ITU Publications

Union internationale des télécommunications
Secteur du développement

Indice mondial de cybersécurité
2020

Indice mondial de cybersécurité 2020

Mesurer l'engagement en matière de cybersécurité

Remerciements

L'Indice mondial de cybersécurité (GCI) est une initiative de l'Union internationale des télécommunications (UIT), l'institution spécialisée des Nations Unies pour les TIC, façonnée et améliorée par le travail d'un large éventail d'experts et de contributeurs au sein des pays et d'autres organisations internationales. L'UIT tient à remercier tous les partenaires et contributeurs de leur travail acharné et de leur engagement en faveur du GCI et, surtout, d'avoir contribué à faire progresser notre compréhension collective des engagements en matière de cybersécurité.

L'UIT tient à souligner tout particulièrement les contributions reçues par la Commission d'études 2 de l'UIT-D et le Groupe de consultation de la direction du Bureau de développement des télécommunications (BDT), ainsi que leurs travaux sur les modifications à apporter au questionnaire du GCI. L'équipe du BDT chargée de la cybersécurité tient à remercier les membres de l'UIT qui ont désigné des experts pour les conseiller dans le processus de pondération. De plus amples informations sur le processus de pondération et la participation des experts sont disponibles dans la section consacrée à la méthodologie. Les contributions des experts suivants des membres de l'UIT ont été d'une aide précieuse pour la détermination des pondérations:

M. Abdelaziz Alzarooni (Autorité de régulation des télécommunications et des services publics numériques (TDRA), Émirats arabes unis), M. Marco Gercke (Cybercrime Research Institute GmbH, Allemagne), Mme Melissa Hathaway (The Potomac Institute for Policy Studies, États-Unis d'Amérique), Vanessa Copetti Cravo (ANATEL, Brésil), M. Scott James Shackelford (Indiana University, Program on Cybersecurity and Internet Governance, États-Unis d'Amérique), M. Gueric Goncalves (ANNSI, Bénin), M. Emmanuel Thekiso (BOCRA, Botswana), M. Dlamini (Ministère des TIC, Eswatini), M. Fillemon Johannes (Ministère des technologies de l'information et de la communication, Namibie), M. Palakiyem ASSIH (Cyber Defense Africa S.A.S., Togo), M. Nawa J. Samatebele (Autorité zambienne sur les technologies de l'information et de la communication, Zambie), M. Gonzalo Díaz de Valdés Olavarrieta (Chili), Mme Jessica Machado Álvarez (Administration de Cuba, Cuba), Mme Raquel Piña (Venezuela), M. Jacobo Bello Joya (Garde nationale du secrétariat de la sécurité et de la protection des citoyens, Mexique), M. Renzo Zegarra (Ministerio de Transportes y Comunicaciones, Pérou), M. Junior McIntyre (Union des télécommunications des Caraïbes (CTU), Trinité-et-Tobago), M. Fernando Hernadez (Organisme de régulation des communications, Uruguay), Mme Anne-Rachel Inné (American Registry for Internet Numbers (ARIN), États-Unis d'Amérique), M. Mohammad Odeh Alsalamin (Jordanie), Mme Nada Khater (Ministère de l'économie numérique et de l'entreprenariat, Jordanie), M. Yusuf Ahmed Buhijji (Ministère des transports et de la communication, Royaume de Bahreïn), Mme Aziza Al Rashdi (Ministère des transports, de la communication et des technologies de l'information, Oman), M. Abdulrahman AlHassan (Autorité nationale de cybersécurité (NCA), Arabie saoudite), M. Mohammad Alawi (Ministère des télécommunications de des technologies de l'information, État de Palestine), M. Khalili Urahman Kabirzoy (Autorité de certification racine (ARCA), Afghanistan), M. Nasratullah Ghafoory (Autorité de certification racine (ARCA), Afghanistan), Mme Xu Ming (Ministère de l'information et de la technologie, Équipe nationale d'intervention en cas d'urgence informatique, Chine), Mme Wan Xinxin (Ministère de l'information et de la technologie, Équipe nationale d'intervention en cas d'urgence informatique, Chine), Mme Catherine M. Subhyadas (Department des communications, Fiji), Puan Lyana Shohaimay (Ministère des communications et du multimédia, Malaisie), Puan Nurul Adiah Hani Husin (Ministère des communications et du multimédia, Malaisie), M. Yan Naung Soe (Centre national de cybersécurité, Département des technologies de l'information et de la cybersécurité, Myanmar), M. Jakkrapong Chavong (Ministère de l'économie et de la société numériques, Thaïlande), M. Alan Olegovich Khubaev (Département de la sécurité informatique, Russie), M. Andrey Sergeevich Zhivov (Département de la coopération internationale, Russie), M. Ilgyz Turganbaev (Comité d'État

des technologies de l'information et des communications, République kirghize), M. Muhamedjan Alymkulov (Comité d'État des technologies de l'information et des communications, République kirghize), M. Vladimir Yuryevich Shurin (Département de la sécurité de l'information du service de la sécurité de l'entreprise unitaire républicaine, Belarus), M. Nestoras Chouliaras (Secrétariat général des télécommunications et de la poste, Ministère de la gouvernance numérique, Grèce), Mme Eglė Vasiliauskaitė (Ministère de la défense nationale, Lituanie), M. Tadas Šakūnas (Ministère de la défense nationale, Lituanie), Mme Radoja (Serbie), M. Matej Šalmík (Centre national de cybersécurité SK-CERT, Slovaquie), M. Rastislav Janota (Centre national de cybersécurité SK-CERT, Slovaquie), M. Aidan Murchland (Royaume-Uni), M. Miguel Pinto (BitSight, États-Unis d'Amérique), Mme Nunil Pantjawati (Indonésie), Mme Intan Rahayu (Indonésie), M. Makaireh JONGA (Équipe d'intervention en cas d'incident informatique (gmCSIRT), Gambie), Mme Banchale Gufu (Kenya), Mme Sonam Choki (Département des technologies de l'information et des télécommunications, Bhutan), Aqeel Taha Saadoon (Secrétariat des TIC, Iraq), et Thar Kadhim Ali (CERTIraq, Iraq).

L'équipe de l'UIT chargée de la cybersécurité tient à remercier les coordonnateurs pour l'indice GCI, qui ont recueilli des données sur les engagements en matière de cybersécurité dans leurs pays respectifs. Ce rapport n'aurait pas été possible sans les coordonnateurs des pays pour l'indice GCI.

L'équipe est reconnaissante envers les nombreux collègues et stagiaires de l'UIT qui ont apporté leur soutien à l'élaboration du présent rapport.

L'équipe présente ses excuses à toutes les personnes ou organisations omises par inadvertance dans cette liste et exprime sa gratitude à tous ceux qui ont contribué à la réalisation du GCI.

Veuillez contacter l'équipe de l'UIT chargée de la cybersécurité à l'adresse gci@itu.int pour tout commentaire ou toute question concernant la présente publication.

© ITU 2021 Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque moyen que ce soit, en partie ou en totalité, sans l'autorisation écrite préalable de l'UIT.

Déni de responsabilité

Les appellations employées dans la présente publication et la présentation des données qui y figurent n'impliquent, de la part de l'UIT, aucune prise de position quant au statut juridique des pays, territoires, villes ou zones, ou de leurs autorités, ni quant au tracé de leurs frontières ou limites. Les références faites à certaines sociétés ou aux produits de certains fabricants n'impliquent pas que l'UIT approuve ou recommande ces sociétés ou ces produits de préférence à d'autres de nature similaire, mais dont il n'est pas fait mention. Sauf erreur ou omission, les noms des produits propriétaires sont reproduits avec une lettre majuscule initiale.

L'UIT a pris toutes les précautions raisonnables pour vérifier les informations contenues dans la présente publication. Cependant, le document publié est distribué sans garantie d'aucune sorte, ni expresse, ni implicite. Son interprétation et son utilisation relèvent de la responsabilité du lecteur. Les avis, résultats et conclusions reproduits dans la présente publication ne reflètent pas nécessairement la position de l'UIT ou de ses membres.

ISBN:

978-92-61-33922-7 (Version électronique)
978-92-61-33932-6 (Version EPUB)
978-92-61-33942-5 (Version Mobi)

Avant-propos

La nécessité d'un cyberespace sûr et sécurisé est devenue plus importante que jamais, d'autant plus que nous sommes tous de plus en plus dépendants des "lignes de vie numériques". L'un des plus grands défis de la pandémie de COVID-19 a été de trouver des moyens de se connecter utilement les uns aux autres, malgré l'incertitude, l'anxiété et le changement. Même avant la pandémie, la cybersécurité était essentielle pour assurer notre sécurité en ligne et nous permettre de remplir nos fonctions quotidiennes essentielles.

Je suis inspirée par la capacité des gens à s'adapter à cet environnement incertain et par leur utilisation de la technologie pour trouver des solutions créatives. De nombreuses organisations, dont l'Union internationale des télécommunications, ont été confrontées à de nouveaux défis liés au travail à distance. La cybersécurité est fondamentalement liée au travail à distance, qu'il s'agisse de gérer les participants aux appels vidéo ou de s'assurer que les documents sont partagés en toute sécurité. L'UIT a donc continué à collaborer avec les pays pour être plus efficace, plus active et produire des résultats dans les domaines où l'on a le plus besoin d'elle.

Lorsque l'Indice mondial de cybersécurité a été lancé pour la première fois en 2015, peu de gens auraient pu imaginer la situation dans laquelle nous nous trouvons actuellement. Cette dernière itération de l'indice mondial de cybersécurité contribuera à promouvoir de nouvelles mesures en faveur d'écosystèmes numériques sécurisés nécessaires à la reprise et à la croissance, en mesurant les types d'engagements pris par les pays en matière de cybersécurité et leur prévalence.

La présente itération révèle que de nombreux pays progressent dans leurs engagements à répondre aux défis de la cybersécurité, malgré les acteurs opportunistes qui ont profité de notre désir d'information, de nos craintes face à la pandémie, du passage au travail à domicile et à l'apprentissage à distance, de la dépendance aux systèmes de santé, etc.

Le rapport sur l'Indice mondial de cybersécurité montre que de nombreux pays ont adopté de nouvelles lois et réglementations en matière de cybersécurité pour traiter de domaines comme la vie privée, les accès non autorisés et la sécurité en ligne. Il met aussi en relief la nécessité d'établir des stratégies et des mécanismes pour renforcer les capacités et aider les gouvernements et les entreprises à mieux se préparer aux cyberrisques croissants et à les atténuer. Plus de la moitié des pays du monde disposent désormais d'une équipe d'intervention en cas d'incident informatique (CIRT) et près des deux tiers d'entre eux ont mis en place une forme de stratégie nationale de cybersécurité pour guider leur position d'ensemble en matière de cybersécurité.

L'Indice mondial de cybersécurité révèle que la cybersécurité est véritablement une question de développement et qu'il est urgent de combler l'écart croissant en matière de cybercapacités

entre les pays développés et les pays en développement en favorisant les connaissances, en améliorant les qualifications et en renforçant les compétences. Nous devons réduire cet écart en remontant à la source et en renforçant les capacités en matière d'infrastructure numérique, de compétences numériques et de ressources dans le monde en développement.

J'espère que l'Indice mondial de cybersécurité continuera d'être un outil de renforcement des capacités utile aux pouvoirs publics, aux décideurs, aux experts en cybersécurité et aux établissements universitaires pour recenser les domaines à améliorer et mettre en évidence les bonnes pratiques pour renforcer la cybersécurité nationale.

Je tiens à remercier les pays de leur engagement et de leur contribution à cet effort, en particulier de leur participation à l'élaboration, à la collecte des données et à la validation de cette itération de l'Indice. J'aimerais également remercier tous ceux qui ont participé au processus des Commissions d'études de leur soutien et de leur concours. J'invite tous les États Membres de l'UIT à continuer de nous fournir des informations actualisées sur les progrès accomplis au regard de leurs engagements en matière de cybersécurité, de façon que nous puissions échanger efficacement des données d'expérience, des travaux de recherche et des solutions afin de créer un cyberespace fiable pour tous.

Doreen Bogdan-Martin
Directrice, Bureau de développement des télécommunications de l'UIT

Résumé analytique

L'Indice mondial de cybersécurité (GCI) a été lancé pour la première fois en 2015 par l'Union internationale des télécommunications (UIT) pour mesurer l'engagement des 193 États Membres de l'UIT et de l'État de Palestine[1] en matière de cybersécurité, afin de les aider à déterminer les domaines à améliorer et d'encourager les pays à prendre des mesures, en les sensibilisant à l'état de la cybersécurité dans le monde. Les risques, les priorités et les ressources en matière de cybersécurité évoluant, le GCI s'est également adapté pour donner un aperçu plus précis des mesures de cybersécurité prises par les pays.

Le présent rapport vise à mieux comprendre les engagements des pays en matière de cybersécurité, à recenser les lacunes, à encourager l'inclusion de bonnes pratiques et à fournir des indications utiles aux pays pour améliorer leur position en matière de cybersécurité.

Les pays ont déclaré utiliser le GCI pour faciliter:

- des discussions dans le cadre de forums officiellement établis qui permettent des auto-évaluations et une meilleure coordination;
- la collecte de renseignements sur les initiatives nationales générales et les ressources utilisées pour gérer la cybersécurité au niveau national;
- les études comparatives relatives aux bonnes pratiques, aux partenaires et aux voisins régionaux;
- la sensibilisation des différentes parties prenantes aux besoins de coordination au niveau national.

Les résultats du GCI montrent une amélioration et un renforcement globaux des cinq piliers du programme cybersécurité, mais aussi que des lacunes régionales en matière de cybercapacité persistent. Des exemples de pratiques dans divers pays ont été mis en évidence dans le rapport.

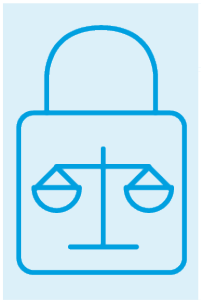
Pays évalués	Année de collecte	Coordonna-teurs dans les pays	Questionnaires soumis	Croissance de la note médiane globale depuis 2018
194	**2020**	**169**	**150**	**9,5%**

L'indice présente 82 questions sur les engagements des États Membres en matière de cybersécurité, réparties sur cinq piliers:

- mesures juridiques;
- mesures techniques;
- mesures organisationnelles;
- renforcement des capacités;
- mesures de coopération.

[1] L'État de Palestine participe aux travaux de l'UIT au titre de la Résolution 99 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires.

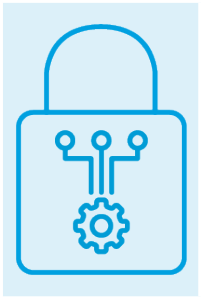
Le tableau ci-dessous montre les engagements mondiaux pour des indicateurs spécifiques par pilier.



Juridique

Évaluer les lois et règlements sur la cybercriminalité et la cybersécurité

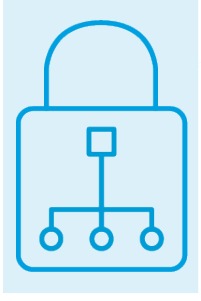
167	Pays disposant d'une forme de législation en matière de cybersécurité
133	Réglementations en matière de protection des données
97	Réglementations en matière d'infrastructures critiques



Technique

Évaluer la mise en œuvre des capacités techniques par le biais des organismes nationaux et sectoriels

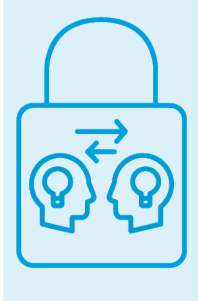
131	CIRT actives
104	Participent à une CIRT régionale
101	Mécanismes de signalement pour la protection en ligne des enfants



Organisationnel

Évaluer les stratégies nationales et les organisations qui mettent en œuvre la cybersécurité

127	Stratégies nationales de cybersécurité
136	Organismes de cybersécurité
86	Stratégies et initiatives de protection en ligne des enfants signalées



Renforcement des capacités

Évaluation des campagnes de sensibilisation, de la formation, de l'éducation et des incitations au renforcement des capacités en matière de cybersécurité

142	Pays menant des activités de sensibilisation à la cybersécurité
94	Pays ayant des programmes de R&D en matière de cybersécurité
98	Pays signalant avoir des secteurs d'activité nationaux dans le domaine de la cybersécurité

Coopération

Évaluation des partenariats entre organismes, entreprises et pays

166	Pays participant à des partenariats public-privé- dans le domaine de la cybersécurité
90	Pays ayant des accords bilatéraux dans le domaine de la cybersécurité
112	Pays ayant des accords multilatéraux dans le domaine de la cybersécurité

Modifications de l'Indice mondial de cybersécurité ayant des incidences sur les notes

- La présente édition de l'Indice mondial de cybersécurité est fondée sur les données communiquées par un nombre record d'États Membres. Le nombre de réponses est passé de 105 lors de l'itération 2013-2014 à 150 questionnaires retournés en 2020.
- Le questionnaire du GCI a été mis à jour. Des questions ont été redéfinies, ajoutées ou supprimées dans chacun des cinq piliers (juridique, technique, organisationnel, renforcement des capacités et mesures de coopération) afin de refléter l'évolution des préoccupations et des efforts en matière de cybersécurité. Les changements apportés au questionnaire ont des répercussions sur les résultats, ces changements étant un facteur pour les notes et les classements des pays.
- Les pondérations diffèrent des itérations précédentes, reflétant, en partie, les changements dans la structure des questions ainsi que l'ajout et la suppression de questions.
- Les pondérations des indicateurs étaient fondées sur des recommandations d'experts. Les membres de l'UIT ont désigné des experts pour les conseiller dans le processus de pondération afin d'attribuer des poids aux indicateurs en fonction de leur importance relative pour la cybersécurité. Les variations dans l'attribution des pondérations peuvent avoir une incidence sur les notes et les classements des pays.
- Une section a été préparée pour donner plus d'informations sur la construction, la composition et les changements récents du questionnaire du GCI (Annexe A).
- De nombreux pays, notamment les pays les plus performants, enregistrent des résultats de plus en plus proches. C'est pourquoi les classements individuels doivent être interprétés avec précaution.
- Certains pays ont refusé de vérifier les données recueillies ou de participer à cette édition de l'Indice mondial de cybersécurité. Les données concernant ces pays (marquées d'un *) ne doivent pas être considérées comme officiellement approuvées par un représentant du pays. Ces données ayant été collectées par le biais de recherches en ligne, les éléments manquants doivent être interprétés comme non trouvés et non comme inexistants.

En outre, la participation des pays peut avoir eu un effet positif sur les notes dans certains cas, car plus un pays contribue au questionnaire, plus il est probable que des réponses affirmatives seront trouvées.

Il existe de nombreux domaines dans lesquels les pays excellent et des domaines dans lesquels il est possible d'intensifier les efforts. Il conviendrait de décourager les pays de se concentrer sur les classements.

Pour les pays qui n'ont pas répondu au questionnaire, des recherches documentaires ont été effectuées à partir des informations publiques disponibles sur les sites Web officiels et dans d'autres ressources. Dans le cas des pays pour lesquels des recherches documentaires ont été effectuées, les données recueillies peuvent ne pas refléter avec précision la situation du pays en matière de cybersécurité. Le GCI ne contient pas de données estimées.

Table des matières

Liste des tableaux et figures

Tableaux

Figures

1 Indice mondial de cybersécurité: historique et contexte

La quatrième itération de l'Indice mondial de cybersécurité (GCI) arrive à un moment très différent de ses prédécesseurs. Lorsque le Programme mondial cybersécurité a été lancé en 2007, le premier iPhone n'était encore qu'à un mois de sa sortie et Facebook n'était ouvert aux utilisateurs hors universités des États-Unis que depuis un an. Un milliard de personnes étaient en ligne et l'on craignait que la quantité de données créées, 255 exaoctets, ne dépasse le stockage disponible[1]. Aujourd'hui, les smartphones ont remodelé la vie quotidienne et les réseaux sociaux se sont imposés dans une sphère plus large de la société. Actuellement, 3,5 milliards de personnes sont en ligne et le monde numérique est estimé à 44 zettaoctets, sans risque de stockage indisponible grâce à l'informatique en nuage[2]. De plus, la prolifération des TIC a eu des répercussions sur l'écosystème national au sens large, donnant naissance à de nouvelles possibilités organisationnelles comme les services d'administration en ligne et à de nouveaux paradigmes économiques et productifs comme l'industrie 4.0 et l'économie numérique au sens large.

Tous les pays sont touchés, dans une certaine mesure, par la fracture numérique et, en tant que catalyseur essentiel de l'économie, de la société et des pouvoirs publics, qui reposent sur des systèmes numériques, la cybersécurité devrait être une priorité absolue.

La pandémie de COVID-19 a considérablement affecté le fonctionnement des sociétés. Lorsque la pandémie a commencé à s'installer en avril 2020, Akamai a constaté que le trafic Internet avait augmenté de 30%[3]. Du télétravail à l'apprentissage à distance, la technologie a joué un rôle essentiel pour que les gens restent connectés. Pour que l'ère numérique réalise son potentiel, un cyberespace sûr et fiable est essentiel. Un an après que l'Organisation mondiale de la santé a déclaré que la COVID-19 était une pandémie et avec l'apparition de nouveaux systèmes de gestion et de la vaccination, notre dépendance aux technologies numériques continue de croître. Tandis que le monde connecte les non-connectés, un cyberespace sûr et digne de confiance doit être garanti.

Les risques en matière de cybersécurité sont de plus en plus largement reconnus[4]. La pandémie actuelle a suscité la méfiance, notamment en ligne. Les données recueillies dans le cadre du GCI constituent le point de départ d'un échange plus large sur la cybersécurité, autour duquel le contexte et les observations locaux sont essentiels pour définir la voie à suivre.

Afin de contribuer à la création d'un cyberespace sûr et fiable au lendemain de la pandémie, le GCI peut servir de point de départ pour comprendre les répercussions de la pandémie sur les efforts de cybersécurité et la manière dont les pays s'efforcent d'aborder la cybersécurité et la confiance. Par exemple, certains pays ont signalé des retards dans l'approbation et l'entrée en vigueur des lois, la mise en œuvre ou l'amélioration des CIRT, l'élaboration ou la révision des

---

1 http://core.xsomo.com.jm/images/web/File/white%20papaers/Expanding_Digital_Universe_IDC_WhitePaper_022507.pdf
2 https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/
3 https://blogs.akamai.com/2020/04/can-the-internet-keep-up-with-the-surge-in-demand.html
4 http://reports.weforum.org/global-risks-report-2020/executive-summary/

stratégies nationales de cybersécurité et l'exécution des efforts de renforcement des capacités. Même les accords de coopération ne bénéficiaient plus de l'interaction et de la collaboration en présentiel.

Il importe que les pouvoirs publics fassent le point sur les politiques et les pratiques en place en matière de cybersécurité, car le monde continue de changer. La cybersécurité a évolué et s'est adaptée, tout comme la façon de la mesurer. Le GCI a mis à jour les questions sur le rôle des CIRT, les accords de coopération, les cadres organisationnels et la sensibilisation du public. Si ces changements rendent le GCI moins comparable dans le temps, cette itération reflète plus fidèlement les engagements actuels des pays.

2 Thèmes principaux

2.1 Mesures juridiques: planifier les interventions futures

Aujourd'hui, de nombreux défis sapent la confiance en ligne et empêchent la société numérique de fonctionner à son plein potentiel. Par exemple, les pertes mondiales dues à la cybercriminalité sont estimées de seulement 1 000 milliards USD en 2020[5] à 6 000 milliards USD en 2021[6]. L'élaboration d'un cadre juridique et réglementaire visant à protéger la société et à favoriser un environnement numérique sûr et sécurisé est essentielle et devrait être à l'origine de tout effort national en matière de cybersécurité.

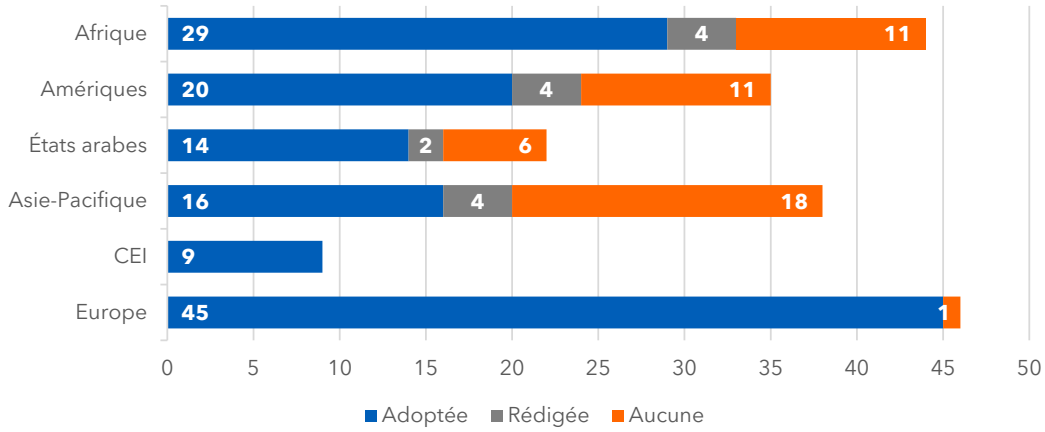
Les cadres juridiques et réglementaires comprennent la mise en place d'une législation définissant ce qui constitue des activités illicites dans le cyberespace ainsi que la définition des outils de procédure nécessaires pour enquêter, engager des poursuites et faire appliquer cette législation, la mise en place de bases de référence en matière de cybersécurité et de mécanismes de conformité pour un ensemble de parties prenantes nationales et des procédures visant à garantir la cohérence avec les obligations internationales.

La quatrième édition de l'Indice mondial de cybersécurité fait le point sur les interventions en matière de cybersécurité dans le cadre juridique d'un pays en mesurant la présence:

- de prescriptions de base que les acteurs publics et privés doivent respecter;
- d'instruments juridiques interdisant les actes préjudiciables.

Protection des données

Figure 1: Pays disposant d'une législation en matière de protection des données



Source: UIT

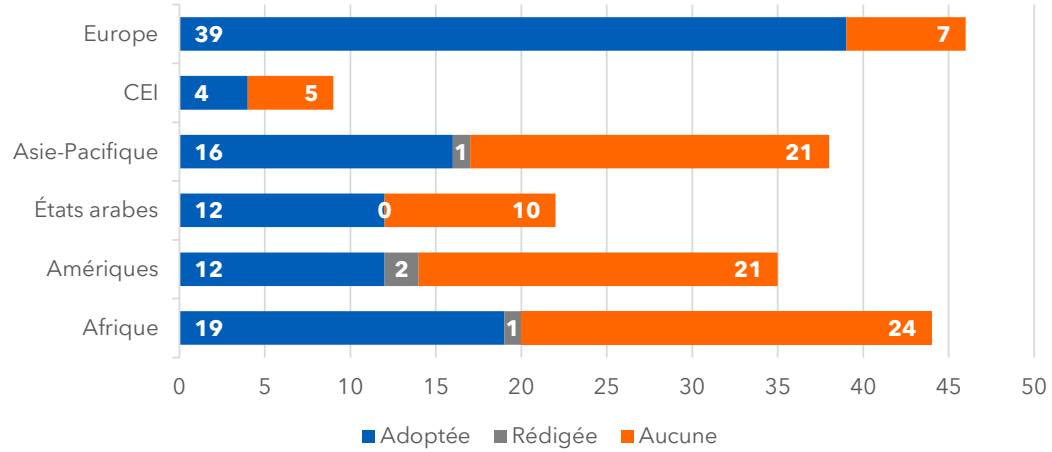
[5] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[6] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

La législation sur la protection des données peut prendre la forme d'une réglementation qui pourrait, par exemple, obliger une organisation à divulguer une violation de la cybersécurité ou établir des exigences d'audit annuel.

À première vue, les défenseurs de la vie privée peuvent noter qu'un nombre important de pays ayant déjà mis en place des réglementations en matière de protection des données et de la vie privée ont travaillé à leur mise à jour. En outre, 133 pays ont signé des réglementations en matière de protection et de confidentialité, 15 sont en cours de rédaction et 46 n'ont pas de réglementation en place. De nombreux pays disposant d'une réglementation existante ont mis à jour leur législation afin de refléter les nouveaux accords et normes.

Depuis la dernière itération, davantage de pays ont mis en œuvre des mesures exigeant la notification des violations. Dans cette édition, 102 pays ont introduit des exigences de notification des violations de données et des incidents dans leur législation et leurs politiques.

Figure 2: Pays disposant de mesures de notification des violations



Source: UIT

Usurpation d'identité et vol de données en ligne

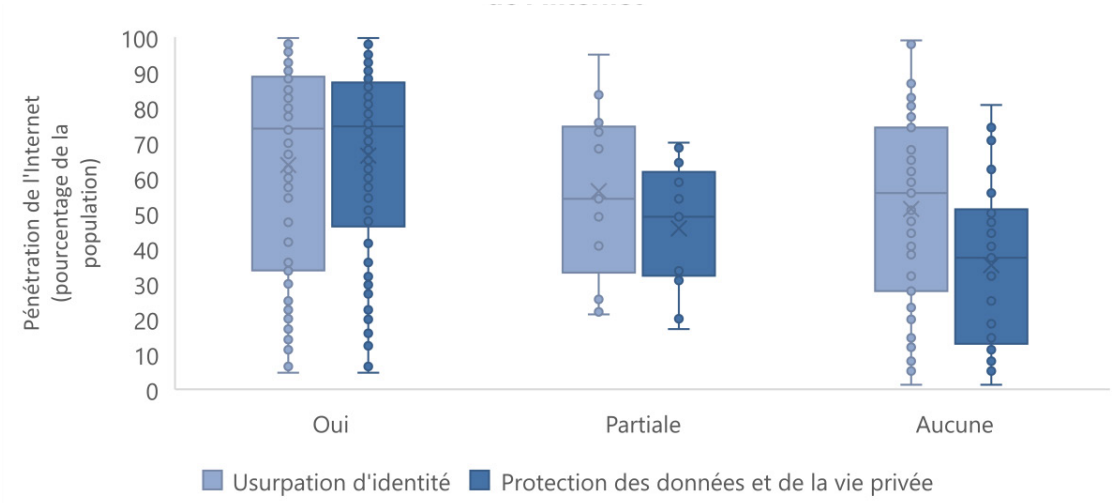
Alors que les pays ont pris des mesures contre l'accès illicite, la législation sur l'usurpation d'identité et le vol de données en ligne ne reçoit toujours pas l'attention voulue. Pourtant, la protection de l'identité en ligne revêt une importance considérable, surtout avec le passage actuel à l'environnement numérique. La population mondiale s'est déplacée en ligne par le biais des réseaux sociaux et des pratiques professionnelles, ce qui nécessite un niveau de sécurité élevé car une identité volée peut compromettre la vie quotidienne, tant sur le plan privé que professionnel.

Figure 3: Pays disposant d'une législation relative au vol d'informations personnelles

Source: UIT

Comme le montre la Figure 4, lorsqu'on examine la pénétration médiane et moyenne de l'Internet, les pays à forte pénétration de l'Internet sont légèrement plus susceptibles de disposer d'une loi ou d'une réglementation sur la protection des données en ligne que les pays à faible pénétration de l'Internet. En revanche, la réglementation sur la protection des données et de la vie privée est plus susceptible de se trouver dans les pays à forte pénétration de l'Internet. Ces tendances reflètent, en partie, les conditions économiques, le développement général et les stratégies en matière de transition numérique des gouvernements. Il convient de noter que certains pays se sont préparés à une plus grande pénétration de l'Internet en adoptant en amont une législation relative au vol d'identité et à la protection des données et de la vie privée.

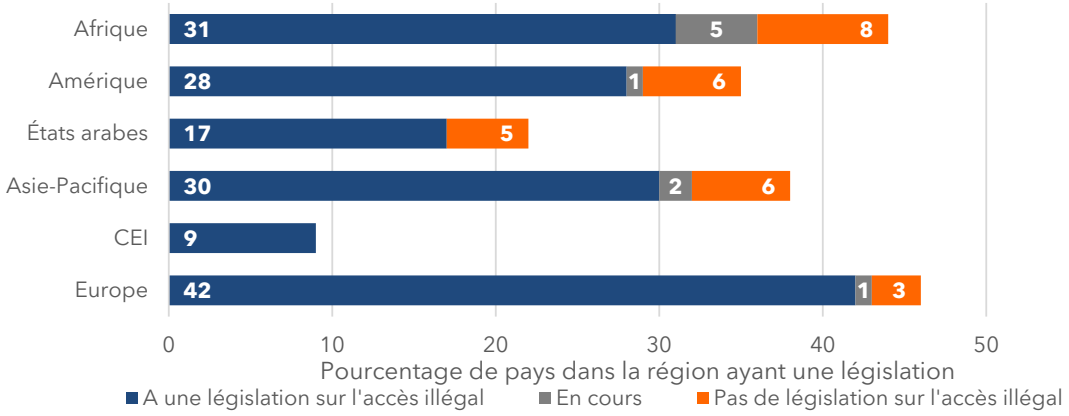
Figure 4: Législation sur l'usurpation d'identité et la protection des données et de la vie privée, représentée en fonction de l'accès à l'Internet (% de la population)



Source: Base de données de l'UIT sur les indicateurs des télécommunications/TIC dans le monde

Comme le montre la Figure 5, la plupart des pays disposent d'une législation sur l'accès illégal, avec peu de différences significatives entre les régions.

Figure 5: Législation sur l'accès illégal



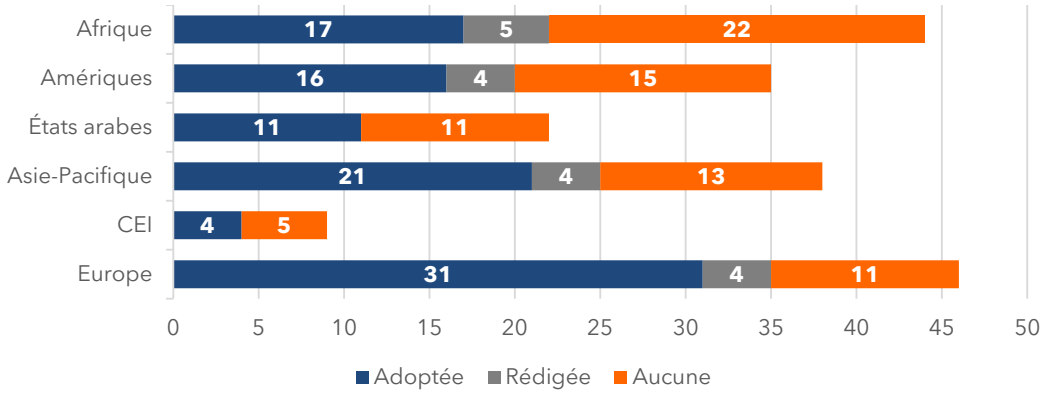
Source: Base de données de l'UIT sur les indicateurs des télécommunications/TIC dans le monde

Comportement antisocial en ligne

Les comportements antisociaux en ligne constituent un défi permanent pour lequel les pays renforcent leur soutien législatif. Le GCI mesure deux aspects: le harcèlement en ligne et le racisme et la xénophobie en ligne.

Le harcèlement en ligne reste un problème persistant: aux États-Unis d'Amérique, en 2020, "41% des Américains ont personnellement subi une forme de harcèlement en ligne"[7] et au moins une femme sur dix dans l'Union européenne a été victime de harcèlement en ligne[8]. Dans une enquête menée auprès d'adultes dans 32 pays, un adulte sur cinq a déclaré avoir été confronté à des discours de haine en ligne[9].

Figure 6: Pays disposant d'une législation sur le harcèlement en ligne



Source: Base de données de l'UIT sur les indicateurs des télécommunications/TIC dans le monde

Au niveau mondial, 100 pays ont adopté une législation érigeant en infraction pénale les cas de harcèlement et d'abus en ligne, 17 sont en train de rédiger et de mettre en œuvre ces

[7] https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/
[8] https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/factsheet_lets_put_an_end_to_violence_against_women_en.pdf
[9] https://blogs.microsoft.com/on-the-issues/2020/11/13/microsoft-study-online-risks-world-kindness-day/#_edn1

mesures et 77 n'ont pas de législation sur le sujet. Cependant, ce qui constitue un abus est souvent mal défini.

Les efforts visant à lutter contre le racisme et la xénophobie en ligne se heurtent à des obstacles de clarté, mais un nombre important de pays sont en train de rédiger une forme de législation dans ce sens. Plusieurs pays étendent ou adaptent les lois hors ligne sur le racisme et la xénophobie au contexte en ligne. Le seuil de ce qui constitue une infraction varie considérablement, car ce qui peut être légal dans un pays peut constituer une infraction punissable dans un autre. Toutefois, certains pays ont décidé de rédiger des dispositions visant spécifiquement les comportements racistes en ligne.

