Présentation du questionnaire relatif à l'Indice de cybersécurité dans le monde (GCI) 2015/16

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 2015/16 et celles requises par la Question 3 de la Commission d'études de l'UIT-D. Il se compose de trois parties distinctes: dans les deux premières, la réponse attendue est "oui" ou "non", tandis que la dernière réponse est libre. 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.

PARTIE 1

1 Existe-t-il une législation relative aux cyberactivités?

1.1 Existe-t-il une loi relative à la lutte contre la cybercriminalité?

Explication: *La législation anti-cybercriminalité désigne les lois concernant l'accès non autorisé, l'atteinte à l'intégrité des données et du système ou l'interception et l'utilisation abusive des systèmes informatiques. Elle comprend le droit procédural et tous les articles en vigueur portant sur la conservation rapide des données informatiques stockées, les ordonnances de production, la collecte de données informatiques en temps réel, l'extradition, l'assistance mutuelle, la confidentialité et les limitations d'utilisation, ainsi que toute jurisprudence en matière de cybercriminalité, d'utilisation abusive d'ordinateurs et d'infractions relatives au contenu. Ces dispositions peuvent relever du droit pénal, de la loi relative à la protection des données, de la loi relative à la liberté d'information ou de la loi relative à la propriété intellectuelle/aux droits d'auteur.*

1.1.1 Existe-t-il une règle juridique de fond en matière de cybercriminalité?

Explication: *Une règle juridique de fond embrasse 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.*

1.1.1.1 Existe-t-il des articles de loi relatifs à l'accès non autorisé aux ordinateurs, aux systèmes et aux données?

Explication: *L'accès non autorisé désigne le fait d'accéder à un ordinateur, à un système ou à des données en utilisant le compte d'une autre personne ou par des moyens détournés (deviner/pirater un mot de passe, usurper une identité, etc.).*

1.1.1.2 Existe-t-il des articles concernant l'atteinte à l'intégrité ou à la modification d'ordinateurs, de systèmes et de données?

Explication: *L'atteinte à l'intégrité/la modification non autorisée désigne toute forme d'intrusion dans un système, un ordinateur ou une base de données, par laquelle des modifications sont apportées à leur configuration initiale; p. ex. introduire, endommager, effacer, détériorer ou altérer de façon générale des données informatiques*.

1.1.1.3 Existe-t-il des articles relatifs à l'interception non autorisée d'ordinateurs, de systèmes et de données?

Explication: *L'interception non autorisée désigne l'acquisition illégale de données informatiques lors de leur transmission privée*.

1.1.2 Existe-t-il des droits procéduraux en matière de cybercriminalité?

Explication: *Les règles définissant la façon dont un tribunal tient ses audiences et détermine le déroulement d'une procédure civile, pénale ou administrative. Ces règles visent à garantir une application juste et cohérente des règles de procédure ou des principes de justice fondamentale applicables dans le cadre de toute affaire portée en justice.*

1.1.2.1 Existe-t-il des articles relatifs à la conservation rapide des données informatiques stockées?

Explication: *La conservation des données est une obligation imposée par l'État à une personne ou à une organisation, par laquelle cette dernière doit protéger un certain type de données contre toute perte ou modification pendant une période déterminée*.

1.1.2.2 Existe-t-il des articles relatifs aux ordonnances de production?

Explication: *Une ordonnance de production est une obligation imposée par l'État à une personne ou à une organisation, par laquelle cette dernière doit communiquer aux forces de l'ordre des données informatiques d'un certain type dans un délai déterminé.*

1.1.2.3 Existe-t-il des articles relatifs à la recherche et à la saisie de données informatiques stockées?

Explication: *La recherche et la saisie de données informatiques désignent des mesures, y compris législatives, habilitant les autorités publiques à rechercher des données informatiques ou un système stockés sur leur territoire, et à y accéder*.

