'utilisation potentielle du nuage afin de renforcer la position des autorités en matière de cybersécurité au niveau national; il n'est pas nécessaire de préciser un logiciel en particulier.)*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

2.8 Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées dans le domaine technique auxquelles votre pays a participé/participe au titre d'activités en matière de cybersécurité? (N.B.: Seuls les pays disposant d'un CIRT, CSIRT ou CERT peuvent indiquer des bonnes pratiques)

Ajouter des liens/url

Ajouter des documents

3 Mesures organisationnelles

3.1 Existe-t-il une stratégie nationale (politique) en matière de cybersécurité?

Explication: *Les politiques en matière de stratégies nationales de cybersécurité ou de plans nationaux pour la protection des infrastructures informatiques sont celles officiellement définies et approuvées par les Etats. Elles peuvent comprendre les engagements suivants: désigner clairement des responsables de la cybersécurité à tous les niveaux de gouvernement (local, régional et fédéral ou national) dotés de rôles et de responsabilités clairement définis; s'engager clairement en faveur d'une cybersécurité publique et transparente; encourager la participation du secteur privé et les partenariats public-privé dans le cadre des initiatives de promotion de la cybersécurité placées sous l'égide des pouvoirs publics; définir une feuille de route relative à la gouvernance qui identifie les parties prenantes principales (Si elle est en cours d'élaboration, veuillez cocher la case "Partiellement" et aller directement à la question 3.8. Si aucune stratégie n'est en place, allez aussi directement à la question 3.8).*

☐ *Oui*

☐ *Non*

☐ *Partiellement (A cocher uniquement dans le cas de projets avancés et prêts à être* adoptés ou vérifiés.)

Ajouter des liens/url

Ajouter des documents

Si vous avez coché "Partiellement", fournissez le projet de stratégie nationale.

3.2 Votre stratégie nationale est-elle:

Explication: *Un document contenant la stratégie nationale de cybersécurité peut accompagner la stratégie nationale relative à l'information, à la technologie ou à la sécurité. (Si vous avez chargé le document contenant la stratégie dans la question précédente, il n'est pas nécessaire de le charger à nouveau; veuillez simplement indiquer la page où figurent les justificatifs nécessaires jusqu'à la question 3.5).*

☐ *indépendante?*

☐ *intégrée dans une autre stratégie nationale de plus grande portée?*

Veuillez indiquer la ou les page(s):

3.3 A quel secteur s'applique-t-elle?

Explication: *La stratégie définit les rôles et les responsabilités en matière de cybersécurité des acteurs du secteur public ou du secteur privé.*

☐ *secteur privé?*

☐ *secteur public?*

Veuillez indiquer la ou les page(s):

3.4 Comporte-t-elle une partie consacrée à:

Explication: *La stratégie comprend des mesures relatives à la protection des infrastructures informatiques essentielles.*

Explication: *Un plan national de résilience permet au pays de se rétablir rapidement et efficacement des conséquences d'une catastrophe (naturelle ou anthropique), notamment grâce à la préservation et à la restauration de ses structures et fonctions de base fondamentales.*

☐ la protection des infrastructures informatiques essentielles?

☐ un plan national de résilience?

Veuillez indiquer la ou les page(s):

3.5 Existe-t-il un plan d'action bien défini concernant la mise en oeuvre par le gouvernement d'une gouvernance en matière de cybersécurité?

Explication: *La stratégie comprend une feuille de route/stratégie prévoyant les étapes de mise en oeuvre et de sa finalisation.*

☐ *Oui*

☐ *Non*

Veuillez indiquer la ou les page(s):

3.6 La stratégie est-elle:

☐ *régulièrement révisée?*

☐ *ouverte au grand public pour consultation?*

Explication: *La stratégie est actualisée au regard des évolutions nationales, technologiques, sociales, économiques et politiques susceptibles de l'affecter.*

Explication: *La stratégie peut être consultée par toutes les parties prenantes concernées, y compris les opérateurs d'infrastructures, les PSI, les universitaires, etc.*

Veuillez indiquer la ou les page(s):

Ajouter le lien concernant les consultations ouvertes.

3.7 Existe-t-il un organisme national responsable:

☐ *de la cybersécurité et de la protection des infrastructures informatiques essentielles?*

☐ *des initiatives/des organismes/des points focaux visant à lutter contre les spams?*

Explication: *L'organisme responsable de la mise en oeuvre de la stratégie/politique nationale en matière de cybersécurité peut comprendre des comités permanents, des groupes de travail officiels, des conseils consultatifs et des centres interdisciplinaires.* Cet organisme peut aussi être directement responsable d'un CIRT national. 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 les normes nouvellement élaborées.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.8 Existe-t-il des indicateurs servant à mesurer le développement de la cybersécurité à l'échelle nationale?