2.2 Mesures techniques: Déploiement accru de CIRT/CERT

Des mécanismes et des structures institutionnelles efficaces au niveau national sont nécessaires pour faire face aux cyberrisques et aux incidents de manière fiable. Les équipes d'intervention en cas d'incident informatique (CIRT) ou les équipes d'intervention en cas d'urgence informatique (CERT) permettent aux pays de réagir aux incidents au niveau national en utilisant un point de contact centralisé et favorisent une action rapide et systématique, permettant aux pays de tirer des enseignements de l'expérience et de renforcer la résilience en matière de cybersécurité.

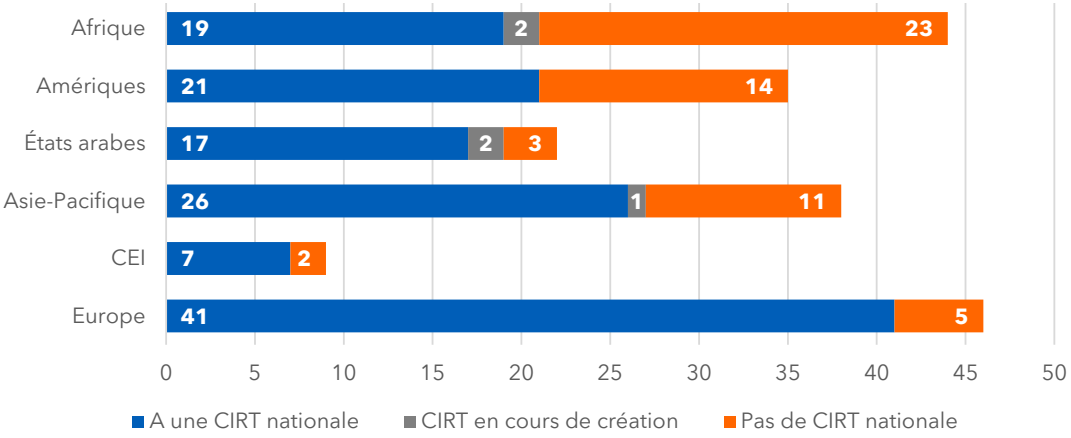
Les CIRT nationales sont souvent créées et mises en œuvre à la suite d'une législation ou d'une politique nationale. Les CIRT peuvent faire partie d'une institution gouvernementale ou être placées sous l'égide d'un ministère spécifique ou d'une autre entité. Lorsque les pays manquent de temps, de connaissances ou de ressources pour mettre en place une CIRT nationale, certains confient les responsabilités de la CIRT à un tiers

De nouvelles CIRT sont créées

À la fin de 2020, 131 pays avaient mis en place des CIRT nationales, dont 10 nouvelles CIRT créées depuis la publication de l'Indice mondial de cybersécurité de 2018. Quatre CIRT nationales supplémentaires sont actuellement en cours de création.

Si de nombreux pays ont progressé dans la mise en œuvre des CIRT, beaucoup d'autres, en particulier les pays les moins avancés (PMA), sont confrontés à des obstacles importants dans la création de CIRT. Le manque de ressources, de connaissances technologiques, d'écosystème de cybersécurité, de recherche et développement, de hiérarchisation des priorités et de volonté politique peut entraver les efforts en matière de mesures techniques pour relever les défis de la cybersécurité.

Figure 7: Nombre de pays disposant d'une CIRT nationale



Source: UIT

Bien que la région Afrique ne soit pas en tête dans le domaine technique, six CIRT supplémentaires ont été créées depuis l'édition de l'Indice mondial de cybersécurité 2018. La situation dans la région s'est améliorée, passant de 13 à 19 pays disposant d'une CIRT nationale. La région des Amériques compte 21 CIRT et la région des États arabes compte 17 pays dotés d'une CIRT nationale. On relèvera que seuls deux pays de la région de la CEI et six pays d'Europe ne disposent pas de CIRT nationales.

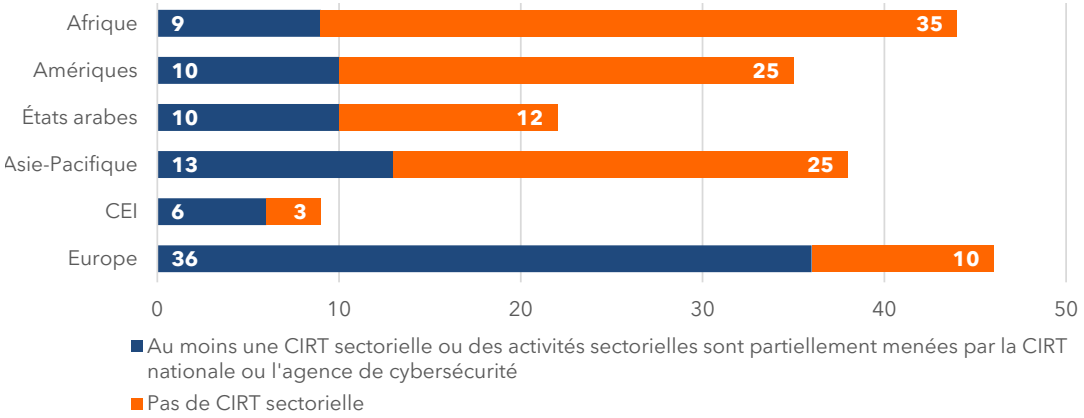
Le GCI suit également les activités des CIRT. Sur les 131 CIRT mises en place, 11 étaient engagées dans toutes les activités suivantes:

- favoriser la sensibilisation à la cybersécurité et la protection en ligne des enfants en fournissant des conseils, des guides, des manuels, des formations et des vidéos;
- fournir des conseils en matière de cybersécurité aux informaticiens;
- réaliser des cyberexercices au cours des deux dernières années;
- collaborer avec des CIRT régionales et le FIRST[10];
- certification par Trusted Introducer[11] ou autre certification reconnue.

Alors que les CIRT nationales traitent des problèmes au niveau national, les CIRT sectorielles répondent aux besoins de cybersécurité d'un secteur spécifique comme la santé, les transports, les télécommunications ou les services publics. D'autres types de CIRT sont au service de sociétés multinationales ou de grandes entreprises, d'universités privées, entre autres, et ces autres types de CIRT n'ont pas été suivies dans le présent rapport sur le GCI.

10 www.first.org
11 www.trusted-introducer.org/

Figure 8: Nombre de CIRT sectorielles



Source: UIT

Comme le montre la Figure 8, deux tiers des pays n'ont pas de CIRT sectorielle. Sur les 76 pays disposant d'une CIRT sectorielle, 37 mènent des campagnes de sensibilisation, des cyberexercices et partagent les informations relatives aux incidents et aux menaces de manière publique ou confidentielle avec leur communauté.

2.3 Mesures organisationnelles: aligner la stratégie

Les mesures organisationnelles examinent les mécanismes de gouvernance et de coordination au sein des pays qui traitent de la cybersécurité. Les mesures organisationnelles consistent notamment à s'assurer que la cybersécurité est maintenue au plus haut niveau de l'exécutif, à attribuer des rôles et des responsabilités pertinents à diverses entités nationales et à les rendre responsables de la situation nationale en matière de cybersécurité.

La présence de mesures organisationnelles ne se retrouve pas toujours dans les pays disposant d'une solide infrastructure de télécommunications. Si l'on compare l'indice de l'infrastructure de télécommunications de l'enquête 2020 sur l'administration électronique de l'ONU, qui fait partie de l'indice de préparation à l'administration électronique[12], aux résultats globaux des mesures organisationnelles, on constate que, même si la tendance est faible, de nombreux pays obtiennent actuellement de bons résultats dans les évaluations de l'infrastructure de télécommunications, mais ne disposent pas des mesures organisationnelles nécessaires pour faire face aux problèmes de cybersécurité.

L'absence de mesures organisationnelles adéquates peut contribuer au manque de clarté des responsabilités et de l'obligation de rendre des comptes dans la gouvernance nationale de la cybersécurité et empêcher une coordination intragouvernementale et intersectorielle efficace.

Importance de stratégies nationales actualisées en matière de cybersécurité

Une stratégie nationale en matière de cybersécurité est souvent la pierre angulaire des mesures organisationnelles au niveau national en matière de cybersécurité. Selon le Guide de l'UIT sur l'élaboration d'une stratégie nationale de cybersécurité, une stratégie nationale en matière de cybersécurité est un cadre ou une stratégie globale qui doit être élaborée, mise en œuvre et exécutée selon une approche multipartite, qui prévoit une action coordonnée en matière de

[12] https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

prévention, de préparation, de réaction et de rétablissement en cas d'incident de la part des pouvoirs publics, du secteur privé et de la société civile[13].

De plus en plus de pays élaborent des stratégies nationales de cybersécurité pour gérer la cybersécurité de manière plus structurée. Une stratégie nationale de cybersécurité peut présenter plusieurs avantages, notamment celui de réunir les parties prenantes concernées, de préciser les priorités nationales et de planifier le renforcement des capacités en matière de cybersécurité.

Avec l'évolution de l'Indice mondial de cybersécurité, l'accent est mis sur les pays qui procèdent à des mises à jour régulières de leur stratégie nationale de cybersécurité, afin de s'assurer qu'ils s'adaptent aux réalités en constante évolution. En effet, disposer d'une stratégie nationale de cybersécurité est un premier pas positif pour la situation en matière de cybersécurité des pays, mais des révisions régulières en fonction de l'évolution des menaces et des priorités en matière de cybersécurité sont nécessaires. Les pays, lorsqu'ils mettent à jour une stratégie nationale de cybersécurité, adoptent généralement un calendrier de 4 à 5 ans. Certains pays ont opté pour des calendriers plus longs, s'étendant sur une décennie ou plus.

Alors que 127 pays disposent d'une stratégie nationale de cybersécurité, qu'elle soit actuelle, qu'elle date de plus de cinq ans ou qu'elle soit en cours d'élaboration, 60 pays ont démontré qu'ils avaient progressé dans la définition d'objectifs plus clairs en révisant et en élaborant de nouvelles stratégies de cybersécurité ou en mettant à jour leur plan d'action.

Protection des infrastructures critiques/résilience nationale

Un aspect important du processus d'élaboration d'une stratégie nationale de cybersécurité consiste à définir un ensemble d'objectifs clairs en matière de protection des infrastructures critiques. Assurer la continuité des opérations au niveau national est un défi permanent pour les pays. Les infrastructures critiques comme les réseaux électriques, les stations de purification de l'eau et les systèmes de transport continuent de faire face à des risques de cybersécurité. Les conséquences potentielles d'un incident touchant les infrastructures critiques sont élevées, et la stratégie devrait se traduire par une attention accrue aux efforts de gestion des risques destinés à réduire la probabilité et l'aggravation d'un événement lourd de conséquences.

Les dépenses de cybersécurité pour les infrastructures critiques devraient augmenter de 9 milliards USD au cours de l'année prochaine pour atteindre 105,99 milliards USD en 2021[14]. Comme les infrastructures critiques, tout comme le reste de la main-d'œuvre, ont évolué vers des situations de travail à distance, elles ont dû faire face à une surface d'exposition aux attaques accrue. ABI Research a constaté que les investissements dans la cybersécurité variaient considérablement en fonction de la région, du secteur et de la connectivité, les dépenses étant les plus élevées dans les secteurs de la défense, des services financiers et des TIC, mais plus faibles dans les secteurs industriels[15].

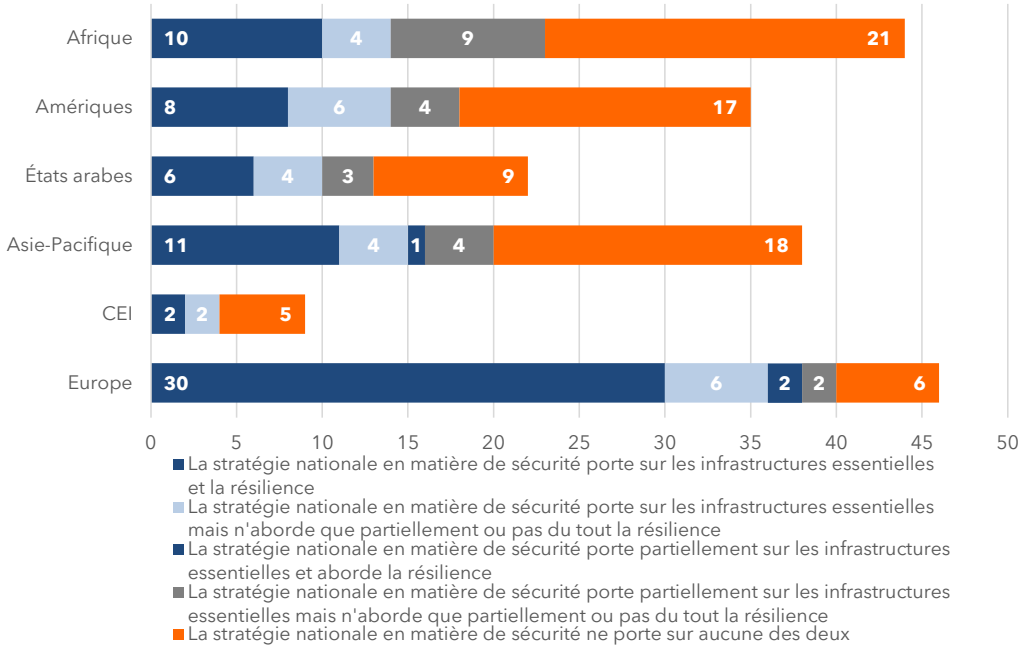
---

13 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

14 https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/

15 https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/

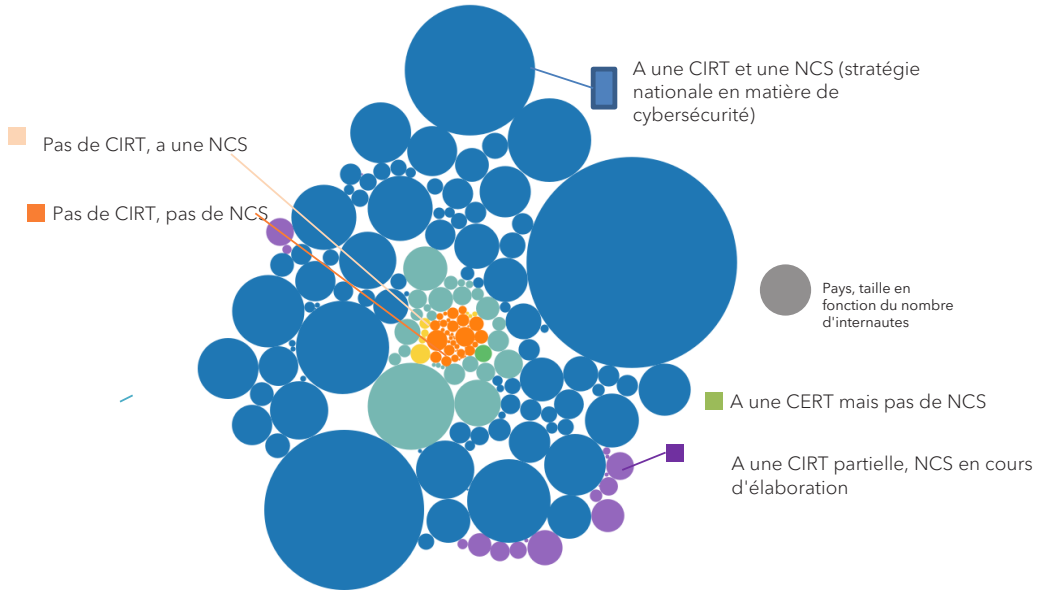
Figure 9: Pays qui abordent la question des infrastructures critiques et de la résilience



Source: UIT

La priorité accordée à la cybersécurité dans le cadre des infrastructures critiques et de la résilience se reflète non seulement dans les engagements budgétaires, mais aussi dans les stratégies nationales de cybersécurité. Les stratégies nationales de cybersécurité traitent plus souvent des infrastructures critiques et/ou de la résilience en matière de cybersécurité. Cependant, de nombreux pays n'abordent ni l'une ni l'autre.

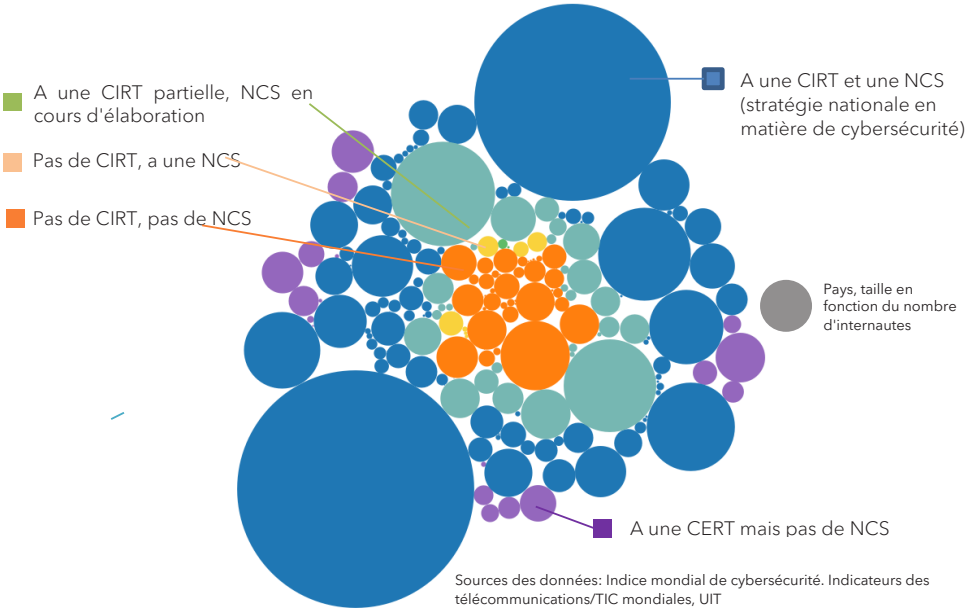
Figure 10: Internautes (selon la couverture d'une équipe CIRT et d'une stratégie nationale de cybersécurité)



Source: Indice mondial de la cybersécurité, indicateurs des télécommunications/TIC dans le monde de l'UIT

Si l'on considère les pays du monde entier en fonction du nombre d'internautes, plus de 95% des internautes se trouvent dans des pays disposant à la fois d'une stratégie nationale de cybersécurité et d'une CIRT nationale.

Figure 11: Taille de la population non connectée (selon la couverture d'une équipe CIRT et d'une stratégie nationale de cybersécurité)



Source: Indice mondial de la cybersécurité, indicateurs des télécommunications/TIC dans le monde de l'UIT

Cependant, les pays les moins connectés sont souvent dépourvus d'une stratégie nationale de cybersécurité et/ou d'une CIRT nationale. Neuf pour cent de la population non connectée vit dans des pays dépourvus de CIRT nationale ou de stratégie nationale de cybersécurité, tandis

que 15% supplémentaires se trouvent dans des pays dépourvus de stratégie, mais disposant d'une CIRT nationale. Plus de la moitié des pays les moins avancés n'ont pas de CIRT et 60% n'ont pas de stratégie nationale de cybersécurité ou n'ont pas encore commencé à en élaborer une.

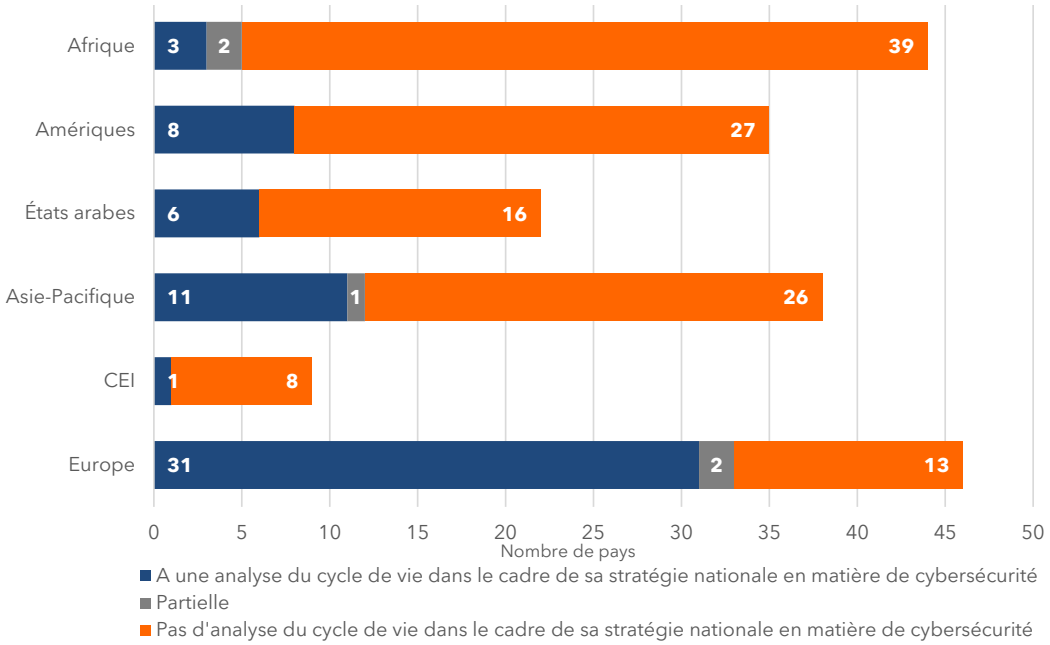
Tableau 1: Nombre de pays disposant d'une stratégie nationale de cybersécurité et d'une équipe CIRT

	Possède une stratégie nationale de cybersécurité	Stratégie nationale de cybersécurité en cours d'élaboration ou >5 ans	Pas de stratégie nationale de cybersécurité
CIRT nationale	90 pays	29	18
Pas de CIRT nationale	7	1	49

Source: UIT

Les pays sans stratégie nationale sont moins susceptibles d'avoir une CIRT. Sans surprise, parmi les 63 pays sans CIRT et les 67 pays sans stratégie nationale de cybersécurité, 49 pays n'ont ni CIRT ni stratégie nationale de cybersécurité.

Figure 12: Évaluation du cycle de vie dans le cadre de la stratégie nationale de cybersécurité

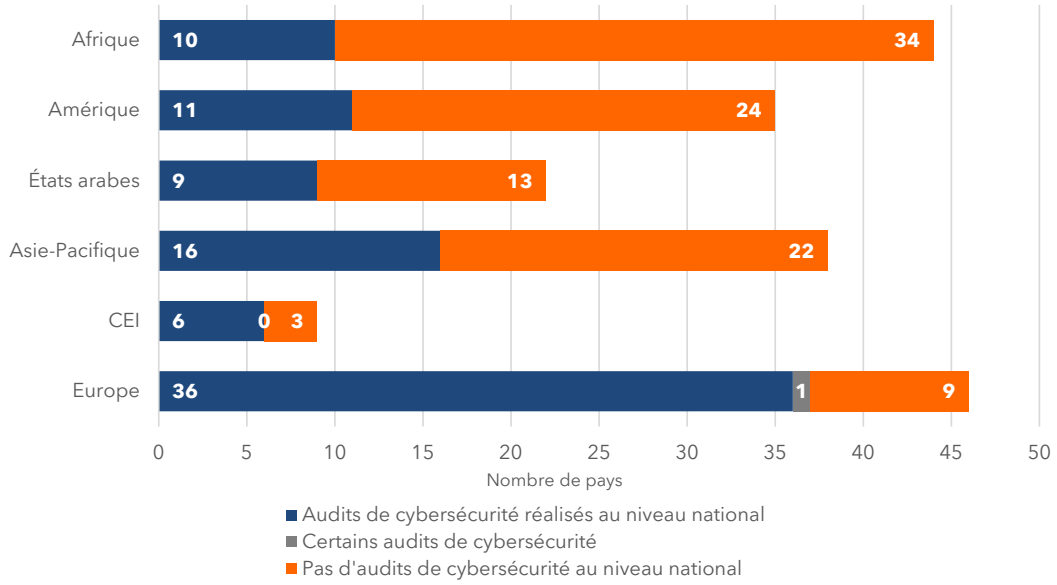


Source: UIT

Disposer d'une stratégie nationale de cybersécurité est une première étape positive pour définir une position en matière de cybersécurité, mais des mises à jour et des révisions régulières sont nécessaires. De nombreux pays qui disposent d'une stratégie nationale de cybersécurité ne la révisent pas et ne la réajustent pas régulièrement en fonction de l'évolution des menaces et des priorités en matière de cybersécurité. Sur les 98 pays qui disposent d'une stratégie

nationale de cybersécurité à jour, seuls 60 intègrent des évaluations du cycle de vie dans le cadre de leur stratégie.

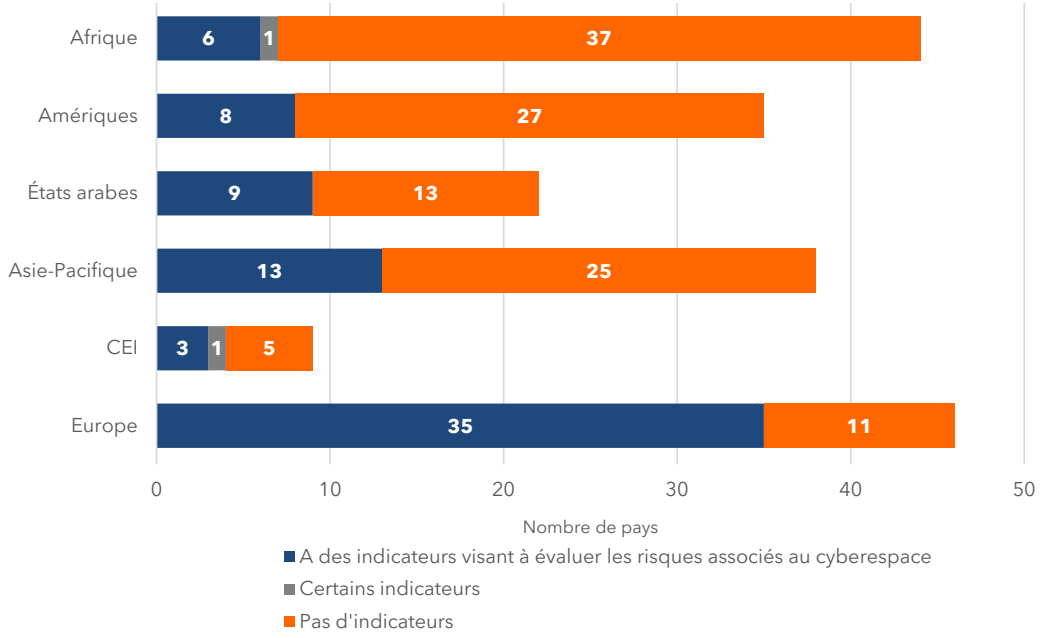
Figure 13: Audits effectués dans le domaine de la cybersécurité au niveau national



Source: UIT

Les audits nationaux de cybersécurité (Figure 13) sont plus courants que les évaluations du cycle de vie. La fréquence de ces audits n'a pas été évaluée dans le cadre de la présente itération de l'ICG.

Figure 14: Indicateurs visant à évaluer les risques liés au cyberespace au niveau national



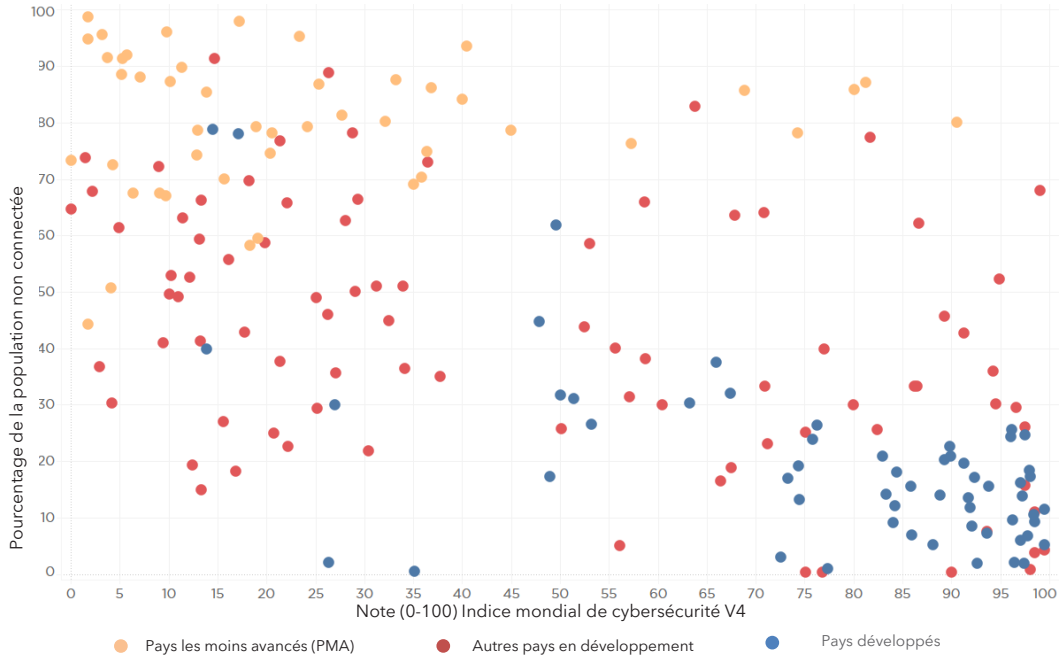
Source: UIT

De même, la plupart des pays ne disposent pas de paramètres pour évaluer les risques liés au cyberespace au niveau national. L'absence de ces paramètres peut rendre plus difficile pour les pays l'évaluation des risques actuels, la hiérarchisation des interventions en matière de cybersécurité et le suivi des progrès.

2.4 Renforcement des capacités en matière de cybersécurité

Le Forum économique mondial estime qu'"environ un million de personnes utilisent Internet pour la première fois chaque jour et que deux tiers de la population mondiale possèdent un appareil mobile"[16]. Si la technologie numérique apporte d'immenses avantages économiques et sociétaux, les cyberrisques peuvent annuler les bénéfices de la numérisation. Il est essentiel de sécuriser le domaine cybernétique par des activités de renforcement des capacités en matière de cybersécurité, car cela contribue à réduire des problèmes comme la fracture numérique et les cyberrisques.

Figure 15: L'indice mondial de cybersécurité et les personnes non connectées



Source: Indice mondial de la cybersécurité, indicateurs des télécommunications/TIC dans le monde de l'UIT

Comme le montre la Figure 15, les pays qui ont tendance à faire moins bien dans l'Indice mondial de cybersécurité sont plus susceptibles de compter parmi les des pays les moins avancés et d'avoir un pourcentage élevé de leur population non connectée. À mesure que cette population commence à être plus connectée, elle a besoin d'un soutien pour renforcer ses capacités en matière de cybersécurité afin de mieux répondre aux menaces. Cependant, de nombreux pays, en particulier les PMA, sont plus susceptibles d'être confrontés à des problèmes de ressources pour combler leur déficit en matière de cybercapacités, notamment un manque de connaissances institutionnelles, des limitations politiques, des pénuries de compétences, entre autres, pour protéger leurs systèmes TIC, à la fois physiquement et virtuellement.

[16] https://reports.weforum.org/global-risks-report-2020/executive-summary/

Plusieurs pays font figure d'exception parmi les pays les moins avancés, comme le Bangladesh, le Bénin, le Rwanda et la Tanzanie, qui ont fait preuve d'un engagement fort en matière de cybersécurité. En particulier, ces pays ont tous déclaré disposer d'une secteur privé national en matière de cybersécurité, une caractéristique essentielle des mesures de renforcement des capacités.

Figure 16: Objectifs de développement durable (8, 9, 10)

Source: ONU (https://sdgs.un.org/goals)

Pour favoriser le travail décent et la croissance économique, construire des infrastructures résilientes, promouvoir une industrialisation inclusive et durable et favoriser l'innovation, tout en réduisant les inégalités au sein des pays et entre eux, le renforcement des capacités en matière de cybersécurité est nécessaire afin de soutenir les processus, les compétences, les ressources et la recherche et développement visant à renforcer les capacités nationales. Les capacités en matière de cybersécurité soutiennent également le développement des capacités collectives et facilitent la coopération et les partenariats internationaux afin de répondre efficacement aux défis de la sécurité numérique liés à la cybernétique.

Les outils et mesures de renforcement des capacités peuvent contribuer à la gestion des cyberrisques, à la protection des citoyens, des infrastructures et des entreprises ainsi qu'à la création de cybercommunautés plus fortes.

Sensibilisation du public à la cybersécurité

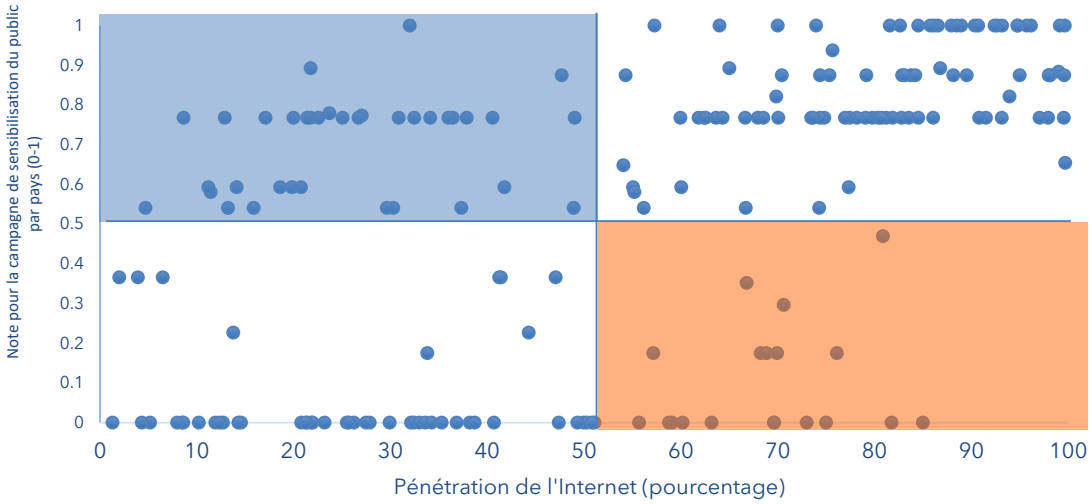
Une sensibilisation efficace à la cybersécurité est essentielle pour que les citoyens, les entreprises, les pouvoirs publics, les jeunes et les organisations restent vigilants. Avec le passage actuel aux services numériques, les pouvoirs publics doivent s'assurer que tous les utilisateurs sont conscients des risques qu'ils encourent en menant des activités numériques.

Lorsque l'on compare les campagnes de sensibilisation du public à la cybersécurité à la pénétration de l'Internet, les pays se répartissent en quatre groupes principaux:

1) faible taux de pénétration de l'Internet/sensibilisation à la cybersécurité (encadré bleu dans la Figure 17): ces pays sont mieux placés pour connecter les personnes non connectées et leur donner les connaissances nécessaires en ligne;
2) faible taux de pénétration de l'Internet/absence de sensibilisation à la cybersécurité: ces pays n'ont pas encore connecté les personnes non connectées et ne proposent pas de ressources de sensibilisation à la cybersécurité;
3) forte taux de pénétration de l'Internet/sensibilisation à la cybersécurité: ces pays sont connectés numériquement et sont engagés dans des activités de sensibilisation à la cybersécurité pour favoriser un comportement sûr en ligne;

4) forte taux de pénétration de l'Internet/absence de sensibilisation à la cybersécurité (case orange de la Figure 17): ces pays sont connectés au numérique, mais leurs populations ne sont pas forcément conscientes des cyberrisques.

Figure 17: Note des campagnes publiques de sensibilisation à la cybersécurité (par pays par rapport à la pénétration de l'Internet)



Source: UIT

Campagne de sensibilisation pour les personnes handicapées et les personnes âgées

Bien que l'Internet et le monde numérique offrent des possibilités sans précédent, le plus souvent il n'est pas tenu compte des personnes handicapées et des personnes âgées lors de la prise de décisions opérationnelles et du choix d'options technologiques. On estime à 752 millions le nombre de personnes âgées de 65 ans ou plus en 2021[17]. Si l'on compare ce chiffre au nombre de pays ayant mené des campagnes de sensibilisation destinées aux personnes handicapées et aux personnes âgées, le résultat est très faible. Sur 194 pays, 18% seulement menaient des campagnes de sensibilisation pour les personnes handicapées et 25% pour les personnes âgées. Le faible nombre de pays engagés dans des campagnes de sensibilisation pour ces deux populations spécifiques est alarmant car il crée une fracture et un fossé numériques profonds, puisque les personnes handicapées et les personnes âgées sont invitées à utiliser des services numériques comme les applications de recherche de contacts COVID-19.