1.1.2.4 Existe-t-il des articles relatifs à la collecte en temps réel de données informatiques?

Explication: *La collecte en temps réel de données désigne des mesures, y compris législatives, autorisant les autorités publiques à collecter ou à enregistrer en temps réel des données de trafic transmises sur leur territoire au moyen d'un système informatique.*

1.1.2.5 Existe-t-il des articles relatifs à l'extradition de personnes s'étant rendues coupables de cybercriminalité?

Explication: *L'extradition est la procédure par laquelle un Etat livre à un autre Etat, qui lui a soumis une requête officielle, une personne accusée ou reconnue coupable d'un acte de cybercriminalité sur le territoire de cet autre Etat.*

1.1.2.6 Existe-t-il des articles relatifs à l'assistance mutuelle?

Explication: *Accord signé entre au moins deux pays visant à recueillir et à échanger des informations en vue de faire respecter le droit public et pénal.*

1.1.2.7 Existe-t-il des articles relatifs à la confidentialité et à la limitation d'utilisation?

Explication: *Une partie est autorisée à utiliser des données à la condition d'adhérer à certaines clauses de confidentialité ou de respecter des modalités spécifiques convenues.*

1.1.3 Existe-t-il une jurisprudence en matière de cybercriminalité ou d'utilisation abusive d'un ordinateur?

Explication: *Les infractions relatives à l'utilisation abusive d'un ordinateur englobent le piratage, l'accès non autorisé à des systèmes informatiques et la propagation délibérée de logiciels malveillants et nuisibles. L'accès non autorisé visant à modifier des ordinateurs comprend l'altération de logiciels et de données, la modification de mots de passe et de paramètres en vue de verrouiller l'accès au système, et le brouillage préjudiciable du système.*

1.2 Existe-t-il une législation ou une réglementation relative à la cybersécurité?

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 mener à bien les dispositions prévues par la loi. On entend donc 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 couvrant: la protection des données, la notification des infractions, les obligations en matière de certification/normalisation et d'audit, la mise en oeuvre des mesures 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 prestataires de services Internet (PSI).*

1.2.1 Existe-t-il une législation ou une réglementation relative à la protection des données?

Explication: *Réglementation se rapportant à la protection des données individuelles, commerciales et gouvernementales contre l'accès, l'altération, la destruction ou l'utilisation non autorisés de données.*

1.2.2 Existe-t-il une législation ou une réglementation relative à la protection des systèmes et réseaux?

Explication: *Cadre juridique destiné à protéger les systèmes et réseaux contre tout brouillage préjudiciable.*

1.2.3 Existe-t-il une législation ou une réglementation relative au signalement des infractions?

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 généralement promulguées en réponse au nombre croissant d'infractions perpétrées*

contre les bases de données de consommateurs, qui contiennent des informations d'identification personnelle.

1.2.3.1 Concernant les données?

Explication: *Lois relatives au signalement des infractions concernant les violations de la protection des données.*

1.2.3.2 Concernant les systèmes et réseaux?

Explication: *Lois relatives au signalement des infractions concernant les violations de la protection des systèmes et réseaux. Ces lois peuvent prévoir une norme en matière de cybersécurité ou d'autres fonctions de base (p. ex., cryptage) visant à protéger les données des consommateurs.*

1.2.4 Existe-t-il une législation ou une réglementation relative à la certification/normalisation en matière de cybersécurité?

Explication: *La réglementation relative à la certification/normalisation en matière de cybersécurité impose aux entités exerçant leurs activités sur le territoire du pays de satisfaire à certaines exigences minimales en la matière. Ces exigences peuvent varier en fonction du secteur d'activité. 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.*

1.2.4.1 A l'intention du secteur public?

Explication: *Une réglementation ayant trait aux mesures obligatoires relatives à la certification/normalisation en matière de cybersécurité imposée aux structures publiques.*

1.2.4.2 A l'intention du secteur privé?

Explication: *Une réglementation ayant trait aux mesures obligatoires relatives à la certification/normalisation en matière de cybersécurité imposée aux structures privées.*

