ANNEXE 1

Mandat

Programme de cybersécurité UIT/BDT

Groupe d'experts chargé de la pondération de l'indice GCI

Mandat

Août 2020

L'Indice GCI

Publié pour la première fois en 2015, l'Indice mondial de cybersécurité (GCI) a pour but d'aider les pays à recenser les domaines dans lesquels des améliorations pourraient être apportées en matière de cybersécurité, de les inciter à agir pour améliorer leur classement à cet égard et d'augmenter par là même le niveau de cybersécurité dans le monde. Grâce aux données recueillies, l'indice GCI permet de mettre en avant des pratiques que les États Membres peuvent mettre en œuvre en fonction de leur contexte national, d'encourager l'adoption de bonnes pratiques et de favoriser une culture mondiale de la cybersécurité.

Le champ d'application et le cadre de l'indice GCI sont définis dans la Résolution 130 (Rév. Dubaï, 2018), de la Conférence de plénipotentiaires de l'UIT, qui porte sur le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication. Le questionnaire du GCI, à partir duquel sont définis des indicateurs, des sous-indicateurs et des micro-indicateurs, est créé et approuvé dans le cadre d'une consultation menée au titre de la Question 3 de la Commission d'études 2: Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité parmi les membres de l'UIT.

Groupe d'experts chargé de la pondération de l'indice GCI

Le Groupe d'experts a pour mission de déterminer la pondération des indicateurs, des sous-indicateurs et des micro- indicateurs de l'indice GCI et de proposer des modifications à apporter au Questionnaire sur l'indice GCI dans l'optique des itérations futures.

Les membres du Groupe d'experts sur l'indice GCI sont nommés en vue de formuler des recommandations détaillées et impartiales pour la distribution de points dans le cadre du modèle GCI. Les recommandations du Groupe d'experts concernant le poids des indicateurs et des sous-indicateurs devraient faire ressortir l'importance d'un indicateur donné pour l'engagement général pris par un État membre en matière de cybersécurité. Les activités concrètes du groupe d'experts sont les suivantes:

- fournir des contributions sur le calcul de l'indice principal et des sous-indices, qui est traité dans l'Annexe B du présent document; et,
- fournir des contributions sur les futures itérations éventuelles de l'indice GCI.

Dans des cas exceptionnels, et avec l'accord de la majorité, l'examen des questions pourra être recommandé par le Groupe d'experts en vue de la prochaine itération de l'indice GCI.

L'UIT assurera les fonctions de secrétariat du Groupe d'experts. Le Groupe d'experts est ouvert à la participation des États Membres et des Membres des Secteurs de l'UIT, en plus des experts ayant participé aux itérations antérieures de l'indice GCI.

La composition du groupe d'experts devrait tenir compte de la diversité régionale, de la diversité des genres, de la diversité des compétences ainsi que de l'équilibre entre les différentes parties prenantes, y compris les gouvernements, le secteur privé et les milieux universitaires.

Processus de pondération

Le processus d'évaluation global se déroule selon les étapes suivantes:

1) L'UIT fournira à chaque membre du Groupe d'experts toutes les données pertinentes, et plus particulièrement:
   a) le tableur des coefficients de pondération, assorti des questions concernant l'Indice GCI;
   b) le mandat, assorti d'un guide pratique et d'explications sur les indicateurs (présent document).
2) Une réunion du Groupe d'experts sur l'indice GCI se tiendra le **15 octobre 2020** afin d'examiner le processus et de répondre aux questions.
3) À l'issue de la première réunion, les membres du Groupe d'experts rempliront de manière indépendante le tableur Excel des coefficients de pondération, en indiquant leur recommandation relative à la pondération pour chaque indicateur, sous-indicateur et micro-indicateur, et le soumettront à l'adresse gci@itu.int avant le **31 octobre 2020.**

4) Une fois que toutes les recommandations auront été soumises par les différents membres du Groupe d'experts, il sera établi une moyenne des recommandations relatives à la pondération et ces recommandations seront regroupées dans un seul et même tableur des coefficients de pondération.

5) La moyenne des recommandations relatives à la pondération sera communiquée aux membres du Groupe d'experts.