Priorité accrue à la sensibilisation à la cybersécurité des petites et moyennes entreprises (PME), du secteur privé et des pouvoirs publics

Les activités commerciales se sont davantage déplacées en ligne pendant la pandémie de COVID-19, ce qui impose des exigences accrues aux pratiques de cybersécurité du secteur privé. Les PME sont souvent la taille d'entreprise la plus courante dans un pays, puisque 90% des entreprises sont des PME, 50% des emplois proviennent des PME et les PME du secteur formel contribuent jusqu'à hauteur de 40% du PIB dans les économies émergentes[18]. Les PME

[17] https://population.un.org/wpp/DataQuery/
[18] https://www.worldbank.org/en/topic/smefinance

sont aussi souvent les moins à même de gérer les questions liées à la cybersécurité. Les PME ont donc besoin d'activités de sensibilisation à la cybersécurité.

Figure 18: Nombre de pays ayant lancé des campagnes de sensibilisation à la cybersécurité à l'intention des PME, du secteur privé et des organismes publics

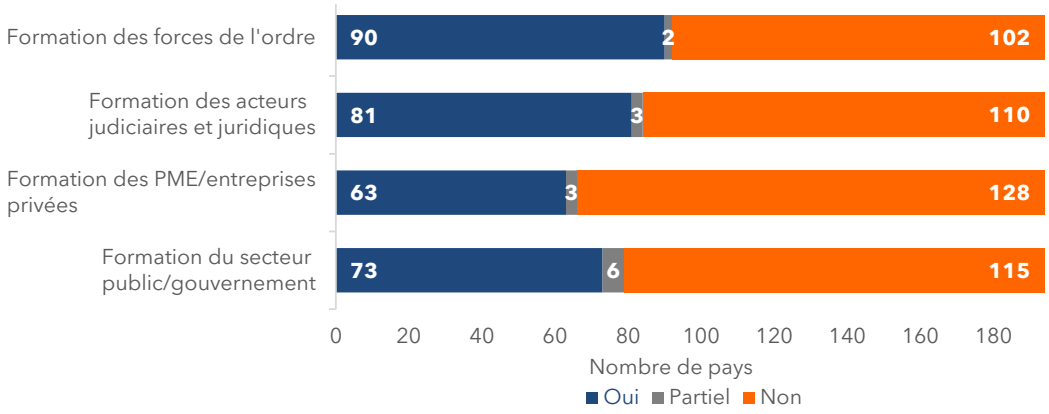
Source: UIT

Les résultats du GCI montrent qu'environ 60% des pays sont, ou ont été au cours des deux dernières années, engagés dans l'amélioration de la sensibilisation aux cyberrisques des PME, des entreprises du secteur privé ou des organismes publics, contre 38% qui n'ont pas signalé de campagne de cybersécurité. Ils se sont engagés en informant le groupe cible sur la sécurité en ligne et les bases de la cybersécurité, en fournissant des ressources, par exemple par le biais de la CIRT nationale ou en proposant des outils pour sécuriser les réseaux. Deux pour cent des pays en sont aux premiers stades de l'élaboration de campagnes ciblant les PME, les entreprises du secteur privé et les organismes publics.

Les gouvernements reconnaissent la nécessité de programmes d'enseignement et de formation sectoriels pour les professionnels de la cybersécurité

Il est de plus en plus important de proposer des programmes de formation pour répondre aux différents besoins du secteur. Les analystes de la cybersécurité prévoient qu'il y aura de 3,5 millions[19] à 4 millions[20] d'emplois dans le secteur de la cybersécurité non pourvus d'ici à 2021. Malgré cet écart attendu, un nombre important de pays doivent encore mettre en place des formations sectorielles et plus de 50% des pays ne disposent pas de programmes adaptés à des secteurs ou à des professions spécifiques comme les forces de l'ordre, les acteurs juridiques, les PME, les entreprises privées et les fonctionnaires.

Figure 19: Nombre de pays disposant de programmes d'enseignement/de formation spécifiques en matière de cybersécurité pour les professionnels



Source: UIT

[19] https://cybersecurityventures.com/jobs/
[20] ESG Research Report: 2019 Digital Work Survey (esg-global.com)

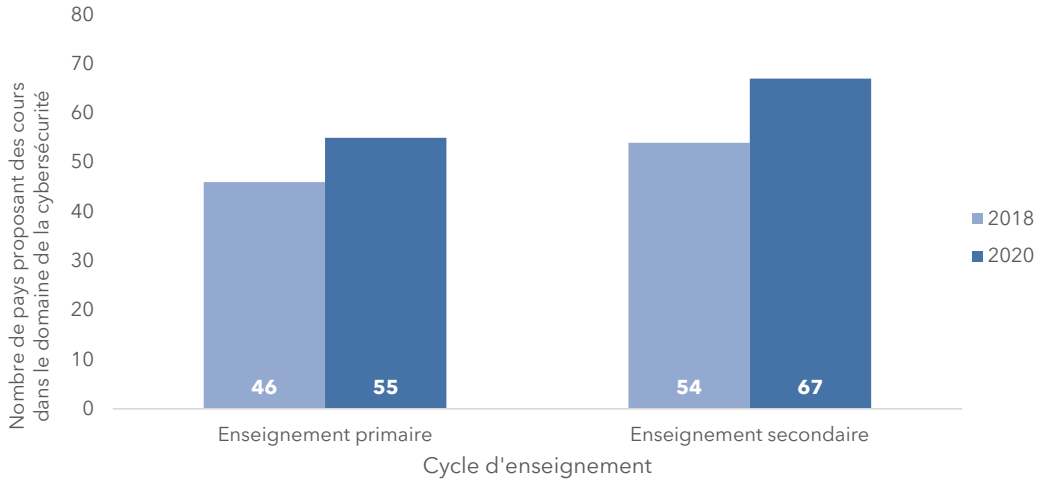
Comme le montre la Figure 19, 46% (90) des pays ont indiqué qu'ils dispensaient une formation à la cybersécurité spécifique à un secteur national aux fonctionnaires du secteur public et des administrations, 41% (81) organisent des exercices de renforcement des capacités sur les questions de cybersécurité pour les professionnels de l'informatique, y compris les PME et le secteur privé, 37% (73) pour les forces de l'ordre, et 32% (63) des pays veillent à ce que les acteurs judiciaires et autres acteurs juridiques ne soient pas laissés pour compte en matière de résilience et de sécurité.

Les pays ont indiqué qu'ils dispensaient ces formations à la cybersécurité par l'intermédiaire de leurs CIRT nationales, de leurs centres nationaux de cybersécurité et de cours approuvés ou avalisés par le gouvernement et dispensés par d'autres institutions régionales et internationales. Certains pays cherchant à augmenter le nombre de professionnels de la cybersécurité, mais n'étant pas en mesure de fournir une formation nationale, ont approuvé une formation internationale fournie par des organismes de certification en cybersécurité comme SANS[21], ISC[2], ICSPA[22] et ISACA[23], entre autres.

Les cours de cybersécurité destinés à l'enseignement primaire et secondaire se généralisent

Les pays ayant évolué vers un enseignement en ligne, des cours sur la sécurité et la cybersécurité en ligne sont dispensés non seulement dans l'enseignement supérieur, mais aussi dans les écoles primaires et secondaires.

Figure 20: Nombre de pays ayant intégré des cours de cybersécurité dans les programmes d'enseignement nationaux (par niveau d'enseignement)



Source: UIT

Comme le montre la Figure 20, les pays intègrent davantage de cours sur la cybersécurité dans les programmes d'enseignement nationaux depuis la publication de l'indice mondial de cybersécurité de 2018. Cinq pour cent de plus de pays, de 46 à 55, proposent des cours d'introduction à la sécurité des enfants sur Internet dans l'enseignement primaire et 7% de plus de pays, de 54 à 67, fournissent des ressources dans les programmes scolaires du secondaire

[21] https://www.sans.org/
[22] https://icspa.org/about-us/
[23] https://www.isaca.org/

pour que les élèves qui souhaitent faire carrière dans la cybersécurité commencent à s'y intéresser dès le plus jeune âge.

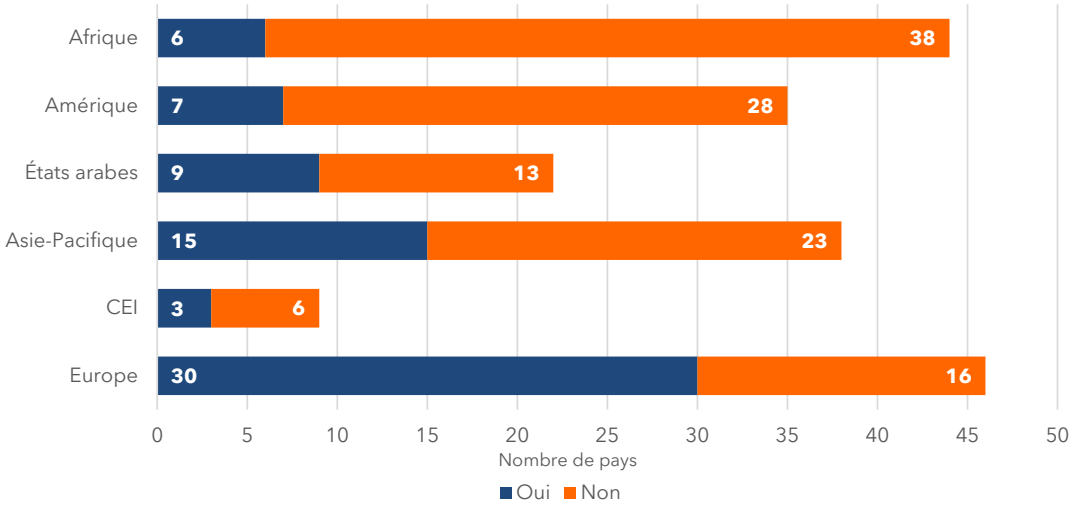
Les incitations gouvernementales pour le développement de la cybersécurité sont à la traîne

L'encouragement de la cybersécurité au niveau national doit s'accompagner de la promotion d'une culture de la cybersécurité, en favorisant un changement d'attitude chez les chefs d'entreprise, qui ne considèrent plus la cybersécurité comme un problème lié aux technologies de l'information, mais adoptent une vision plus globale qui valorise le rôle de la cybersécurité dans l'amélioration de l'efficacité et des performances globales des entreprises. La prééminence de la cybersécurité au sein des organisations est un processus qui nécessite la disponibilité d'infrastructures et de mécanismes pour encourager l'adoption de la cybersécurité. Les pays qui favorisent le développement de la cybersécurité dans le secteur privé et encouragent la création d'entreprises liées à la cybersécurité se distinguent par l'intégration d'incitations dans leur cadre de cybersécurité.

Les pays peuvent favoriser l'adoption de la cybersécurité dans le secteur privé par le biais de mécanismes incitatifs comme des incitations fiscales fondées sur des paramètres de cybersécurité, des exonérations fiscales ou l'inclusion de normes de cybersécurité dans les contrats. Ces mesures encourageront les acteurs du secteur privé à donner la priorité à la cybersécurité dans les structures et les processus opérationnels, ce qui permettra d'améliorer le dispositif de cybersécurité d'un pays à court, moyen et long terme.

Toutefois, la présente édition du GCI montre que 124 pays n'ont créé aucune incitation à la cybersécurité, ce qui montre la nécessité pour les États Membres d'adopter de tels encouragements pour accélérer la mise en œuvre de mesures de cybersécurité.

Figure 21: Nombre de pays disposant d'un mécanisme d'incitation au renforcement des capacités en matière de cybersécurité



Source: UIT

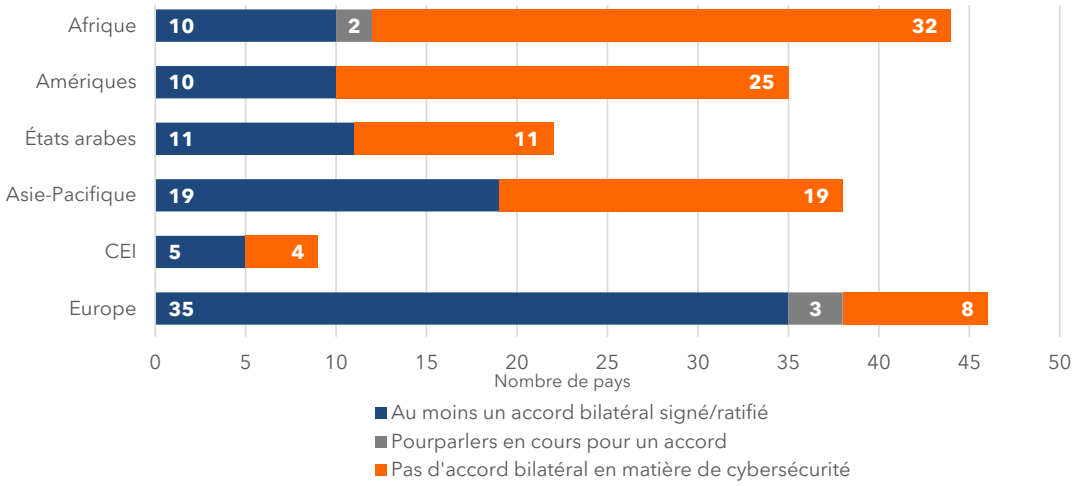
2.5 Mesures de coopération: Aborder l'action collective en matière de cybersécurité

De plus en plus, les risques de cybersécurité ne connaissent pas de frontière[24] et la collaboration reste un outil essentiel pour relever ces défis. La cybersécurité demeure une question transnationale en raison de l'interconnexion croissante et de la corrélation des infrastructures. La sécurité du cyberécosystème mondial ne peut être garantie ou gérée par une seule partie prenante et elle nécessite une coopération nationale, régionale et internationale pour étendre sa portée et ses effets. Dans ce pilier de la coopération, le questionnaire a rassemblé les pays ayant un accord bilatéral ou multilatéral et ceux engagés dans des partenariats interinstitutions et public-privé. Les objectifs classiques de la coopération en matière de cybersécurité sont l'harmonisation des mesures de sécurité minimales, le partage des informations et des bonnes pratiques et la codification des normes de comportement.

Accords bilatéraux et multilatéraux

Les accords bilatéraux et multilatéraux sont essentiels pour codifier les normes et les comportements et renforcer la coopération internationale en matière de cybersécurité.

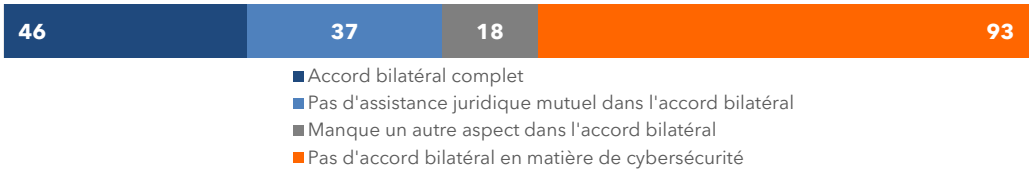
Figure 22: Pays parties à des accords bilatéraux en matière de cybersécurité



Les données extraites montrent que 90 pays ont conclu un accord bilatéral en matière de cybersécurité. Concernant les accords suivis dans le GCI, on constate que certains pays concluent des accords de cybersécurité dans le domaine du renforcement des capacités. Dans certains cas, l'accord porte uniquement sur le partage de renseignements, la cybersécurité n'étant pas toujours l'élément central de l'accord mais faisant partie d'autres sujets. Pour 37 pays, les accords bilatéraux comprennent à la fois des mesures de partage de renseignements et de renforcement des capacités mais ne portent pas sur l'entraide judiciaire.

[24] https://risk.lexisnexis.com/global/en/insights-resources/infographic/cybercrime-report-infographic-july-december-2019

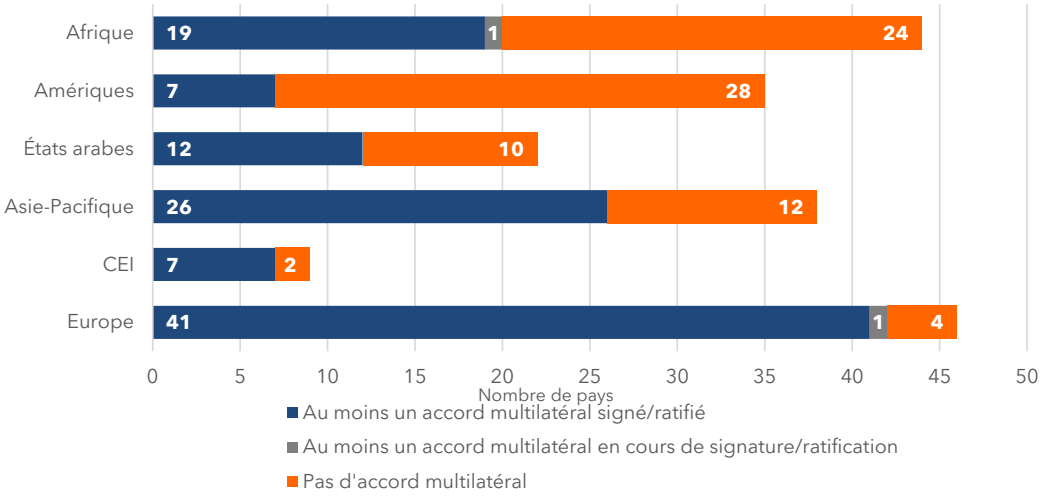
Figure 23: Pays ayant conclu un accord bilatéral en matière de cybersécurité (par thèmes couverts)



Source: UIT

Compte tenu du problème en matière d'action collective que pose la cybersécurité, certains pays se sont efforcés d'assurer la signature non seulement d'accords bilatéraux, mais aussi d'accords multilatéraux. Pour la présente itération de l'Indice mondial de cybersécurité, les accords multilatéraux sont ceux conclus entre trois parties ou plus, y compris les gouvernements et les organisations régionales, mais à l'exclusion des conventions internationales comme la Convention de Budapest sur la cybercriminalité.

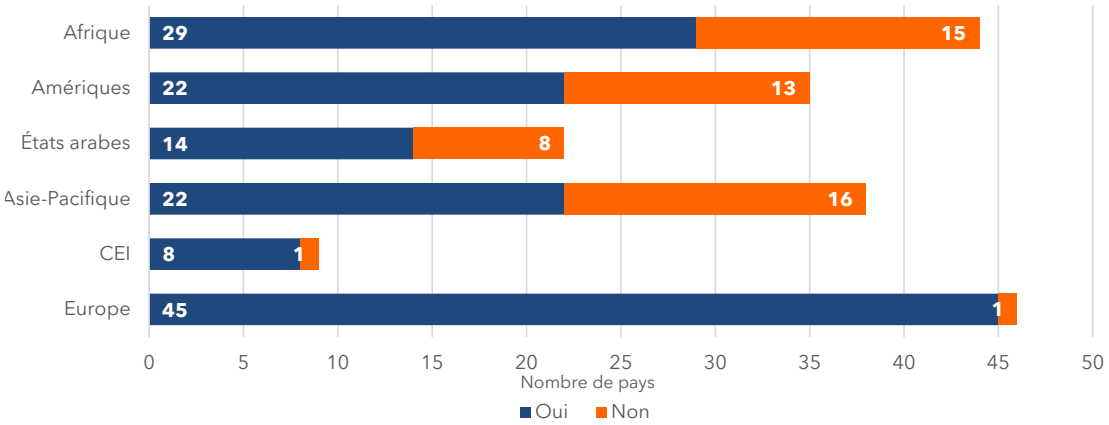
Figure 24: Nombre de pays parties à des accords multilatéraux en matière de cybersécurité (signés et ratifiés)



Source: UIT

Les pays sont plus susceptibles d'avoir un accord multilatéral qu'un accord bilatéral, avec près de 57% des pays ayant signé un accord multilatéral contre 46% des pays ayant signé un accord bilatéral. En outre, de nombreux pays (99) ont signé ou ratifié un accord multilatéral sur le partage de l'information et le renforcement des capacités.

Figure 25: Participation à des activités internationales



Source: UIT

Au-delà de la coopération officielle entre deux ou plusieurs pays, la participation à des activités internationales permet aux pays de comprendre les bonnes pratiques et les nouvelles méthodes pour faire face aux menaces de cybersécurité. Au cours des deux dernières années, 140 pays ont participé à des activités internationales telles que des conférences, des ateliers, des partenariats et des conventions sur la cybersécurité avec d'autres pays.

Partenariats entre le secteur public et le secteur privé

Au-delà de la collaboration avec d'autres pays, les pays collaborent avec des acteurs du secteur privé. Les partenariats entre le secteur public et le secteur privé (PPP) sont essentiels aux efforts de cybersécurité, qu'il s'agisse du partage de renseignements exploitables, de l'échange de bonnes pratiques ou de la communication des besoins et des priorités en matière de recherche et développement. Le Tableau 2 présente le nombre de pays participant à des PPP internationaux et/ou nationaux.

Tableau 2: Pays participant à des PPP internationaux et/ou nationaux

	PPP international	PPP international en cours de réalisation	Pas de PPP international
PPP national	62	0	14
PPP national en cours de réalisation	1	0	0
Pas de PPP national	12	1	104

Source: UIT

Pour participer à l'écosystème de la cybersécurité au sens large, certains pays ont organisé des conférences et des ateliers, tandis que d'autres ont chargé des entreprises du secteur privé de mettre au point des formations pour le secteur public. Un nombre croissant de pays ont déclaré avoir créé des parcs scientifiques et technologiques pour renforcer leur écosystème de cybersécurité. Ces plates-formes peuvent servir de lieu de rencontre entre les secteurs privé et public et permettre de dispenser des formations, d'organiser des ateliers, d'aider les jeunes entreprises et d'accueillir des concours. Ce type d'initiative intersectorielle vise à

créer un écosystème de cybersécurité, en partageant les connaissances et les compétences des différentes parties prenantes, qu'il s'agisse de chercheurs, d'étudiants, d'experts en cybersécurité, de start-up, d'institutions gouvernementales ou d'entreprises étrangères. Les données recueillies et rassemblées montrent que près de la moitié des pays ont au moins un type de partenariat, avec 86 pays participant, ou sur le point de participer, à un PPP international ou national, 60 d'entre eux étant engagés à la fois dans des partenariats nationaux et internationaux.

2.6 Protection en ligne des enfants

Figure 26: Rapports de la série de l'UIT sur la protection en ligne des enfants

Source: UIT

Comme l'indiquent les lignes directrices de l'UIT sur la protection en ligne des enfants, cette protection est un défi mondial qui nécessite une approche mondiale[25]. Les lignes directrices sont arrivées à un moment où l'apprentissage à distance a signifié que les enfants sont plus souvent en ligne que jamais, et les enfants sont plus exposés aux risques pendant la pandémie de COVID-19. Contrairement aux générations précédentes qui ont été poussées à l'apprentissage à distance par la radio en raison de pandémies[26], les technologies numériques ont permis de créer des expériences éducatives interactives et bidirectionnelles qui favorisent non seulement la connexion entre les élèves et le matériel pédagogique, mais aussi entre eux.

Les lignes directrices de l'UIT sur la protection en ligne des enfants ont été conçues pour aider les enfants, les parents et les éducateurs à gérer les risques en ligne, tout en profitant du potentiel de la technologie numérique et en renforçant leurs compétences numériques. En outre, les lignes directrices fournissent également des recommandations aux décideurs pour accélérer la création et l'adoption de stratégies nationales efficaces de protection en ligne des enfants et de plans d'action, ainsi que pour favoriser la participation du secteur privé à l'élaboration de ces politiques.

À cet égard, les questions relatives à la protection en ligne des enfants permettent d'évaluer dans quelle mesure les pays se sont préparés à la génération numérique, grâce à plusieurs éléments

25 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx
26 https://www.washingtonpost.com/education/2020/04/03/chicago-schools-closed-during-1937-polio-epidemic-kids-learned-home-over-radio/

comme les lois existantes pour protéger les enfants en ligne, le mécanisme de notification des problèmes en ligne, les campagnes de sensibilisation et les programmes scolaires. Elles permettent aussi de recenser les pays qui ont créé et suivent une stratégie pour protéger les enfants en ligne.

Figure 27: Pays disposant d'une stratégie de protection en ligne des enfants

Source: UIT

D'après le questionnaire, 86 pays sur 194 ont déclaré avoir pris des mesures pour protéger les enfants en ligne. Toutefois, les données recueillies montrent que seuls 13% des 194 pays disposent d'une stratégie autonome consacrée à la protection en ligne des enfants. En revanche, 30% ont des initiatives de protection en ligne des enfants intégrées dans des stratégies, des législations ou des initiatives plus larges sur la cybercriminalité.

Les résultats montrent également que la région Europe obtient de bons résultats en matière de protection en ligne des enfants, 89% des pays ayant pleinement mis en œuvre des lois relatives à la protection en ligne des enfants. En outre, 101 mécanismes de signalement ont été enregistrés dans le monde, y compris des lignes d'assistance, des sites web, des adresses électroniques et des réseaux sociaux, et 81 pays sont allés plus loin en partageant leurs stratégies de protection en ligne des enfants et des initiatives plus larges.

2.7 Conclusion

La cybersécurité fait l'objet d'une évolution constante des comportements et des pratiques. Qu'il s'agisse d'une urgence sanitaire mondiale, du changement climatique, du vieillissement des populations ou d'un autre défi futur, les technologies numériques offrent un outil séduisant pour faire avancer le monde. Lorsque les objectifs de développement durable (ODD) seront atteints en 2030, 90% de la population mondiale prévue, soit 7,5 milliards de personnes, seront en ligne[27], avec un nombre estimé de 24,1[28] à 125 milliards[29] de dispositifs IoT (Internet des objets) connectés. Pour que les efforts déployés dans le cadre des ODD soient soutenus, la cybersécurité sera nécessaire pour garantir que les solutions numériques sont sûres, fiables et dignes de confiance.

L'un des enseignements de la pandémie de COVID-19 est que les problèmes d'action collective, comme la santé ou la cybersécurité, doivent être abordés selon une méthode interdisciplinaire et globale. Pour mettre en œuvre tous les piliers du GCI – mesures juridiques, techniques,

27 https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/
28 https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devices-in-2030--generating-1-5-trillion-annual-revenue-301061873.html
29 https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

organisationnelles, de renforcement des capacités et de coopération – il faudra connecter les individus entre eux et instaurer la confiance. Au-delà de la collaboration à l'intérieur des pays, ces derniers devront peut-être soutenir d'autres États moins à même de relever les défis de la cybersécurité, comme les pays les moins avancés, les petits États insulaires en développement et les pays en développement sans littoral.

Pour aller de l'avant, les pays doivent se pencher sur leurs forces et leurs faiblesses en matière de cybersécurité et tirer parti de leurs avantages concurrentiels pour promouvoir la cybercapacité et la santé en général. L'indice mondial de cybersécurité peut aider les pays à entamer ce processus. Pour le poursuivre, les pays peuvent avoir besoin d'envisager:

- des évaluations régulières de leurs engagements en matière de cybersécurité, y compris des indicateurs cohérents;
- le développement continu des CIRT nationales et la poursuite de la mise en place de CIRT sectorielles;
- le suivi et la mise à jour des stratégies nationales de cybersécurité avec des plans de mise en œuvre clairs;
- l'inclusion et la diversité, notamment des groupes sous-représentés tels que les femmes et les jeunes, au sein de la main-d'œuvre du secteur de la cybersécurité;
- la participation régulière à des activités internationales pour partager les bonnes pratiques, les études de cas et améliorer la capacité de préparation et de réaction;
- l'amélioration de la capacité en matière de cybersécurité des micro, petites et moyennes entreprises (MPME); et
- des échanges réguliers avec tous les acteurs concernés par la cybersécurité, y compris le secteur privé, les établissements universitaires et la société civile.

3 Résultats du GCI: notes et classement

3.1 Notes et classement des pays au niveau mondial

Le tableau suivant présente la note et le classement de chaque pays qui a répondu au questionnaire.

Tableau 3: Résultats du GCI: notes et classement au niveau mondial

Nom du pays	Note	Classement
États-Unis d'Amérique **	100	1
Royaume-Uni	99,54	2
Arabie saoudite	99,54	2
Estonie	99,48	3
Corée (Rép. de)	98,52	4
Singapour	98,52	4
Espagne	98,52	4
Fédération de Russie	98,06	5
Émirats arabes unis	98,06	5
Malaisie	98,06	5
Lituanie	97,93	6
Japon	97,82	7
Canada**	97,67	8
France	97,6	9
Inde	97,5	10
Turquie	97,49	11
Australie	97,47	12
Luxembourg	97,41	13
Allemagne	97,41	13
Portugal	97,32	14
Lettonie	97,28	15
Pays-Bas**	97,05	16
Norvège**	96,89	17
Maurice	96,89	17
Brésil	96,6	18
Belgique	96,25	19
Italie	96,13	20

Nom du pays	Note	Classement
Oman	96,04	21
Finlande	95,78	22
Égypte	95,48	23
Indonésie	94,88	24
Viet Nam	94,59	25
Suède	94,55	26
Qatar	94,5	27
Grèce	93,98	28
Autriche	93,89	29
Pologne	93,86	30
Kazakhstan	93,15	31
Danemark	92,6	32
Chine	92,53	33
Croatie	92,53	33
Slovaquie	92,36	34
Hongrie	91,28	35
Israël**	90,93	36
Tanzanie	90,58	37
Macédoine du Nord	89,92	38
Serbie	89,8	39
Azerbaïdjan	89,31	40
Chypre	88,82	41
Suisse**	86,97	42
Ghana	86,69	43
Thaïlande	86,5	44
Tunisie	86,23	45
Irlande	85,86	46

(suite)

Nom du pays	Note	Classement
Nigéria	84,76	47
Nouvelle-Zélande**	84,04	48
Malte	83,65	49
Maroc	82,41	50
Kenya	81,7	51
Mexique	81,68	52
Bangladesh	81,27	53
Iran (République islamique d')	81,07	54
Géorgie	81,06	55
Bénin	80,06	56
Rwanda	79,95	57
Islande	79,81	58
Afrique du Sud**	78,46	59
Bahreïn	77,86	60
Philippines	77	61
Roumanie	76,29	62
Moldova	75,78	63
Uruguay	75,15	64
Koweït	75,07	65
Rép. dominicaine	75,05	66
Slovénie	74,93	67
République tchèque	74,37	68
Monaco	72,57	69
Ouzbékistan	71,11	70
Jordanie	70,96	71
Ouganda	69,98	72
Zambie	68,88	73
Chili	68,83	74
Côte d'Ivoire	67,82	75
Costa Rica	67,45	76
Bulgarie	67,38	77
Ukraine	65,93	78
Pakistan	64,88	79
Albanie	64,32	80
Colombie	63,72	81
Cuba	58,76	82
Sri Lanka	58,65	83
Paraguay	57,09	84
Brunéi Darussalam	56,07	85
Pérou	55,67	86
Monténégro	53,23	87
Botswana	53,06	88
Bélarus	50,57	89
Arménie**	50,47	90
Argentine	50,12	91
Kirghizistan	49,64	92
Cameroun	45,63	93
Népal (République du)	44,99	94
Tchad	40,44	95
Burkina Faso**	39,98	96
Malawi	36,83	97
Zimbabwe	36,49	98
Myanmar	36,41	99
Sénégal	35,85	100
Liechtenstein**	35,15	101
Soudan	35,03	102
Panama	34,11	103
Algérie	33,95	104
Togo	33,19	105
Jamaïque**	32,53	106
Gambie	32,12	107
Suriname	31,2	108
Liban**	30,44	109
Bosnie-Herzégovine	29,44	110
Samoa	29,33	111
Fidji	29,08	112
Libye	28,78	113
Guyana	28,11	114
Éthiopie	27,74	115
Venezuela	27,06	116
Andorre**	26,38	117
Papouasie-Nouvelle-Guinée**	26,33	118
Équateur	26,3	119

(suite)

Nom du pays	Note	Classement
Mongolie	26,2	120
Sierra Leone	25,31	121
État de Palestine	25,18	122
Mozambique	24,18	123
Madagascar**	23,33	124
Trinité-et-Tobago	22,18	125
République arabe syrienne**	22,14	126
Nauru**	21,42	127
Tonga**	20,95	128
Iraq**	20,71	129
Guinée**	20,53	130
R.d.p. Lao	20,34	131
Cambodge**	19,12	132
Mauritanie	18,94	133
Bhoutan	18,34	134
Eswatini	18,23	135
Cabo Verde	17,74	136
Somalie	17,25	137
Tadjikistan**	17,1	138
Barbade	16,89	139
Bolivie (État pluri-national de)	16,14	140
Sao Tomé-et-Principe	15,64	141
Antigua-et-Barbuda	15,62	142
Congo (Rép. du)**	14,72	143
Turkménistan**	14,48	144
Kiribati	13,84	145
San Marin	13,83	146
Bahamas	13,37	147
El Salvador**	13,3	148
Seychelles**	13,23	149
Guatemala	13,13	150
Angola	12,99	151
Vanuatu	12,88	152
Saint-Christophe-et-Niévès**	12,44	153
Saint-Vincent-et-les-Grenadines**	12,18	154
Namibie	11,47	155
Niger	11,38	156
Gabon	11,36	157
Sainte-Lucie**	10,96	158
Belize	10,29	159
Mali**	10,14	160
Guinée-Bissau	9,85	161
Libéria	9,72	162
Grenade	9,41	163
Lesotho	9,08	164
Nicaragua**	9	165
Îles Salomon	7,08	166
Haïti	6,4	167
Tuvalu**	5,78	168
Soudan du Sud**	5,75	169
Rép. dém. du Congo	5,3	170
Afghanistan	5,2	171
Îles Marshall**	4,9	172
Timor-Leste**	4,26	173
Dominique	4,2	174
Comores**	3,72	175
République centra-fricaine**	3,24	176
Maldives**	2,95	177
Honduras**	2,2	178
Djibouti	1,73	179
Burundi	1,73	179
Érythrée**	1,73	179
Guinée équato-riale**	1,46	180
Rép. pop. dém. de Corée**	1,35	181
Micronésie*	0	182
Vatican*	0	182
Yémen*	0	182

* aucune donnée recueillie
** pas de réponse au questionnaire

3.2 Notes et classement des pays au niveau régional

Tableau 4: Résultats du GCI: région Afrique

Nom du pays	Note globale	Classement régional
Maurice	96,89	1
Tanzanie	90,58	2
Ghana	86,69	3
Nigéria	84,76	4
Kenya	81,7	5
Bénin	80,06	6
Rwanda	79,95	7
Afrique du Sud **	78,46	8
Ouganda	69,98	9
Zambie	68,88	10
Côte d'Ivoire	67,82	11
Botswana	53,06	12
Cameroun	45,63	13
Tchad	40,44	14
Burkina Faso**	39,98	15
Malawi	36,83	16
Zimbabwe	36,49	17
Sénégal	35,85	18
Togo	33,19	19
Gambie	32,12	20
Éthiopie	27,74	21
Sierra Leone	25,31	22
Mozambique	24,18	23
Madagascar	23,33	24
Guinée**	20,53	25
Eswatini	18,23	26
Cabo Verde	17,74	27
Sao Tomé-et-Principe	15,64	28
Congo (Rép. du)**	14,72	29
Seychelles**	13,23	30
Angola	12,99	31
Namibie	11,47	32
Niger	11,36	33
Gabon	11,38	34
Mali**	10,14	35
Guinée-Bissau	9,85	36
Libéria	9,72	37
Lesotho	9,08	38
Soudan du Sud **	5,75	39
Rép. dém. du Congo	5,3	40
République centrafricaine**	3,24	41
Burundi	1,73	42
Érythrée**	1,73	42
Guinée équatoriale**	1,46	43

* pas de données
** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

Tableau 5: Résultats du GCI: région des Amériques

Nom du pays	Note globale	Classement régional
États-Unis d'Amérique**	100	1
Canada**	97,67	2
Brésil	96,6	3
Mexique	81,68	4
Uruguay	75,15	5
Rép. dominicaine	75,07	6
Chili	68,83	7
Costa Rica	67,45	8
Colombie	63,72	9
Cuba	58,76	10
Paraguay	57,09	11
Pérou	55,67	12
Argentine	50,12	13
Panama	34,11	14
Jamaïque**	32,53	15
Suriname	31,2	16

Tableau 5: Résultats du GCI: région des Amériques (suite)

Nom du pays	Note globale	Classement régional
Guyana	28,11	17
Venezuela	27,06	18
Équateur	26,3	19
Trinité-et-Tobago	22,18	20
Barbade	16,89	21
Bolivie (État plurinational de)	16,14	22
Antigua-et-Barbuda	15,62	23
Bahamas	13,37	24
El Salvador**	13,3	25
Guatemala	13,13	26
Saint-Christophe-et-Niévès	12,44	27
Saint-Vincent-et-les-Grenadines**	12,18	28
Sainte-Lucie**	10,96	29
Belize	10,29	30
Grenade	9,41	31
Nicaragua	9	32
Haïti	6,4	33
Dominique	4,2	34
Honduras**	2,2	35