Explication: *Existence d'exercices d'évaluation comparative, nationaux ou sectoriels, officiels 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 ISO/IEC 27004, une norme définissant les* mesures relatives à la gestion de la sécurité des informations*.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.9 L'évaluation des risques en matière de cybersécurité est-elle régulière?

Explication: *Un processus méthodique permettant l'identification, l'analyse et l'évaluation des risques.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.10 Existe-t-il un indice de cybersécurité permettant d'évaluer les risques?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.11 Des audits généraux sont-ils effectués dans le domaine de la cybersécurité?

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.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

3.12 Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées concernant les mesures organisationnelles auxquelles votre pays a participé/participe au titre d'activités en matière de cybersécurité?

Ajouter des liens/url

Ajouter des documents

4 Activités de renforcement des capacités

4.1 Des campagnes de sensibilisation à la cybersécurité sont-elles élaborées et mises en oeuvre?

Explication: *La sensibilisation du public comprend les efforts déployés pour promouvoir des campagnes de publicité à grande échelle visant à toucher autant de personnes que possible, mais aussi l'appui des ONG, des institutions, des organisations, des PSI, des bibliothèques, des organisations du commerce locales, des centres communautaires, des revendeurs d'informatique, des collèges, des programmes de formation pour adultes, des écoles et des organisations parents-enseignants, afin de faire passer les messages relatifs à un comportement sûr en ligne. Il peut s'agir de la création de portails et de sites Internet de sensibilisation, de la distribution de matériel pédagogique et de mesures incitatives en faveur de l'adoption de la cybersécurité.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4.2 Les campagnes de sensibilisation du public ciblent-elles…

☐ *les organisations?*

☐ *la société civile?*

☐ *les adultes?*

☐ *les jeunes et les enfants?*

☐ *d'autres organismes associés?*

Indiquer et numéroter les liens/url correspondant à chaque case cochée.

Indiquer et numéroter les documents correspondant à chaque case cochée.

4.3 Existe-t-il un cadre concernant la certification et l'accréditation des professionnels de la cybersécurité…

Explication: *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 internationales en matière de cybersécurité. Ces certifications, accréditations et normes sont, entre autres, les suivantes: connaissance de la sécurité dans le nuage informatique (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Conseil de l'Europe), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), PRMIA (Professional Risk Managers International Association), PMP (Project Management Institute), etc.*

☐ *dans le secteur public?*

☐ *dans le secteur privé?*

Ajouter des liens/url

Ajouter des documents

4.4 Votre gouvernement/organisation élabore-t-il/elle des séances de formation professionnelle sur la cybersécurité ou encourage-t-il/elle leur tenue…

Explication: *Existence de programmes pédagogiques nationaux ou sectoriels et de formation professionnelle promouvant l'organisation de cours sur la cybersécurité au sein des ressources humaines (dans le domaine technique, des sciences sociales, etc.) et la certification de professionnels dans le secteur public et privé.*

☐ *à l'intention des agents chargés de faire appliquer la loi (agents de police ou agents des forces de l'ordre)?*

☐ *à l'intention du personnel judiciaire ou d'autres acteurs juridiques (juges, avocats, conseillers juridiques, magistrats, auxiliaires juridiques)?*

☐ *à l'intention des organisations?*

☐ *à l'intention du secteur public?*

☐ *à l'intention de la société civile?*

☐ *autres*

Indiquer et numéroter les liens/url correspondant à chaque case cochée.

Indiquer et numéroter les documents correspondant à chaque case cochée.

4.5 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 l'organisation 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.*

L'élaboration de mots de passe efficaces et la non-divulgation d'informations personnelles en ligne sont quelques-unes des compétences en matière de cybersécurité. Les métiers de la cybersécurité sont, entre autres: cryptologue, juriste spécialisé, spécialiste en gestion de crise, architecte de sécurité et expert des tests d'intrusion.

☐ *dans l'enseignement primaire?*

☐ *dans l'enseignement secondaire?*

☐ *dans l'enseignement supérieur?*

☐ *autres*

Indiquer et numéroter les liens/url correspondant à chaque case cochée.

Indiquer et numéroter les documents correspondant à chaque case cochée.