1.2.5 La législation ou la réglementation impose-t-elle la mise en oeuvre d'un cadre de cybersécurité?

Explication: *Un cadre de cybersécurité prévoit, entre autres, des mesures techniques et organisationnelles, telles que les pare-feu, les listes de contrôle d'accès définissant les rôles et les responsabilités en matière de sécurité, l'assurance (individuelle) contre la cybercriminalité.*

1.2.5.1 Au secteur public?

1.2.5.2 Aux opérateurs d'importance vitale?

Explication: *Il s'agit de systèmes dont dépendent la sécurité générale, la sécurité économique et la santé publique d'un pays. Il s'agit, entre autres, des secteurs de la défense nationale, de la banque et de la finance, des télécommunications, du transport, de la santé et de l'énergie.*

1.2.5.3 Au secteur privé?

1.2.6 La législation ou la réglementation impose-t-elle des audits de cybersécurité?

Explication: *Un audit de sécurité est une évaluation méthodique 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.*

1.2.6.1 Au secteur public?

1.2.6.2 Aux opérateurs d'importance vitale?

1.2.6.3 Au secteur privé?

1.2.7 Existe-t-il une législation ou une réglementation qui détaille la protection de la vie privée?

Explication: *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 techniques, technologies et facteurs utilisés pour protéger les données, les préférences et les messages sensibles et privés. La loi sur la protection des données est un exemple de législation de ce type.*

1.2.8 Existe-t-il une législation ou une réglementation relative aux signatures numériques et aux transactions électroniques?

***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 réalisé(e) 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.*

1.2.9 Existe-t-il une législation ou une réglementation relative à la responsabilité des PSI?

***Explication**: PSI responsables de la violation des droits d'auteur résultant d'actes perpétrés par leurs utilisateurs. Les prestataires tenus d'informer la police, le CERT ou tout(e) autre organisme responsable/autorité nationale d'une opération électronique illicite effectuée sur leurs infrastructures, au titre de l'obligation de la surveillance active du réseau.*

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

1.3 Existe-t-il une formation sur la cybersécurité à l'intention des membres des forces de l'ordre ou d'autres acteurs de la scène juridique?

***Explication**: Processus formel visant à former les acteurs juridiques à la sécurité informatique.*

1.3.1 A l'intention des forces de l'ordre (police et autres agents des forces de l'ordre)?

1.3.2 A l'intention des acteurs judiciaires et d'autres acteurs du droit (juges, avocats, assistants juridiques, etc.)?

1.3.3 La formation est-elle régulière?

Explication: *Formation périodique ou régulière*.

2 Disposez-vous de mesures techniques?

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

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. 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.*

2.1.1 Est-elle investie d'un mandat gouvernemental?

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

2.1.2 Le CIRT/CSIRT/CERT réalise-t-il régulièrement des exercices de cybersécurité?

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?*

2.1.3 Le CIRT/CSIRT/CERT est-il affilié au Forum of Incident Response Security Teams (FIRST)?

Explication: *Membre titulaire ou agent de liaison du FIRST.*

2.1.4 Le CIRT/CSIRT/CERT est-il affilié à d'autres équipes d'intervention d'urgence (CERT régional)?

Explication: *Toute forme de relation, officielle ou non, entretenue avec n'importe quel autre CERT, au sein du pays ou non, ou adhésion à un groupe régional de CERT.*

2.2 Existe-t-il un CERT gouvernemental?

Explication: *Un CERT/CIRT/CSIRT gouvernemental est une entité qui intervient en cas d'incident relatif à la sécurité informatique ou à la cybersécurité affectant uniquement les institutions publiques. Outre les services d'intervention, cette entité peut aussi fournir des services de prévention, tels que des analyses de vulnérabilité ou des audits de sécurité. Contrairement au CERT national, qui intervient auprès des secteurs public et privé, le CERT gouvernemental réserve ses services aux composantes du secteur public exclusivement.*

2.3 Existe-t-il des CERT sectoriels?

Explication: *Un CERT/CIRT/CSIRT sectoriel 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 CERT sectoriels sont généralement créés pour des secteurs vitaux, tels que la santé, les services publics, les services d'urgence et la finance. Contrairement au CERT gouvernemental, qui intervient auprès du secteur public, le CERT sectoriel réserve ses services aux composantes d'un seul secteur d'activité.*

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

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.*

2.4.1 Dans le secteur public?

2.4.2 Dans le secteur privé?

2.5 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.*

2.5.1 Dans le secteur public?

2.5.2 Dans le secteur privé?

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

2.7 Existe-t-il des mesures et outils techniques destinés à garantir la cybersécurité, tels que des logiciels antivirus ou antispam, qui soient proposés aux personnes handicapées?

