Programme de cybersécurité UIT-D

Indice mondial de cybersécurité – cinquième édition

Modèle de référence (méthodologie)

TABLE DES MATIÈRES

Histoire et contexte

Publié pour la première fois en 2015, l'Indice mondial de cybersécurité (GCI) a pour but d'aider les pays à se mobiliser davantage en faveur de la cybersécurité en mettant en évidence les domaines de la cybersécurité dans lesquels ils obtiennent de bons résultats et ceux dans lesquels des améliorations pourraient être apportées, et en attirant l'attention sur les bonnes pratiques. Grâce aux données recueillies, l'Indice GCI permet de mettre en avant des activités que les États Membres peuvent mener 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), qui a été adoptée par la Conférence de plénipotentiaires de l'Union internationale des télécommunications (UIT) et 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. Dans cette résolution, les États Membres sont invités "*à appuyer les initiatives de l'UIT en matière de cybersécurité, y compris l'Indice mondial de cybersécurité (GCI), afin de promouvoir les stratégies gouvernementales et de diffuser des informations concernant les mesures prises dans l'ensemble des entreprises et des secteurs*". À terme, le but est d'encourager une culture mondiale de la cybersécurité et de l'intégrer au cœur des technologies de l'information et de la communication.

Les éditions de l'Indice mondial de cybersécurité (GCI) seront conformes aux recommandations de l'UIT-D formulées dans la Résolution 45 (Rév. Kigali, 2022), qui contient une description claire des travaux menés au titre de l'Indice GCI et recommande au BDT "d'examiner les résultats des travaux relatifs à l'Indice mondial de cybersécurité (GCI), pour fournir des orientations au BDT concernant les initiatives relatives à la cybersécurité, en tenant compte notamment des lacunes recensées dans le cadre du processus lié à l'Indice GCI".

Précisions sur les éditions précédentes:

Édition (nom)	GCIv1	GCIv2	GCIv3	GCI 2020 (GCIv4)
Édition (numéro)	1	2	3	4
Pays participant	105 pays	136 pays	155 pays	169 pays
Année de collecte de données	2013-2014	2016	2017-2018	2020
Année de publication	2015	2017	2019	2021
Notes	En partenariat avec ABI Research			

Le questionnaire sur le GCI, y compris ses indicateurs, sous-indicateurs et micro-indicateurs, est mis à jour entre deux éditions au titre de la Question de la Commission d'études de l'UIT-D intitulée "*Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité parmi les membres de l'UIT*".

Compte tenu de l'intérêt que les États Membres continuent de manifester pour l'Indice GCI, l'UIT établit actuellement une cinquième édition (GCIv5) en concertation avec le Groupe d'experts sur l'Indice GCI, ainsi qu'il est recommandé dans la Résolution 45 (Rév. Kigali, 2022).

Champ d'application

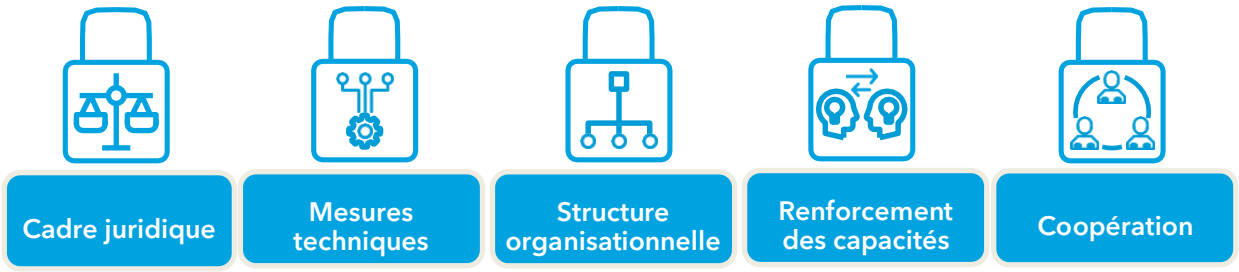
L'Indice mondial de cybersécurité (GCI) est un indice composite qui associe différents indicateurs relatifs à la cybersécurité pour permettre des mesures. Il est fondé sur les cinq piliers du Programme mondial cybersécurité. Les domaines d'activité du Programme mondial constituent les cinq piliers du GCI, dont les principaux objectifs sont de mesurer:

- les types d'engagements, les niveaux d'engagement et l'évolution dans le temps des engagements des pays en matière de cybersécurité;
- les progrès accomplis sur le plan des engagements pour la cybersécurité selon une perspective mondiale;
- les progrès accomplis sur le plan des engagements pour la cybersécurité selon une perspective régionale;
- la différence marquée entre les engagements en faveur de la cybersécurité: la différence entre les niveaux de participation des pays aux initiatives de cybersécurité.