4.6 Investit-on dans les programmes de R&D en matière de cybersécurité:

Explication: *Les programmes de recherche en matière de cybersécurité comportent, entre autres, des analyses de logiciels malveillants et de la vulnérabilité des systèmes, des études cryptographiques, 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 "pots de miel" ("honey-pot") et les modules matériels de sécurité. La présence d'un organisme national de supervision facilitera la coordination entre les institutions ainsi que le partage des ressources.*

☐ *dans le secteur public*

☐ *dans le secteur privé*

☐ *dans les établissements d'enseignement supérieur (établissements universitaires)*

☐ *moyennant un organisme officiel reconnu au niveau national, chargé de superviser les activités de R&D en matière de cybersécurité*

☐ *moyennant un organisme officiellement reconnu chargé de superviser les activités de renforcement des capacités en matière de cybersécurité*

☐ *autres*

Indiquer et numéroter les liens/url correspondant à chaque case cochée.

Indiquer et numéroter les documents correspondant à chaque case cochée.

4.7 L'Etat a-t-il mis en place des mesures incitatives visant à encourager le renforcement des capacités en matière de cybersécurité?

Explication: *Toute mesure incitative à l'initiative du gouvernement visant à encourager le renforcement des capacités en matière de cybersécurité (exonérations fiscales, subventions, financements, prêts, élimination des déchets électroniques et autres incitations d'ordre financier et économique, ou encore organisme institutionnel national consacré à la cybersécurité et chargé de surveiller 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.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4.8 Le secteur de la cybersécurité s'est-il développé à l'échelle locale?

Explication: *Un environnement économique, politique et social favorable au développement de la cybersécurité facilitera la croissance du secteur privé autour de cette activité. Les campagnes de sensibilisation, le développement des compétences des ressources humaines, le renforcement des capacités et les mesures incitatives du gouvernement soutiendront le marché des produits et services liés à la cybersécurité. L'existence d'un secteur d'activité local axé sur la cybersécurité atteste d'un tel environnement et encouragera la croissance du marché de la cyberassurance et de jeunes entreprises spécialisées dans ce domaine.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4.9 Existe-t-il un marché de la cyberassurance?

Explication: *Le terme cyberassurance désigne un produit d'assurance destiné à protéger les entreprises et les individus contre les risques liés à Internet et plus généralement, à l'infrastructure des technologies de l'information et aux activités y afférentes*.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4.10 Un soutien est-il apporté aux jeunes entreprises spécialisées dans le domaine de la cybersécurité et à leur développement?

Explication: *Mécanismes mis en place en vue de soutenir le développement des jeunes entreprises (incitations fiscales, parcs technologiques, zone de libre-échange, etc.) et des petites et moyennes entreprises du secteur de la cybersécurité*.

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

4.11 Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées concernant le renforcement des capacités auxquelles votre pays a participé/participe dans le cadre des activités de cybersécurité?

Ajouter des liens/url

Ajouter des documents

Veuillez énumérer ici les bonnes pratiques si aucun lien ou document n'a été fourni.

5 Mesures de coopération

5.1 Existe-t-il des accords bilatéraux de coopération en matière de cybersécurité avec:

Explication: *Les accords bilatéraux (ou accords entre deux parties) désignent toute forme de partenariat officiel, national ou sectoriel, visant à partager des informations ou des ressources relatives à la cybersécurité avec un autre Etat, une entité régionale ou une organisation internationale (coopération ou échange d'informations, d'expertise, de technologies et d'autres ressources).*

☐ *des Etats ou des Etats Membres?*

☐ *des organisations internationales?*

☐ *autres*

5.2 L'accord ou les accords sont-ils:

☐ *juridiquement contraignants?*

☐ *axés sur le partage d'informations?*

☐ *axés sur le partage de ressources?*

☐ *juridiquement non contraignants (informels)?*

☐ *en attente de ratification?*

5.3 Existe-t-il des accords multilatéraux de coopération en matière de cybersécurité?

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

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

5.4 Les accords sont-ils:

☐ *juridiquement contraignants?*

☐ *axés sur le partage d'informations?*

☐ *axés sur le partage de ressources?*

☐ *juridiquement non contraignants (informels)?*

☐ *en attente de ratification?*

5.5 Votre gouvernement/organisation participe-t-il/elle à des forums/associations internationaux/les ayant trait à la cybersécurité?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

5.6 Existe-t-il des partenariats public-privé avec:

Explication: *On entend par partenariats public-privé les initiatives associant le secteur public et le secteur privé. Les critères de mesure de cet indicateur de performance peuvent être le nombre de partenariats public-privé officiels, nationaux ou sectoriels, favorisant le partage d'informations (renseignements relatifs aux menaces) et de 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.*

☐ *des entreprises locales?*

☐ *des entreprises étrangères?*

5.7 Existe-t-il des partenariats:

Explication: *Cet indicateur de performance désigne toute forme de partenariat existant entre les différentes organisations gouvernementales 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.*

☐ *entre les organisations?*

☐ *au sein d'une organisation?*

Ajouter des liens/url

Ajouter des documents

5.8 Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées dans le domaine de la coopération auxquelles votre pays a participé/participe au titre d'activités en matière de cybersécurité?