3 Disposez-vous de structures organisationnelles?

3.1 Existe-t-il une stratégie nationale 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.*

3.1.1 Votre stratégie nationale est-elle indépendante?

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.*

3.1.1.1 S'applique-t-elle au secteur privé?

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

3.1.1.2 S'applique-t-elle au secteur public?

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

3.1.1.3 Existe-t-il une partie consacrée à la protection des infrastructures informatiques essentielles?

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

3.1.1.4 Existe-t-il une feuille de route relative à la gouvernance?

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

3.1.1.5 La stratégie est-elle régulièrement révisée?

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

3.1.1.6 La stratégie peut-elle être consultée par le grand public?

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

3.1.1.7 La stratégie contient-elle un plan national de résilience?

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.*

3.1.2 Votre stratégie de cybersécurité fait-elle partie d'une autre stratégie nationale de plus grande portée?

3.1.2.1 Existe-t-il une partie consacrée à la protection des infrastructures informatiques essentielles?

Explication: *Ces infrastructures vitales sont des systèmes dont dépendent la sécurité en général, la sécurité économique et la santé publique d'un pays. Il s'agit, entre autres, des secteurs de la défense nationale, de la banque et de la finance, des télécommunications, du transport, de la santé et de l'énergie.*

3.1.2.2 Existe-t-il une feuille de route relative à la gouvernance en matière de cybersécurité?

3.1.3 Définit-elle les priorités du secteur public?

3.1.4 Si aucune stratégie de cybersécurité n'est en place, y en a-t-il une en cours d'élaboration?

3.1.5 La stratégie, existante ou en cours d'élaboration, prévoit-elle des mesures en faveur des personnes handicapées?

3.2 Existe-t-il un organisme national chargé de la cybersécurité?

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.

3.2.1 Existe-t-il un organisme chargé de la protection des infrastructures informatiques essentielles?

3.2.2 Existe-t-il un organisme national jouant le rôle de pivot pour ce qui est des spams?

3.3 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*.*

3.3.1 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.*

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

3.3.1.2 Les résultats sont-ils associés à une note ou à une estimation à des fins d'amélioration future?

3.3.2 Les audits de cybersécurité sont-ils réguliers?

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.*

3.3.2.1 Sont-ils obligatoires?

Explication: *Imposés par des réglementations internes ou sectorielles, ou par l'adhésion à aux normes de certification ISO270001.*

4 Menez-vous des activités de renforcement des capacités?

4.1 Existe-t-il un organisme de normalisation au sein du pays?

Explication: *La normalisation constitue un bon indicateur du niveau de maturité d'une technologie, et l'apparition de nouvelles normes dans des domaines clés souligne l'importance vitale de ces instruments. Bien que la cybersécurité ait toujours relevé de la sécurité nationale et fasse l'objet d'un traitement différent selon les pays, des normes reconnues par tous facilitent les approches communes. 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. Cet indicateur mesure l'existence d'un organisme national de normalisation en matière de cybersécurité et d'activités relatives à l'élaboration et à la mise en oeuvre de normes en la matière.*

4.1.1 Elabore-t-il ses propres normes en matière de cybersécurité?

Explication: *Les normes en matière de cybersécurité sont des règles techniques, figurant généralement dans des publications, qui visent à protéger le cyberenvironnement d'un utilisateur ou d'une organisation. Cet environnement englobe l'ensemble des utilisateurs, réseaux, dispositifs, logiciels, processus, informations en mémoire ou en cours de transmission, applications, services et systèmes qui peuvent être raccordés directement ou indirectement à des réseaux. Le principal objectif est de réduire les risques, y compris de prévenir ou d'atténuer les attaques contre la cybersécurité. Certains pays adoptent des normes internationales, les adaptent à leur environnement local et les qualifient de normes nationales. D'autres (disposant de solides capacités en matière de recherche et développement [R&D]) créent des normes qui acquièrent une reconnaissance internationale et s'ajoutent aux nouvelles normes universelles.*