L'Indice mondial de cybersécurité, qui a pour but d'aider les pays à repérer les domaines dans lesquels des améliorations pourraient être apportées en matière de cybersécurité, permet à ce titre d'améliorer le niveau général de la cybersécurité dans le monde. Il permet aussi de recueillir les bonnes pratiques, que les pays peuvent utiliser pour améliorer leurs propres pratiques en matière de cybersécurité et harmoniser davantage leurs méthodes.

Cadre conceptuel

L'Indice mondial de cybersécurité est axé sur les cinq piliers ci-après, qui représentent les grands domaines de l'engagement des pays en faveur de la cybersécurité:



Mesures juridiques: les outils législatifs, tels que les lois, les règlements et les politiques, définissent les droits, responsabilités et protections prévus sur des questions essentielles du point de vue de la cybersécurité, telles que l'interdiction de certains comportements sanctionnés par la loi ou les conditions réglementaires minimales.

Mesures techniques: s'ils ne prennent pas des mesures techniques adaptées et ne se dotent pas de capacités leur permettant de détecter des incidents et d'y réagir, les États Membres et les entités qui leur sont rattachées resteront vulnérables face aux cyberrisques, qui peuvent compromettre les avantages découlant de l'adoption des technologies numériques de l'information. En conséquence, les États Membres doivent avoir les capacités de concevoir des stratégies visant la mise 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.

Mesures organisationnelles: la mise en œuvre d'une initiative nationale appelle des mesures organisationnelles. 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.

Mesures relatives au renforcement des capacités: le renforcement des capacités est intrinsèque aux 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'activité englobe le renforcement des connaissances et des compétences de l'ensemble de la population, des professionnels dont le travail est lié à la cybersécurité et des spécialistes du secteur.

Mesures relatives à la coopération: les mesures de cybersécurité sont plus efficaces lorsqu'elles sont fondées sur des informations émanant de tous les secteurs et de toutes les disciplines, et doivent faire l'objet d'une approche globale et multipartite. Parce qu'elle renforce le dialogue et la coordination, la coopération permet d'élargir le champ d'application de la cybersécurité. Des activités telles que des initiatives conjointes, le partage d'informations, des formations et d'autres activités qui créent des liens entre les professionnels, les fonctionnaires et d'autres intervenants cherchant à améliorer la cybersécurité peuvent faire partie de ce domaine d'activité.

Méthode de calcul

La cinquième édition du questionnaire sur le GCI est organisée autour de cinq piliers: les mesures juridiques, les mesures techniques, les mesures organisationnelles, les mesures de développement des capacités et les mesures relatives à la coopération. Ces piliers comprennent au total 20 indicateurs, 64 sous-indicateurs et 28 micro-indicateurs, examinés dans 83 questions. Les questions visent à obtenir une granularité exploitable des informations relatives aux engagements en matière de cybersécurité tout en conservant une vision globale. Les indicateurs se trouvent dans le questionnaire sur le GCI (Annexe A).

Le choix des indicateurs dépend des critères ci-après:

- pertinence par rapport aux piliers du Programme mondial cybersécurité;
- pertinence par rapport au champ d'application et au cadre conceptuel de l'Indice mondial de cybersécurité;
- capacité des États Membres à répondre avec précision aux questions;
- possibilité de réaliser une vérification croisée au moyen de données secondaires.

La présente édition utilise des réponses ternaires (oui, partiellement, non) pour éliminer toute évaluation fondée sur des opinions et toute partialité potentielle en faveur de certains types de réponses. En outre, un système ternaire simple permet une évaluation plus rapide et plus complexe car il n'appelle pas de longues réponses, ce qui accélère et rationalise la fourniture de réponses et leur évaluations ultérieure. Le répondant ne devrait confirmer que la présence ou l'absence de solutions spécifiques de cybersécurité prédéfinies.