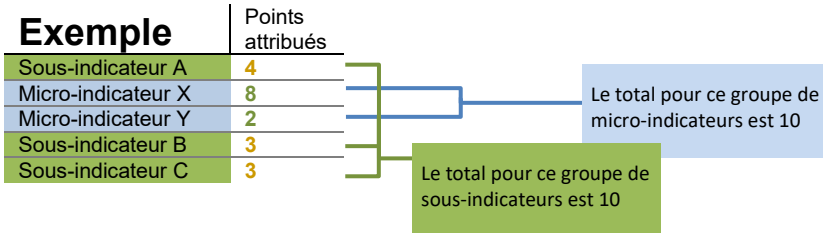
ANNEXE A

Comment attribuer les coefficients de pondération

Vous ne devez examiner les coefficients de pondération que pour les piliers relevant de votre domaine de compétence. Les coefficients de pondération attribués aux piliers pour lesquels vous avez indiqué que vous ne possédiez pas de compétences spécialisées ne seront pas pris en considération

L'Indice GCI repose sur un modèle hiérarchique imbriqué. Chaque "branche" du modèle sera désignée dans le présent document par le terme "groupe", par exemple un groupe d'indicateurs, un groupe de sous-indicateurs et un groupe de micro-indicateurs.

Dans chaque groupe, vous pouvez attribuer 10 points. Vous devez attribuer davantage de points aux indicateurs/sous-indicateurs/micro-indicateurs qui revêtent plus d'importance, en fonction de votre domaine de compétence.

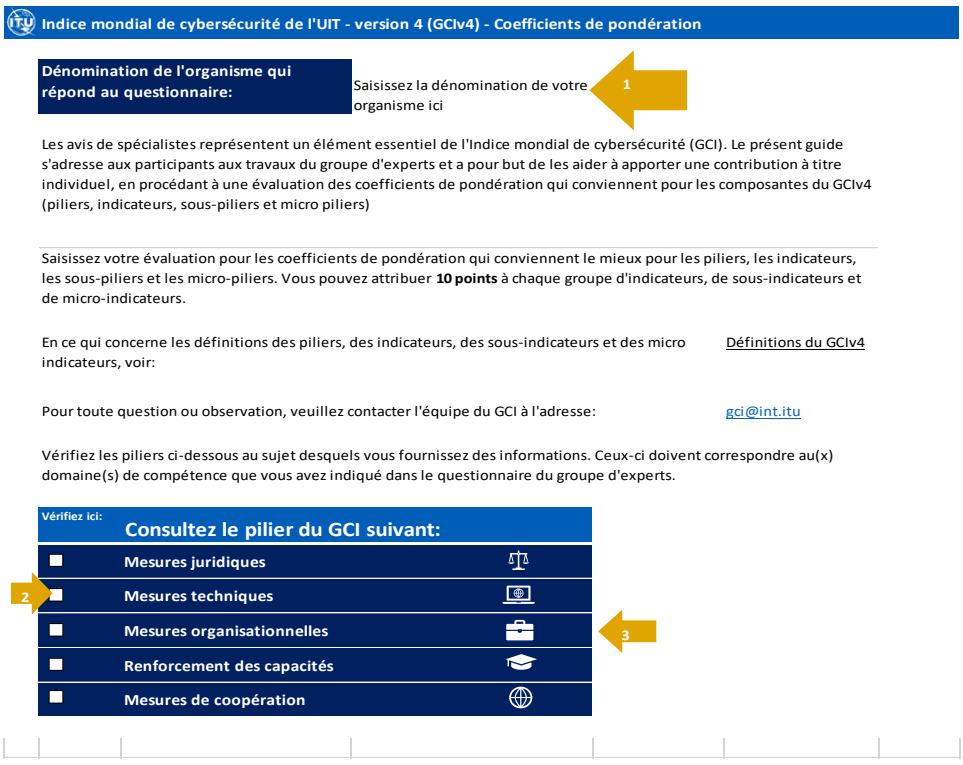


Comment utiliser le tableur des coefficients de pondération

Les présentes instructions concernent le tableur *GCI-Questionnaire-weightage-calculation.xlsx*.

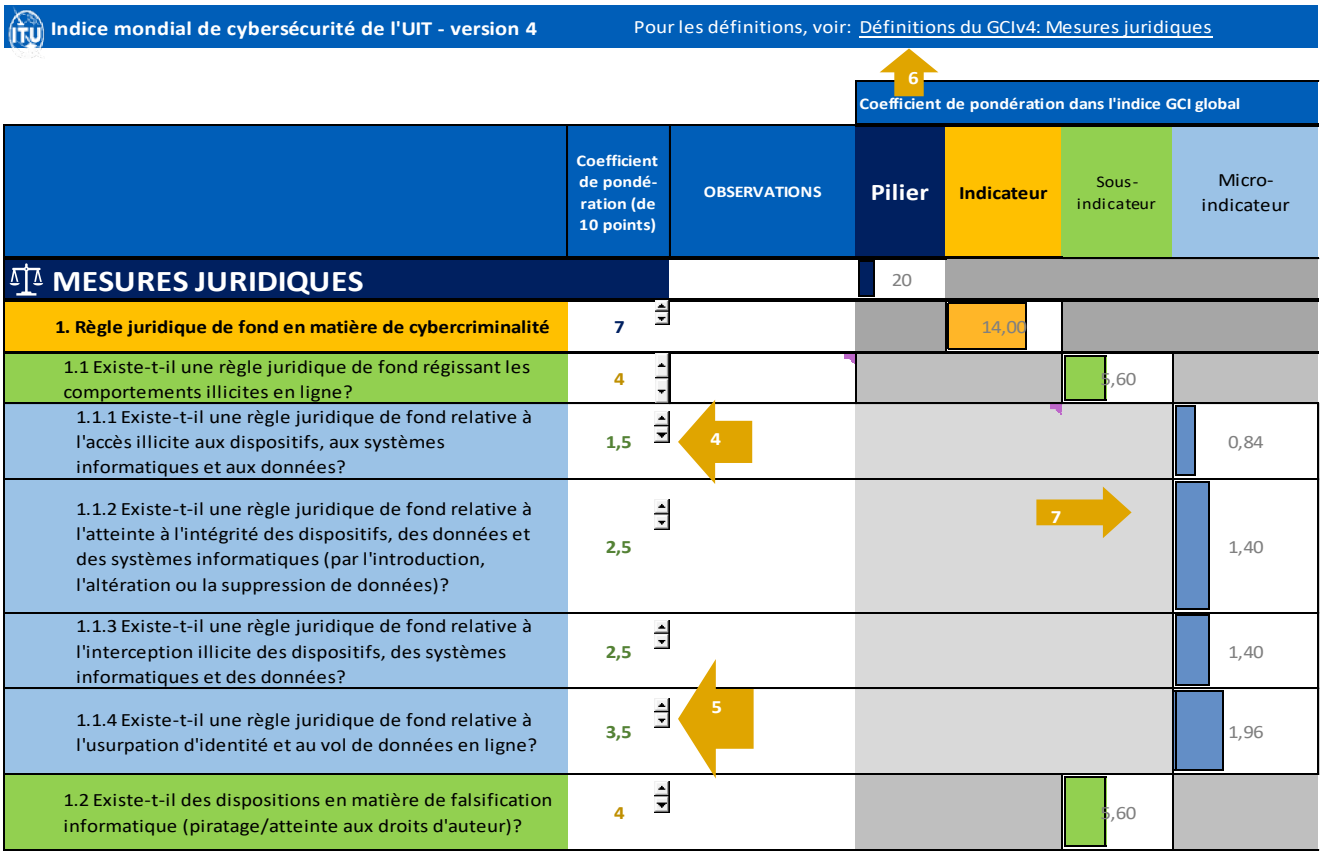
Ce fichier est destiné à être utilisé au format Microsoft Excel. Il se peut que certaines fonctions ne puissent pas être utilisées avec d'autres programmes.

Pour commencer



1) Saisissez votre nom.
2) Vérifier les piliers pour lesquels vous évaluez les coefficients de pondération. Ceux-ci devraient correspondre au domaine de compétence que vous avez indiqué.
3) Vous pouvez cliquer sur le nom ou l'icône correspondant à chaque pilier, afin de naviguer vers le pilier pour lequel vous apportez des éléments d'information.

Insérer les coefficients de pondération



4) Modifiez le coefficient de pondération d'un indicateur, d'un sous-indicateur ou d'un micro-indicateur en tapant le nombre indiqué dans la cellule ou en utilisant les boutons de défilement pour augmenter ou réduire le nombre.
   a) Vous disposez de 10 points à attribuer dans un même groupe. Si vous dépassez ce nombre ou attribuez un nombre moins élevé, toutes les cellules d'un groupe deviendront rouges, comme indiqué ci-dessous:

   b) Les flèches de défilement vers le haut et vers le bas transformeront le nombre en nombre entier.
   c) Pour saisir des fractions, faites précéder le nombre du signe =. Par exemple, =1/3 pour ⅓.
   d) Si vous ne souhaitez pas attribuer la totalité des 10 points, ou si vous souhaitez attribuer un nombre plus élevé, veuillez en faire mention dans les observations. Votre pondération sera rééquilibrée sur 10 pour les réponses des experts dont la moyenne arithmétique est calculée.
5) Vous pouvez formuler des observations sur la pondération de l'indicateur, du sous-indicateur ou du micro-indicateur dans la colonne Observations.
6) Vous pouvez cliquer sur le lien *GCIv4 Definitions* pour mieux comprendre ce que l'on entend par indicateur.

7) La section "coefficient de pondération dans l'indice GCI global" indique quel sera le coefficient de pondération de cet indicateur, en fonction de votre notation, dans l'indice GCI final. Vous ne pouvez ni modifier ni changer ces cellules.

Pour finir

1) Une fois que vous avez terminé, cliquez sur "Sauvegarder" (pour en savoir plus sur la manière de procéder, voir les instructions du service d'assistance de Microsoft), en ajoutant votre nom à la fin. Ex. *GCI-Questionnaire-weightage-calculations-**NAME**.xlsx*

2) Insérez votre tableur en pièce jointe d'un courrier électronique, que vous enverrez à l'adresse gci@itu.int avant la date fixée.

ANNEXE B

Définition des piliers et des indicateurs

Cadre juridique

La législation constitue une mesure cruciale pour fournir un cadre harmonisé permettant aux différentes entités de s'appuyer sur des bases législatives et réglementaires communes, qu'il s'agisse de l'interdiction de certains actes délictueux ou d'obligations réglementaires minimales.

Les critères de mesure du cadre juridique peuvent être l'existence d'institutions et de cadres juridiques relatifs à la cybersécurité et à la cybercriminalité. Le cadre juridique comprend les indicateurs de performance suivants:

- **Règle juridique de fond en matière de cybercriminalité**

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 et les comportements.

- **Réglementation relative à la cybersécurité**

Une réglementation est une règle qui se fonde sur un texte de loi spécifique et qui vise à l'appliquer.

Mesures techniques

S'ils ne prennent pas des mesures techniques adaptées et ne se dotent pas de capacités permettant de détecter des incidents et d'y réagir, les États Membres et les entités qui leur sont rattachées resteront vulnérables aux cyberrisques, qui sont de nature à compromettre les avantages découlant de l'adoption des technologies numériques de l'information.

En conséquence, les États Membres doivent être à même de concevoir des stratégies visant à mettre en place des critères de sécurité et des mécanismes d'accréditation minimaux acceptés pour les applications et les systèmes logiciels... Les critères d'évaluation des mesures techniques peuvent être l'existence d'institutions et de cadres techniques traitant de la cybersécurité, approuvés ou créés par l'État Membre. Le sous-groupe comprend les indicateurs de performance suivants:

- **Équipes d'intervention nationales/gouvernementales en cas d'incident**

Les équipes d'intervention en cas d'incident informatique, également appelées équipes CIRT/CSIRT/CERT, sont des entités organisationnelles qui ont pour mission de coordonner et d'appuyer les interventions en cas d'évènements ou d'incidents en matière de sécurité informatique au niveau national.

- **Équipes CIRT/CSIRT/CERT sectorielles**

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 donné. Les équipes CERT sectorielles sont généralement créées pour des secteurs aussi essentiels que les soins de santé, les services d'utilité publique, les services d'urgence et le secteur financier.

- **Cadre national pour la mise en œuvre des normes en matière de cybersécurité**

Il est indispensable d'adopter un ou plusieurs cadres nationaux pour la mise en œuvre de 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, sans toutefois s'y limiter, 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.

- **Protection en ligne des enfants (COP)**

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 d'autres mécanismes et fonctionnalités techniques mis en place pour contribuer à la protection en ligne des enfants.

Structures organisationnelles

La mise en œuvre d'une initiative nationale, quelle qu'elle soit, appelle des mesures sur le plan de l'organisation et des procédures. L'État Membre doit fixer un objectif stratégique général, assorti d'un plan détaillé sur la mise en œuvre, l'exécution et la mesure. Des structures telles que des organismes nationaux doivent être constituées pour appliquer la stratégie et évaluer la réussite ou l'échec du plan. Les critères de mesure des structures organisationnelles sont l'existence et le nombre d'institutions et de stratégies axées sur l'organisation du développement de la cybersécurité au niveau national. Le sous-groupe comprend les indicateurs de performance suivants:

- **Stratégie/politique nationale en matière de cybersécurité**

L'élaboration d'une politique visant à promouvoir la cybersécurité devrait figurer parmi les toutes premières priorités 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 Membre; prévenir les cyberattaques contre les infrastructures essentielles et lutter contre ces cyberattaques; et limiter au maximum les dommages dus aux cyberattaques et raccourcir les délais nécessaires pour le rétablissement.

- **Organisme responsable**

L'organisme responsable de la mise en œuvre 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.

- **Indicateurs relatifs à la cybersécurité**

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. On citera par exemple les exercices basés sur la norme ISO/CEI 27004, qui définit les mesures relatives à la gestion de la sécurité de l'information.

Mesures relatives au renforcement des capacités

Le renforcement des capacités est intrinsèque aux trois premières catégories de mesures (juridiques, techniques et organisationnelles). Comprendre la technologie, le risque et les conséquences peut faciliter l'élaboration d'une législation ainsi que de politiques et de stratégies mieux conçues ainsi qu'une meilleure distribution des divers rôles et responsabilités. Ce domaine d'études est abordé le plus souvent sous l'angle de la technologie. Pourtant, il présente de nombreuses implications socio-économiques et politiques.

Un cadre de renforcement des capacités visant à promouvoir la cybersécurité devrait inclure la sensibilisation et la disponibilité des ressources. Le sous-groupe comprend les indicateurs de performance suivants:

- **Campagnes de sensibilisation du public à la cybersécurité**

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 associations professionnelles 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.

- **Formation à l'intention des professionnels de la cybersécurité**

Existence de programmes de formation professionnelle sectoriels visant à sensibiliser le grand public (journée, semaine ou mois de sensibilisation à la cybersécurité au niveau national, 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 de professionnels dans le secteur public ou privé.

Cet indicateur tient également compte de l'existence d'un ou plusieurs cadres approuvés (ou entérinés) 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, sans toutefois s'y limiter, les suivantes: Connaissance de la sécurité dans le nuage informatique (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK et Cybersecurity Forensic Analyst (ISC²).

- **Programmes d'études nationaux et programmes universitaires**

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

- **Programmes de recherche-développement en matière de cybersécurité**

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 reconnu au niveau national et chargé de superviser le programme.

- **Secteur de la cybersécurité à l'échelle nationale**

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'œuvre, 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 start-up dans le domaine de la cybersécurité et de marchés de la cyberassurance associés.

- **Mécanismes incitatifs**

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, prêts, mise à disposition d'infrastructures et autres incitations d'ordre économique et financier, ou encore organisme institutionnel spécialisé, reconnu au niveau national et chargé de superviser les activités de renforcement des capacités dans ce domaine).

Mesures relatives à la coopération

Étant donné que la cybersécurité nécessite des informations émanant de tous les secteurs et de toutes les disciplines, elle doit faire l'objet d'une approche multipartite. Parce qu'elle renforce le dialogue et la coordination, la coopération permet d'élargir le champ d'application de la cybersécurité. Le partage d'informations, déjà difficile entre différentes disciplines et entre opérateurs du secteur privé, l'est encore plus au niveau international. Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

- **Accords bilatéraux**

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, de compétences spécialisées, de technologies et d'autres ressources).

- **Participation à des mécanismes internationaux (forums)**

Il peut s'agir de 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.

- **Accords multilatéraux**

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, de compétences spécialisées, de technologies et d'autres ressources).

- **Partenariats secteur public- secteur privé**

On entend par partenariats secteur public- secteur 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, de compétences spécialisées, de technologie et/ou de ressources), qu'ils soient nationaux ou internationaux.

- **Partenariats interorganismes**

Cet indicateur de performance désigne toute forme de partenariat officiel entre les différents organismes publics d'un État Membre (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.

_____