4.1.2 Adopte-t-il des normes internationales existantes en matière de cybersécurité?

Explication: *Les normes en matière de cybersécurité sont des règles techniques, figurant généralement dans des publications, qui visent à protéger le cyberenvironnement d'un utilisateur ou d'une organisation. Cet environnement englobe l'ensemble des utilisateurs, réseaux, dispositifs, logiciels, processus, informations en mémoire ou en cours de transmission, applications, services et systèmes qui peuvent être raccordés directement ou indirectement à des réseaux. Le principal objectif est de réduire les risques, y compris de prévenir ou d'atténuer les attaques contre la cybersécurité. Certains pays adoptent des normes internationales, les adaptent à leur environnement local et les qualifient de normes nationales. D'autres (disposant de solides capacités en matière de R&D) créent des normes qui acquièrent une reconnaissance internationale et s'ajoutent aux nouvelles normes universelles.*

4.2 Existe-t-il des bonnes pratiques nationales ou sectorielles en termes de cybersécurité ou

est-il nécessaire d'élaborer des lignes directrices en la matière?

Explication: *Les bonnes pratiques sont des méthodes ou des procédures ayant fait leurs preuves. Les adopter réduit non seulement les risques d'échec, mais permet aussi de gagner en efficacité.*

4.3 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.

4.3.1 Dans le secteur public?

4.3.2 Dans les établissements d'enseignement supérieur?

4.3.3 Existe-t-il un organisme institutionnel national qui supervise les activités de R&D en matière de cybersécurité?

4.4 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.*

4.4.1 A l'intention des organisations?

Explication: *Campagnes de sensibilisation ciblant les organisations.*

4.4.2 A l'intention de la société civile?

Explication: *Campagnes de sensibilisation ciblant le grand public.*

4.4.2.1 A l'intention des adultes (>18 ans)?

4.4.2.2 A l'intention des jeunes (12-17 ans)?

4.4.2.3 A l'intention des enfants (<12 ans)?

4.4.3. Dans le cadre des campagnes de sensibilisation, le public est-il au courant des avantages que procure l'utilisation de solutions en matière de cybersécurité (logicielles, matérielles, axées sur les services)?

4.4.4. Ces solutions (logicielles, matérielles, axées sur les services) sont-elles mises à la disposition du public?

Explication: *Mise à disposition gratuite ou à prix réduit, par exemple, dans le cadre d'une campagne de sensibilisation*.

4.5 Votre organisation/gouvernement élabore ou encourage-t-il/elle l'organisation de séances de formation professionnelle sur la cybersécurité?

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.*

4.5.1 A l'intention des organisations?

4.5.2 A l'intention du secteur public?

4.5.3 A l'intention de la société civile?

4.6 Votre organisation/gouvernement élabore ou encourage-t-il/elle la mise au point de programmes pédagogiques ou universitaires ayant trait à la cybersécurité?

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.*

4.6.1 Dans l'enseignement primaire?

4.6.2 Dans l'enseignement secondaire?

4.6.3 Dans l'enseignement supérieur?

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.*

4.7.1 Existe-t-il un organisme institutionnel national supervisant les activités de renforcement des capacités en matière de cybersécurité?

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.*

4.8.1 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*.

4.8.1.1 Accordez-vous des subventions aux entreprises et autres entités qui ne sont pas en mesure de se procurer une cyberassurance sur un marché libre?