Ajouter des liens/url

Ajouter des documents

6 Enquête additionnelle: protection des enfants en ligne

1)

2)

3)

4)

5)

6)

6.1 Existe-t-il des mesures visant la protection en ligne des enfants?

☐ *Oui*

☐ *Non*

6.1.1 Existe-t-il une législation en matière de protection en ligne des enfants?

Explication: *Il s'agit d'un ensemble de lois qui établissent clairement que tout crime commis contre un enfant dans le monde réel peut également,* mutatis mutandis*, être commis sur Internet ou par le truchement de tout autre réseau électronique. Il peut également s'agir de lois interdisant certains types de comportement qui ne peuvent exister que sur Internet, par exemple le fait d'inciter les enfants à distance à participer ou à assister à des jeux 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*

☐ *Partiellement (Uniquement dans le cas de projets de loi avancés et prêts à être adoptés ou vérifiés)*

Ajouter des liens/url

Ajouter des documents

6.2 Existe-t-il une organisation/entité chargée de la protection en ligne des enfants?

Explication: *Existence d'une organisation nationale chargée de la protection en ligne des enfants.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

6.2.1 Existe-t-il un mécanisme public permettant de signaler des cas liés à la protection en ligne des enfants?

Explication: *Numéro de téléphone, adresse électronique et site web au moyen desquels les parties concernées peuvent rendre compte d'incidents ou d'inquiétudes concernant la sécurité en ligne d'un enfant.*

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

6.2.2 Existe-t-il des dispositifs et des fonctionnalités techniques contribuant à la protection en ligne des enfants?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

6.2.3 Existe-t-il des activités, organisées par des organisations gouvernementales ou non, visant à aider et à informer les parties prenantes sur la façon de protéger les enfants en ligne?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

6.2.4 Existe-t-il des programmes de formation sur la protection en ligne des enfants, à l'intention:

☐ *des éducateurs?*

☐ *des parents?*

☐ *des enfants?*

Ajouter des liens/url

Ajouter des documents

6.3 Existe-t-il une stratégie nationale relative à la protection en ligne des enfants?

☐ *Oui*

☐ *Non*

Ajouter des liens/url

Ajouter des documents

6.4 Existe-t-il des campagnes de sensibilisation à la protection en ligne des enfants à l'intention:

☐ *des adultes?*

☐ *des jeunes?*

☐ *des enfants?*

Ajouter des liens/url

Ajouter des documents

7 Addendum: enquête d'opinion

7.1 Quelle importance accordez-vous à la sensibilisation à la cybersécurité, étape fondamentale pour garantir la sécurité dans le cyberespace?

a) Pas d'importance

b) Importance moyenne

c) Importance normale

d) Grande importance

7.2 Quels sont les groupes cibles des campagnes de sensibilisation à la cybersécurité dans votre pays?

a) Enfants
b) Jeunes
c) Etudiants
d) Personnes âgées
e) Personnes handicapées
f) Institutions privées
g) Organismes publics
h) Autres

7.3 Quel est le groupe visé en priorité? Veuillez classer les différents groupes par ordre d'importance décroissant (de 1 à 6)

a) Enfants
b) Jeunes
c) Etudiants
d) Personnes âgées
e) Personnes handicapées
f) Institutions privées
g) Organismes publics
h) Autres

7.4 Sur quels thèmes les campagnes de sensibilisation à la cybersécurité actuelles portent-elles? (Plusieurs choix possibles)

a) Sécurité de l'Internet
b) Confidentialité
c) Fraude
d) Hameçonnage (phishing)
e) Logiciels malveillants
f) Protection en ligne des enfants
g) Autres

7.5 Quel est le niveau d'importance de chaque thème? Veuillez classer les thèmes ci-après par ordre d'importance décroissant et expliquer les raisons de cet ordre

a) Sécurité de l'Internet
b) Confidentialité
c) Fraude
d) Hameçonnage (phishing)
e) Logiciels malveillants
f) Protection en ligne des enfants
g) Autres

7.6 Avez-vous bénéficié de l'assistance ou de la collaboration d'UIT en matière de cybersécurité?

a) Si oui, veuillez préciser. Que pensez-vous de l'efficacité de cette assistance/collaboration? Selon vous, quels domaines spécifiques de la cybersécurité méritent une attention accrue?

b) Si non, veuillez expliquer pourquoi, et comment nous pouvons vous aider?

_____