Pour garantir l'exactitude des réponses, il sera demandé aux pays de confirmer leur réponse en utilisant la fonction de téléchargement de documents justificatifs et d'URL. Une rubrique "commentaires" sera ajoutée à chaque pilier pour permettre aux pays de décrire des bonnes pratiques illustrant les effets de leur évolution dans le domaine de la cybersécurité.

Dans la présente cinquième édition et dans toutes les éditions suivantes de l'Indice GCI, les résultats de l'Indice GCI seront organisés en niveaux d'engagement, conformément à la Résolution 45 adoptée à la Conférence mondiale de développement des télécommunications tenue à Kigali (Rwanda) en 2022, dans laquelle les États Membres ont recommandé que les pays soient représentés par niveaux, plutôt que selon un classement individuel, afin de rendre compte plus précisément des points forts et des améliorations à apporter dans chaque pays. Le Groupe d'expert chargé de la méthodologie sera donc prié de recommander un classement par niveau adéquat dans le cadre de ses réunions.

Étapes du processus d'évaluation global selon l'Indice GCI

1) Le questionnaire relatif au GCI est modifié en tenant compte des observations communiquées par les États Membres et le Groupe d'experts sur l'Indice GCI. Le questionnaire est soumis à la réunion de la Commission d'études 2 afin que celle-ci l'examine plus avant.
2) Conformément à la Résolution 45 (Rév. Kigali, 2022), un "Groupe d'experts sur l'Indice GCI" continuera de fournir des conseils sur l'Indice mondial de cybersécurité et, en particulier, la méthodologie, la structure, les questions et la pondération.
3) Un groupe de travail par correspondance relevant du Groupe d'experts sur l'Indice GCI est créé et composé d'experts, ainsi que de représentants des États Membres le souhaitant, afin de formuler des recommandations et des observations sur le questionnaire.
4) Le secrétariat du BDT apporte les modifications voulues en s'appuyant sur les résultats des consultations avec le Groupe de travail par correspondance avant que la direction du BDT approuve le questionnaire, ou soumet une partie ou l'ensemble du questionnaire au Groupe de travail par correspondance pour qu'il continue de formuler des observations.
5) Le questionnaire approuvé est envoyé à la traduction pour qu'il soit traduit dans les six (6) langues officielles de l'ONU.
6) Deux autres réunions du Groupe d'experts sur l'Indice GCI sont organisées pour mener des consultations sur le classement par niveau et la répartition pondérée.
7) La Directrice du BDT envoie à tous les États Membres de l'UIT et à l'État de Palestine une lettre les invitant à participer à l'enquête sur l'Indice GCI. Dans cette lettre, elle leur communique des informations sur l'Indice GCI et les prie de désigner un coordonnateur qui sera chargé de collecter toutes les données pertinentes sur le pays et de remplir le questionnaire relatif au GCI.
8) Les coordonnateurs désignés sont officiellement invités à répondre au questionnaire en passant par un portail en ligne.
9) Le secrétariat du BDT collecte des données secondaires pour les pays qui répondent au questionnaire et, pour ce faire, accomplit notamment les tâches suivantes:
    - recenser toutes les réponses, pièces justificatives, liens et autres éléments manquants;
    - demander au coordonnateur d'apporter des précisions chaque fois que nécessaire;

- envoyer le projet de questionnaire corrigé à chaque coordonnateur pour approbation définitive;
- utiliser le questionnaire validé pour en analyser les réponses et établir la notation et le classement.

10) Le secrétariat du BDT collecte des données primaires pour les pays qui ne répondent pas au questionnaire et, pour ce faire, accomplit notamment les tâches suivantes:

- faire rédiger par l'UIT la première réponse au questionnaire en s'appuyant sur des données accessibles au public et en menant des recherches en ligne;
- envoyer le projet de questionnaire aux coordonnateurs pour examen;
- demander aux coordonnateurs d'apporter des précisions et de renvoyer le projet de questionnaire;
- envoyer le projet de questionnaire corrigé à chaque coordonnateur pour approbation finale;
- utiliser le questionnaire validé pour en analyser les réponses et établir la notation et le classement.