4.8.2 Existe-t-il des mesures incitatives favorisant le développement du secteur de la cybersécurité?

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, élimination des déchets électroniques et autres incitations d'ordre économique et financier, 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.*

4.8.2.1 Un soutien est-il apporté aux jeunes entreprises spécialisées dans le domaine de la cybersécurité?

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.*

5 Existe-t-il des mesures de coopération?

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

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 État, une entité régionale ou une organisation internationale (coopération ou échange d'informations, d'expertise, de technologies et d'autres ressources).*

5.1.1 Avec des Etats?

5.1.1.1 L'accord est-il juridiquement contraignant

Explication: *Expression juridique courante indiquant que, un accord ayant été conclu intentionnellement, certaines actions sont désormais requises ou interdites par la loi*.

5.1.1.1.1 Pour le partage d'informations?

Explication: *Le partage d'informations désigne la mise en commun de renseignements relatifs aux menaces.*

5.1.1.1.2 Pour le partage de ressources?

Explication: *Le partage de ressources désigne le partage de personnel (détachement, affectation ou autre mission temporaire confiée aux employés), de locaux, d'équipements, et d'autres outils et services.*

5.1.1.2 L'accord est-il juridiquement non contraignant, informel ou en attente de ratification?

5.1.1.2.1 Pour le partage d'informations?

5.1.1.2.2 Pour le partage de ressources?

Explication: *Il peut s'agir de ressources humaines, de locaux, d'équipements, etc*.

5.1.2 Avec des organisations internationales?

5.1.2.1 L'accord est-il juridiquement contraignant?

5.1.2.1.1 Pour le partage d'informations?

5.1.2.1.2 Pour le partage de ressources?

Explication: *Il peut s'agir de ressources humaines, de locaux, d'équipements, etc*.

5.1.2.2 L'accord est-il juridiquement non contraignant, informel ou en attente de ratification?

5.1.2.2.1 Pour le partage d'informations?

5.1.2.2.2 Pour le partage de ressources?

Explication: *Il peut s'agir de ressources humaines, de locaux, d'équipements, etc*.

5.2 Existe-t-il des accords multilatéraux ou internationaux 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 États 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.*

5.2.1 L'accord est-il juridiquement contraignant?

5.2.1.1 Pour le partage d'informations?

5.2.1.2 Pour le partage de ressources?

Explication: *Il peut s'agir de ressources humaines, de locaux, d'équipements, etc*.

5.2.2 L'accord est-il juridiquement non contraignant, informel ou en attente de ratification?

5.2.2.1 Pour le partage d'informations?

5.2.2.2 Pour le partage de ressources?

Explication: *Il peut s'agir de ressources humaines, de locaux, d'équipements, etc*.

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

5.4 Existe-t-il des partenariats public-privé?

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.*

5.4.1 Avec des entreprises locales?

5.4.1.1 Pour le partage d'informations?

5.4.1.2 Pour le partage de ressources?

5.4.2 Avec des entreprises étrangères?

5.4.2.1 Pour le partage d'informations?

5.4.2.2 Pour le partage de ressources?

Explication: *Il peut s'agir de ressources humaines, de locaux, d'équipements*.

5.5 Existe-t-il des partenariats interorganisations?

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.*

5.5.1 Pour le partage d'informations?

5.5.2 Pour le partage de ressources?

Explication: *Il peut s'agir de ressources humaines, de locaux, d'équipements.*

PARTIE 2

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

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

Explication: *Il est généralement nécessaire de mettre en place 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 être également nécessaire de promulguer de nouvelles lois ou d'adapter les lois existantes afin d'interdire 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).*

1.2 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.*

1.2.1 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.*

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

1.2.3 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?

1.2.4 Existe-t-il des programmes de formation sur la protection en ligne des enfants?

1.2.4.1 A l'intention des éducateurs?

1.2.4.2 A l'intention des parents?

1.2.4.3 A l'intention des enfants?

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

1.4 Existe-t-il des campagnes de sensibilisation à la protection en ligne des enfants?

1.4.1.1 A l'intention des adultes (>18 ans)?

1.4.1.2 A l'intention des jeunes (12-17 ans)?

1.4.1.3 A l'intention des enfants (<12 ans)?

PARTIE 3

Addendum: enquête d'opinion

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

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

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

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

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

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?

_____