* pas de données
** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

Tableau 6: Résultats du GCI: région des États arabes

Nom du pays	Note globale	Classement régional
Arabie saoudite	99,54	1
Émirats arabes unis	98,06	2
Oman	96,04	3
Égypte	95,48	4
Qatar	94,5	5
Tunisie	86,23	6
Maroc	82,41	7
Bahreïn	77,86	8
Koweït	75,05	9
Jordanie	70,96	10
Soudan	35,03	11
Algérie	33,95	12
Liban**	30,44	13
Libye	28,78	14
État de Palestine	25,18	15
République arabe syrienne **	22,14	16
Iraq**	20,71	17
Mauritanie	18,94	18
Somalie	17,25	19
Comores**	3,72	20
Djibouti	1,73	21
Yémen*	0	22

* pas de données
** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

Tableau 7: Résultats du GCI: région Asie-Pacifique

Nom du pays	Note globale	Classement régional
Corée (Rép. de)	98,52	1
Singapour	98,52	1
Malaisie	98,06	2
Japon	97,82	3
Inde	97,49	4
Australie	97,47	5
Indonésie	94,88	6
Viet Nam	94,55	7
Chine	92,53	8
Thaïlande	86,5	9
Nouvelle-Zélande**	84,04	10
Bangladesh	81,27	11
Iran (République islamique d')	81,06	12
Philippines	77	13

Tableau 7: Résultats du GCI: région Asie-Pacifique (suite)

Nom du pays	Note globale	Classement régional
Pakistan	64,88	14
Sri Lanka	58,65	15
Brunéi Darussalam	56,07	16
Népal (République du)	44,99	17
Myanmar	36,41	18
Samoa	29,33	19
Fidji	29,08	20
Papouasie-Nouvelle-Guinée**	26,33	21
Mongolie	26,2	22
Nauru**	21,42	23
Tonga**	20,95	24
R.d.p. Lao	20,34	25
Cambodge**	19,12	26
Bhoutan	18,34	27
Kiribati	13,84	28
Vanuatu	12,88	29
Îles Salomon	7,08	30
Tuvalu**	5,78	31
Afghanistan	5,2	32
Îles Marshall **	4,9	33
Timor-Leste**	4,26	34
Maldives**	2,95	35
Rép. pop. dém. de Corée**	1,35	36
Micronésie*	0	37

* pas de données
** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

Tableau 8: Résultats du GCI: région CEI

Nom du pays	Note globale	Classement régional
Fédération de Russie	98,06	1
Kazakhstan	93,15	2
Azerbaïdjan	89,31	3
Ouzbékistan	71,11	4
Belarus	50,57	5
Arménie**	50,47	6
Kirghizistan	49,64	7
Tadjikistan**	17,1	8
Turkménistan**	14,48	9

* pas de données
** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

Tableau 9: Résultats du GCI: région Europe

Nom du pays	Note globale	Classement régional
Royaume-Uni	99,54	1
Estonie	99,48	2
Espagne	98,52	3
Lituanie	97,93	4
France	97,6	5
Turquie	97,5	6
Luxembourg	97,41	7
Allemagne	97,41	7
Portugal	97,32	8
Lettonie	97,28	9
Pays-Bas**	97,05	10
Norvège**	96,89	11
Belgique	96,25	12
Italie	96,13	13
Finlande	95,78	14
Suède	94,59	15
Grèce	93,98	16
Autriche	93,89	17
Pologne	93,86	18
Danemark	92,6	19
Croatie	92,53	20
Slovaquie	92,36	21
Hongrie	91,28	22
Israël**	90,93	23

Tableau 9: Résultats du GCI: région Europe (suite)

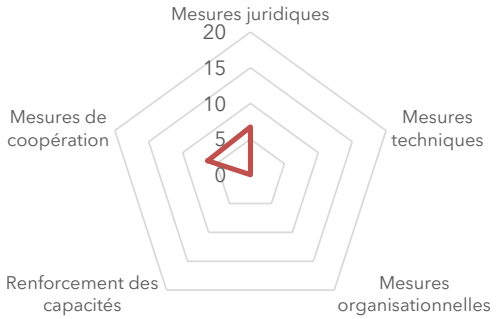
Nom du pays	Note globale	Classement régional
République de Macédoine du Nord	89,92	24
Serbie	89,8	25
Chypre	88,82	26
Suisse**	86,97	27
Irlande	85,86	28
Malte	83,65	29
Géorgie	81,07	30
Islande	79,81	31
Roumanie	76,29	32
Moldova	75,78	33
Slovénie	74,93	34
République tchèque	74,37	35
Monaco	72,57	36
Bulgarie	67,38	37
Ukraine	65,93	39
Albanie	64,32	40
Monténégro	53,23	41
Liechtenstein**	35,15	42
Bosnie-Herzégovine	29,44	43
Andorre**	26,38	44
Saint-Marin	13,83	45
Vatican*	0	46

* pas de données
** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

4 Indice mondial de cybersécurité 2020: Profils par pays

Région Afrique

Angola (République d')



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

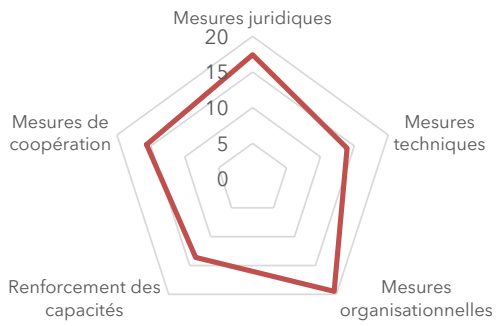
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
12,99	6,70	0,00	0,00	0,00	6,30

Source: Indice mondial de cybersécurité V4, UIT, 2020

Bénin (République du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures organisationnelles

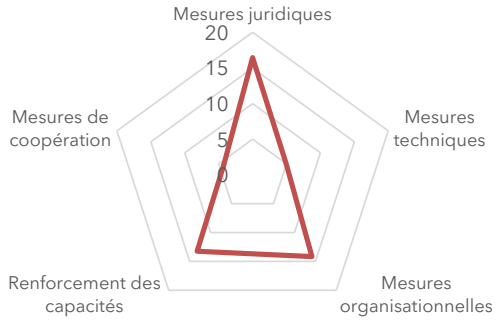
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
80,06	17,42	13,94	19,48	13,60	15,63

Source: Indice mondial de cybersécurité V4, UIT, 2020

Botswana (République du)



Niveau de développement:

Pays en développement, Pays sans littoral

Domaine(s) de force relative

Mesures juridiques

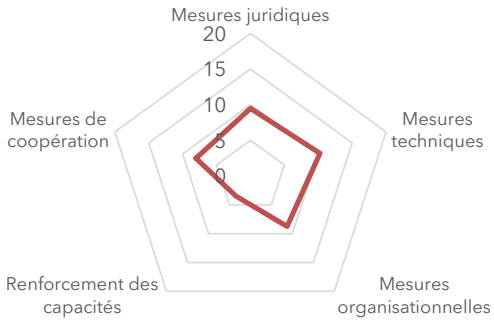
Domaine(s) de croissance potentielle

Mesures de coopération, Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
53,06	16,44	4,95	14,16	13,23	4,26

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Burkina Faso***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), Pays sans littoral

Domaine(s) de force relative

Mesures techniques

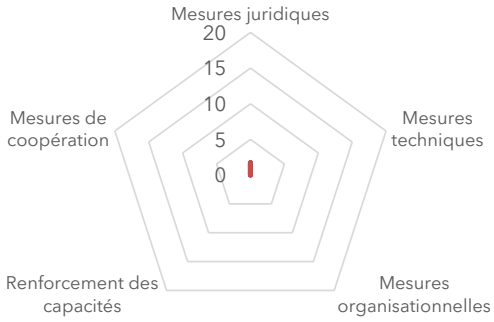
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
39,98	9,47	10,25	8,75	3,47	8,04

Source: Indice mondial de cybersécurité V4, UIT, 2020

Burundi (République du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), Pays sans littoral

Domaine(s) de force relative

Mesures juridiques

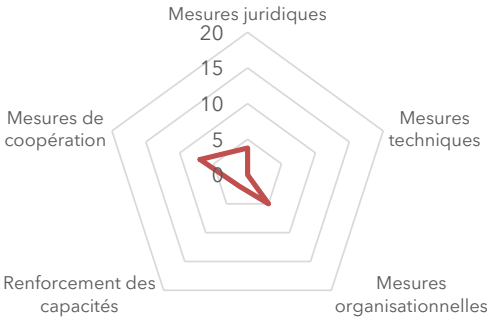
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
1,73	1,73	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Cabo Verde (République du)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération

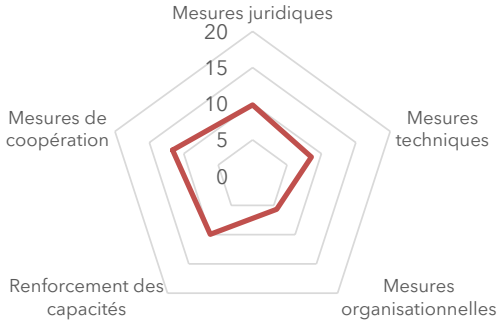
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
17,74	3,77	0,00	5,00	1,96	7,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Cameroun (République du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures de coopération

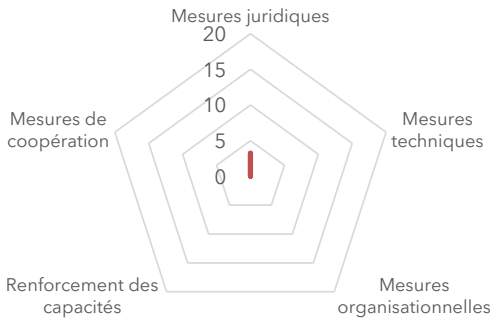
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
45,63	9,84	8,54	5,67	9,95	11,63

Source: Indice mondial de cybersécurité V4, UIT, 2020

*République centrafricaine***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques

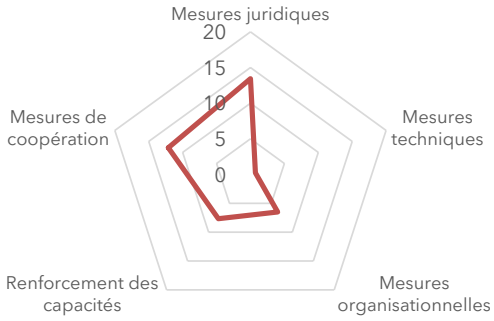
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
3,24	3,24	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Tchad (République du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques

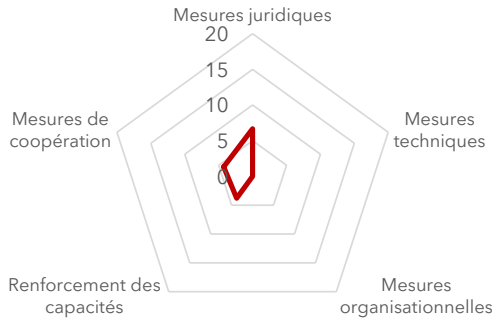
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
40,44	13,43	0,73	6,50	7,67	12,11

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Congo (République du)***



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

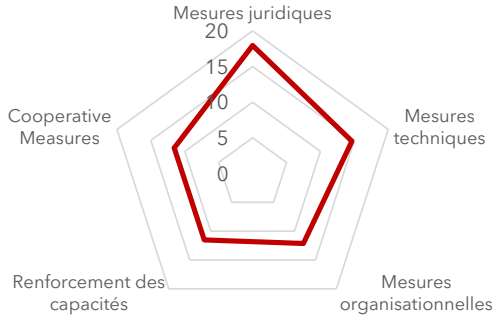
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
14,72	6,66	0,00	0,00	3,80	4,26

Source: Indice mondial de cybersécurité V4, UIT, 2020

Côte d'Ivoire (République de)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

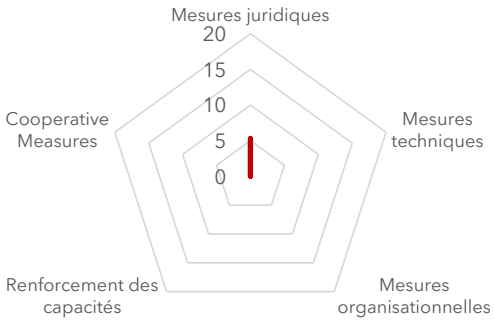
Domaine(s) de croissance potentielle

Renforcement des capacités, mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
67,82	17,95	14,65	12,14	11,53	11,55

Source: Indice mondial de cybersécurité V4, UIT, 2020

République démocratique du Congo



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

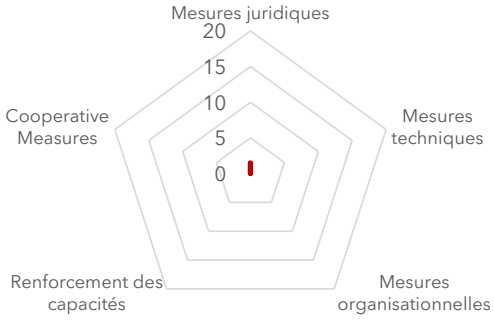
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
5,30	5,30	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Guinée équatoriale (République de)***



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

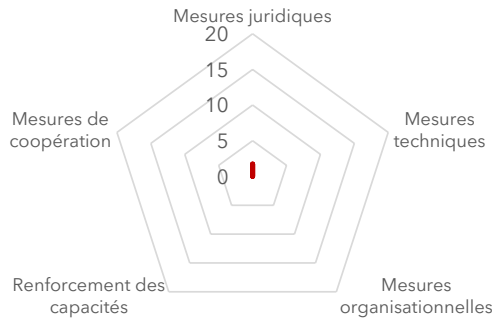
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
1,46	1,46	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Érythrée***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

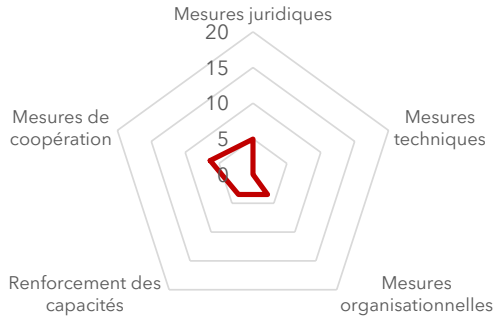
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
1,73	1,73	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Eswatini (Royaume d')



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures de coopération

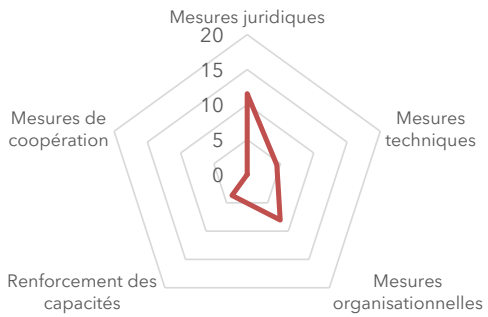
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
18,23	4,96	0,00	3,49	3,47	6,31

Source: Indice mondial de cybersécurité V4, UIT, 2020

Éthiopie (République démocratique d')



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques

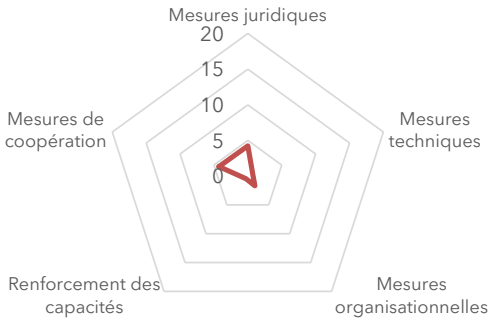
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
27,74	11,56	4,46	8,03	3,69	0,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

République gabonaise



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures de coopération

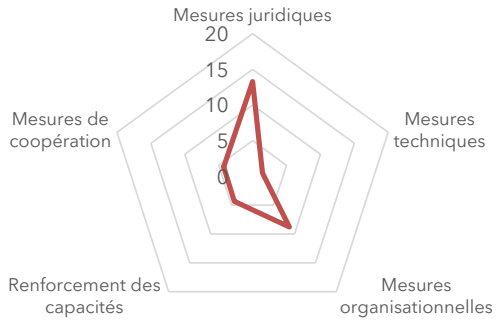
Domaine(s) de croissance potentielle

Mesures techniques, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
11,38	4,24	0,73	1,69	0,46	4,26

Source: Indice mondial de cybersécurité V4, UIT, 2020

Gambie (République de)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

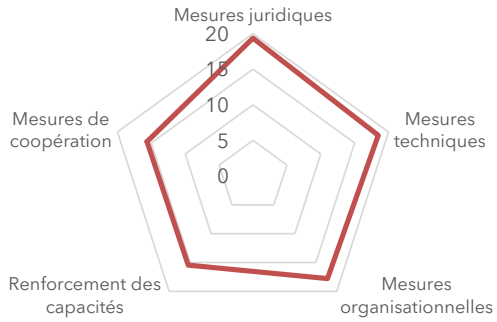
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
32,12	13,28	1,46	8,78	4,34	4,26

Source: Indice mondial de cybersécurité V4, UIT, 2020

Ghana



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, techniques

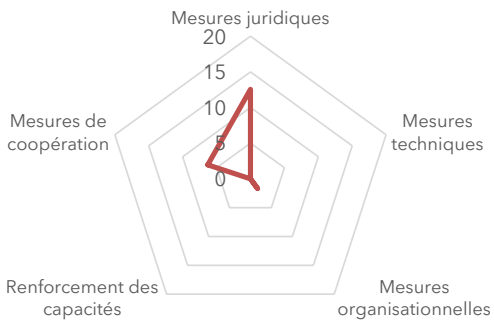
Domaine(s) de croissance potentielle

Renforcement des capacités, Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
86,69	19,35	18,48	17,78	15,44	15,63

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Guinée (République de)***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

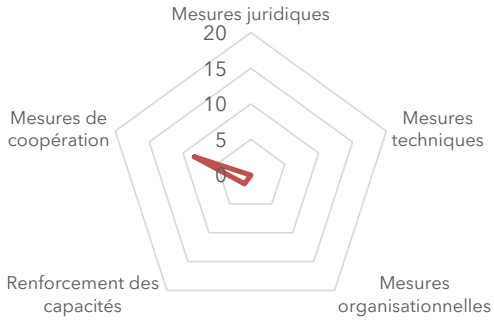
Domaine(s) de croissance potentielle

Mesures techniques, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
20,53	12,54	0,00	1,69	0,00	6,30

Source: Indice mondial de cybersécurité V4, UIT, 2020

Guinée-Bissau (République de)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération

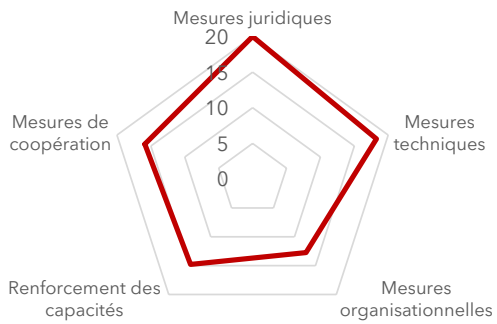
Domaine(s) de croissance potentielle

Mesures juridiques, techniques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
9,85	0,00	0,00	0,00	1,52	8,33

Source: Indice mondial de cybersécurité V4, UIT, 2020

Kenya (République du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, techniques

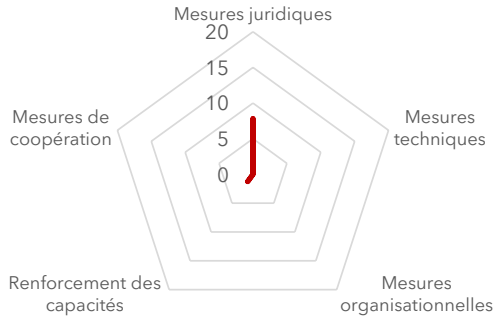
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
81,70	20,00	18,27	12,75	14,79	15,89

Source: Indice mondial de cybersécurité V4, UIT, 2020

Lesotho (Royaume du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), Pays sans littoral

Domaine(s) de force relative

Mesures juridiques

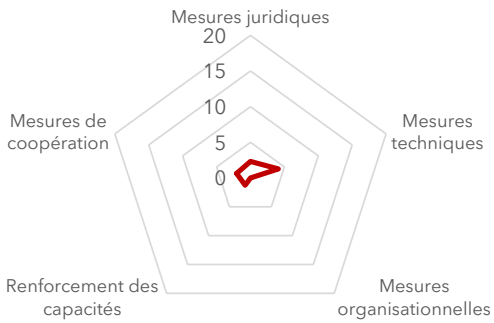
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
9,08	7,82	0,00	0,00	1,26	0,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Libéria (République du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures techniques

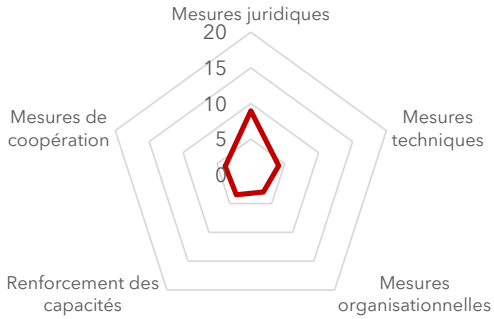
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
9,72	2,31	4,11	0,00	1,26	2,04

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Madagascar (République de)***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

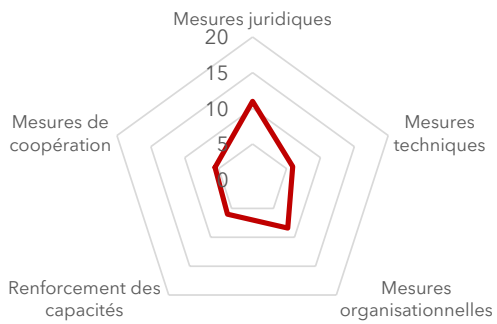
Domaine(s) de croissance potentielle

Mesures organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
23,33	8,96	4,11	3,00	3,47	3,78

Source: Indice mondial de cybersécurité V4, UIT, 2020

Malawi



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques, organisationnelles

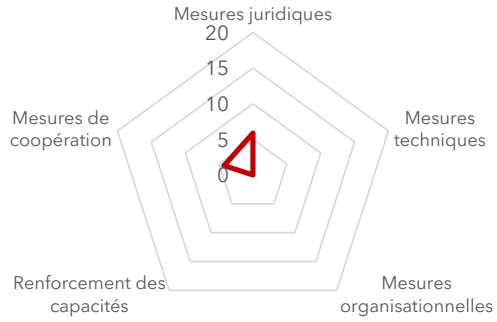
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
36,83	10,98	5,92	8,40	6,00	5,54

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Mali (République du)***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques

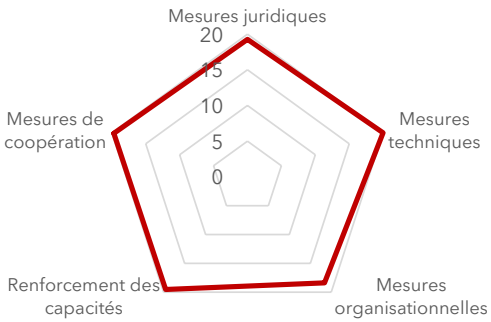
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
10,14	5,89	0,00	0,00	0,00	4,26

Source: Indice mondial de cybersécurité V4, UIT, 2020

Maurice (République de)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures techniques, de coopération, renforcement des capacités

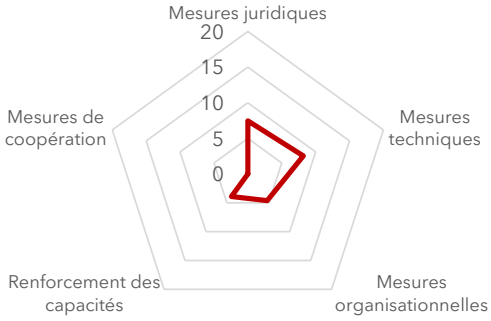
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
96,89	19,27	20,00	18,38	19,54	19,70

Source: Indice mondial de cybersécurité V4, UIT, 2020

Mozambique (République du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures techniques, juridiques

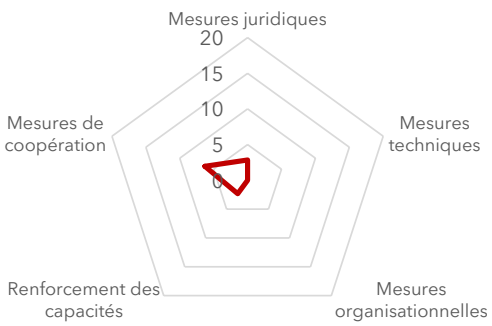
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
24,181	7,46	8,19	4,62	3,92	0,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Namibie (République de)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures de coopération

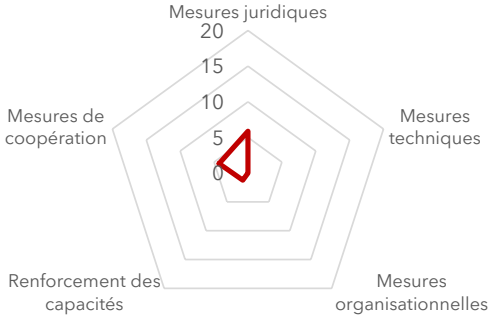
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
11,47	2,84	0,00	0,00	2,34	6,30

Source: Indice mondial de cybersécurité V4, UIT, 2020

Niger (République du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA**),** pays sans littoral

Domaine(s) de force relative

Mesures juridiques, de coopération

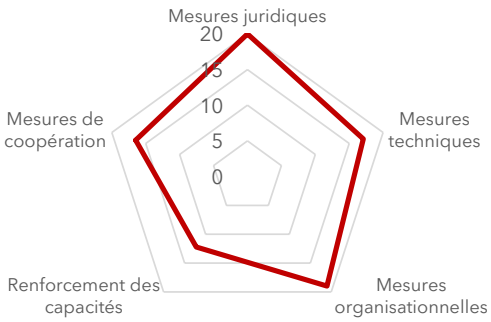
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
11,36	5,87	0,00	0,00	1,23	4,26

Source: Indice mondial de cybersécurité V4, UIT, 2020

Nigéria (République fédérale du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

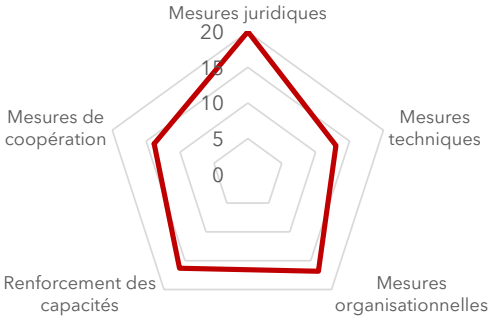
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
84,76	20,00	17,09	18,98	12,21	16,48

Source: Indice mondial de cybersécurité V4, UIT, 2020

Rwanda (République du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques

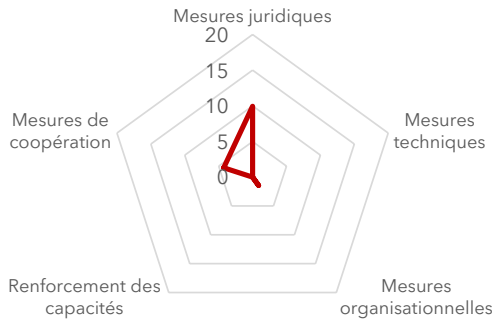
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
79,95	20,00	13,00	16,83	16,30	13,82

Source: Indice mondial de cybersécurité V4, UIT, 2020

Sao Tomé-et-Principe (République démocratique de)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

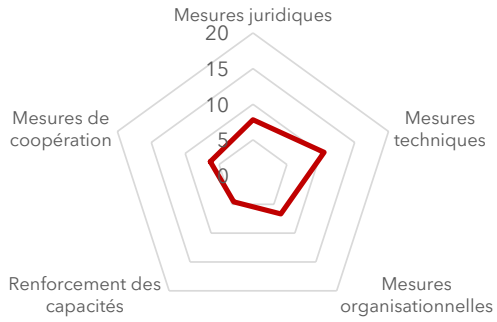
Domaine(s) de croissance potentielle

Mesures techniques, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
15,64	9,94	0,00	1,44	0,00	4,26

Source: Indice mondial de cybersécurité V4, UIT, 2020

Sénégal (République du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures techniques

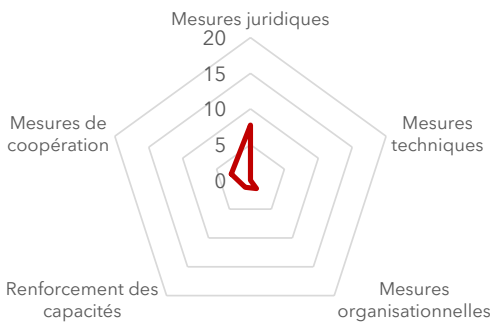
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
35,85	7,82	10,50	6,66	4,58	6,30

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Seychelles (République des)***



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

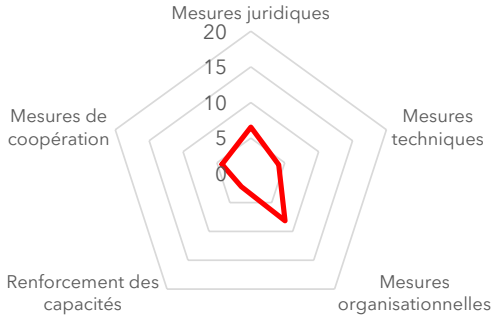
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
13,23	7,73	0,00	1,44	1,23	2,83

Source: Indice mondial de cybersécurité V4, UIT, 2020

Sierra Leone



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures organisationnelles

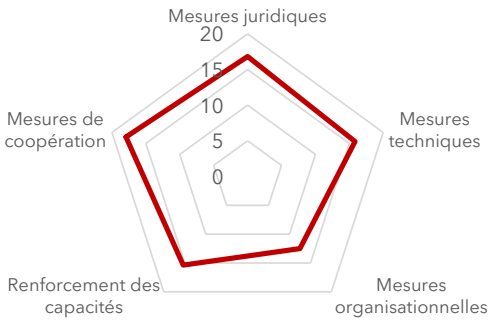
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
25,31	6,54	4,11	8,16	2,24	4,26

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Afrique du Sud (République d')***



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures de coopération

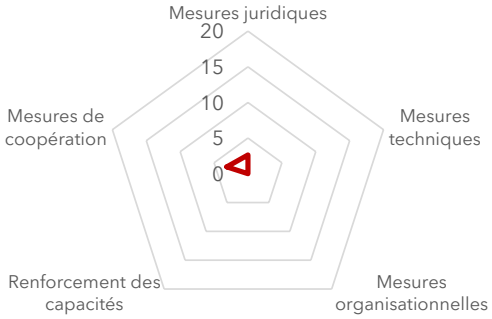
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
78,46	16,82	15,85	12,50	15,37	17,93

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Soudan du Sud (République du)***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures de coopération

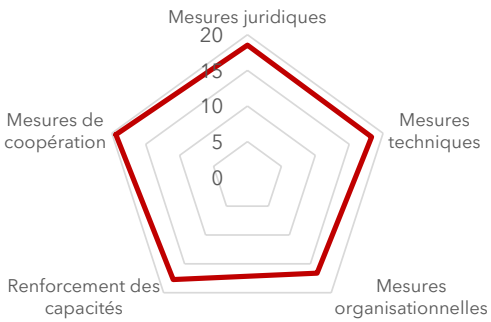
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
5,75	2,63	0,00	0,00	0,00	3,12

Source: Indice mondial de cybersécurité V4, UIT, 2020

Tanzanie (République unie de)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures de coopération

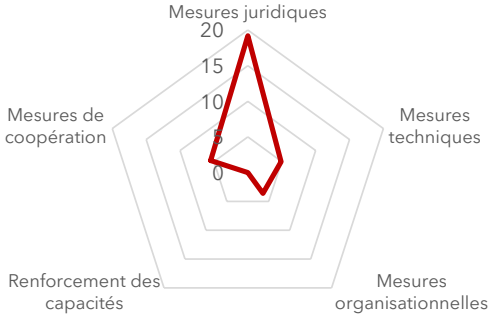
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
90,58	18,54	18,31	16,60	17,72	19,41

Source: Indice mondial de cybersécurité V4, UIT, 2020

République togolaise



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

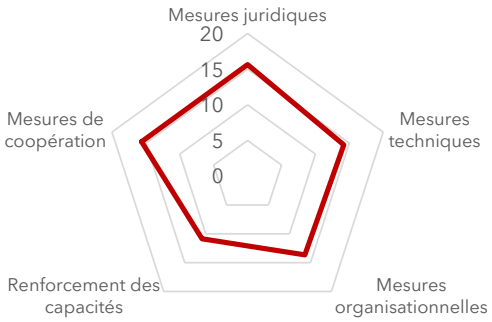
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
33,19	19,19	4,90	3,61	0,00	5,49

Source: Indice mondial de cybersécurité V4, UIT, 2020

Ouganda (République d')



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Renforcement des capacités

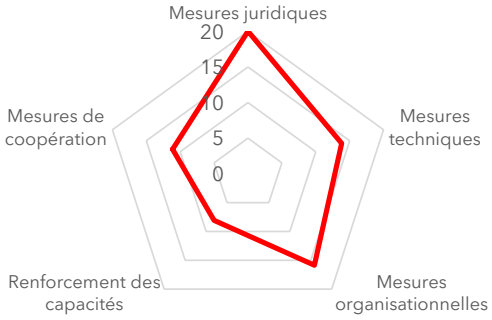
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
69,98	15,64	14,19	13,65	10,87	15,63

Source: Indice mondial de cybersécurité V4, UIT, 2020

Zambie (République de)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques

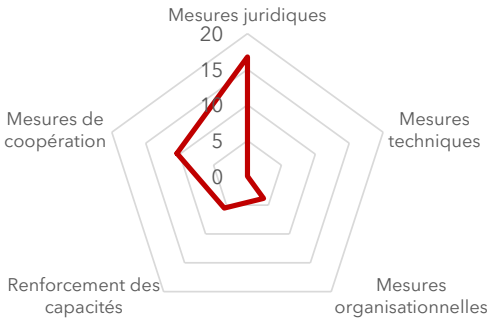
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
68,88	20,00	13,82	15,86	8,07	11,12

Source: Indice mondial de cybersécurité V4, UIT, 2020

Zimbabwe (République du)



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures juridiques

Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
36,49	16,73	0,00	3,84	5,52	10,40

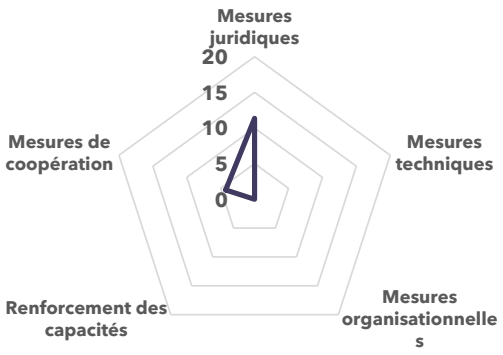
Source: Indice mondial de cybersécurité V4, UIT, 2020

** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

* pas de données

Région des Amériques

Antigua-et-Barbuda



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

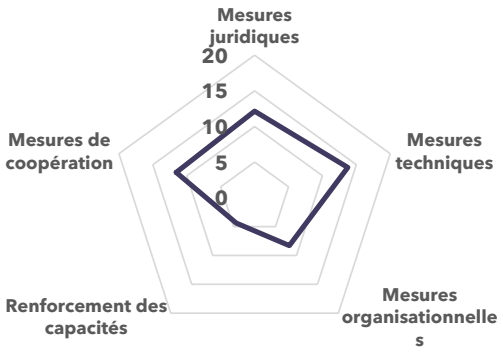
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
15,62	11,36	0,00	0,00	0,00	4,26

Source: Indice mondial de cybersécuritéV4, UIT

République d'Argentine



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures techniques

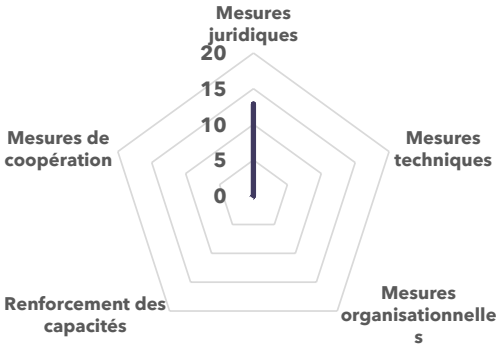
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
50,12	12,15	13,75	8,29	4,38	11,55

Source: Indice mondial de cybersécuritéV4, UIT

Bahamas (Commonwealth des)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

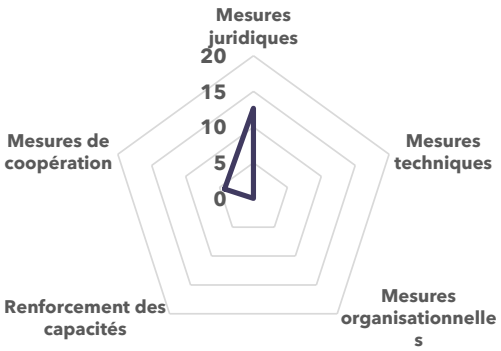
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
13,37	12,85	0,00	0,00	0,52	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Barbade



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

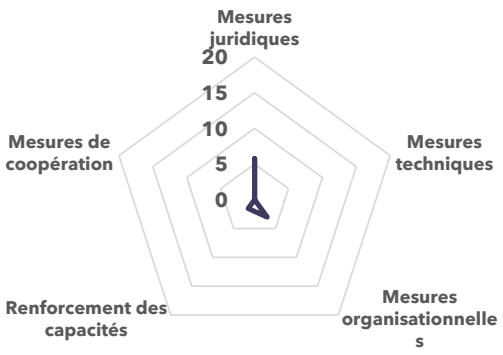
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
16,89	12,63	0,00	0,00	0,00	4,26

Source: Indice mondial de cybersécuritéV4, UIT

Belize



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

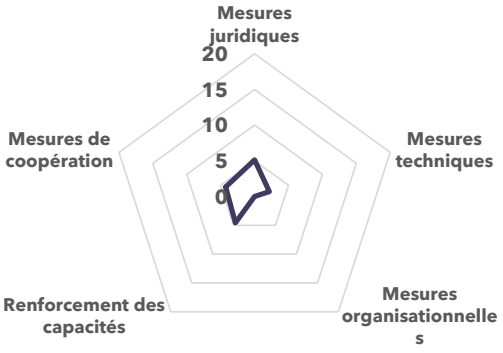
Domaine(s) de croissance potentielle

Mesures techniques, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
10,29	5,77	0,00	3,01	1,52	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Bolivie (État plurinational de)



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures juridiques, de coopération, renforcement des capacités

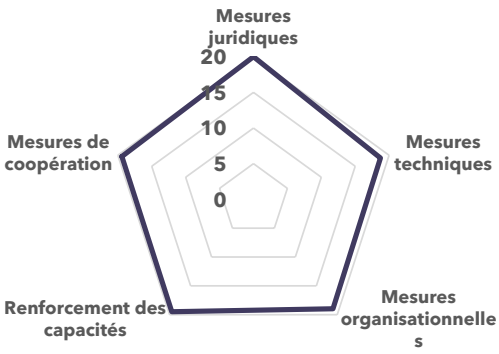
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
16,14	5,13	2,18	0,00	4,58	4,26

Source: Indice mondial de cybersécuritéV4, UIT

Brésil (République fédérative du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

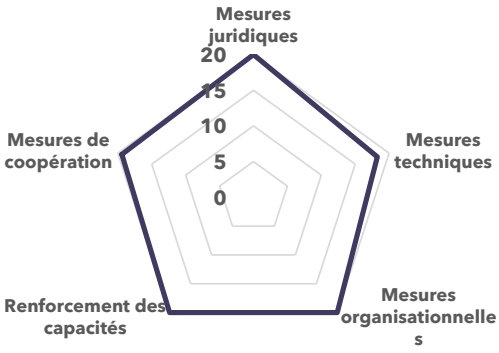
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
96,60	20,00	18,73	18,98	19,48	19,41

Source: Indice mondial de cybersécuritéV4, UIT

*Canada***



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, organisationnelles, de coopération

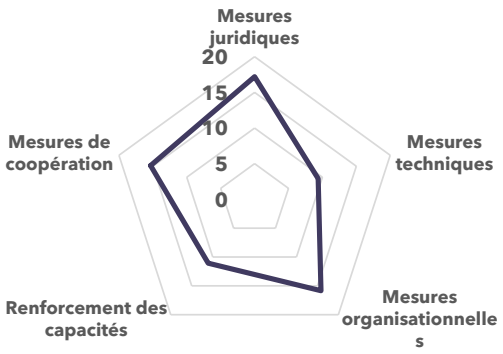
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,67	20,00	18,27	20,00	20,00	19,41

Source: Indice mondial de cybersécuritéV4, UIT

Chili



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

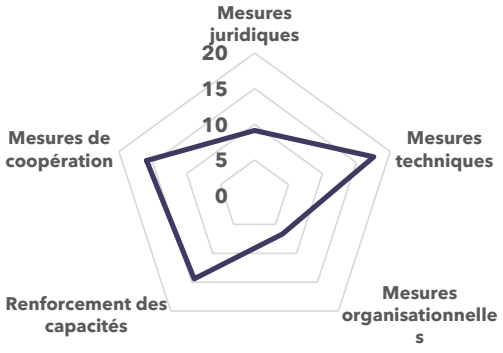
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
68,83	17,20	9,39	15,84	11,07	15,33

Source: Indice mondial de cybersécuritéV4, UIT

Colombie (République de)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures techniques

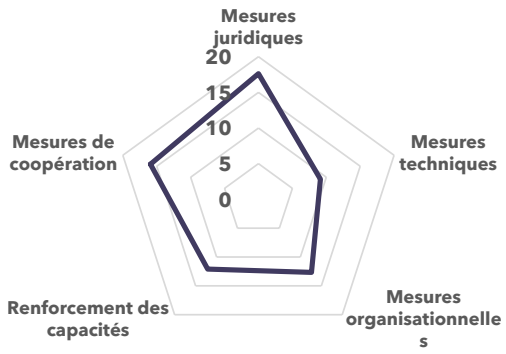
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
63,72	9,14	17,58	6,67	14,42	15,93

Source: Indice mondial de cybersécuritéV4, UIT

Costa Rica



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

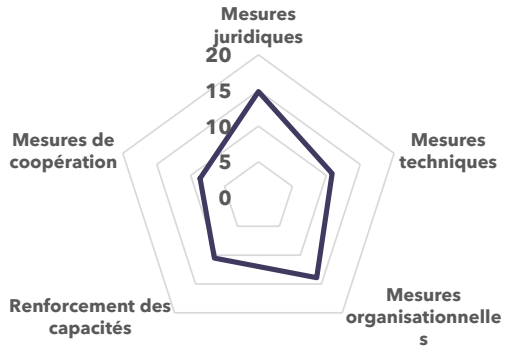
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
67,45	17,62	9,14	12,66	12,11	15,93

Source: Indice mondial de cybersécuritéV4, UIT

Cuba



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

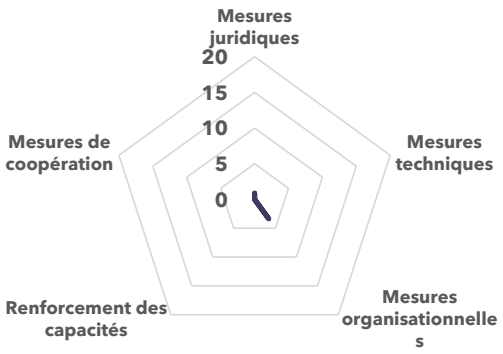
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
58,76	14,85	10,87	13,91	10,52	8,61

Source: Indice mondial de cybersécuritéV4, UIT

Dominique (Commonwealth de la)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures organisationnelles

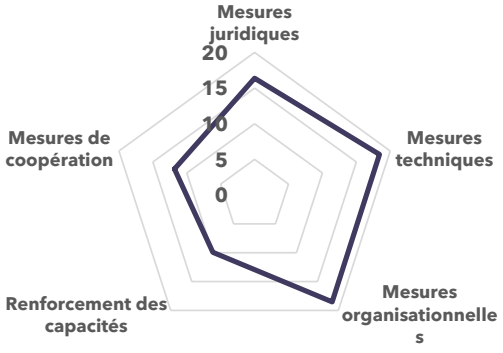
Domaine(s) de croissance potentielle

Mesures techniques, de coopération, Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
4,20	0,85	0,00	3,35	0,00	0,00

Source: Indice mondial de cybersécuritéV4, UIT

République dominicaine



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures organisationnelles

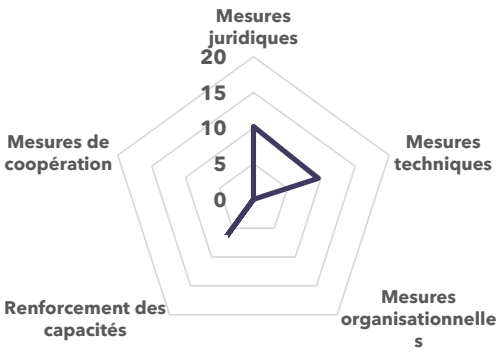
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
75,07	16,38	18,42	18,52	9,94	11,81

Source: Indice mondial de cybersécuritéV4, UIT

Équateur



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

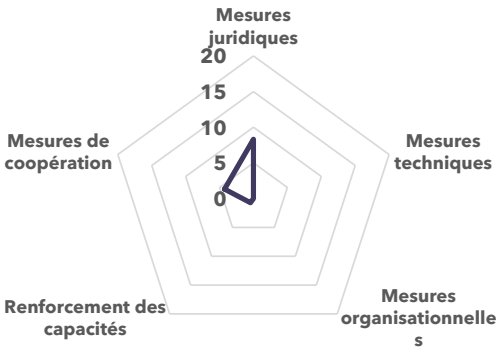
Domaine(s) de croissance potentielle

Mesures organisationnelles, Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
26,30	10,22	9,55	0,00	6,53	0,00

Source: Indice mondial de cybersécuritéV4, UIT

*El Salvador (République d')***



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, techniques

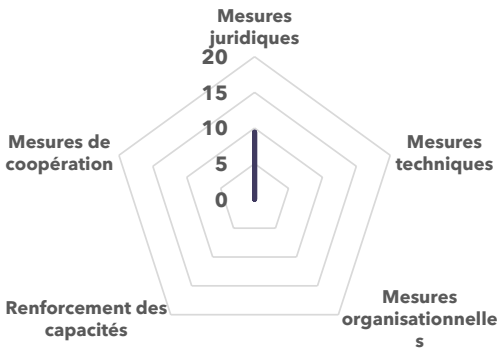
Domaine(s) de croissance potentielle

Mesures organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
13,30	8,32	0,00	0,00	0,72	4,26

Source: Indice mondial de cybersécuritéV4, UIT

Grenade



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

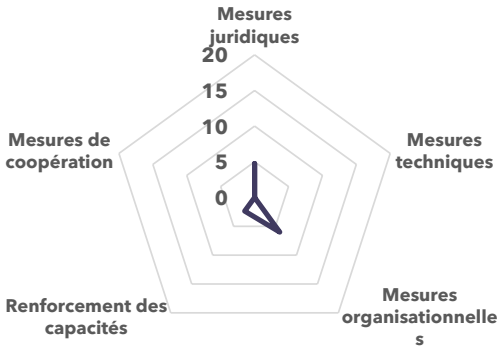
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
9,41	9,41	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Guatemala (République du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures organisationnelles

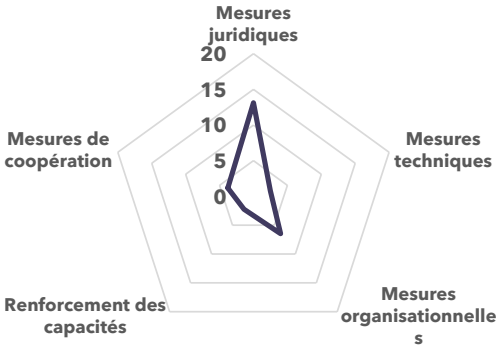
Domaine(s) de croissance potentielle

Mesures techniques, de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
13,13	4,76	0,00	6,01	2,36	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Guyana



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

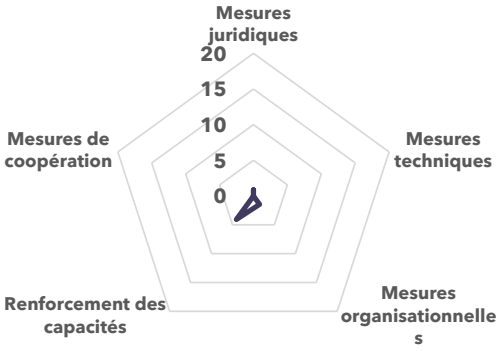
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
28,11	13,12	2,50	6,47	2,24	3,78

Source: Indice mondial de cybersécuritéV4, UIT

Haïti (République d')



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération

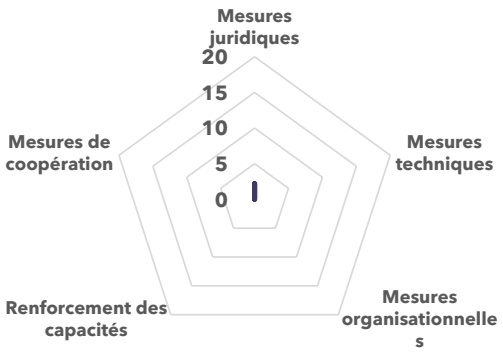
Domaine(s) de croissance potentielle

Mesures techniques, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
6,40	0,85	0,00	1,46	4,09	0,00

Source: Indice mondial de cybersécuritéV4, UIT

*Honduras (République du)***



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

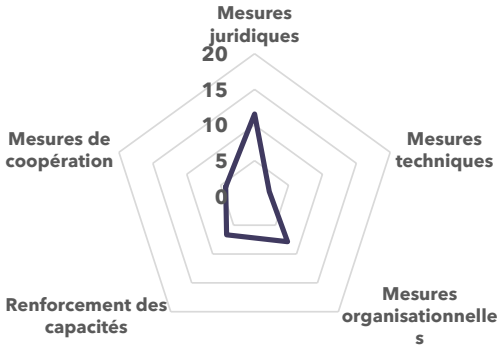
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
2,20	2,20	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécuritéV4, UIT

*Jamaïque***



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

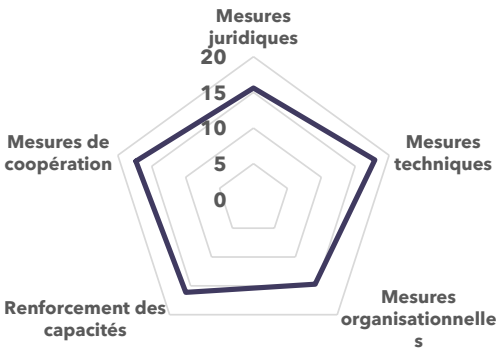
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
32,53	11,54	2,18	7,87	6,68	4,26

Source: Indice mondial de cybersécuritéV4, UIT

Mexique



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures de coopération

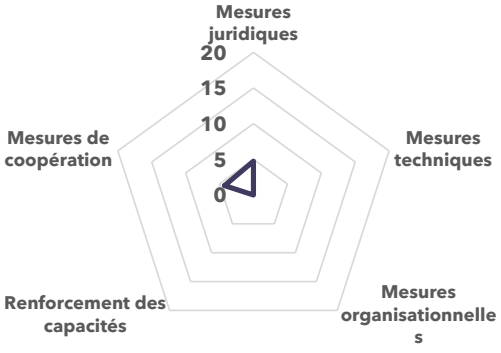
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
81,68	15,61	17,90	14,70	16,13	17,34

Source: Indice mondial de cybersécuritéV4, UIT

*Nicaragua***



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, renforcement des capacités

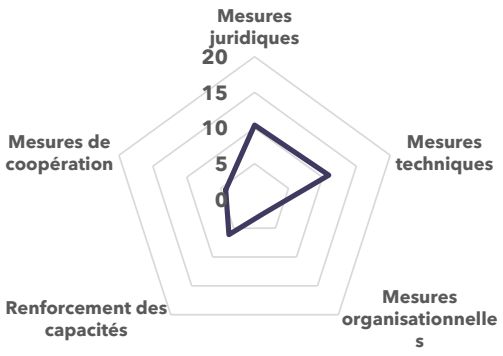
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération,

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
9,00	4,74	0,00	0,00	0,00	4,26

Source: Indice mondial de cybersécuritéV4, UIT

Panama (République du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures techniques, juridiques

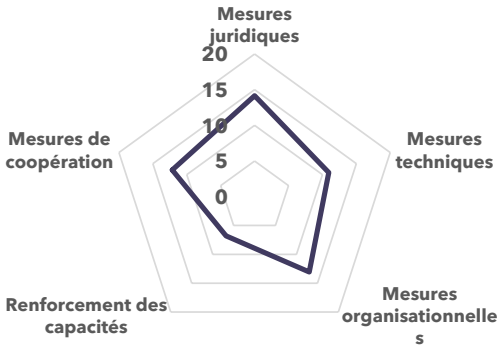
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
34,11	10,41	10,94	2,37	6,12	4,26

Source: Indice mondial de cybersécuritéV4, UIT

Paraguay (République du)



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures juridiques

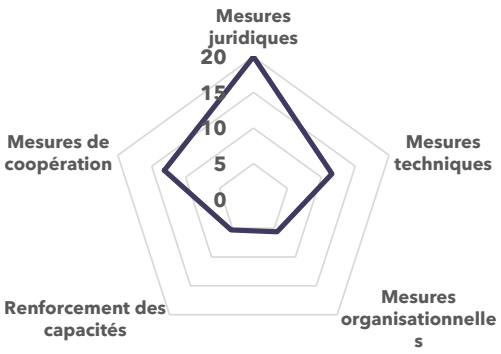
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
57,09	14,15	10,94	13,06	6,79	12,14

Source: Indice mondial de cybersécuritéV4, UIT

Pérou



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

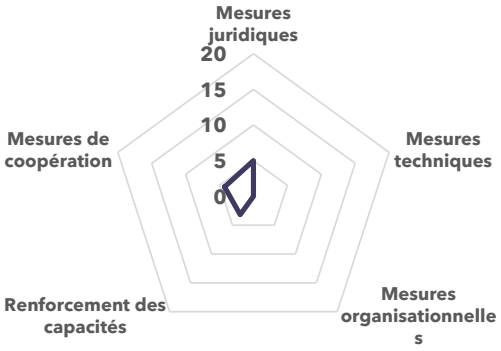
Domaine(s) de croissance potentielle

Mesures organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
55,67	20,00	11,58	5,63	5,32	13,15

Source: Indice mondial de cybersécuritéV4, UIT

Saint-Christophe-et-Niévès (Fédération de)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

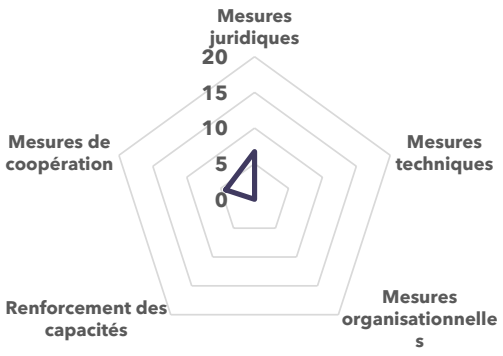
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
12,44	5,00	0,00	0,00	3,18	4,26

Source: Indice mondial de cybersécuritéV4, UIT

*Sainte-Lucie***



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

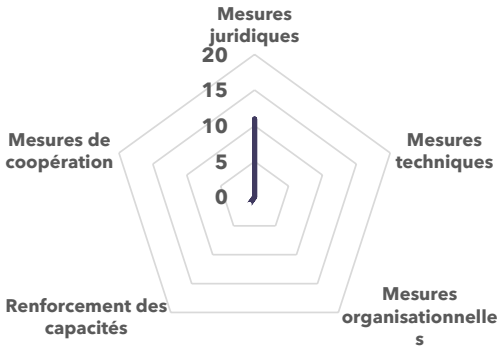
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
10,96	6,70	0,00	0,00	0,00	4,26

Source: Indice mondial de cybersécuritéV4, UIT

*Saint-Vincent-et-les-Grenadines***



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

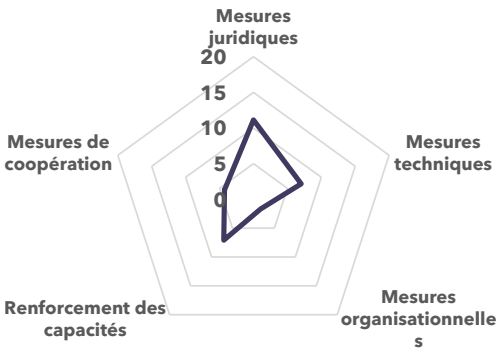
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
12,18	10,95	0,00	0,00	1,23	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Suriname (République du)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

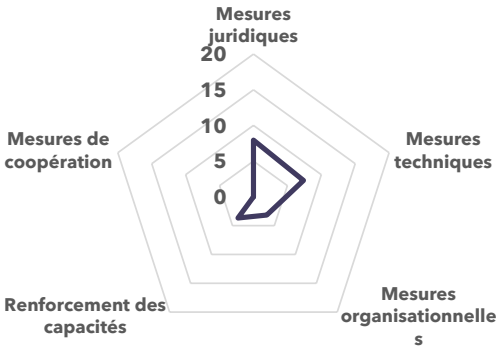
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
31,20	11,13	7,04	1,69	7,08	4,26

Source: Indice mondial de cybersécuritéV4, UIT

Trinité-et-Tobago



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

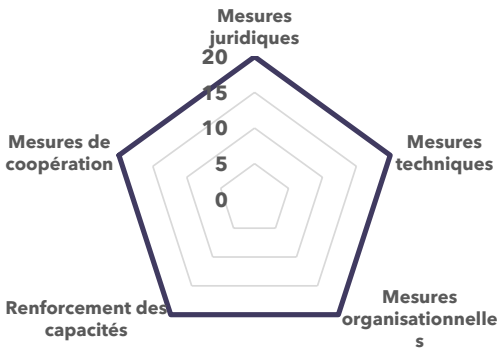
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
22,18	7,94	7,38	3,18	3,69	0,00

Source: Indice mondial de cybersécuritéV4, UIT

*États-Unis d'Amérique***



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, organisationnelles, de coopération, renforcement des capacités

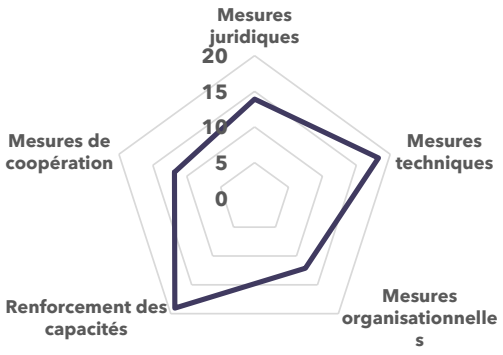
Domaine(s) de croissance potentielle

Sans objet

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
100,00	20,00	20,00	20,00	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Uruguay (République orientale de l')



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Renforcement des capacités

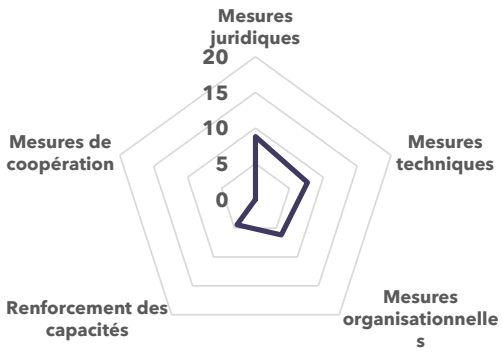
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Mesures de coopération	Renforcement des capacités
75,15	13,90	18,27	12,13	19,04	11,81

Source: Indice mondial de cybersécuritéV4, UIT

Venezuela (République bolivarienne du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Mesures de coopération	Renforcement des capacités
27,06	8,80	7,67	6,17	4,41	0,00

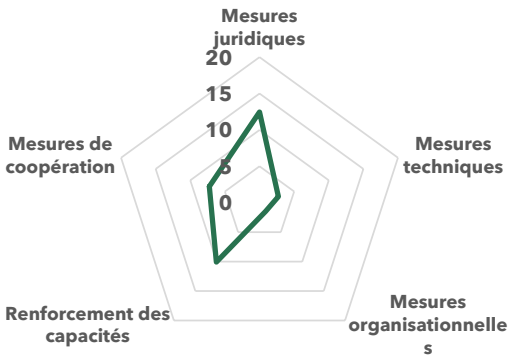
Source: Indice mondial de cybersécuritéV4, UIT

** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

* pas de données

Région des États arabes

Algérie (République algérienne démocratique et populaire)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

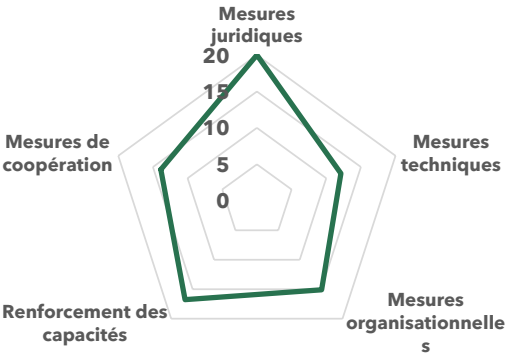
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
33,95	12,46	2,73	1,44	10,07	7,25

Source: Indice mondial de cybersécuritéV4, UIT

Bahreïn (Royaume du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

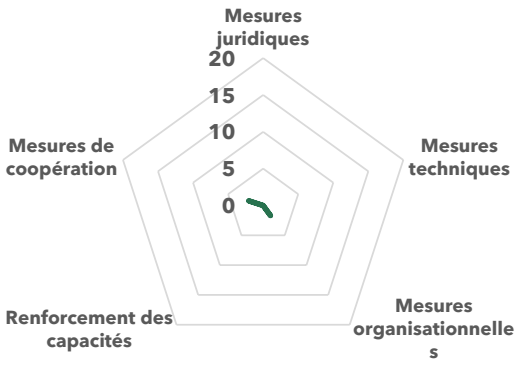
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
77,86	20,00	12,12	15,11	16,77	13,86

Source: Indice mondial de cybersécuritéV4, UIT

*Comores (Union des)***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération

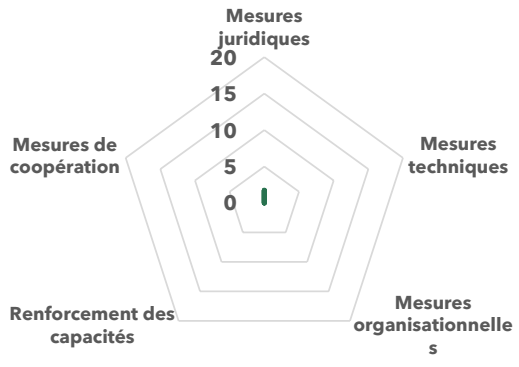
Domaine(s) de croissance potentielle

Mesures juridiques, techniques, renforcement des capacités

					Mesures juridiques
Note globale	0,00	**Mesures techniques**	**Mesures organisationnelles**	**Renforcement des capacités**	**Mesures de coopération**
3,72	0,00	0,00	1,69	0,00	2,04

Source: Indice mondial de cybersécuritéV4, UIT

Djibouti (République de)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

Domaine(s) de croissance potentielle

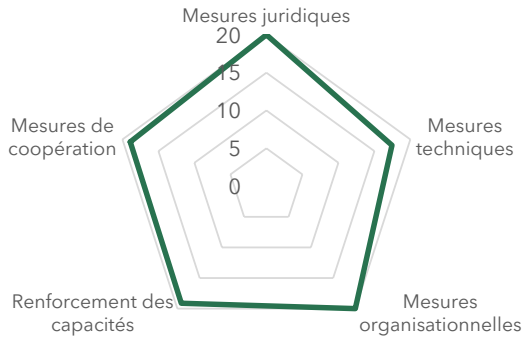
Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	**Mesures juridiques**	**Mesures techniques**	**Mesures organisationnelles**	**Renforcement des capacités**	**Mesures de coopération**
1,73	1,73	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Égypte (République arabe d')

Égypte



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, organisationnelles

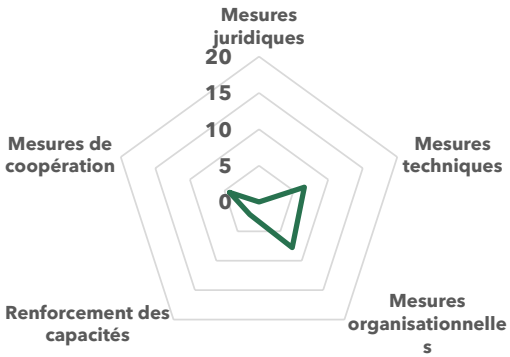
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
95,48	20,00	17,45	20,00	19,12	18,91

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Iraq (République d')***



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures organisationnelles

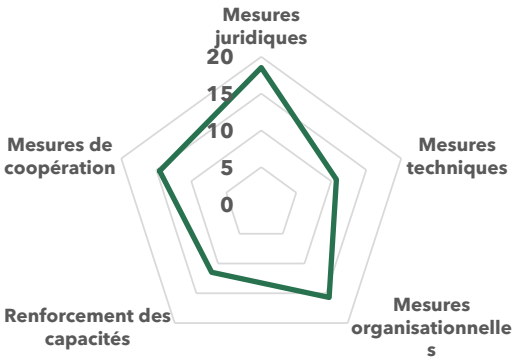
Domaine(s) de croissance potentielle

Mesures juridiques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
20,71	0,00	6,56	7,75	2,14	4,26

Source: Indice mondial de cybersécuritéV4, UIT

Jordanie (Royaume hachémite de)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

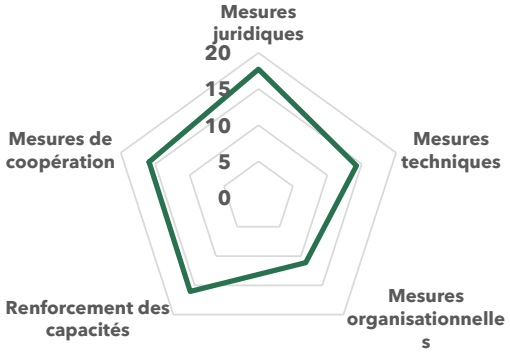
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
70,96	18,53	10,74	15,70	11,47	14,51

Source: Indice mondial de cybersécuritéV4, UIT

Koweït (État du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

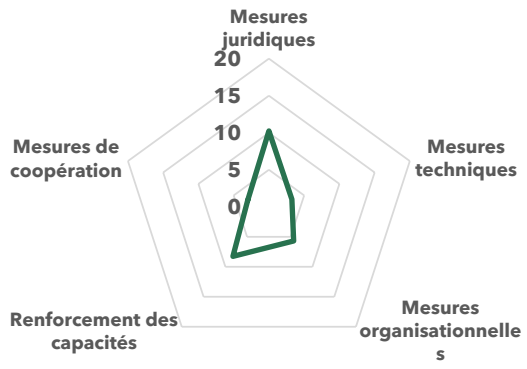
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
75,05	17,74	14,25	11,13	16,05	15,90

Source: Indice mondial de cybersécuritéV4, UIT

*Liban***



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

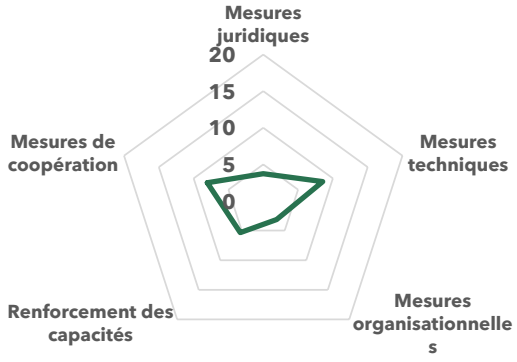
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
30,44	10,24	3,27	5,69	8,26	2,99

Source: Indice mondial de cybersécuritéV4, UIT

Libye (État de)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures techniques, de coopération

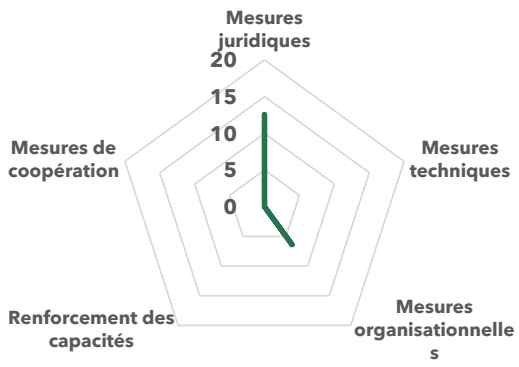
Domaine(s) de croissance potentielle

Mesures juridiques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
28,78	3,73	8,54	3,13	5,34	8,04

Source: Indice mondial de cybersécuritéV4, UIT

Mauritanie (République islamique de)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

Domaine(s) de croissance potentielle

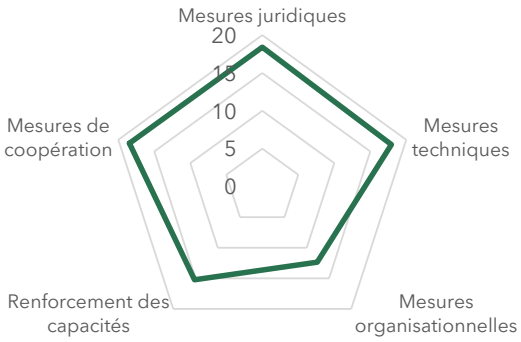
Mesures techniques, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
18,94	12,55	0,00	6,39	0,00	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Maroc (Royaume du)

Maroc



Niveau de développement:

Pays en développement

Domaine(s) de force relative

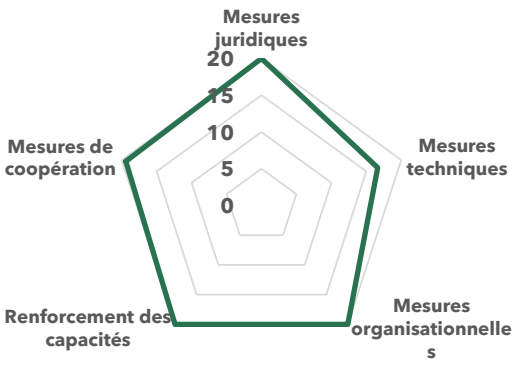
Mesures juridiques, de coopération

Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
82,41	18,40	17,94	12,37	15,24	18,46

Oman (Sultanat d')



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, organisationnelles, renforcement des capacités

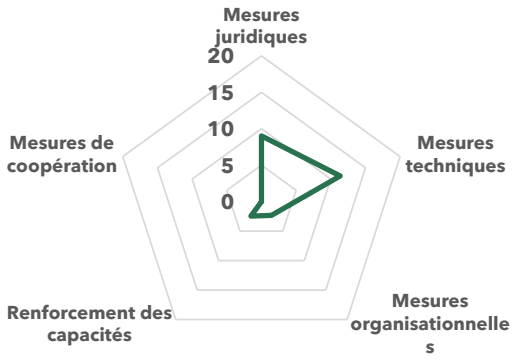
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
96,04	20,00	16,64	20,00	20,00	19,41

Source: Indice mondial de cybersécuritéV4, UIT

État de Palestine



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures techniques

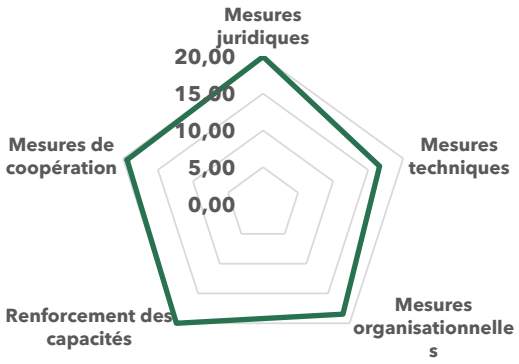
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
25,18	9,02	11,36	2,34	2,46	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Qatar (État du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, renforcement des capacités

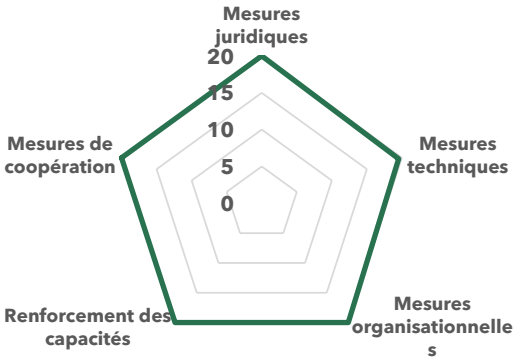
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
94,50	20,00	16,64	18,46	20,00	19,41

Source: Indice mondial de cybersécuritéV4, UIT

Arabie saoudite (Royaume d')



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, organisationnelles, de coopération, renforcement des capacités

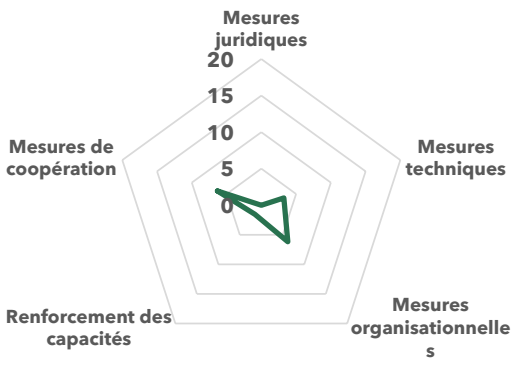
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
99,54	20,00	19,54	20,00	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Somalie (République fédérale de)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures organisationnelles, de coopération

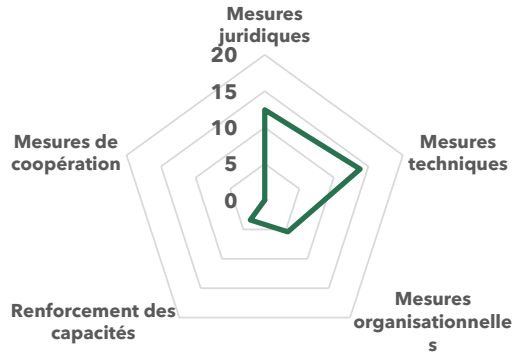
Domaine(s) de croissance potentielle

Mesures juridiques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
17,25	0,00	3,25	6,17	1,52	6,31

Source: Indice mondial de cybersécuritéV4, UIT

Soudan (République du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures techniques

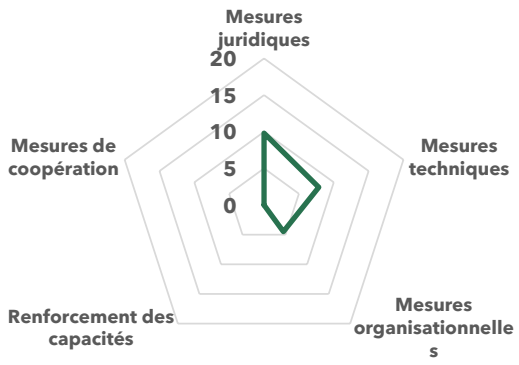
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
35,03	12,43	13,81	5,41	3,38	0,00

Source: Indice mondial de cybersécuritéV4, UIT

*République arabe syrienne***



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

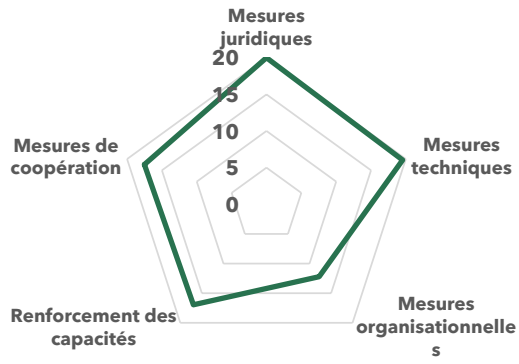
Domaine(s) de croissance potentielle

Renforcement des capacités, mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
22,14	9,80	7,85	4,49	0,00	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Tunisie



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, techniques

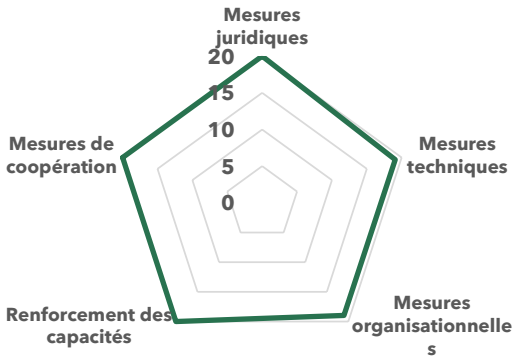
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
86,23	20,00	19,54	12,21	16,96	17,52

Source: Indice mondial de cybersécuritéV4, UIT

Émirats arabes unis



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, de coopération, Renforcement des capacités

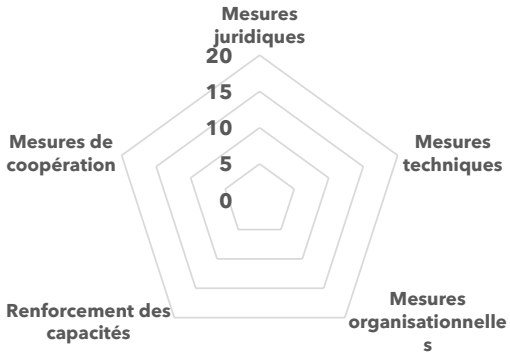
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
98,06	20,00	19,08	18,98	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

*Yémen (République du)**



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

N/A

Domaine(s) de croissance potentielle

N/A

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
0	**0**	**0**	**0**	0	0

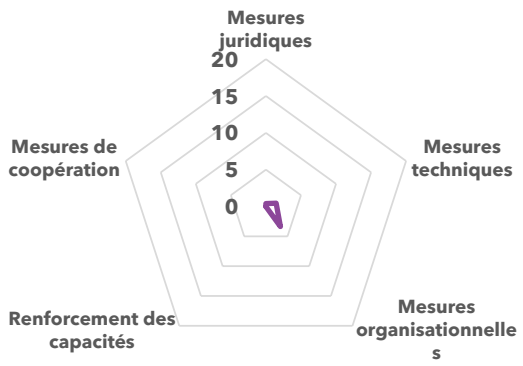
Source: Indice mondial de cybersécuritéV4, UIT

** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

* pas de données

Région Asie-Pacifique

Afghanistan



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures organisationnelles

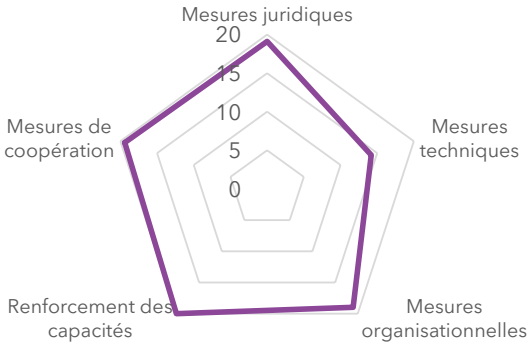
Domaine(s) de croissance potentielle

Renforcement des capacités, mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
5,20	0,40	1,46	3,35	0,00	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Australie



Niveau de développement:

Pays développé

Domaine(s) de force relative

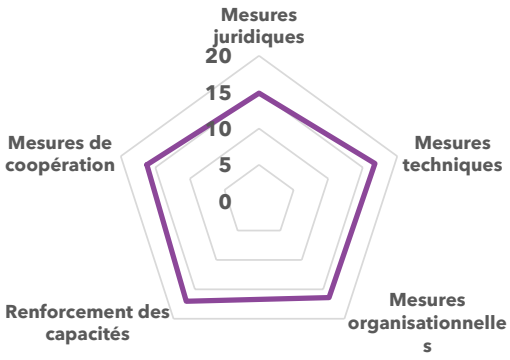
Mesures juridiques, renforcement des capacités

Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,47	20,00	19,08	18,98	20,00	19,41

Bangladesh (République populaire du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Renforcement des capacités, mesures techniques

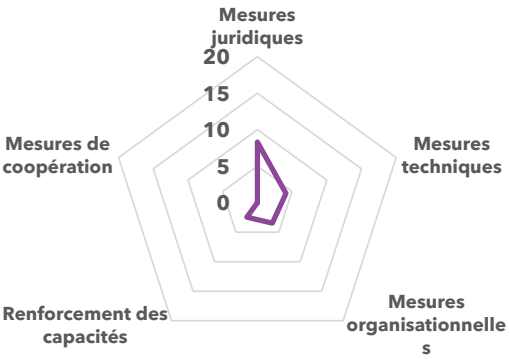
Domaine(s) de croissance potentielle

Mesures juridiques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
81,27	14,86	16,77	16,39	17,03	16,22

Source: Indice mondial de cybersécuritéV4, UIT

Bhoutan (Royaume du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques

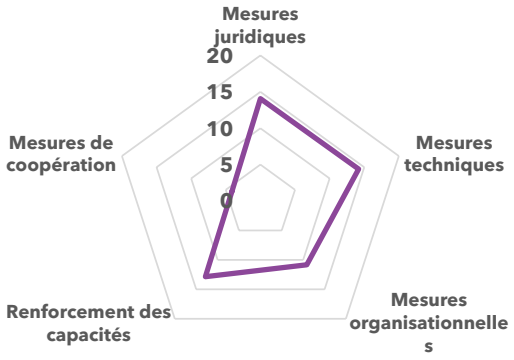
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
18,34	8,30	4,12	3,47	2,45	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Brunéi Darussalam



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, techniques

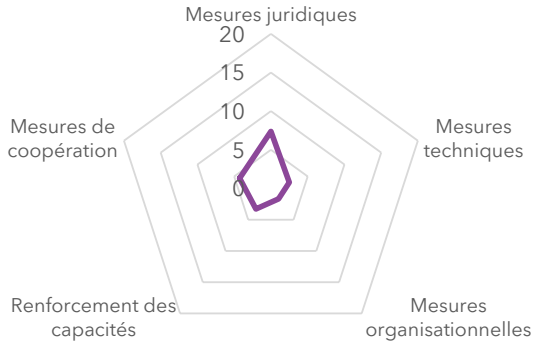
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
56,07	14,06	14,19	10,84	12,85	4,12

Source: Indice mondial de cybersécuritéV4, UIT

*Cambodge (Royaume du)***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

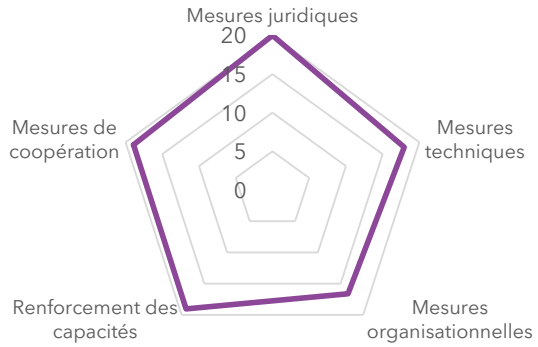
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
19,12	7,38	2,50	1,69	3,29	4,26

Source: Indice mondial de cybersécurité V4, UIT, 2020

Chine (République populaire de)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

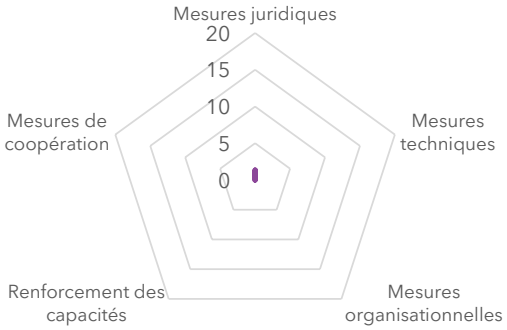
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
92,53	20,00	17,94	16,63	19,04	18,91

Source: Indice mondial de cybersécurité V4, UIT, 2020

*République populaire démocratique de Corée***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures juridiques

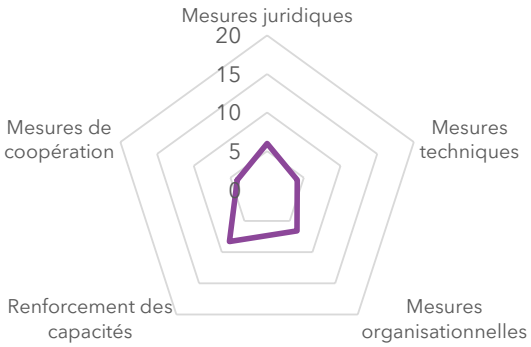
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
1,35	1,35	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécuritéV4, UIT

Fidji (République des)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

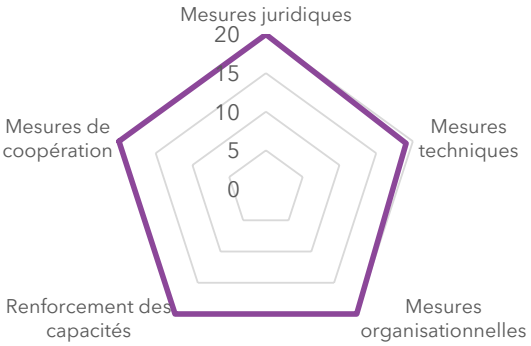
Renforcement des capacités

Domaine(s) de croissance potentielle

Mesures techniques, de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
29,08	5,99	4,11	6,59	8,31	4,07

Inde (République d')



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, de coopération, renforcement des capacités

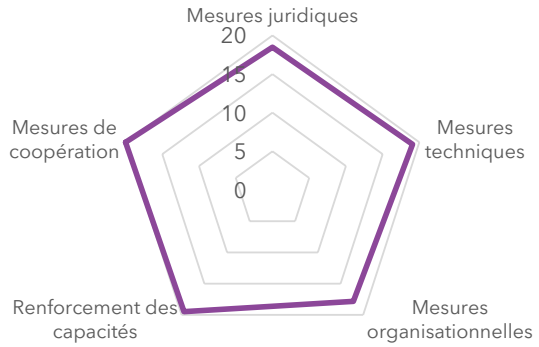
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,49	20,00	19,08	18,41	20,00	20,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Indonésie (République d')



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures de coopération, renforcement des capacités

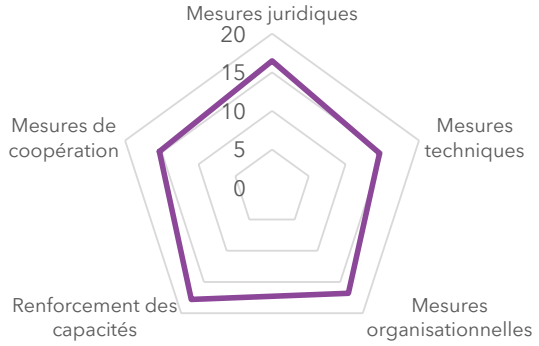
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
94,88	18,48	19,08	17,84	19,48	20,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Iran (République islamique d')



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Renforcement des capacités, mesures organisationnelles

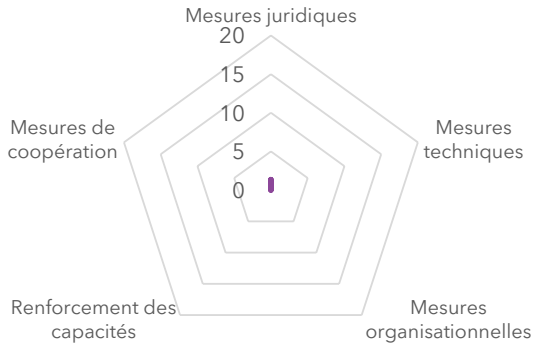
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
81,06	16,48	14,63	16,82	17,80	15,33

Source: Indice mondial de cybersécurité V4, UIT, 2020

Corée (République de)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

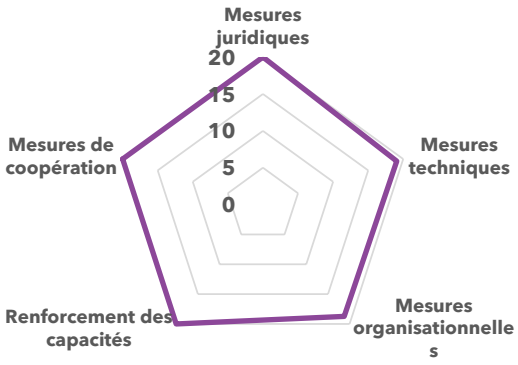
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
1,35	1,35	0,00	0,00	0,00	0,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Japon



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, de coopération, renforcement des capacités

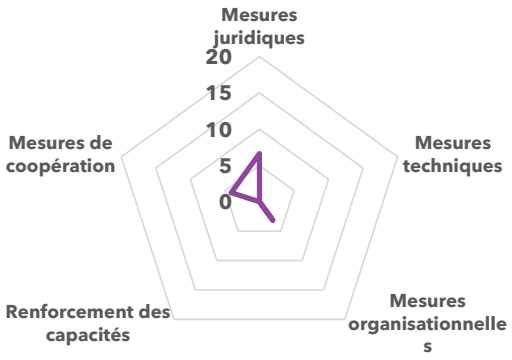
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,82	20,00	19,08	18,74	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Kiribati (République de)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

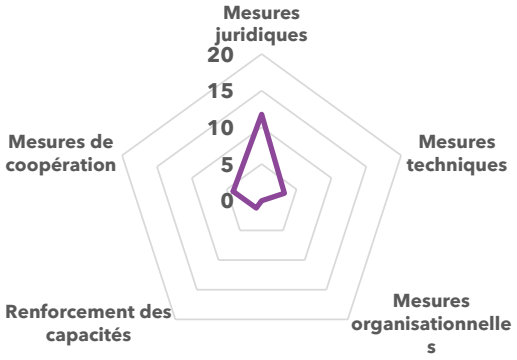
Domaine(s) de croissance potentielle

Mesures techniques, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
13,84	6,64	0,00	3,13	0,00	4,07

Source: Indice mondial de cybersécuritéV4, UIT

République démocratique populaire Lao



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques

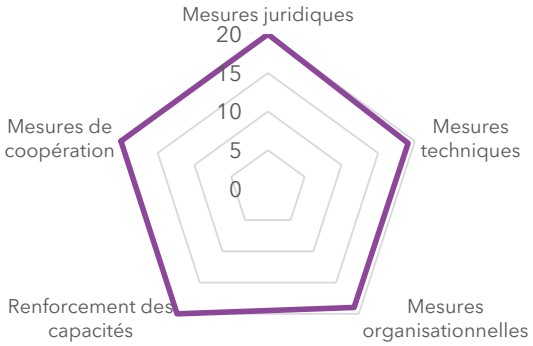
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
20,34	11,77	3,27	0,00	1,23	4,07

Source: Indice mondial de cybersécuritéV4, UIT

Malaisie



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, de coopération, renforcement des capacités

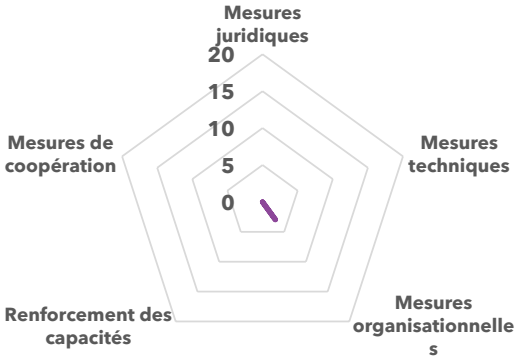
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
98,06	20,00	19,08	18,98	20,00	20,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Maldives (République des)***



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures organisationnelles

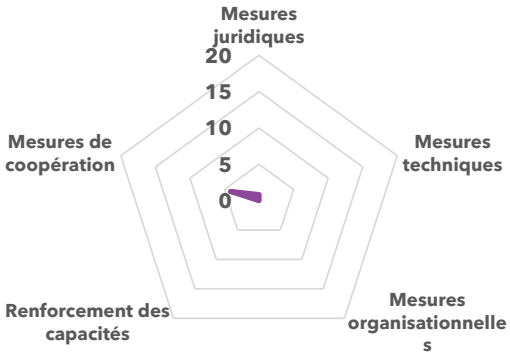
Domaine(s) de croissance potentielle

Mesures juridiques, techniques, de coopération, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
2,95	0,00	0,00	2,95	0,00	0,00

Source: Indice mondial de cybersécuritéV4, UIT

*Îles Marshall (République des)***



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération

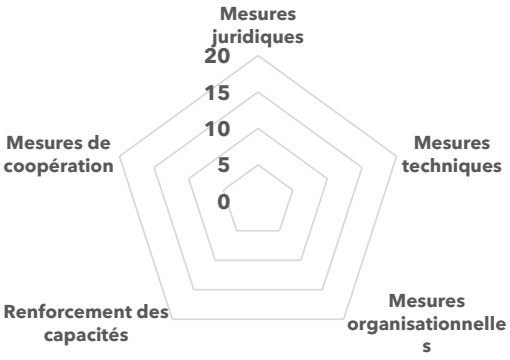
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
4,90	0,83	0,00	0,00	0,00	4,07

Source: Indice mondial de cybersécuritéV4, UIT

*Micronésie (États fédérés de)**



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

sans objet

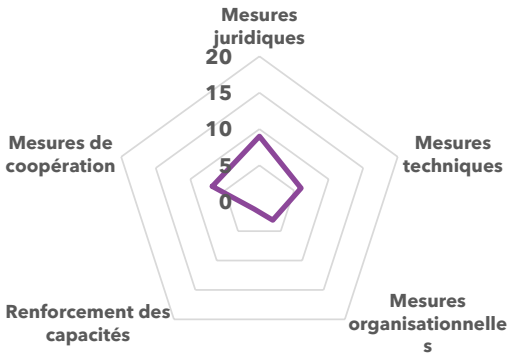
Domaine(s) de croissance potentielle

sans objet

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
0	**0**	**0**	**0**	0	0

Source: Indice mondial de cybersécuritéV4, UIT

Mongolie



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures juridiques

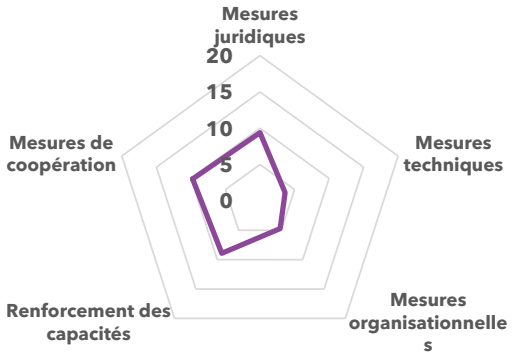
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
26,20	9,00	6,02	3,13	1,23	6,82

Source: Indice mondial de cybersécuritéV4, UIT

Myanmar (Union du)



Niveau de développement:

Pays en développement, pays les moins avancés (PMA)

Domaine(s) de force relative

Mesures de coopération, juridiques

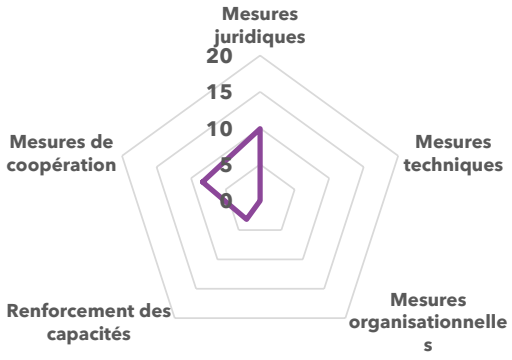
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
36,41	9,39	3,64	4,71	8,92	9,75

Source: Indice mondial de cybersécuritéV4, UIT

*Nauru (République de)***



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

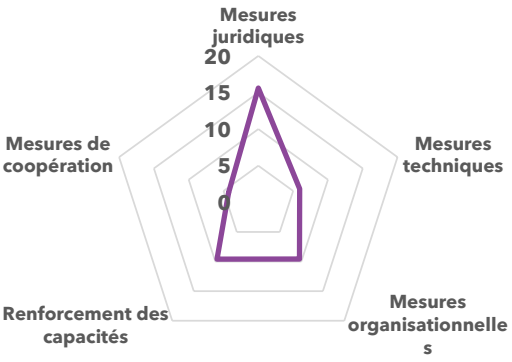
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
21,42	9,91	0,00	0,00	3,18	8,33

Source: Indice mondial de cybersécuritéV4, UIT

*Népal (République démocratique fédérale du)***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), pays sans littoral

Domaine(s) de force relative

Mesures juridiques

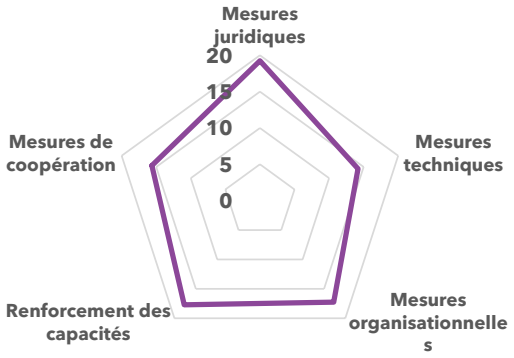
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
44,99	15,61	5,94	9,58	9,60	4,26

Source: Indice mondial de cybersécuritéV4, UIT

*Nouvelle-Zélande***



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques

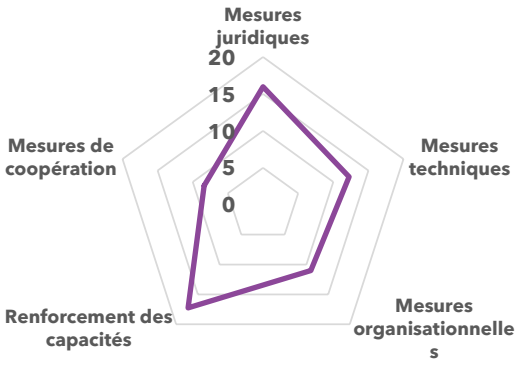
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
84,04	19,24	14,19	17,27	17,71	15,63

Source: Indice mondial de cybersécuritéV4, UIT

Pakistan (République islamique du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Renforcement des capacités

Domaine(s) de croissance potentielle

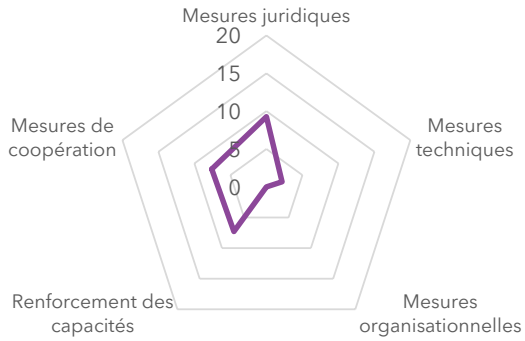
Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
64,88	15,97	12,26	11,01	17,25	8,38

Source: Indice mondial de cybersécuritéV4, UIT

*Papouasie-Nouvelle-Guinée***

Papouasie-Nouvelle-Guinée



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques

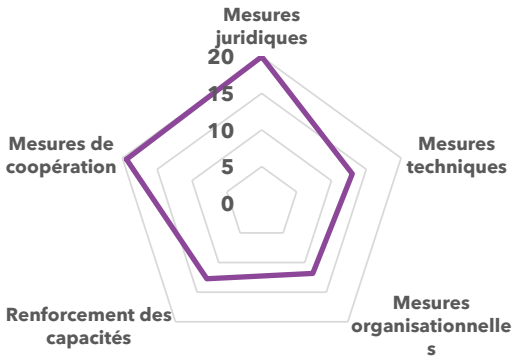
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
26,33	9,26	2,18	0,00	7,30	7,59

Source: Indice mondial de cybersécurité V4, UIT, 2020

Philippines (République des)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, de coopération

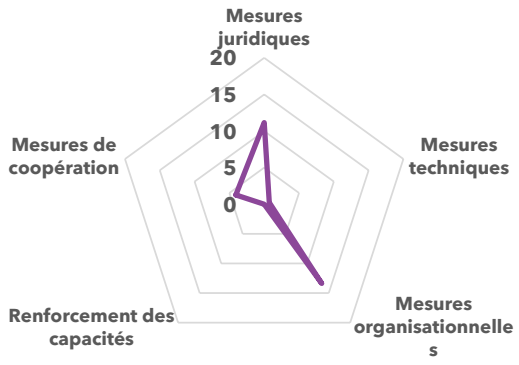
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
77,00	20,00	13,00	11,85	12,74	19,41

Source: Indice mondial de cybersécuritéV4, UIT

Samoa (État indépendant de)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures organisationnelles

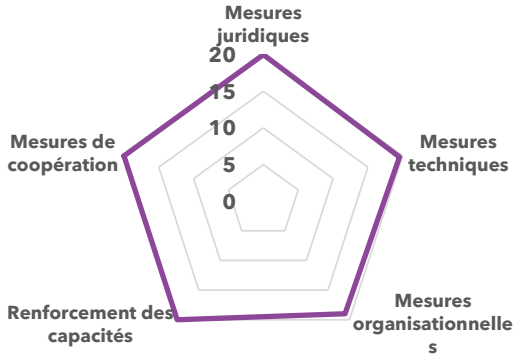
Domaine(s) de croissance potentielle

Renforcement des capacités, mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
29,33	11,15	0,73	13,37	0,00	4,07

Source: Indice mondial de cybersécuritéV4, UIT

Singapour (République de)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures juridiques, de coopération, renforcement des capacités

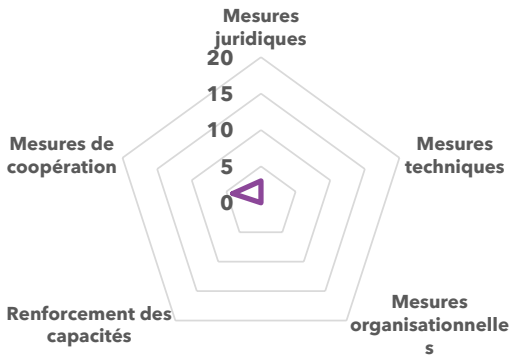
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
98,52	20,00	19,54	18,98	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Îles Salomon



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération, juridiques

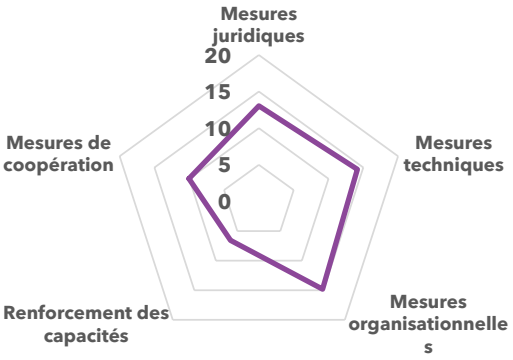
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
7,08	3,00	0,00	0,00	0,00	4,07

Source: Indice mondial de cybersécuritéV4, UIT

Sri Lanka (République socialiste démocratique du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures organisationnelles, techniques

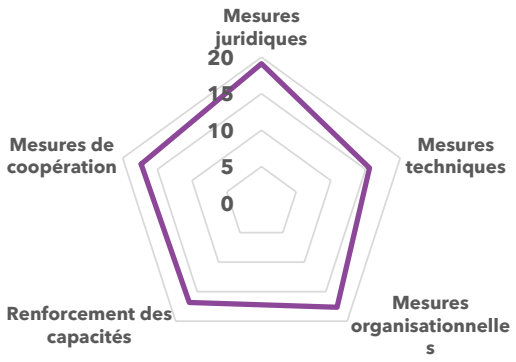
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
58,65	13,05	14,15	14,82	6,58	10,04

Source: Indice mondial de cybersécuritéV4, UIT

Thaïlande



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

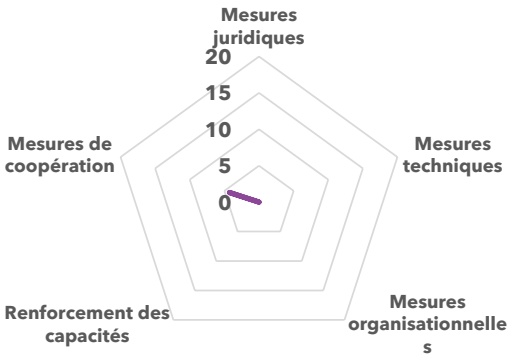
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
86,50	19,11	15,57	17,64	16,84	17,34

Source: Indice mondial de cybersécuritéV4, UIT

*Timor-Leste (République démocratique du)***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération

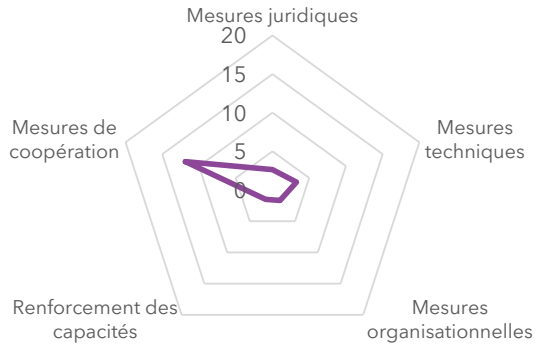
Domaine(s) de croissance potentielle

Mesures juridiques, techniques, organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
4,26	0,00	0,00	0,00	0,00	4,26

Source: Indice mondial de cybersécuritéV4, UIT

*Tonga (Royaume de)***



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération

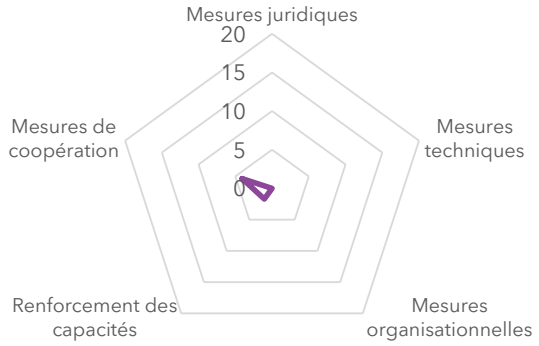
Domaine(s) de croissance potentielle

Mesures organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
20,95	2,63	3,27	1,69	1,52	11,85

Source: Indice mondial de cybersécurité V4, UIT, 2020

*Tuvalu***



Niveau de développement:

Pays en développement, pays les moins avancés (PMA), petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération

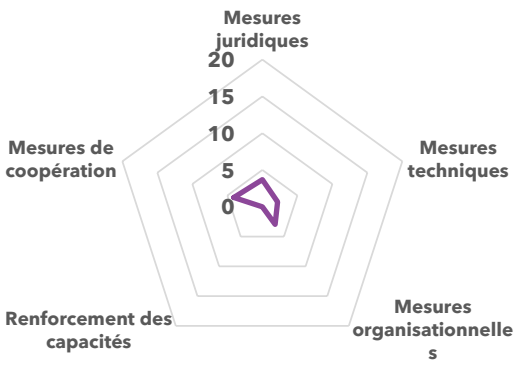
Domaine(s) de croissance potentielle

Mesures juridiques, techniques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
5,78	0,00	0,00	0,00	1,71	4,07

Source: Indice mondial de cybersécurité V4, UIT, 2020

Vanuatu (République de)



Niveau de développement:

Pays en développement, petit État insulaire en développement (PEID)

Domaine(s) de force relative

Mesures de coopération

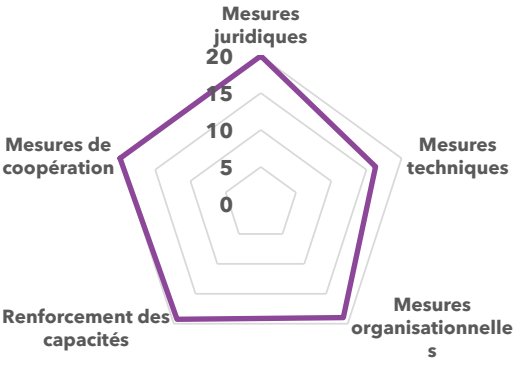
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
12,88	3,69	2,18	2,95	0,00	4,07

Source: Indice mondial de cybersécuritéV4, UIT

Viet Nam (République socialiste du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, de coopération

Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
94,55	20,00	16,31	18,98	19,26	20,00

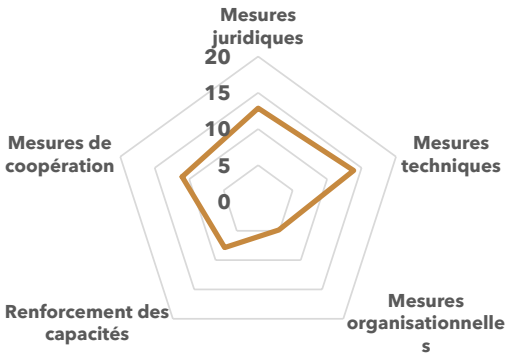
Source: Indice mondial de cybersécuritéV4, UIT

** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

* pas de données

Région de la Communauté d'États indépendants

*Arménie (République d')***



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures techniques

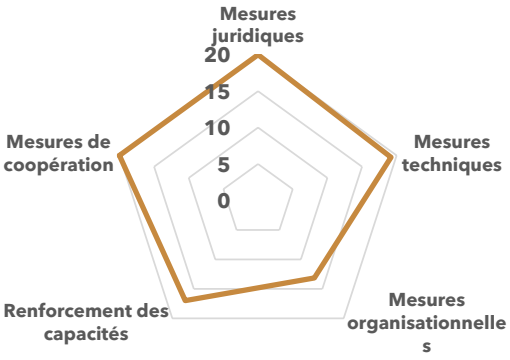
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
50,47	12,87	13,86	4,87	7,85	11,02

Source: Indice mondial de cybersécuritéV4, UIT

Azerbaïdjan (République d')



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures juridiques, de coopération

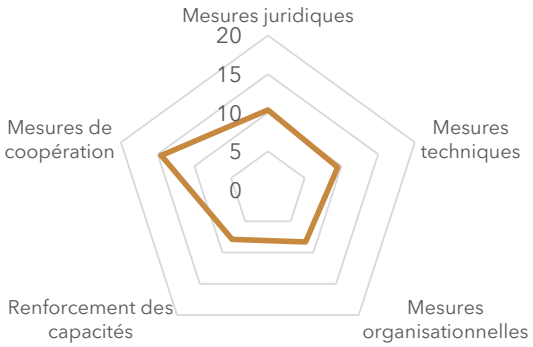
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
89,31	20,00	19,19	13,14	16,99	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Bélarus (République du)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération

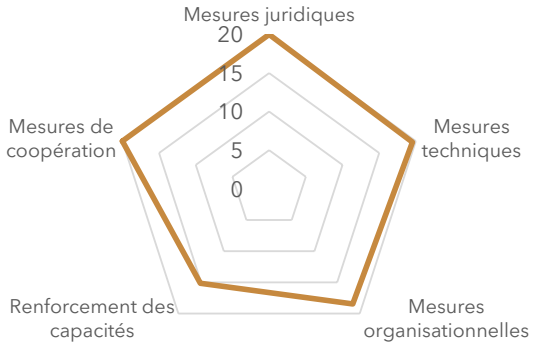
Domaine(s) de croissance potentielle

Mesures organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
50,57	10,36	9,50	8,31	7,88	14,51

Source: Indice mondial de cybersécurité V4, UIT, 2020

Kazakhstan (République du)



Niveau de développement:

Pays en développement

Domaine(s) de force relative

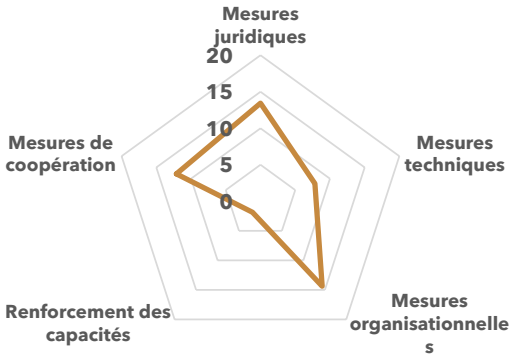
Mesures juridiques, de coopération

Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
93,15	20,00	19,54	18,46	15,15	20,00

République kirghize



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures organisationnelles, juridiques

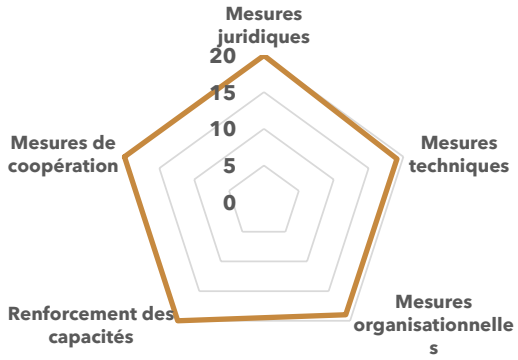
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
49,64	13,43	7,85	14,37	1,87	12,11

Source: Indice mondial de cybersécuritéV4, UIT

Fédération de Russie



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, de coopération, renforcement des capacités

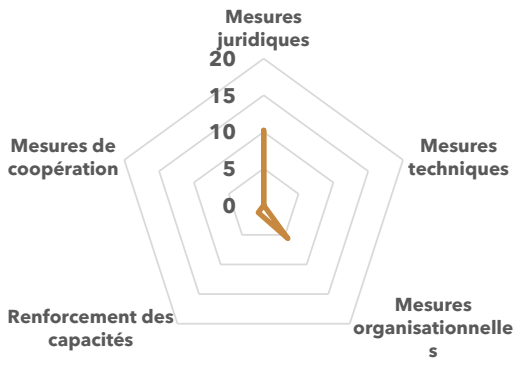
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
98,06	20,00	19,08	18,98	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

*Tadjikistan (République du)***



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures juridiques

Domaine(s) de croissance potentielle

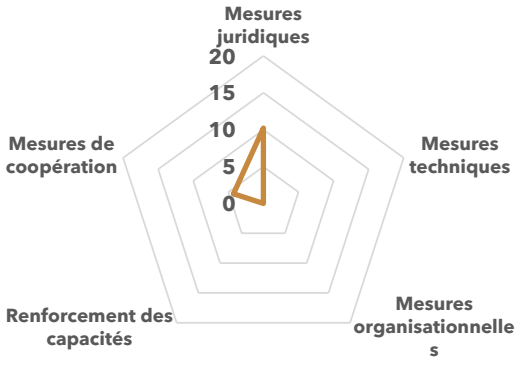
Mesures techniques, de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
17,10	10,22	0,00	5,63	1,25	0,00

Source: Indice mondial de cybersécuritéV4, UIT

** pas de réponse au questionnaire/données recueillies par l'équipe du GCI
* pas de données

*Turkménistan***



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures juridiques

Domaine(s) de croissance potentielle

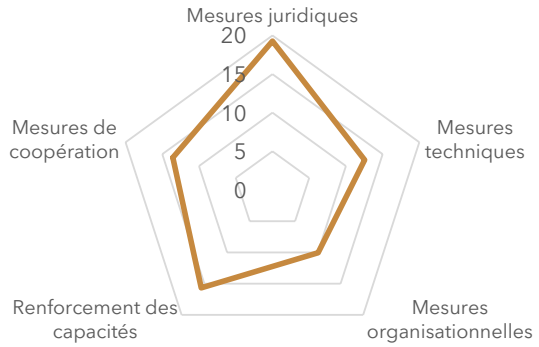
Mesures techniques, organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
14,48	10,22	0,00	0,00	0,00	4,26

Source: Indice mondial de cybersécuritéV4, UIT

** pas de réponse au questionnaire/données recueillies par l'équipe du GCI
* pas de données

Ouzbékistan (République d')



Niveau de développement:

Pays en développement, pays sans littoral

Domaine(s) de force relative

Mesures juridiques

Domaine(s) de croissance potentielle

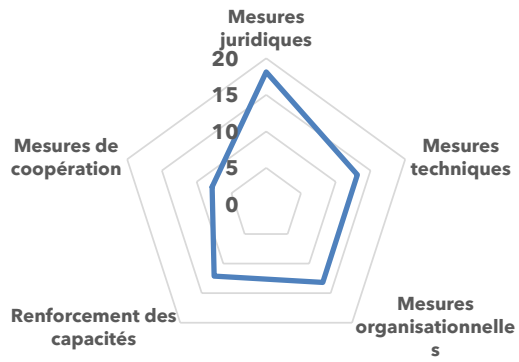
Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
71,11	19,27	12,56	10,05	15,68	13,56

Source: Indice mondial de cybersécurité V4, UIT, 2020

Europe

Albanie (République d')



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques

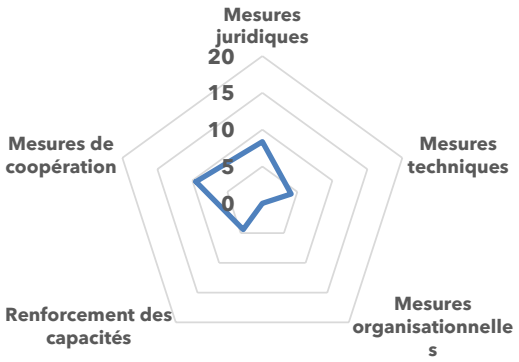
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
64,32	18,13	13,12	13,18	12,12	7,78

Source: Indice mondial de cybersécuritéV4, UIT

*Andorre (Principauté d')***



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération

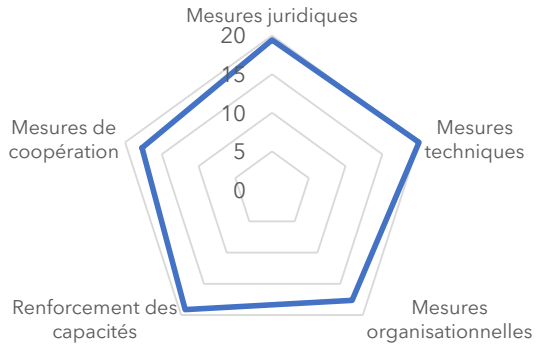
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
26,38	8,37	4,11	0,00	4,41	9,49

Source: Indice mondial de cybersécuritéV4, UIT

Autriche



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures techniques

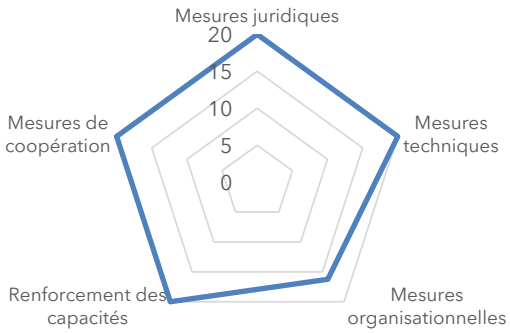
Domaine(s) de croissance potentielle

Mesures organisationnelles, de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
93,89	19,43	20,00	17,64	19,13	17,70

Source: Indice mondial de cybersécurité V4, UIT, 2020

Belgique



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, techniques, de coopération, renforcement des capacités

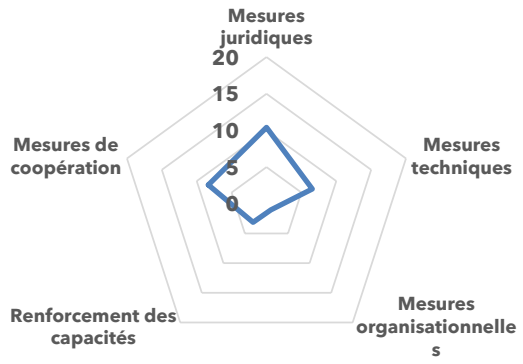
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
96,25	20,00	20,00	16,25	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Bosnie-Herzégovine



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques

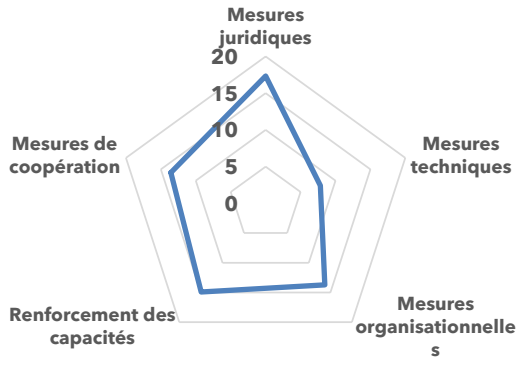
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
29,44	10,41	6,56	1,02	3,12	8,33

Source: Indice mondial de cybersécuritéV4, UIT

Bulgarie (République de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques

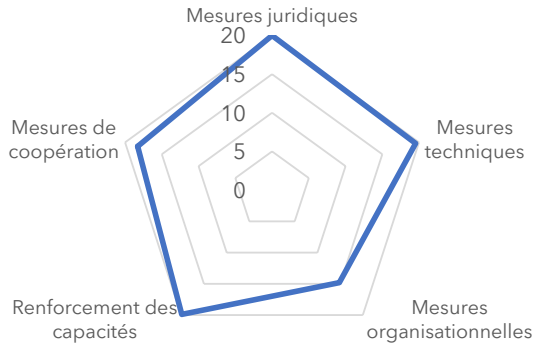
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
67,38	17,34	7,84	13,72	14,92	13,57

Source: Indice mondial de cybersécuritéV4, UIT

Croatie (République de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, renforcement des capacités

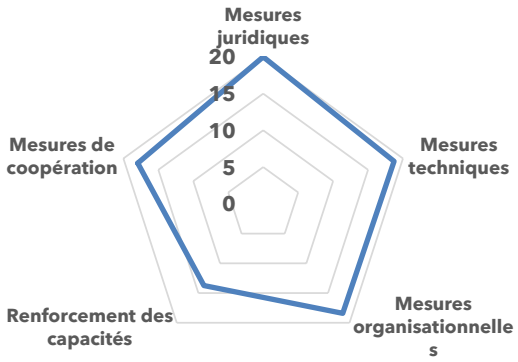
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
92,53	20,00	19,54	14,80	19,89	18,29

Source: Indice mondial de cybersécurité V4, UIT, 2020

Chypre (République de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques

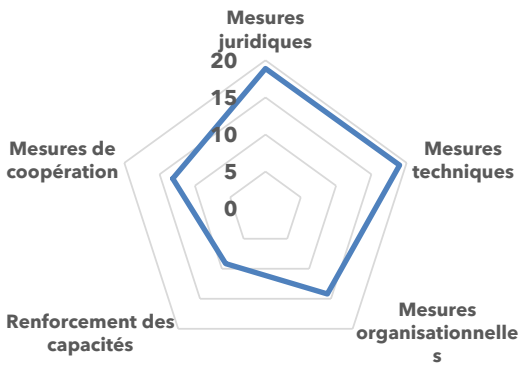
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
88,82	20,00	18,73	18,41	13,73	17,94

Source: Indice mondial de cybersécuritéV4, UIT

République tchèque



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures techniques, juridiques

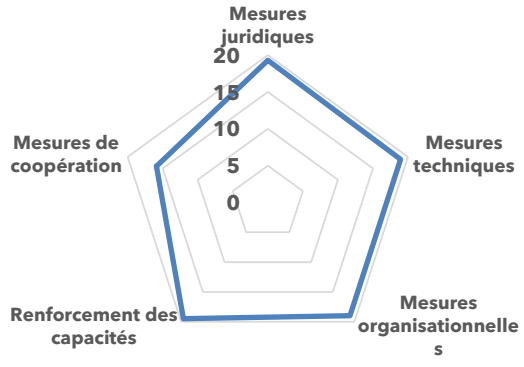
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
74,37	18,89	19,00	14,20	9,14	13,14

Source: Indice mondial de cybersécuritéV4, UIT

Danemark



Niveau de développement:

Pays développé

Domaine(s) de force relative

Renforcement des capacités, mesures juridiques

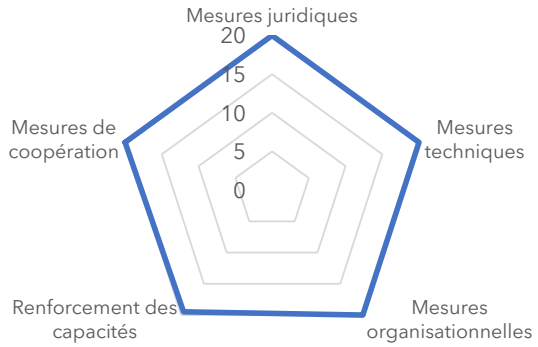
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
92,60	19,30	18,94	18,98	19,48	15,89

Source: Indice mondial de cybersécuritéV4, UIT

Estonie (République d')



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, techniques, organisationnelles, de coopération

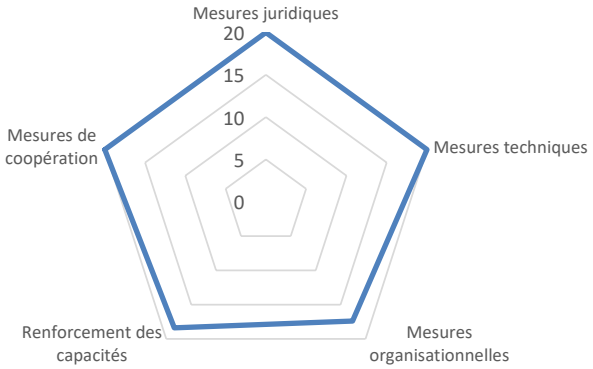
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
99,48	20,00	20,00	20,00	19,48	20,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Finlande



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, techniques, de coopération

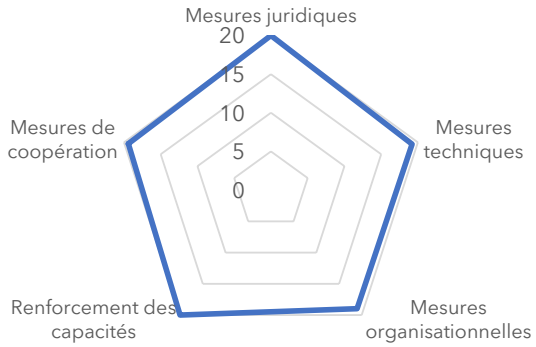
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
92,07	20,00	20,00	14,33	17,74	20,00

Source: Indice mondial de cybersécuritéV4, UIT

France



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, renforcement des capacités

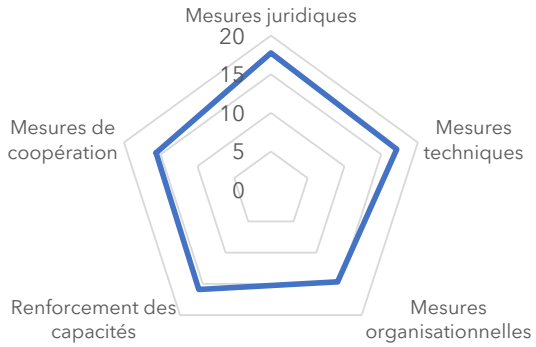
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,60	20,00	19,21	18,98	20,00	19,41

Source: Indice mondial de cybersécurité V4, UIT, 2020

Géorgie



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques

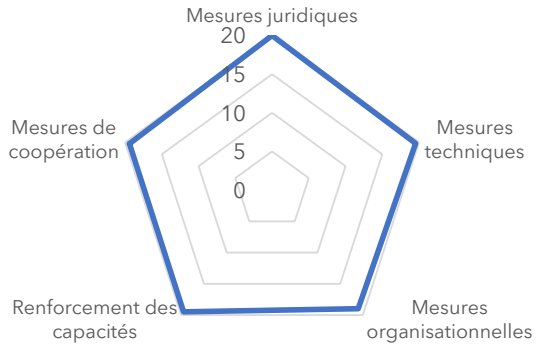
Domaine(s) de croissance potentielle

Mesures organisationnelles, de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
81,07	17,75	17,13	14,67	15,89	15,63

Source: Indice mondial de cybersécurité V4, UIT, 2020

Allemagne (République fédérale d')



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, techniques, renforcement des capacités, mesures de coopération

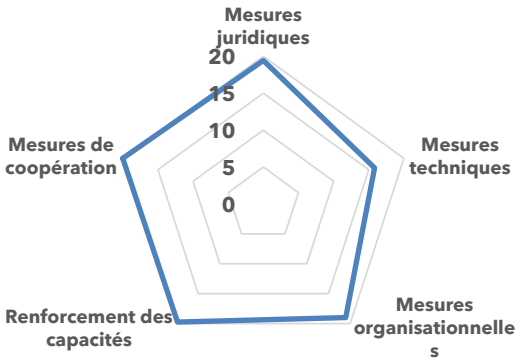
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,41	20,00	19,54	18,98	19,48	19,41

Source: Indice mondial de cybersécurité V4, UIT, 2020

Grèce



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération, renforcement des capacités, mesures juridiques

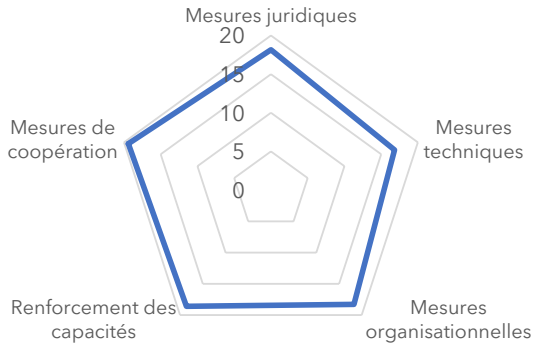
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
93,98	19,43	15,83	18,98	19,74	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Hongrie



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération, renforcement des capacités

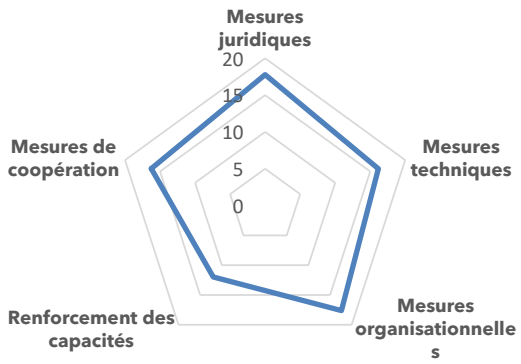
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
91,28	18,16	16,82	18,29	18,60	19,41

Source: Indice mondial de cybersécurité V4, UIT, 2020

Islande



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, organisationnelles

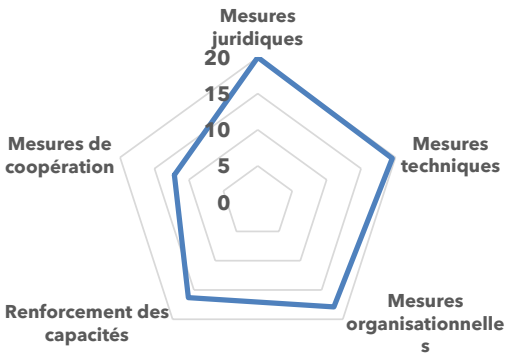
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
79,81	17,78	16,17	17,62	11,99	16,25

Source: Indice mondial de cybersécuritéV4, UIT

Irlande



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, techniques

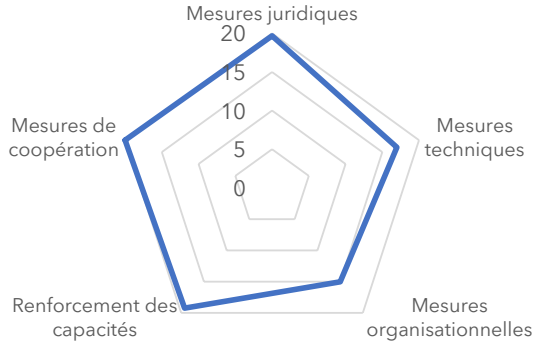
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
85,86	20,00	19,54	17,89	16,32	12,11

Source: Indice mondial de cybersécuritéV4, UIT

*Israël (État d')***



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération, juridiques

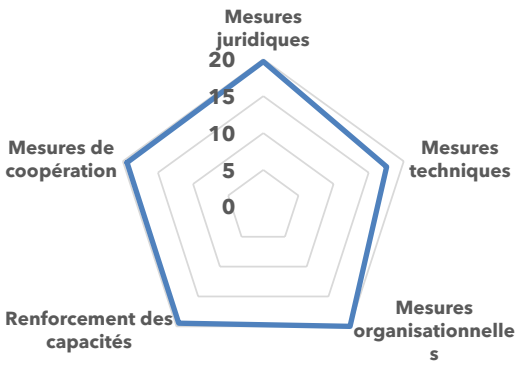
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
90,93	19,68	16,99	15,02	19,24	20,00

Source: Indice mondial de cybersécurité V4, UIT, 2020

Italie



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures organisationnelles

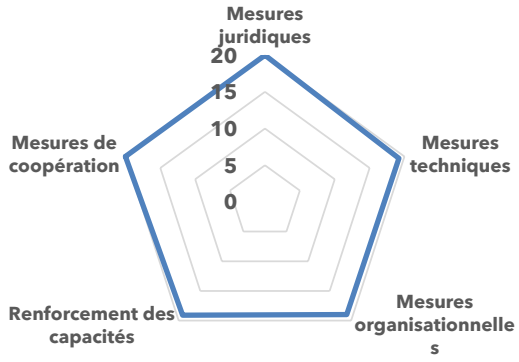
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
96,13	19,68	17,56	20,00	19,48	19,41

Source: Indice mondial de cybersécuritéV4, UIT

Lettonie (République de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, de coopération, techniques, renforcement des capacités

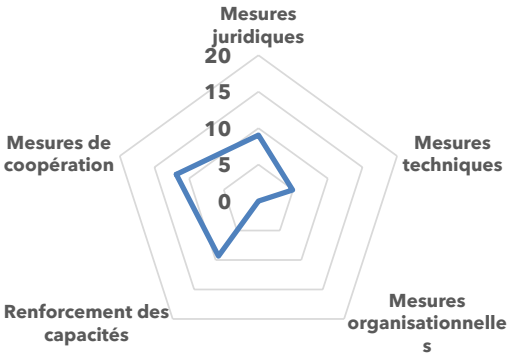
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,28	20,00	19,21	18,98	19,09	20,00

Source: Indice mondial de cybersécuritéV4, UIT

*Liechtenstein (Principauté de)***



Niveau de développement:

Pays développé, pays sans littoral

Domaine(s) de force relative

Mesures de coopération

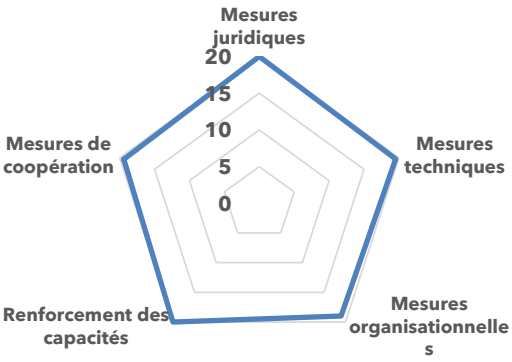
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
35,15	9,04	4,93	0,00	9,34	11,85

Source: Indice mondial de cybersécuritéV4, UIT

Lituanie (République de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, renforcement des capacités, mesures techniques, de coopération

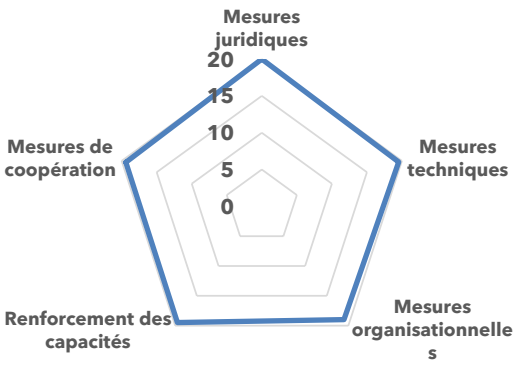
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,93	20,00	19,54	18,98	20,00	19,41

Source: Indice mondial de cybersécuritéV4, UIT

Luxembourg



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, renforcement des capacités, mesures techniques, de coopération

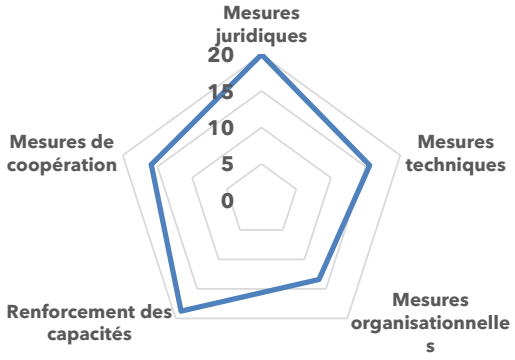
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,41	20,00	19,54	18,98	19,48	19,41

Source: Indice mondial de cybersécuritéV4, UIT

Malte



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques

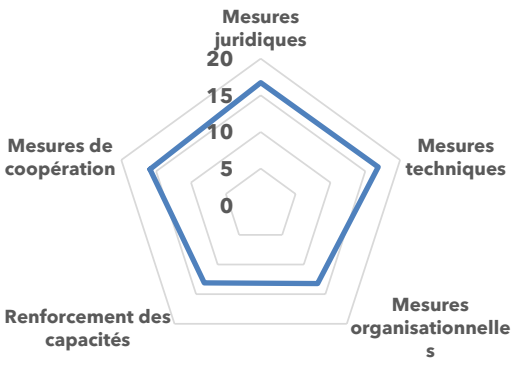
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
83,65	20,00	15,59	13,41	18,76	15,89

Source: Indice mondial de cybersécuritéV4, UIT

Moldova (République de)



Niveau de développement:

Pays développé, pays sans littoral

Domaine(s) de force relative

Mesures techniques

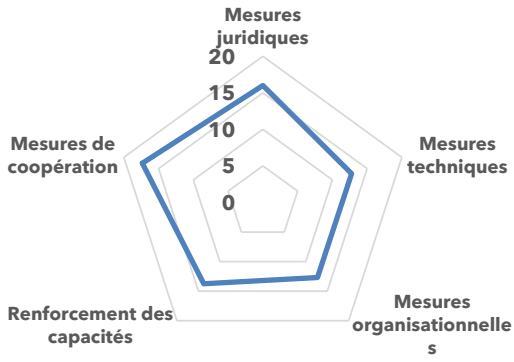
Domaine(s) de croissance potentielle

Mesures organisationnelles, Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
75,78	16,73	16,86	13,21	13,09	15,89

Source: Indice mondial de cybersécuritéV4, UIT

Monaco (Principauté de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération

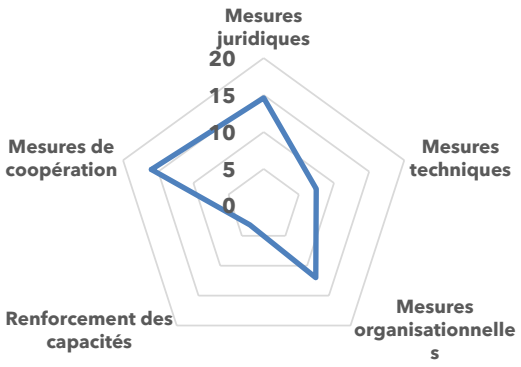
Domaine(s) de croissance potentielle

Mesures techniques, organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
72,57	16,00	12,77	12,70	13,75	17,34

Source: Indice mondial de cybersécuritéV4, UIT

Monténégro



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération

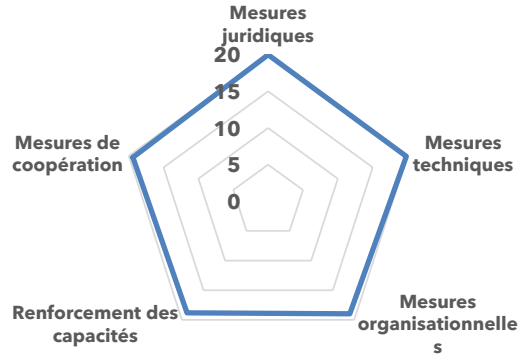
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
53,23	14,61	7,48	12,00	3,18	15,97

Source: Indice mondial de cybersécuritéV4, UIT

*Pays-Bas (Royaume des)***



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, techniques, de coopération

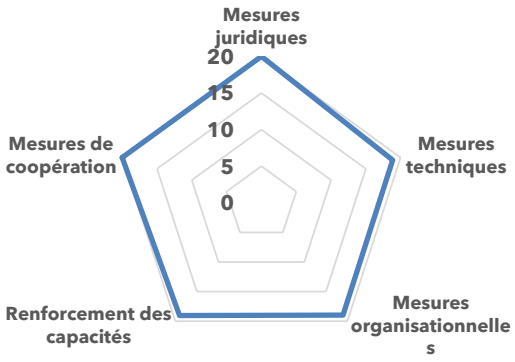
Domaine(s) de croissance potentielle

Mesures organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,05	20,00	19,84	18,98	18,82	19,41

Source: Indice mondial de cybersécuritéV4, UIT

*Norvège***



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, mesures de coopération

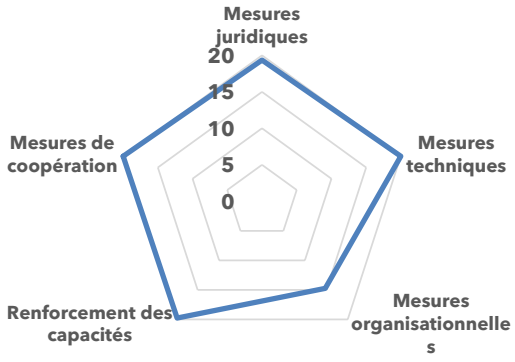
Domaine(s) de croissance potentielle

Renforcement des capacités, mesures techniques, juridiques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
96,89	20,00	18,86	18,98	19,04	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Pologne (République de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures techniques, de coopération, juridiques, renforcement des capacités

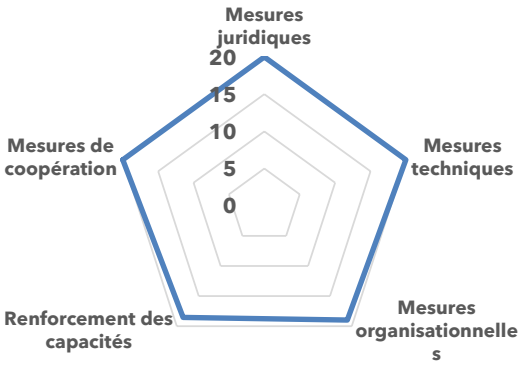
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
93,86	19,35	20,00	14,74	19,77	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Portugal



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, techniques de coopération

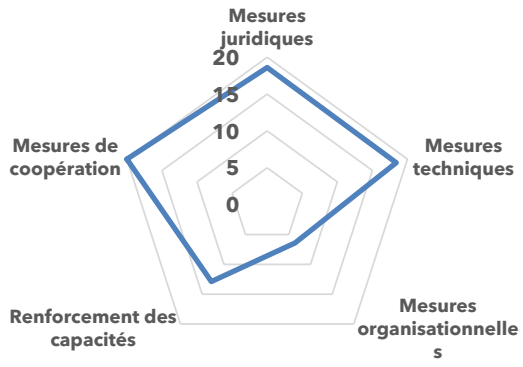
Domaine(s) de croissance potentielle

Mesures organisationnelles, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,32	20,00	20,00	18,98	18,34	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Roumanie



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération

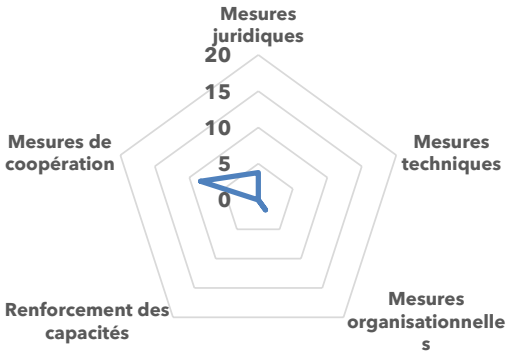
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
76,29	18,60	18,40	6,42	12,88	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Saint-Marin (République de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération

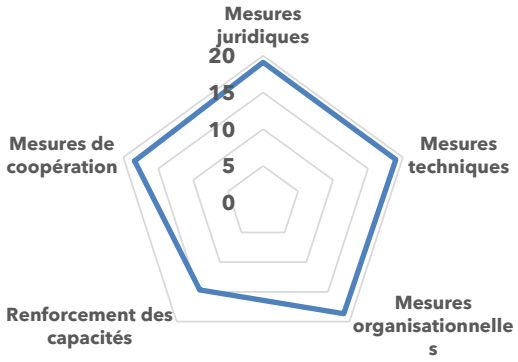
Domaine(s) de croissance potentielle

Mesures techniques, renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
13,83	3,77	0,00	1,69	0,00	8,37

Source: Indice mondial de cybersécuritéV4, UIT

Serbie (République de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, techniques, organisationnelles, de coopération

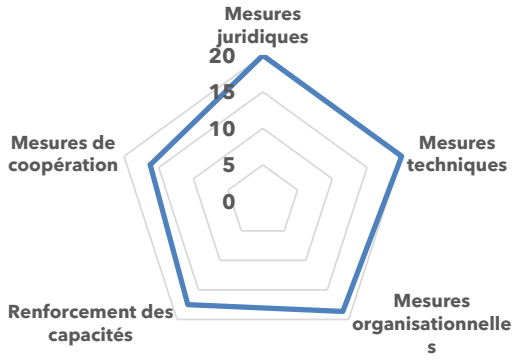
Domaine(s) de croissance potentielle

Renforcement des capacités

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
89,80	19,10	18,99	18,67	14,66	18,38

Source: Indice mondial de cybersécuritéV4, UIT

République slovaque



Niveau de développement:

Pays développé, pays sans littoral

Domaine(s) de force relative

Mesures juridiques, techniques

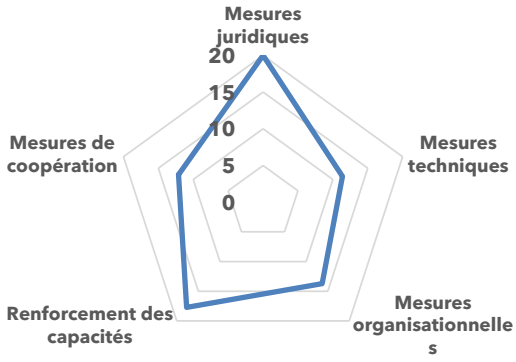
Domaine(s) de croissance potentielle

Mesures de coopération

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
92,36	20	20	18,64	17,50	16,22

Source: Indice mondial de cybersécuritéV4, UIT

Slovénie (République de)



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques

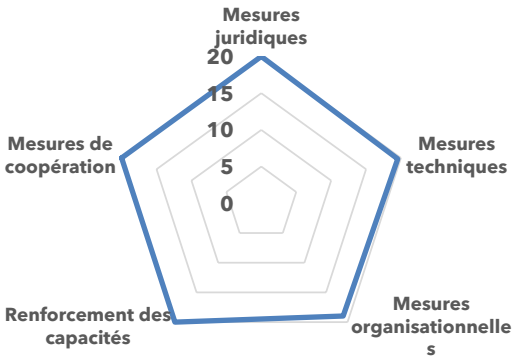
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
74,93	20	11,38	13,71	17,72	12,11

Source: Indice mondial de cybersécuritéV4, UIT

Espagne



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, de coopération, renforcement des capacités, mesures techniques

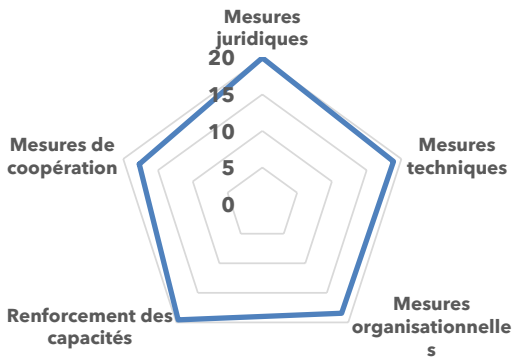
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
98,52	20,00	19,54	18,98	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Suède



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques

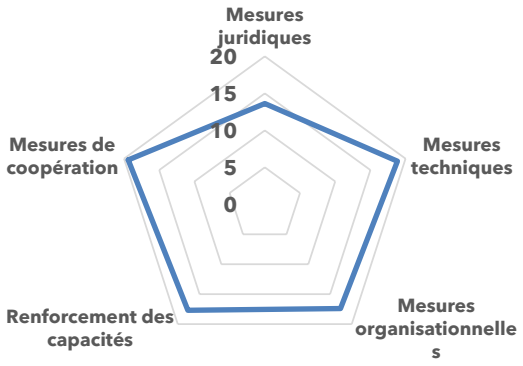
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
94,59	20,00	18,86	18,46	19,57	17,70

Source: Indice mondial de cybersécuritéV4, UIT

*Suisse (Confédération)***



Niveau de développement:

Pays développé, pays sans littoral

Domaine(s) de force relative

Mesures techniques, de coopération

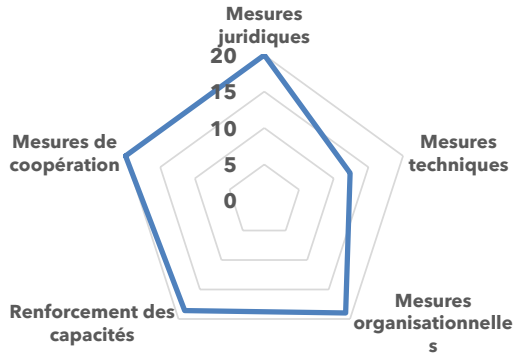
Domaine(s) de croissance potentielle

Mesures juridiques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
86,97	13,62	18,85	17,40	17,69	19,41

Source: Indice mondial de cybersécuritéV4, UIT

Macédoine du Nord (République de)



Niveau de développement:

Pays développé, sans littoral

Domaine(s) de force relative

Mesures juridiques, de coopération

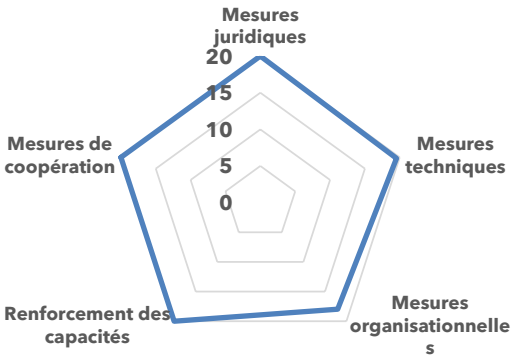
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
89,92	20,00	12,37	18,98	18,57	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Turquie



Niveau de développement:

Pays en développement

Domaine(s) de force relative

Mesures juridiques, de coopération, techniques, renforcement des capacités

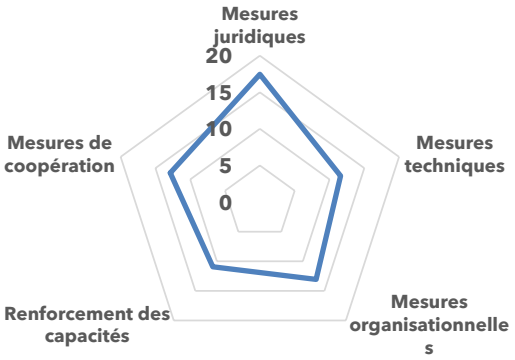
Domaine(s) de croissance potentielle

Mesures organisationnelles

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Renforcement des capacités	Mesures de coopération
97,50	20,00	19,54	17,96	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

Ukraine



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures de coopération

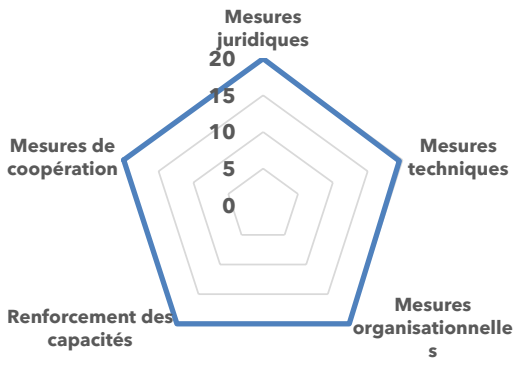
Domaine(s) de croissance potentielle

Mesures juridiques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Mesures de coopération	Renforcement des capacités
65,93	17,46	11,60	13,06	10,94	12,87

Source: Indice mondial de cybersécuritéV4, UIT

Royaume-Uni de Grande-Bretagne et d'Irlande du Nord



Niveau de développement:

Pays développé

Domaine(s) de force relative

Mesures juridiques, organisationnelles, de coopération, renforcement des capacités

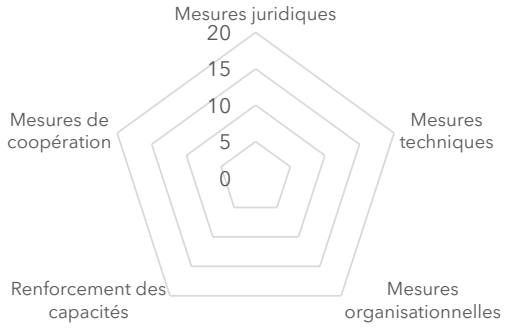
Domaine(s) de croissance potentielle

Mesures techniques

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Mesures de coopération	Renforcement des capacités
99,54	20,00	19,54	20,00	20,00	20,00

Source: Indice mondial de cybersécuritéV4, UIT

*Vatican**



Niveau de développement:

Pays développé, pays sans littoral

Domaine(s) de force relative

sans objet

Domaine(s) de croissance potentielle

sans objet

Note globale	Mesures juridiques	Mesures techniques	Mesures organisationnelles	Mesures de coopération	Renforcement des capacités
0	**0**	**0**	**0**	0	0

Source: Indice mondial de cybersécurité V4, UIT, 2020

** pas de réponse au questionnaire/données recueillies par l'équipe du GCI

* pas de données

Glossaire

Abréviation	Définition
CERT	Équipe d'intervention en cas d'urgence informatique, marque déposée par l'université Carnegie Mellon
CIRT*	Équipe d'intervention en cas d'incident informatique, *voir les termes connexes CSIRT, CERT*
CSIRT	Équipe d'intervention en cas d'incident relatif à la sécurité informatique
DPP	Protection des données personnelles et de la vie privée
GCI-1/2/3/4	Itération de l'Indice mondial de cybersécurité
IC	Infrastructure critique
MLAT	Traité d'assistance juridique mutuelle
MPME	Micro, petites et moyennes entreprises
NCS	Stratégie nationale en matière de cybersécurité
ODC	Autres pays en développement
ONG	Organisation non gouvernementale
ONU	Organisation des Nations Unies
PDSL	Pays en développement sans littoral
PEID	Petits États insulaires en développement
PMA	Pays les moins avancés
PME	Petites et moyennes entreprises
PPP	Partenariat public-privé
RGPD	Règlement général sur la protection des données (UE)
TIC	Technologies de l'information et de la communication
TO	Technologie opérationnelle
UE	Union européenne
UIT	Union internationale des télécommunications

Annexe A: Méthodologie

A1. Portée et cadre du GCI

Le mandat de l'Indice mondial de cybersécurité (GCI) découle de la Résolution de plénipotentiaires 130 (Rév. Dubaï, 2018) de l'UIT 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 (TIC). Plus précisément, les pays 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*". L'objectif du GCI est de favoriser une culture mondiale de la cybersécurité et son intégration au cœur des TIC.

Tableau A1: Participation à l'Indice mondial de cybersécurité et années de collecte des données

	GCI-1	GCI-2	GCI-3	GCI-4
Pays ayant désigné un coordonnateur	105	136	155	169
Années de collecte des données	2013-2014	2016	2017-2018	2020
Année de publication	2015	2017	2019	2021

Le GCI est établi à partir des données fournies par les membres de l'UIT, y compris les personnes intéressées, les experts et les acteurs du secteur en tant que partenaires contributeurs avec l'Australia Strategic Policy Institute, FIRST (Forum des équipes de sécurité et d'intervention en cas d'incidents), l'Université de Grenoble (France), l'Université de l'Indiana, INTERPOL, le Centre régional de cybersécurité UIT-Arabe à Oman, l'Agence coréenne de l'Internet et de la sécurité, NTRA Égypte, Red Team Cyber, The Potomac Institute of Policy Studies, UNICRI, University of Technology Jamaica, ONUDC et la Banque mondiale.

Portée du GCI

L'indice mondial de cybersécurité (GCG) est un indice composite d'indicateurs, évoluant à chaque itération, qui surveille le niveau d'engagement en matière de cybersécurité dans les cinq piliers du Programme mondial cybersécurité (GCA). Ses principaux objectifs sont de mesurer:

- le type, le niveau et l'évolution dans le temps de l'engagement en matière de cybersécurité au sein des pays et par rapport aux autres pays;
- les progrès de l'engagement des pays en matière de cybersécurité dans une perspective mondiale;
- les progrès de l'engagement en matière de cybersécurité dans une perspective régionale;
- la fracture de l'engagement en matière de cybersécurité (c'est-à-dire la différence entre les pays en matière de niveau d'engagement dans les initiatives de cybersécurité).

L'objectif du GCI est d'aider les pays à identifier les domaines à améliorer en matière de cybersécurité et de les encourager à prendre des mesures dans ces domaines. Il peut aussi donner la possibilité de contribuer à élever le niveau général d'engagement en matière de cybersécurité dans le monde, d'harmoniser les pratiques et de favoriser une culture mondiale de la cybersécurité. Le GCI vise à illustrer des exemples de réussite dans le domaine de la cybersécurité qui pourraient servir de bonnes pratiques et de lignes directrices aux pays dont l'environnement national est similaire.

A2. Cadre de l'UIT pour la coopération en matière de cybersécurité

La cybersécurité est un domaine multidisciplinaire et son application concerne tous les secteurs et toutes les parties prenantes, tant verticalement qu'horizontalement. Afin d'accroître le développement des capacités nationales, des efforts doivent être consentis par les forces politiques, économiques et sociales. Pour cela, on peut faire appel aux services du maintien de l'ordre et aux Ministères de la justice, aux établissements scolaires et aux Ministères de l'éducation, aux opérateurs du secteur privé et aux concepteurs de technologie, aux partenariats public-privé et à la coopération intra-étatique.

Le cadre de l'UIT pour la coopération internationale multipartite en matière de cybersécurité vise à créer des synergies entre les initiatives actuelles et futures et se concentre sur les cinq piliers suivants, qui sont les éléments constitutifs d'une culture nationale de la cybersécurité.

Tableau A2: Description des piliers du GCI 2020

Mesures juridiques	
	Mesures fondées sur l'existence de cadres juridiques traitant de la cybersécurité et de la cybercriminalité.
	Les mesures juridiques (y compris la législation, la réglementation et la législation sur le filtrage du spam) autorisent un État à mettre en place des mécanismes d'intervention de base par le biais d'enquêtes et de poursuites pénales et par l'imposition de sanctions en cas de non-respect ou de violation de la loi. Un cadre législatif établit les bases minimales d'un comportement sur lequel d'autres capacités de cybersécurité peuvent être construites. Fondamentalement, l'objectif est de disposer d'une législation suffisante pour harmoniser les pratiques au niveau régional/international et simplifier la lutte internationale contre la cybercriminalité.
Mesures techniques	
	Mesures fondées sur l'existence d'institutions et de cadres techniques traitant de la cybersécurité.
	Le développement et l'utilisation efficaces des TIC ne sont possibles que dans un environnement de confiance et de sécurité. Les pays doivent donc élaborer et mettre en place des critères de sécurité minimaux acceptés et des systèmes d'accréditation pour les applications logicielles et les systèmes. Ces efforts doivent être complétés par la mise en place d'un organisme national chargé des cyberincidents, d'une entité gouvernementale faisant autorité et d'un cadre national de surveillance, d'alerte et de réaction aux incidents.
Mesures organisationnelles	

Tableau A2: Description des piliers du GCI 2020 (suite)

	Mesures fondées sur l'existence d'institutions, de politiques et de stratégies de coordination pour le développement de la cybersécurité au niveau national.
	Les mesures organisationnelles comprennent le recensement des objectifs et des plans stratégiques en matière de cybersécurité ainsi que la définition officielle des rôles, des responsabilités et des obligations de rendre compte des institutions pour assurer leur mise en œuvre. Ces mesures sont indispensables pour entériner l'élaboration et la mise en œuvre d'une position en matière de cybersécurité efficace. L'État doit fixer des cibles et des objectifs stratégiques généraux ainsi qu'un plan global de mise en œuvre, d'exécution et de mesure. Des agences nationales doivent être présentes pour mettre en œuvre la stratégie et évaluer les résultats. En l'absence d'une stratégie nationale, d'un modèle de gouvernance et d'un organe de surveillance, les efforts déployés dans les différents secteurs deviennent contradictoires, ce qui empêche toute harmonisation efficace du développement de la cybersécurité.
Renforcement des capacités	
	Mesures fondées sur l'existence de programmes de recherche et développement, d'éducation et de formation, de professionnels certifiés et d'organismes du secteur public favorisant le renforcement des capacités.
	Le renforcement des capacités comprend des campagnes de sensibilisation du public, un cadre pour la certification et l'accréditation des professionnels de la cybersécurité, des cours de formation professionnelle en cybersécurité, des programmes éducatifs ou des cursus universitaires, etc. Ce pilier est intrinsèque aux trois premiers piliers (juridique, technique et organisationnel). La cybersécurité est le plus souvent abordée sous l'angle technologique alors qu'elle a de nombreux aspects socio-économiques et politiques. Le renforcement des capacités humaines et institutionnelles est essentiel pour sensibiliser les secteurs, renforcer les connaissances et le savoir-faire, trouver des solutions systématiques et appropriées et favoriser la formation de professionnels qualifiés.
Mesures de coopération	
	Mesures fondées sur l'existence de partenariats, de cadres de coopération et de réseaux de partage de renseignements.
	En raison du niveau d'interconnexion sans précédent entre les États, la cybersécurité est une responsabilité partagée et un défi transnational. Une coopération accrue peut permettre le développement de capacités de cybersécurité beaucoup plus solides, contribuant à atténuer les cyberrisques et à améliorer les enquêtes sur les agents malveillants, leur appréhension et leur poursuite.

A3. Changements essentiels par pilier

Mesures juridiques

Les mesures juridiques évaluent les interventions juridiques en matière de cybersécurité et ont été mises à jour pour mieux refléter le droit matériel national lié à la cybersécurité.

- Sur la base des recommandations du groupe de consultation de la direction du BDT, le droit procédural n'est plus mesuré dans l'Indice mondial de cybersécurité. Au lieu de cela, l'accent est mis sur la clarté dans plusieurs domaines, notamment l'usurpation d'identité, le harcèlement en ligne et le racisme.
- Les questions relatives aux mesures juridiques ont été initialement élaborées en suivant les recommandations de conventions comme la Convention de Budapest sur la cybercriminalité. Cependant, les réponses s'attachent désormais à mettre en évidence les

lois nationales mises en œuvre uniquement, et ne rassemblent plus les ratifications de ces conventions. Néanmoins, étant donné les incidences des conventions internationales et leur rôle dans la création d'engagements contraignants, les conventions internationales comme la Convention de Budapest sont désormais évaluées dans le cadre des activités internationales de mesures de coopération.

- Comme les individus sont de plus en plus souvent en ligne, un cyberespace digne de confiance qui favorise également la diversité et l'inclusion exige d'examiner des questions comme la vie privée ainsi que le harcèlement, l'intimidation, la manipulation psychologique, la pornographie infantile et le racisme. La présente itération de l'indice mondial de cybersécurité a ajouté des questions sur ces sujets.

Mesures techniques

Le pilier technique a été restructuré pour mieux refléter le mode de fonctionnement des CIRT, notamment:

- les équipes d'intervention en cas d'incident informatique - les CIRT gouvernementales et nationales ont été combinées en un seul indicateur;
- la certification des CIRT est un élément important pour donner un aperçu de la capacité à faire face aux cyberincidents. Pour évaluer les niveaux de maturité des CIRT[1] nationales, le modèle de certification SIM3 a été ajouté. Les groupes de travail CSIRT (TF-CSIRT)/ Trusted Introducer utilisent le modèle SIM3 comme base d'évaluation et les membres "certifiés" ont le plus haut niveau de maturité. Les itérations futures de l'Indice mondial de cybersécurité exploreront plus en profondeur les modèles de maturité de sécurité pour les CIRT.

Mesures organisationnelles

- La cybersécurité étant un processus continu, les pays sont encouragés à réexaminer et à réviser régulièrement les stratégies nationales de cybersécurité (au moins tous les cinq ans) afin de déterminer si elles sont toujours pertinentes compte tenu de l'évolution de l'environnement de risque, si elles reflètent toujours les objectifs nationaux et pour comprendre quels ajustements sont nécessaires. Sur la base de cette recommandation, les pays qui n'ont pas réaffirmé ou mis à jour leur stratégie nationale de cybersécurité au cours des cinq dernières années ont reçu des points partiels sur les indicateurs relatifs à cette stratégie.
- La mise au point de mécanismes de protection en ligne des enfants devrait figurer parmi les priorités vitales des pays, surtout au moment où la pandémie de COVID-19 a contraint les enfants à étudier en ligne. Si Internet apporte des avantages considérables à l'éducation et à l'épanouissement des enfants, il les expose également à des risques en ligne. La plupart des pays ont pris des initiatives en faveur de la protection en ligne des enfants, notamment en créant des sites web et des médias sociaux avec des supports pédagogiques spécialisés, des jeux informatifs et des guides pour les enfants, les parents et les éducateurs. Afin de distinguer les interventions ad hoc de celles qui sont structurées dans le cadre d'une stratégie plus large et définie, ces dernières ont reçu des notes complètes, tandis que les pays ayant mis en place des initiatives ponctuelles ou sporadiques ont reçu des notes partielles.

Développement des capacités

Les indicateurs de ce pilier sont stables depuis la deuxième itération du GCI. Dans la présente itération, la portée a été élargie pour inclure la sensibilisation au soutien du gouvernement aux petites et moyennes entreprises (PME), car ces dernières jouent un rôle important en tant

[1] Aussi connues sous la dénomination CSIRT/CERT, les CIRT sont des entités organisationnelles chargées de coordonner et d'appuyer les interventions en réponse à des événements ou des incidents en matière de sécurité informatique au niveau national.

qu'acteurs de l'économie numérique et des chaînes d'approvisionnement, notamment dans une période de transition vers le commerce électronique. De plus, les PME ont besoin de soutien pour la gestion des cyberrisques.

Mesures de coopération

Ce pilier indique si les accords sont signés ou ratifiés, indépendamment du fait qu'ils soient juridiquement contraignants. Les accords qui entrent dans la catégorie des accords bilatéraux et multilatéraux ont été précisés. La Convention de Budapest, qui était précédemment comptabilisée dans les accords multilatéraux, est désormais comptabilisée dans l'activité internationale.

A4. Méthodologie de calcul

Le questionnaire utilisé pour le GCI fournit une valeur pour les 20 indicateurs élaborés à partir de 82 questions. Cela permet d'atteindre le niveau de détail requis et d'améliorer la précision et la qualité des réponses. Les indicateurs se trouvent dans le questionnaire du GCI (Annexe B).

Les indicateurs utilisés pour calculer le GCI ont été sélectionnés en fonction de:

- la pertinence par rapport aux cinq piliers du GCI;
- la pertinence par rapport aux principaux objectifs et au cadre conceptuel du GCI;
- la disponibilité et la qualité des données; et
- la possibilité de vérifications croisées avec des données secondaires.

Le GCI est fondé sur une carte de développement de la cybersécurité qu'un pays peut prendre en compte pour améliorer son engagement en matière de cybersécurité. Le questionnaire a été élaboré sur la base de cinq piliers différenciés par cinq couleurs spécifiques. Dans les graphiques du présent rapport, la profondeur du trajet indique un niveau de développement plus élevé de l'engagement.

Le présent rapport indique quelles sont les tendances régionales et mondiales. Pour garantir l'exactitude des réponses, les pays ont été invités à les étayer en téléchargeant des documents et des URL. Une section de commentaires a été ajoutée à chaque pilier pour permettre aux pays de présenter des bonnes pratiques qui témoignent des effets de leur évolution en matière de cybersécurité.

Les pays se sont vu proposer des réponses binaires ou ternaires pour les 82 questions des 20 indicateurs des 5 piliers. La section commentaire a été utilisée pour détailler le stade de mise en œuvre dans le cas où un élément était en phase de projet ou de mise en œuvre.

Une fois les questionnaires retournés, ils ont fait l'objet de deux validations par deux validateurs différents. Des points partiels ont été accordés si la réponse faisait référence à un projet ou à un stade de mise en œuvre ou si elle ne répondait pas spécifiquement à tous les éléments de la question. Ce mode d'évaluation ternaire a permis d'éviter les évaluations basées sur des opinions et les biais subjectifs grâce à un tableau contenant des éléments spécifiques à présenter pour une réponse positive ou partielle.

À cette fin, la quatrième édition du questionnaire de l'Indice mondial de cybersécurité et toute documentation connexe ont été soumises par le Secrétariat du BDT à la réunion du Groupe du rapporteur de la Question 3 de la Commission d'études 2 en octobre 2019, où le questionnaire

a été approuvé avant son lancement. En mars 2020, lors de la réunion de la CE, le BDT a informé la Question 3 de l'état d'avancement et a consulté les pays pour qu'ils désignent des experts dans le domaine de la cybersécurité afin de participer au processus de répartition des pondérations.

Flux global du processus GCI

1) Une lettre d'invitation est envoyée à tous les États Membres de l'UIT et à l'État de Palestine les informant de l'initiative et demandant que soit désigné un coordonnateur chargé de collecter toutes les données pertinentes et de remplir le questionnaire en ligne du GCI. Pendant l'enquête en ligne, le coordonnateur agréé est officiellement invité par l'UIT à répondre au questionnaire.
2) Collecte de données primaires (pour les pays qui ne répondent pas au questionnaire):
    - l'UIT élabore un premier projet de réponse au questionnaire en utilisant les données disponibles publiquement et les recherches en ligne;
    - le projet de questionnaire est envoyé aux coordonnateurs pour examen;
    - les coordonnateurs améliorent la précision du projet de questionnaire et le retournent;
    - le projet de questionnaire corrigé est envoyé à chaque coordonnateur pour approbation finale;
    - le questionnaire validé est utilisé pour l'analyse, la notation et le classement.
3) Collecte de données secondaires (pour les pays qui répondent au questionnaire):
    - l'UIT recense les réponses, documents justificatifs, liens, etc. manquants;
    - le cas échéant, le coordonnateur améliore la précision des réponses;
    - le projet de questionnaire corrigé est envoyé à chaque coordonnateur pour approbation finale;
    - le questionnaire validé est utilisé pour l'analyse, la notation et le classement.

Note: si un pays ne désigne pas de coordonnateur pour le questionnaire du GCI, l'UIT établira un contact avec le coordonnateur institutionnel figurant dans le répertoire général de l'UIT.

Pondération

Contrairement aux itérations précédentes, qui ont une échelle de 0 à 1, la présente itération du CGI est sur une échelle de 0 à 100, chaque pilier étant pondéré à 20 points.

En tant qu'indice composite pondéré, chaque indicateur, sous-indicateur et micro-indicateur se voit attribuer un poids en fonction de son importance relative pour le groupe d'indicateurs. La pondération peut avoir un impact significatif sur les notes finales et des techniques différentes produiront des classements différents.

Le GCI a adopté une approche participative, en utilisant le processus d'allocation budgétaire (PAB). Cette approche tenait compte du fait que les pondérations sont, fondamentalement, des jugements de valeur, et qu'il fallait prendre en considération une grande variété d'apports d'experts.

Dans le cadre de l'approche d'allocation budgétaire, les experts disposaient d'un "budget" donné qu'ils pouvaient répartir au sein d'un groupe d'indicateurs, en allouant un montant plus important aux indicateurs jugés plus importants. Les experts ont été invités à formuler des

recommandations de pondération pour les piliers dans lesquels ils avaient des compétences techniques.

Comme toutes les réponses des pays à la base des données étaient des données d'enquête notifiées, vérifiées par l'équipe de l'UIT, la pondération n'a pas tenu compte de la qualité statistique des données.

Participation du groupe d'experts chargé de la pondération

En octobre 2020, les États Membres de l'UIT et les membres du secteur privé ont été invités par lettre circulaire à désigner des experts pour participer à la présente itération de l'Indice mondial de cybersécurité. Les experts désignés étaient affiliés à des établissements universitaires, des groupes de réflexion, des ministères des TIC, des organismes de réglementation et des organismes de normalisation.

Les experts qui ont contribué aux itérations précédentes de l'Indice mondial de cybersécurité ont également été invités à formuler des recommandations en matière de pondération.

Au total, 84 experts ont participé à l'exercice et ont été invités à formuler des recommandations de pondération dans les piliers liés à leurs domaines de compétences techniques.

Agrégation

Les groupes d'indicateurs ont été agrégés en utilisant des moyennes arithmétiques pondérées. Cela signifie qu'un pays obtenant de mauvais résultats dans un domaine peut récupérer une partie de sa note en obtenant de bons résultats ailleurs.

Comme indiqué dans le Guide de l'OCDE sur les indices composites, "*l'utilité marginale d'une augmentation de la note absolue faible serait beaucoup plus élevée que celle d'une note absolue élevée dans le cadre d'une agrégation géométrique. Par conséquent, un pays serait fortement incité à s'intéresser aux secteurs/activités/alternatives ayant une faible note si l'agrégation était géométrique plutôt que linéaire*" (33). Cependant, pour des raisons de clarté et de compréhension, une approche linéaire a été jugée plus compréhensible et exploitable.

Analyse de sensibilité

Compte tenu de l'importance de la pondération dans les notes finales des pays, des analyses de sensibilité ont été effectuées, notamment:

- inclusion/exclusion d'indicateurs individuels;
- différents systèmes de pondération (pondération égale, méthode d'allocation budgétaire, extrêmes des recommandations d'experts);
- différents systèmes d'agrégation (moyennes pondérées, additif).

Classements

Les pays ont été classés selon leur note finale, en utilisant une méthode de classement "dense". Des notes égales entraînent le même classement. Le pays suivant après deux ou plusieurs pays de même rang reçoit le numéro ordinal suivant.

Annexe B: Questionnaire de l'Indice de cybersécurité mondial (4ème édition)

Le présent questionnaire a été élaboré et examiné par les participants à la réunion du Groupe du Rapporteur pour la Question 3/2 (Sécurisation des réseaux d'information et de communication: Bonnes pratiques pour créer une culture de la cybersécurité) de la Commission d'études 2 de l'UIT-D. Cette réunion a servi de cadre pour rechercher l'approbation des Membres en vue de la publication de la 4ème version de l'Indice mondial de cybersécurité de l'UIT.

Le questionnaire se compose de cinq parties, dans lesquelles il faut répondre oui ou non et cocher les cases figurant devant chaque élément, le cas échéant. Il doit être rempli en ligne. Chaque répondant a reçu (dans un courriel officiel de l'UIT) une adresse URL unique et des informations de connexion à fournir dans les réponses. Il permet également aux répondants de télécharger des documents pertinents (et des URL) pour chaque question en tant qu'informations complémentaires. Les informations fournies par les répondants à ce questionnaire ne sont pas censées être de nature confidentielle.

Tableau B1: Questionnaire du GCI: Mesures juridiques

1. Règle juridique de fond en matière de cybercriminalité

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B1: Questionnaire du GCI: Mesures juridiques (suite)

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

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B1: Questionnaire du GCI: Mesures juridiques (suite)

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B1: Questionnaire du GCI: Mesures juridiques (suite)

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

On entend par réglementation en matière de cybersécurité les principes auxquels doivent se soumettre diverses parties prenantes, qui émanent et font partie de la mise en œuvre de la législation régissant: la protection des données, la notification des infractions, les obligations relatives à la certification/normalisation en matière de cybersécurité, la mise en 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.

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B1: Questionnaire du GCI: Mesures juridiques (suite)

2.2 Le signalement des atteintes aux données/incidents?

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

2.3 Les obligations en matière d'audits de cybersécurité?

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

2.4 La mise en œuvre des normes?

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B1: Questionnaire du GCI: Mesures juridiques (suite)

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours dans le domaine juridique auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité.

Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui

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

Tableau B2: Questionnaire du GCI: Mesure techniques

1. Équipe CIRT/CSIRT/CERT nationale/gouvernementale.

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

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B2: Questionnaire du GCI: Mesure techniques (suite)

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B2: Questionnaire du GCI: Mesure techniques (suite)

2. Équipes CIRT/CSIRT/CERT sectorielles

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

2.2.2 Participation active aux cyberexercices nationaux?

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B2: Questionnaire du GCI: Mesure techniques (suite)

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

4. Protection en ligne des enfants

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours dans le domaine technique auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité.

Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui.

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

Tableau B3: Questionnaire GCI: Mesures organisationnelles

1. Stratégie nationale en matière de cybersécurité

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B3: Questionnaire GCI: Mesures organisationnelles (suite)

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B3: Questionnaire GCI: Mesures organisationnelles (suite)

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

2. Organisme responsable

Explication: L'organisme responsable de la mise en 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. Il peut appartenir au gouvernement et avoir le pouvoir d'obliger d'autres agences et organismes nationaux à mettre en œuvre les politiques et à adopter des normes.

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B3: Questionnaire GCI: Mesures organisationnelles (suite)

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

3. Indicateurs relatifs à la cybersécurité

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B3: Questionnaire GCI: Mesures organisationnelles (suite)

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours concernant les mesures organisationnelles auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité.

Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui.

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

Tableau B4: Questionnaire du GCI: Renforcement des capacités

1. Campagnes de sensibilisation du public à la cybersécurité

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

Explication: ONG, organisations communautaires.

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B4: Questionnaire du GCI: Renforcement des capacités (suite)

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

2. Formation à l'intention des professionnels de la cybersécurité

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

Ces programmes comprennent la formation sur la cybersécurité à l'intention des membres des forces de l'ordre, du personnel judiciaire ou d'autres acteurs de la scène juridique et désignent des formations professionnelles et techniques pouvant être organisées de manière récurrente à l'intention des agents de police ou agents des forces de l'ordre, des juges, avocats, conseillers juridiques, magistrats, auxiliaires juridiques ainsi que de toute autre professionnel dans le domaine juridique ou dans le domaine de l'application de la loi. Cet indicateur tient également compte de l'existence d'un ou plusieurs cadres approuvés (ou ratifiés) par le gouvernement concernant la certification et l'accréditation de professionnels sur la base de normes internationalement reconnues en matière de cybersécurité. Ces certifications, accréditations et normes sont notamment les suivantes: Connaissance de la sécurité dans le nuage informatique (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK et Cybersecurity Forensic Analyst (ISC^2).

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B4: Questionnaire du GCI: Renforcement des capacités (suite)

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B4: Questionnaire du GCI: Renforcement des capacités (suite)

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

3.1 Dans l'enseignement primaire?

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

3.2 Dans l'enseignement secondaire?

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

3.3 Dans l'enseignement supérieur?

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

4. Programmes de recherche-développement en matière de cybersécurité

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

Tableau B4: Questionnaire du GCI: Renforcement des capacités (suite)

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

5. Secteur de la cybersécurité à l'échelle nationale

Explication: Un environnement économique, politique et social favorable au développement de la cybersécurité facilite la croissance du secteur privé autour de cette activité. L'existence de campagnes de sensibilisation du public, le développement de la main-d'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 startups dans le domaine de la cybersécurité et de marchés de la cyberassurance associés.

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B4: Questionnaire du GCI: Renforcement des capacités (suite)

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

6.2 Créer un secteur de la cybersécurité?

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours concernant les mesures de renforcement des capacités auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité.

Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui.

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

Tableau B5: Questionnaire du GCI: Mesures de coopération

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Tableau B5: Questionnaire du GCI: Mesures de coopération (suite)

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

3. Accords multilatéraux en matière de cybersécurité

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

Tableau B5: Questionnaire du GCI: Mesures de coopération (suite)

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

4. Partenariats avec le secteur privé

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

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

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

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

5. Partenariats interorganismes

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

Tableau B5: Questionnaire du GCI: Mesures de coopération (suite)

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

Explication: Coopération entre les ministères ou les organismes spécialisés.

☐ *Oui*

☐ *Non*

Ajouter des liens/URL

Ajouter des documents

Veuillez indiquer certaines des bonnes pratiques/réalisations/avancées en cours concernant les mesures de coopération auxquelles votre pays a participé/participe au titre d'activités relatives à la cybersécurité.

Veuillez décrire la ou les pratiques de manière détaillée dans l'encadré ci-dessous et fournir des liens à l'appui.

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

Union internationale des télécommunications (UIT)
Bureau de développement des télécommunications (BDT)
Bureau du Directeur
Place des Nations
CH-1211 Genève 20
Suisse

Courriel: bdtdirector@itu.int
Tél.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Adjoint au directeur et Chef du Département de l'administration et de la coordination des opérations (DDR)
Place des Nations
CH-1211 Genève 20
Suisse

Courriel: bdtdeputydir@itu.int
Tél.: +41 22 730 5131
Fax: +41 22 730 5484

Département des réseaux et de la société numériques (DNS)
Courriel:: bdt-dns@itu.int
Tél.: +41 22 730 5421
Fax: +41 22 730 5484

Département du pôle de connaissances numériques (DKH)
Courriel: bdt-dkh@itu.int
Tél.: +41 22 730 5900
Fax: +41 22 730 5484

Département des partenariats pour le développement numérique (PDD)
Courriel: bdt-pdd@itu.int
Tél.: +41 22 730 5447
Fax: +41 22 730 5484

Afrique

Ethiopie
International Telecommunication Union (ITU) Bureau régional
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopie

Courriel: itu-ro-africa@itu.int
Tél.: +251 11 551 4977
Tél.: +251 11 551 4855
Tél.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroun
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroun

Courriel: itu-yaounde@itu.int
Tél.: + 237 22 22 9292
Tél.: + 237 22 22 9291
Fax: + 237 22 22 9297

Sénégal
Union internationale des télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Sénégal

Courriel: itu-dakar@itu.int
Tél.: +221 33 859 7010
Tél.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU) Bureau de zone
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Courriel: itu-harare@itu.int
Tél.: +263 4 77 5939
Tél.: +263 4 77 5941
Fax: +263 4 77 1257

Amériques

Brésil
União Internacional de Telecomunicações (UIT)
Bureau régional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Courriel: itubrasilia@itu.int
Tél.: +55 61 2312 2730-1
Tél.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

La Barbade
International Telecommunication Union (ITU) Bureau de zone
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Courriel: itubridgetown@itu.int
Tél.: +1 246 431 0343
Fax: +1 246 437 7403

Chili
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chili

Courriel: itusantiago@itu.int
Tél.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Courriel: itutegucigalpa@itu.int
Tél.: +504 2235 5470
Fax: +504 2235 5471

Etats arabes

Egypte
International Telecommunication Union (ITU) Bureau régional
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypte

Courriel: itu-ro-arabstates@itu.int
Tél.: +202 3537 1777
Fax: +202 3537 1888

Asie-Pacifique

Thaïlande
International Telecommunication Union (ITU) Bureau régional
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailande

Adresse postale:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Courriel: itu-ro-asiapacific@itu.int
Tél.: +66 2 574 9326 – 8
+66 2 575 0055

Indonésie
International Telecommunication Union (ITU) Bureau de zone
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonésie

Courriel: itu-ro-asiapacific@itu.int
Tél.: +62 21 381 3572
Tél.: +62 21 380 2322/2324
Fax: +62 21 389 5521

Pays de la CEI

Fédération de Russie
International Telecommunication Union (ITU) Bureau régional
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Fédération de Russie

Courriel: itumoscow@itu.int
Tél.: +7 495 926 6070

Europe

Suisse
Union internationale des télécommunications (UIT)
Bureau pour l'Europe
Place des Nations
CH-1211 Genève 20
Suisse
Courriel: eurregion@itu.int
Tél.: +41 22 730 5467
Fax: +41 22 730 5484

Union internationale des télécommunications
Place des Nations
CH-1211 Genève 20
Suisse

ISBN 978-92-61-33922-7

Publié en Suisse
Genève, 2021
Crédits photos: Shutterstock