11) Un rapport contenant des résumés des principales tendances et bonnes pratiques est élaboré en prenant en considération les recommandations du Groupe d'experts sur l'Indice GCI sur le classement par niveau et la pondération.

Note: Si un pays ne désigne pas de coordonnateur pour le questionnaire relatif au GCI, l'UIT s'adressera au coordonnateur institutionnel du Répertoire général de l'UIT.

ANNEXE A: DÉFINITION DES PILIERS ET INDICATEURS

Mesures juridiques

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. Il comprend les indicateurs de performance ci-après.

1.1 Lois relatives à la 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.

1.2 Réglementation relative à la cybersécurité

Une réglementation est une règle ou un principe régissant un comportement ou une pratique; il s'agit, en particulier, d'un tel acte pris par une autorité et maintenu par celle-ci. Une réglementation est une règle qui se fonde sur un texte de loi spécifique et qui vise à l'appliquer[1]. On entend par réglementation relative à la cybersécurité la législation régissant la protection des données, la notification des infractions, les obligations relatives à la certification/normalisation en matière de cybersécurité, la mise en œuvre des mesures de cybersécurité, les obligations en matière d'audits de cybersécurité, la protection de la vie privée, la protection en ligne des enfants, les signatures numériques et les transactions électroniques, et la responsabilité des fournisseurs de services Internet.

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 ci-après.

1.1 Équipes nationales/gouvernementales d'intervention en cas d'incident informatique

Les CIRT (équipes d'intervention en cas d'incident informatique), CERT (équipes d'intervention en cas d'urgence informatique) et CSIRT (équipes de réponse aux incidents de sécurité informatique) 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

---

[1] https://www.oed.com/view/Entry/161427?redirectedFrom=regulation.

national. Elles doivent fournir les capacités nécessaires au niveau national pour identifier les cybermenaces, se défendre contre elles, y réagir et les gérer, ainsi que pour renforcer la sécurité dans le cyberespace au niveau de l'État nation. Outre cette capacité, elles doivent pouvoir collecter elles-mêmes des renseignements afin de ne pas devoir compter sur des signalements de seconde main des incidents de sécurité, qu'ils émanent de clients de la CIRT ou d'autres sources.

1.2 Équipes CERT/CIRT/CSIRT 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 dans un secteur d'activité spécifique. Les équipes CERT sectorielles sont généralement créées pour des secteurs essentiels, tels que la santé, les services publics, les services d'urgence, l'énergie, l'enseignement supérieur et le secteur financier.

1.3 Cadre national pour la mise en œuvre des normes 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, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.

Mesures 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 ci-après.

1.1 Stratégie/politique nationale 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.

1.2 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.

1.3 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.

1.4 Stratégies et initiatives de protection en ligne des enfants

Pour promouvoir des environnements en ligne sûrs pour les enfants du monde entier, une stratégie nationale de protection en ligne des enfants devrait être complétée par un plan d'action. Il sera nécessaire de mettre en place un ensemble de politiques 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.

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 comprendre la sensibilisation et la disponibilité des ressources. Le sous-groupe comprend les indicateurs de performance ci-après.

1.1 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.

1.2 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).

1.3 Programmes pédagogiques sur la cybersécurité intégrés aux programmes universitaires nationaux

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.

1.4 Programmes de recherche et développement portant sur la 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.

1.5 Secteur national de la cybersécurité

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.

1.6 Mécanismes incitatifs publics

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 comprend les indicateurs de performance ci-après.

1.1 Accords de cybersécurité 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).

1.2 Accords de cybersécurité 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).

1.3 Traités d'entraide judiciaire dans le domaine de la cybersécurité

Il peut s'agir de la ratification d'accords internationaux contenant des dispositions relatives à l'entraide judiciaire et à la cybersécurité.

1.4 Partenariats public-privé

On entend par partenariats public-privé (PPP) les initiatives associant le secteur public et le secteur privé. Il peut prendre la forme d'un contrat à long terme entre une partie privée et une entité publique, visant la fourniture d'un bien ou d'un service public, au titre duquel la partie privée assume un risque important et la responsabilité de la direction, et la rémunération dépend de la performance[2]. 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.

1.5 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.

---

[2] https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships.