Aperçu général des outils existants d'évaluation des capacités nationales en matière de cybersécurité (GOAT)

FORUM
MONDIAL SUR LA
CYBER
EXPERTISE

Auteurs

Le présent document a été élaboré par le Groupe de travail A – Groupe d'étude sur la stratégie et les évaluations – du Forum mondial sur la cyberexpertise (GFCE), dans le cadre d'un projet relevant de son Programme de travail pour 2020. Les membres de l'équipe de projet sont les suivants:

- Carolin Weisser Harris, Centre mondial de capacité en matière de cybersécurité (GCSCC).
- Ian Wallace, Président du Groupe de travail A du GFCE sur la stratégie et les politiques générales.
- James Boorman, Centre océanien de cybersécurité (OCSC).
- Orhan Osmani et Marwan Ben Rached, Union internationale des télécommunications (UIT).
- Melissa Hathaway et Francesca Spidalieri, Institut Potomac d'études politiques (PIPS).
- Radu Serrano, e-Governance Academy (eGA).
- Kerry-Ann Barrett, Organisation des États américains (OEA).

L'équipe de projet tient à exprimer sa reconnaissance à l'Institut australien de stratégie politique (ASPI), à l'Agence de l'Union européenne pour la cybersécurité (ENISA), à la MITRE Corporation et à la Banque mondiale pour leurs observations et leurs contributions, ainsi qu'à Kathleen Bei, du secrétariat du GFCE, pour l'appui qu'elle a apporté sur le plan de la conception, de la logistique et de l'organisation. L'équipe de projet tient également à remercier l'UIT d'avoir révisé et édité le présent document et d'en avoir assuré la traduction en arabe, français, russe et espagnol.

Table des matières

Introduction

La communauté mondiale redouble d'efforts pour mieux cerner les choix nationaux en matière de cybersécurité, afin de repérer les lacunes et de prendre des décisions plus éclairées sur les interventions et les investissements propres à renforcer les capacités en matière de cybersécurité. Des instituts de recherche, des organisations régionales et des entreprises ont mis au point des cadres, des modèles et des indices et les ont appliqués dans le monde entier, créant ainsi une base de connaissances sur le degré de cybermaturité des pays et leur niveau de préparation face aux cybermenaces croissantes qui pèsent sur les gouvernements, le secteur, les entreprises et les particuliers.

Les réactions positives qu'a suscité la session sur l'évaluation des cybercapacités organisée lors de la 5ème réunion du GFCE en avril 2020 ont souligné la nécessité de faire connaître les outils existants d'évaluation des capacités en matière de cybersécurité et de décrire de manière détaillée les méthodologies, les résultats et les effets de ces outils, afin d'aider la communauté du GFCE (bénéficiaires, bailleurs de fonds et responsables de la mise en œuvre) à choisir des outils et des approches adaptés aux besoins du moment ainsi qu'aux disparités en matière de connaissances.

En conséquence, le présent document vise à faciliter le processus de prise de décisions, en donnant une vue d'ensemble des différents outils, des approches, des avantages et des résultats qui leur sont associés, ainsi que des mesures à prendre et des personnes à contacter si un pays souhaite faire l'objet d'une évaluation.

Le Groupe de travail sur la stratégie et les évaluations du GFCE a tout particulièrement choisi des outils permettant d'évaluer les capacités d'un pays en matière de cybersécurité. En conséquence, il a retenu les outils suivants:

- Lutter contre la cybercriminalité: Outil de renforcement des capacités, Banque mondiale.
- La cybermaturité dans la région Asie-Pacifique, Institut australien de stratégie politique (ASPI).
- Indice de préparation à la lutte contre la cybercriminalité, version 2.0 (CRI), Institut Potomac d'études politiques, (PIPS).
- Modèle de maturité des capacités en matière de cybersécurité pour les nations (CMM), Centre mondial de capacités en matière de cybersécurité (GCSCC).
- Cadre pour l'élaboration et la mise en œuvre d'une stratégie de cybersécurité (CSDI), MITRE Corporation.
- Indice mondial de cybersécurité (GCI), Union internationale des télécommunications (UIT).
- Cadre d'évaluation des capacités nationales (CECN), Agence de l'Union européenne pour la cybersécurité (ENISA).
- Indice national de cybersécurité (NCSI), e-Governance Academy (eGA).

D'autres outils répondant au critère ci-dessus seront ajoutés dans le document à mesure qu'ils seront identifiés.

Aux fins du présent document, un questionnaire a été envoyé aux organisations responsables de chaque outil, afin d'obtenir des informations sur les points suivants:

- Responsable(s) de la mise en œuvre et coordonnées.
- Thèmes et questions.
- Indicateurs.

- Méthodologie, collecte des données et contrôle de la qualité.
- Résultats et présentation.
- Incidences et avantages.
- Rôle dans la coordination des activités de renforcement des capacités de cybersécurité et du processus de mise en correspondance du GFCE.

Lutter contre la cybercriminalité: Outil de renforcement des capacités

Banque mondiale

L'outil d'évaluation du renforcement des capacités de la Banque mondiale, intitulé "Lutter contre la cybercriminalité: Outil d'évaluation du renforcement des capacités ("Outil d'évaluation")", a été élaboré dans le cadre du projet de lutte contre la cybercriminalité pour aider les pays en développement à recenser les domaines prioritaires, de manière à faciliter la répartition des ressources limitées dont ils disposent aux fins du renforcement des capacités.

À la différence des autres cadres d'évaluation, l'outil d'évaluation est un outil d'autodiagnostic qui comprend neuf dimensions, à savoir: 1) Cadre non juridique; 2) Cadre juridique; 3) Droit matériel; 4) Droit procédural; 5) Eléments de preuve électroniques; 6) Compétence; 7) Sauvegardes; 8) Coopération internationale; et 9) Renforcement des capacités.

L'outil d'évaluation peut être utilisé à la fois dans le cadre d'une activité autonome menée par un pays pour son propre usage, et en tant qu'outil essentiel de diligence raisonnable pour permettre aux groupes de travail spéciaux opérationnels de déterminer si un pays est prêt à lutter contre la cybercriminalité.

Vue d'ensemble

Dernière date de mise à jour de l'outil	La dernière mise à jour de la publication a été effectuée en 2017. Nous actualisons actuellement l'outil d'évaluation existant, processus qui devrait être achevé en juillet 2021.
Quel est le nom de l'outil d'évaluation?	Lutter contre la cybercriminalité: Outil d'évaluation du renforcement des capacités
Quel est le nom de l'organisation qui gère l'outil?	Banque mondiale
Quels sont les responsables de la mise en œuvre des évaluations?	L'outil constitue un bien public mondial. Chacun peut se rendre sur le site (voir ci-dessous) et télécharger et utiliser l'outil, qui est conçu à des fins d'auto-évaluation.
Veuillez fournir des liens vers l'outil et toute information supplémentaire	https://www.combattingcybercrime.org/
Qui faut-il contacter pour discuter de l'organisation d'une évaluation?	M. David Satola, Conseiller principal, Vice-Présidence juridique, Banque mondiale
Couverture géographique	Mondiale
Qui peut utiliser l'outil?	• Décideurs • Législateurs • Autorités chargées de l'application des lois • Société civile des pays en développement • Toute personne intéressée

Quels sont les thèmes ou les sujets abordés?	Sur le plan conceptuel, l'évaluation s'articule autour des neuf dimensions suivantes: • **Cadre non juridique**: porte sur les stratégies et politiques nationales et d'autres questions de nature non juridique, par exemple la coopération avec le secteur privé. • **Cadre juridique**: porte sur le droit national et l'adhésion éventuelle d'un pays à un traité. • **Droit matériel**: traite des activités qui ont été érigées en infraction. • **Droit procédural**: traite principalement des questions d'enquête. • **Éléments de preuve électroniques**: porte sur l'admissibilité et le traitement des éléments de preuve numériques dans le contexte de la cybercriminalité. • **Compétence**: Traite essentiellement de la manière dont la compétence à l'égard du délit est déterminée. • **Garanties**, axées sur trois éléments: "procédure régulière", protection des données et liberté d'expression; • **Coopération internationale**, l'accent étant mis, premièrement, sur l'extradition et, deuxièmement, sur les niveaux formels et informels d'assistance juridique mutuelle (MLA); et • **Renforcement des capacités**: porte à la fois sur le renforcement des capacités institutionnelles (par exemple, les académies de formation des forces de l'ordre) et humaines, l'accent étant mis sur les besoins en formation des forces de l'ordre, du ministère public et de l'appareil judiciaire.
Quels sont les thèmes ou sujets traités par le GFCE?	Politiques générales et stratégie ☒ Stratégies ☒ Évaluations ☐ Mesures de renforcement de la confiance et normes ☐ Cyberdiplomatie ☒ Droit international dans le cyberspace Gestion des incidents et protection des infrastructures essentielles de l'information (CIIP) ☒ Intervention en cas d'incident de sécurité informatique ☐ Examen et analyse des incidents ☐ Exercices de cybersécurité ☒ Protection des infrastructures essentielles de l'information Cybercriminalité ☒ Cadres juridiques/Droit de la cybercriminalité ☒ Application de la loi dans le cyberespace ☒ Formation en matière de cybercriminalité ☒ Prévention de la cybercriminalité Culture et compétences ☒ Sensibilisation à la cybersécurité ☒ Éducation et formation ☒ Perfectionnement de la main-d'œuvre

	Normes ☐ Normes relatives à un Internet ouvert ☐ Internet des objets
Types d'indicateurs	Indicateurs quantitatifs et qualitatifs
Combien d'indicateurs sont utilisés et comment sont-ils appliqués?	L'outil d'évaluation comprend **115** indicateurs, regroupés autour de neuf dimensions: Cadre non juridique, Cadre juridique, Droit matériel, Droit procédural, Eléments de preuve électroniques, Compétence, Sauvegardes, Coopération internationale et Renforcement des capacités. Dans le tableau d'évaluation, les neuf dimensions sont subdivisées en quatre niveaux. Le **niveau 1** désigne chaque domaine (dimension). Le **niveau 2** fixe un cadre général pour chaque question, qui est posée au **niveau 3** et peut être affinée au **niveau 4**. La dernière colonne (indicateur) sert à indiquer une réponse "oui/non" ou un choix unique parmi un éventail de réponses.
Méthodologie – Quel type d'évaluation est utilisé?	**Propre au cas**: L'équipe chargée de la lutte contre la cybercriminalité procède à une évaluation initiale d'un pays client sur la base de recherches documentaires, puis communique ses conclusions et vérifie et valide les évaluations avec les autorités gouvernementales compétentes du pays client
Méthode de collecte des données primaires	• Informations accessibles au public • Documents non publiés • Questionnaires et enquêtes • Observations • Documents et dossiers • Entretiens individuels
Procédez-vous à la collecte de données secondaires?	Oui. À l'issue des recherches documentaires initiales, l'équipe se rend dans le pays client et consulte les autorités gouvernementales responsables, pour vérifier et valider l'évaluation initiale. • Observations • Documents et dossiers
Quels mécanismes adoptez-vous pour garantir l'exactitude des données recueillies?	Les membres de l'équipe chargée de la lutte contre la cybercriminalité, dirigée par le Conseil principal pour les TIC à la Banque mondiale, possèdent généralement des connaissances générales/compétences spécialisées dans le domaine de la cybercriminalité et s'occupent de diverses questions liées aux TIC à la Banque mondiale. En outre, l'évaluation initiale menée par les membres de l'équipe est vérifiée et validée par les autorités gouvernementales responsables dans les pays clients, afin de garantir l'exactitude des données recueillies.
Quels sont les principaux résultats de l'évaluation?	Un "Rapport d'évaluation du renforcement des capacités de lutte contre la cybercriminalité" pour chaque pays client est établi à chaque itération.
Format de présentation des résultats de l'évaluation	• Rapport d'évaluation du renforcement des capacités de lutte contre la cybercriminalité (PDF) • Outil de visualisation (graphiques Excel)
Les résultats de l'évaluation peuvent-ils être publiés?	Oui. Cependant, la publication des résultats de l'évaluation est laissée à la discrétion du pays client.

Comment accéder aux rapports précédents?	L'accès aux rapports précédents est laissé à la discrétion du pays client.
Quels sont les éléments qui attestent de résultats concrets?	L'équipe a procédé à des évaluations du renforcement des capacités de lutte contre la cybercriminalité pour des pays clients des régions Afrique et Asie-Pacifique, à savoir la Namibie, l'Éthiopie, le Kenya, les États fédérés de Micronésie et le Myanmar. En outre, l'équipe a reçu de nouvelles demandes d'évaluation émanant de 22 pays (Bénin, Burundi, République démocratique du Congo, Gambie, Libéria, Mali, Niger, Nigéria, République du Congo, Sierra Leone, Tanzanie, Ouganda, Zambie, Burkina Faso, Cabo Verde, Comores, Maroc, Cameroun, Mauritanie, Rwanda et Sénégal). De plus, l'une de nos organisations partenaires, à savoir l'Office des Nations Unies contre la drogue et le crime (ONUDC), a adopté l'outil d'évaluation comme méthode exclusive d'évaluation de la préparation à la lutte contre la cybercriminalité. Enfin, l'équipe a présenté l'outil d'évaluation lors des manifestations suivantes: Réunion annuelle du GFCE à Singapour (2018) et réunions des groupes de travail à La Haye (2018 et 2019); réunion annuelle du Conseil de l'Europe à Strasbourg (2019); conférences annuelles de l'Association internationale des procureurs (IAP) en République sudafricaine (2018) et en Argentine (2019); réunion commune du Conseil de l'Europe et de l'Union africaine (UA) sur le renforcement des capacités en matière de lutte contre la cybercriminalité en Afrique (2018); et Colloque sur le droit international à Hong Kong (Chine) (2019).
Quels sont les avantages d'une évaluation?	L'outil d'évaluation permet de procéder à une évaluation efficace et universellement applicable de l'aptitude d'un pays à garantir l'objectivité, la diversité et l'accessibilité. La combinaison de ces trois caractéristiques de l'outil d'évaluation permet aux décideurs et aux législateurs de déterminer la meilleure façon d'affecter les ressources. • **Objectivité**: la réponse à chaque question de l'outil d'évaluation se présente dans toute la mesure du possible sous une forme binaire "oui/non" ou correspond à un choix précis entre un petit nombre d'options. • **Diversité**: chaque critère est "pondéré". L'outil d'évaluation utilise environ 115 indicateurs qui s'articulent autour de neuf thèmes (ou dimensions). • **Facilité de compréhension**: l'évaluation est représentée sous forme de graphique dans un seul diagramme en étoile. Ce graphique aide le pays client à déterminer si ses pratiques actuelles sont conformes aux bonnes pratiques internationales. Chaque dimension du graphique général peut également être analysée à un niveau plus détaillé, en indiquant les résultats obtenus au regard de chacun des différents sous-critères.
Avez-vous recours à un processus de calcul de la pondération?	Oui. Cependant, le processus spécifique de calcul de la pondération n'est pas communiqué aux utilisateurs, afin d'éviter toute manipulation de l'outil d'évaluation.
Adoptez-vous un mécanisme de notation et/ou de classement dans votre évaluation?	Non. Il n'y a pas de notation ou de classement des résultats.

Détails

À quelles questions essentielles l'outil peut-il contribuer à répondre?	• Existe-t-il des stratégies et des politiques nationales en matière de cybersécurité? (**Cadre non juridique**) • Existe-t-il une législation nationale sur la cybercriminalité? Le pays a-t-il adhéré à des traités sur la cybercriminalité? (**Cadre juridique**) • Un pays érige-t-il en infractions les délits classiques commis par/via des activités informatiques ou les nouveaux cyberdélits? (**Droit matériel**) • Existe-t-il des lois de procédure régissant les enquêtes et les poursuites en matière de cybercriminalité? (**Droit procédural**) • Un pays a-t-il mis en place des règles propres à la recevabilité et au traitement des éléments de preuve électroniques? (**Éléments de preuve électroniques**) • Comment un pays détermine-t-il la compétence en matière de cybercriminalité? (**Compétence**) • Un pays garantit-il une "procédure régulière" (protection des données et liberté d'expression) à ses citoyens? (**Garanties**) • Un pays a-t-il mis en œuvre des procédures d'extradition ou des principes formels/informels en matière d'entraide judiciaire au niveau international? (**Coopération internationale**) • Existe-t-il des institutions ou des programmes de renforcement des capacités en matière de lutte contre la cybercriminalité à l'intention des responsables de l'application des lois, des procureurs et des juges? (**Renforcement des capacités**)
À quel stade du cycle de vie de la stratégie l'évaluation doit-elle être effectuée?	• Lancement • Inventaire et analyse • Élaboration de la stratégie • Mise en œuvre • Suivi et évaluation Lorsque l'outil d'évaluation sera utilisé pour la première fois, il permettra de disposer d'une base de référence, tandis que la mise à jour périodique des résultats à l'aide de l'outil facilitera le suivi des progrès accomplis.
Comment l'évaluation contribue-t-elle à harmoniser d'autres activités?	L'outil d'évaluation permet d'identifier les domaines prioritaires d'un pays au regard des neuf dimensions, ce qui permet de cibler l'affectation des ressources limitées en matière de renforcement des capacités, en vue d'établir une stratégie nationale de renforcement des capacités de lutte contre la cybercriminalité. L'outil d'évaluation peut donc être utilisé à la fois en tant qu'activité autonome menée par un pays et en tant qu'outil essentiel de diligence raisonnable, pour permettre aux groupes de travail spéciaux opérationnels de déterminer si un pays est prêt à lutter contre la cybercriminalité.
Quel est le rôle de l'évaluation dans le processus de mise en correspondance du GFCE?	L'outil d'évaluation contribuera au processus de mise en correspondance du GFCE, en fournissant un point de comparaison solide et objectif pour planifier et mettre en œuvre les activités de renforcement des capacités en matière de cybersécurité.

Quelles études de cas ou références sont disponibles concernant les avantages de l'outil?	Comme indiqué ci-dessus, les bons résultats obtenus à l'issue des évaluations du renforcement des capacités de lutte contre la cybercriminalité effectuées dans un certain nombre de pays clients et le fait que notre organisation partenaire, l'ONUDC, ait reconnu l'outil d'évaluation et l'utilise désormais comme méthode exclusive d'évaluation de la préparation à la lutte contre la cybercriminalité, témoignent des avantages de cet outil.
Quels sont les mécanismes propres à garantir l'indépendance, l'impartialité et la neutralité de vos résultats?	• L'outil d'évaluation a été évalué et validé par nos organisations partenaires, à savoir le Conseil de l'Europe, l'UIT, l'ONUDC, la Conférence des Nations unies sur le commerce et le développement (CNUCED), le Bureau du Procureur général de la République de Corée (KSPO) et le GCSCC (Université d'Oxford). • Un groupe d'experts indépendants a contribué à déterminer les pondérations de chaque indicateur dans l'outil d'évaluation.

La cybermaturité dans la région Asie-Pacifique

Institut australien de stratégie politique (International Cyber Policy Centre)

La publication intitulée "La cybermaturité dans la région Asie-Pacifique" est un rapport annuel publié par l'Institut australien de stratégie politique (ASPI), qui cerne les tendances en matière de cybermaturité dans la région Asie-Pacifique. Cette publication porte sur un large échantillon géographique et économique de la région, qui comprend 25 pays d'Asie du Sud, du Nord et du Sud-Est, du Pacifique Sud et d'Amérique du Nord.

La méthode de "mesure de la cybermaturité" consiste à évaluer les différents aspects des capacités des États en matière de cybersécurité. Le modèle, qui a été affiné grâce à la participation d'experts et de parties prenantes de la région Asie-Pacifique, permet d'évaluer efficacement l'évolution des stratégies des États et les mutations technologiques. Dans ce contexte, la "maturité" est attestée par la présence, la mise en œuvre effective et le fonctionnement de structures, de politiques, de législations et d'organisations liées à la cybersécurité. Ces indicateurs de cybermaturité englobent les structures politiques et législatives de l'ensemble des pouvoirs publics, les mesures prises face à la cybercriminalité financière, l'organisation militaire, la puissance économique des entreprises et la situation du numérique, ainsi que les niveaux de sensibilisation de la société à la cybersécurité.

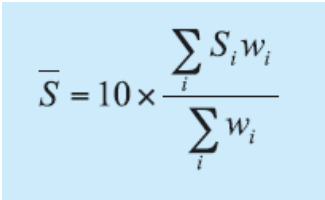
La base de recherche qui sous-tend chacun de ces groupes d'indicateurs a été établie exclusivement à partir d'informations relevant du domaine public; en d'autres termes, les conclusions figurant dans le rapport se fondent uniquement sur des documents en libre accès.

Vue d'ensemble

Dernière date de mise à jour de l'outil	2017
Quel est le nom de l'outil d'évaluation?	La cybermaturité dans la région Asie-Pacifique
Quel est le nom de l'organisation qui gère l'outil?	Institut australien de politique stratégique (ASPI)
Quels sont les responsables de la mise en œuvre des évaluations?	Institut australien de politique stratégique (ASPI)
Veuillez fournir des liens vers l'outil et toute information supplémentaire	https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017
Qui faut-il contacter pour discuter de l'organisation d'une évaluation?	Mme Danielle Cave, Directrice adjointe, International Cyber Policy Centre, ASPI M. Tom Uren, Analyste principal, International Cyber Policy Centre, ASPI M. Bart Hogeveen, Chef du renforcement des capacités de cybersécurité, ASPI
Couverture géographique	Régionale
Qui peut utiliser l'outil?	Le rapport est accessible à tous.

Quels sont les thèmes ou les sujets abordés?	**1 Gouvernance** La question de la gouvernance a trait à l'approche organisationnelle de l'État en matière de cybersécurité, notamment en ce qui concerne la composition des organismes publics s'occupant de ces questions; à la volonté et à la capacité du législateur; et à l'engagement de l'État concernant les questions de cyberpolitique internationale, par exemple la gouvernance de l'Internet, l'application du droit international et l'élaboration de normes ou de principes. Ces indicateurs fournissent des orientations pour l'engagement diplomatique et la mobilisation des gouvernements, des organismes de développement, des responsables de l'application de la loi et du secteur privé dans les États de la région Asie-Pacifique. **2 Lutte contre la cybercriminalité financière** La cybercriminalité financière est un problème majeur pour tous les États de la région Asie-Pacifique. Elle a de très lourdes répercussions sur la population de la région et engendre des pertes financières importantes. Comprendre la capacité de l'État à lutter contre la cybercriminalité financière peut orienter l'action en matière de répression, notamment par le partage d'informations et l'aide au renforcement des capacités émanant du secteur public et du secteur privé. **3 Application militaire** Cette question traite de la structure organisationnelle militaire de l'État (le cas échéant) en ce qui concerne le cyberespace et des positions connues de l'État sur l'utilisation du cyberespace par ses forces armées. Cela peut orienter l'action militaire entre États ainsi que l'action diplomatique et politico-militaire. Étant donné que les utilisations militaires du cyberespace, en particulier les capacités nationales, constituent une question sensible pour tous les pays de la région Asie-Pacifique, ce domaine doit être examiné avec le plus grand soin avant que les États cherchent ou acceptent d'entamer une collaboration. **4 Économie numérique et entreprises** La question de savoir si l'État mesure l'importance du cyberespace et de l'économie numérique et intérêt qu'ils présentent sur le plan économique est un indicateur de cybermaturité. Cela peut orienter l'action concernant le renforcement des capacités, les liens commerciaux au niveau régional et la collaboration entre les pouvoirs publics et les entreprises en matière de cybersécurité. **5 Mobilisation sociale** La sensibilisation et la mobilisation du public concernant les questions liées au cyberespace, par exemple la gouvernance de l'Internet, la censure de l'Internet et la cybercriminalité, sont un indicateur de la maturité du débat public entre le gouvernement et les citoyens. Les programmes éducatifs relatifs aux TIC et aux questions liées au cyberespace peuvent également témoigner d'un niveau élevé de compréhension des questions techniques et des différents enjeux. La proportion de la population d'un État disposant d'une connectivité à l'Internet témoigne de la nature de la mobilisation des entreprises et des particuliers dans le cyberespace, de la qualité de l'infrastructure des TIC et du niveau de confiance des citoyens dans le commerce numérique. Cela peut fournir des orientations aux organismes de développement désireux de mettre en place des économies régionales et aux entreprises qui souhaitent développer les échanges commerciaux dans la région.

Quels sont les thèmes ou sujets traités par le GFCE?	Politiques générales et stratégie ☒ Stratégies ☒ Évaluations ☒ Mesures de renforcement de la confiance et normes ☒ Cyberdiplomatie ☒ Le droit international dans le cyberespace Gestion des incidents et protection des infrastructures essentielles de l'information ☒ Intervention en cas d'incident de sécurité informatique ☐ Examen et analyse des incidents ☐ Exercices de cybersécurité ☒ Protection des infrastructures essentielles de l'information Cybercriminalité ☒ Cadres juridiques/Droit de la cybercriminalité ☒ Application de la loi dans le cyberespace ☐ Formation en matière de cybercriminalité ☐ Prévention de la cybercriminalité Cybercriminalité ☒ Cadres juridiques/Droit de la cybercriminalité ☒ Application de la loi dans le cyberespace ☐ Formation en matière de cybercriminalité ☐ Prévention de la cybercriminalité Culture et compétences ☒ Sensibilisation à la cybersécurité ☒ Éducation et formation ☒ Perfectionnement de la main-d'œuvre Normes ☐ Normes relatives à un Internet ouvert ☐ Internet des objets
Types d'indicateurs	Indicateurs quantitatifs et indicateurs qualitatifs
Combien d'indicateurs sont utilisés et comment sont-ils appliqués?	La "mesure de la cybermaturité" comprend 10 indicateurs. Ces indicateurs ont été pondérés en fonction de leur importance pour la cybermaturité d'un État. Un groupe de cyberexperts et de parties prenantes issus d'organismes publics et du secteur privé les a pondérés sur une échelle de 1 à 10, 1 signifiant "pas du tout important" et 10 "extrêmement important". La moyenne de ces pondérations effectuées par des experts pour chaque catégorie a ensuite été calculée, afin d'obtenir un facteur de pondération pouvant être utilisé dans le calcul d'une note globale.

	Enfin, chaque pays a été évalué en fonction des 10 facteurs, sur une échelle de 0 à 10 (10 correspondant au plus haut niveau de maturité). Les évaluations étaient fondées sur de nombreuses recherches qualitatives et quantitatives dans la documentation librement disponible et, dans la mesure du possible, sur une comparaison avec les études et les résultats de 2014, 2015 et 2016. La note globale de chaque pays est la somme des notes obtenues pour chaque facteur, pondérée par l'importance moyenne calculée. Pour faciliter l'interprétation, les notes globales ont été converties en pourcentage de la note la plus élevée, compte tenu des pondérations attribuées:  $\overline{S} = 10 \times \frac{\sum_i S_i w_i}{\sum_i w_i}$ où $\overline{S}$ = note pondérée, S = note et w = poids.
Méthodologie – Quel type d'évaluation est utilisé	Comparative, avec classement
Méthode de collecte de données primaires	Informations provenant de sources libres
Procédez-vous à la collecte de données secondaires?	• Entretiens • Questionnaires et enquêtes • Observations • Groupes spécialisés
Quels mécanismes adoptez-vous pour garantir l'exactitude des données recueillies?	Les ambassades et hauts commissariats des pays couverts par le rapport sont invités à vérifier les faits relatifs au profil de leur pays.
Quels sont les principaux résultats de l'évaluation?	• Profils individuels des pays • Classement comparatif régional • Aperçu des tendances régionales • Évaluation des possibilités de coopération internationale
Format de présentation des résultats de l'évaluation	Rapport
Les résultats de l'évaluation peuvent-ils être publiés?	Oui. Les résultats sont publiés dans un rapport.
Comment accéder aux rapports précédents?	https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2016 https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2015 https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2014
Quels sont les éléments qui attestent de résultats concrets?	Voir la réponse à la question "Références" ci-dessous.

Quels sont les avantages d'une évaluation?	Voir la réponse à la question sur le "stade du cycle de vie de la stratégie" ci-dessous.
Avez-vous recours à un processus de calcul de la pondération?	Oui, voir la réponse à la question sur les "indicateurs et la façon dont ils sont appliqués" ci-dessus.
Adoptez-vous un mécanisme de notation et/ou de classement dans votre évaluation?	Oui, voir la réponse à la question sur les "indicateurs et la façon dont ils sont appliqués" ci-dessus.

Examen détaillé

À quelles questions essentielles l'outil peut-il contribuer à répondre?	Quelles sont les tendances régionales en matière de cybermaturité dans la région Asie-Pacifique? Comment les pays de la région Asie-Pacifique se situent-ils par rapport aux cinq questions de fond qui composent la cybermaturité? Quelles sont les possibilités de coopération internationale avec les pays de la région Asie-Pacifique?
À quel stade du cycle de vie de la stratégie l'évaluation doit-elle être effectuée?	Ce paramètre analyse la région Asie-Pacifique d'un point de vue comparatif. Aux fins de l'élaboration d'une cyberstratégie nationale, les rapports sont les mieux adaptés aux stades du lancement, de l'inventaire et du suivi et de l'évaluation. Lors de l'élaboration d'une approche régionale ou d'un "panorama" régional, l'outil convient bien pour la définition d'un programme, les analyses stratégiques et la comparaison des pratiques nationales. Du fait de son cycle annuel, le rapport est utile pour le suivi et l'évaluation ainsi que pour les analyses des tendances.
Comment l'évaluation contribue-t-elle à harmoniser d'autres activités?	Le rapport constitue une source d'analyse faisant autorité, qui repose sur des données factuelles et des éléments de preuve et s'adresse aux décideurs nationaux, régionaux, du secteur public ou privé.
Quel est le rôle de l'évaluation dans le processus de mise en correspondance du GFCE?	Le rapport offre l'occasion de mener des discussions entre les bénéficiaires et les fournisseurs de capacités en matière de cybersécurité.
Quelles études de cas ou références sont disponibles concernant les avantages de l'outil?	Le rapport est souvent cité dans les médias: • https://www.zdnet.com/article/only-us-tops-australia-in-asia-pacific-cyber-maturity-aspi/ • https://www.theaustralian.com.au/commentary/opinion/threat-posed-by-evil- nations-and-criminals-in-cyberland-is-rising/news-story/fdebd93f3dc0206afe0705e6f6ec045c • https://vovworld.vn/en-US/spotlight/vietnam-ranks-9th-in-cyber-maturity-in- asiapacific-region-379580.vov • https://theaseanpost.com/article/cyberattack-malaysia-imminent-or-imagined

	Le rapport est cité dans des discours, notamment d'hommes politiques (australiens) de premier plan: • https://www.rusi.org.au/resources/Documents/2015_10_05%20Brodtman.pdf Le rapport est utilisé comme source dans d'autres publications politiques et universitaires, par exemple: • https://www.austcyber.com/resources/sector-competitiveness-plan/executive- summary • https://www.swp-berlin.org/fileadmin/contents/projects/BCAS2015_Maurer_Tim_Web.pdf • https://www.standards.org.au/getmedia/952ea009-ffc2-490a-905f- 8f731fa84a52/Pacific-Islands-Cyber-Security-Standards-Cooperation- Agenda.pdf.aspx
Quels sont les mécanismes propres à garantir l'indépendance, l'impartialité et la neutralité de vos résultats?	En tant que groupe de réflexion reconnu, l'ASPI est régi par sa charte, qui consacre les principes d'indépendance et d'impartialité. En outre, le rapport est rédigé sur la base de sources ouvertes et vérifiables. Les observations ou conclusions ne sont pas soumises à l'approbation d'un gouvernement ou d'un bailleur de fonds et sont conformes aux pratiques courantes en matière de rigueur analytique.
Veuillez ajouter toute information supplémentaire	Le rapport a été publié pour la dernière fois en décembre 2017, en prévision d'un nouveau financement et d'une réévaluation des résultats des éventuels travaux de recherche.

Indice de préparation à la lutte contre la cybercriminalité (IPC) – Version 2.0

Institut Potomac d'études politiques (PIPS)

L'Indice de préparation à la lutte contre la cybercriminalité (IPC) − Version 2.0 est une méthodologie complète, comparative et empirique permettant d'évaluer l'engagement et la capacité d'un pays à protéger ses infrastructures et ses services numériques nationaux, dont dépendent sa croissance économique et sa résilience au niveau national. Le document intitulé "Indice de préparation à la lutte contre la cybercriminalité − Version 2.0" s'inspire de la version précédente (2013), intitulée "Indice de préparation à la lutte contre la cybercriminalité − Version 1.0", qui fournissait le premier cadre méthodologique permettant d'évaluer la capacité à lutter contre la cybercriminalité. L'outil d'évaluation IPC peut aider les pays à repérer les lacunes existantes, à renforcer leur position actuelle en matière de cybersécurité et à mieux gérer les risques liés au cyberespace au niveau national.

Depuis 2013, l'outil IPC a été appliqué dans plus de 100 pays et 14 rapports détaillés ont été établis.

Vue d'ensemble

Dernière date de mise à jour de l'outil	Nous ajoutons régulièrement de nouvelles questions et de nouveaux indicateurs à chacun des sept éléments essentiels de l'outil.
Quel est le nom de l'outil d'évaluation?	Indice de préparation à la lutte contre la cybercriminalité − Version *2*.0
Quel est le nom de l'organisation qui gère l'outil?	Institut Potomac d'études politiques (PIPS)
Quels sont les responsables de la mise en œuvre des évaluations?	Membres de l'équipe chargée de la préparation à la lutte contre la cybercriminalité (Mme Melissa Hathaway et Mme Francesca Spidalieri)
Veuillez fournir des liens vers l'outil et toute information supplémentaire	• Site web du PIPS: https://www.potomacinstitute.org/academic-centers/cyber- readiness-index • Portail Cybil: https://cybilportal.org/tools/cyber-readiness-index-2-0/
Qui faut-il contacter pour discuter de l'organisation d'une évaluation?	• Melissa Hathaway, maître de recherche, PIPS, et responsable, IPC, Directrice de recherche: hathawayglobal@icloud.com • Francesca Spidalieri, Codirectrice de recherche, IPC: francescaspidalieri@gmail.com
Couverture géographique	Mondiale
Qui peut utiliser l'outil?	• Dirigeants mondiaux • Gouvernements nationaux/régionaux • Ministères/organismes gouvernementaux • Organismes s'occupant de cybersécurité/décideurs • Établissements universitaires • Experts en cybersécurité • Chercheurs à titre individuel

Quels sont les thèmes ou les sujets abordés?	L'Indice IPC – Version 2.0 utilise plus de 70 indicateurs uniques se rapportant à sept éléments essentiels, pour mettre en évidence les activités liées à la capacité de lutte contre la cybercriminalité qui sont déjà menées et déterminer les domaines à améliorer dans les catégories suivantes: 1) **Stratégie nationale**: Publication d'une stratégie nationale; désignation d'une autorité compétente; identification des principales entités gouvernementales et des principales entités commerciales responsables de la mise en œuvre; mécanismes propres à protéger les infrastructures essentielles; identification des services essentiels; identification des normes nationales relatives à la continuité des services. 2) **Intervention en cas d'incident**: Publication d'un plan d'intervention en cas d'incident; identification des dépendances intersectorielles; éléments de preuve démontrant que le plan est exécuté et mis à jour; publication d'une évaluation des cybermenaces; création d'une équipe d'intervention en cas d'incident informatique (CSIRT); ressources financières et humaines. 3) **Cybercriminalité et application des lois**: Ratification d'un traité international sur la cybercriminalité; efforts déployés pour réduire la cybercriminalité; capacité institutionnelle à lutter contre la cybercriminalité; engagement à passer en revue les lois et mécanismes existants; efforts pour remettre en état les infrastructures infectées; formation des forces de l'ordre et renforcement des capacités. 4) **Partage des informations**: Politique en matière de partage de l'information; structure institutionnelle permettant de transmettre des informations à des organismes gouvernementaux et/ou au secteur; éléments de preuve démontrant l'existence de mécanismes de coordination entre les différents secteurs et intervenants; capacité et processus permettant au gouvernement de déclassifier les informations obtenues par les services de renseignement. 5) **Investissements dans la recherche-développement, l'éducation et les capacités**: Mécanismes d'incitations du gouvernement pour encourager l'innovation et les investissements dans le domaine de la cybersécurité; ressources financières et ressources humaines pour la recherche-développement et le transfert de technologie; programmes relatifs à la cybersécurité sanctionnées par un diplôme; parrainage de campagnes de sensibilisation à la cybersécurité et de programmes éducatifs. 6) **Diplomatie commerciale**: Identification de la cybersécurité comme un élément essentiel de la politique étrangère et des négociations économiques internationales; mise en place d'un personnel spécialisé dans la cyberdiplomatie au sein du Ministère des affaires étrangères d'un pays; participation à des accords internationaux, multinationaux et régionaux en matière de cybersécurité et application de ces accords. 7) **Défense et réponse aux crises**: création au niveau national et dans le secteur militaire et/ou en dehors du secteur militaire d'une organisation ayant pour mission d'assurer la cyberdéfense; éléments de preuve démontrant la réalisation de cyberexercices au niveau national avec des partenaires commerciaux et/ou internationaux; établissement de normes favorisant un comportement responsable des États au sein du cyberespace; mise en place de dispositifs d'aide rapide.

	Pour une description complète de chaque élément essentiel, veuillez vous reporter à la méthodologie complète, disponible à l'adresse: https://www.potomacinstitute.org/images/CRIndex2.0.pdf
Quels sont les thèmes ou sujets traités par le GFCE?	Politiques générales et stratégie ☒ Stratégies ☒ Évaluations ☒ Mesures de renforcement de la confiance et normes ☒ Cyberdiplomatie ☒ Le droit international dans le cyberespace Gestion des incidents et protection des infrastructures essentielles de l'information (CIIP) ☒ Equipes d'intervention en cas d'incident de sécurité informatique ☒ Examen et analyse des incidents ☒ Exercices de cybersécurité ☒ Protection des infrastructures essentielles de l'information Cybercriminalité ☒ Cadres juridiques/législation sur la cybercriminalité ☒ Application de la loi dans le cyberespace ☒ Formation en matière de cybercriminalité ☒ Prévention de la cybercriminalité Culture et compétences ☒ Sensibilisation à la cybersécurité ☒ Éducation et formation ☒ Perfectionnement de la main-d'œuvre Normes ☒ Normes internationales et/ou nationales
Types d'indicateurs	La collecte de données dans le cadre de l'indice CRI 2.0 est qualitative et chaque indicateur est évalué au regard de quatre catégories principales: 1) Déclarations/stratégies/politiques; 2) Organisation/autorité compétente; 3) Ressources; et 4) Mise en œuvre.
Combien d'indicateurs sont utilisés et comment sont-ils appliqués?	L'indice CRI 2.0 utilise plus de 70 indicateurs répartis sur sept éléments essentiels pour évaluer l'état actuel d'un pays en matière de cybersécurité et recenser les domaines qui sont pleinement opérationnels, partiellement opérationnels ou pour lesquels les éléments de preuve sont insuffisants. Tous les indicateurs de l'indice CRI présentent une structure commune, et les questions posées dans une version de la méthodologie sont comparables à des questions similaires dans les versions précédentes ou futures. Chaque indicateur se voit attribuer la même importance et est ensuite décrit dans le rapport de pays comme s'inscrivant dans un contexte plus général, en fonction des besoins, des capacités, des priorités et des objectifs du pays.

Méthodologie – Quel type d'évaluation est utilisé?	L'indice CRI 2.0 utilise des sources primaires, notamment des stratégies nationales, des politiques, des législations, des déclarations officielles des dirigeants, des évaluations nationales et des rapports nationaux, etc., pour évaluer l'aptitude des pays à lutter contre la cybercriminalité et élaborer des profils nationaux détaillés. ⇨ Les pays ne sont pas classés les uns par rapport aux autres.
Méthode de collecte de données primaires	• Informations provenant de sources libres • Documents confidentiels non publiés ou documents officiels • Entretiens/observations • Documents et dossiers
Procédez-vous à la collecte de données secondaires?	Oui. La collecte de données secondaires est effectuée pour corroborer, modifier ou développer les informations recueillies lors de notre analyse des sources primaires et des entretiens avec des fonctionnaires et des experts du pays.
Quels mécanismes adoptez-vous pour garantir l'exactitude des données recueillies?	Tous nos travaux de recherche sont fondés sur des sources primaires et des documents officiels, puis corroborés par des fonctionnaires et/ou des experts en la matière du pays
Quels sont les principaux résultats de l'évaluation?	Des rapports de pays détaillés sont publiés sur le site web du PIPS et sont accessibles au public dans les six langues de l'ONU. Ces rapports peuvent aider les gouvernements à mettre au point leurs pratiques et politiques en matière de cybersécurité et fournissent un plan des priorités requises pouvant être appliqué concrètement, afin de renforcer leurs capacités en matière de cybersécurité et de déterminer les mesures à prendre pour réduire les risques, indépendamment de leurs compétences spécialisées internes.
Format de présentation des résultats de l'évaluation	• Rapports de pays détaillés • Outil de visualisation (graphique radar et graphique "Harvey Balls") • Présentation PowerPoint, si le pays en fait la demande
Les résultats de l'évaluation peuvent-ils être publiés?	Oui. Tous les rapports de pays du CRI sont accessibles au public sur la page web du PIPS consacrée à l'indice CRI: https://www.potomacinstitute.org/academic-centers/cyber-readiness-index.
Comment accéder aux rapports précédents?	Voir ci-dessus.
Quels sont les éléments qui attestent de résultats concrets?	L'indice CRI a directement influencé les politiques de préparation à la lutte contre la cybercriminalité et la réflexion des dirigeants dans les pays et organisations suivants: Australie, Azerbaïdjan, Bangladesh, Bosnie-Herzégovine, Bulgarie, Canada, Chine, République tchèque, Égypte, Estonie, France, Géorgie, Allemagne, Islande, Inde, Indonésie, Israël, Italie, Japon, Jordanie, Kirghizistan, Lituanie, Mexique, Pays-Bas, Nouvelle-Zélande, Oman, Philippines, Pologne, Roumanie, Arabie saoudite, Serbie, Slovaquie, Afrique du Sud, Suède, Suisse, Ukraine, Royaume-Uni; Forum africain des équipes d'intervention en cas d'incident informatique (Africa CERT), équipe d'intervention en cas d'incident informatique pour la région Asie-Pacifique (APCERT), UIT, Banque

	interaméricaine de développement (BID), Organisation du traité de l'Atlantique Nord (OTAN), Conseil nordique, Organisation des États américains (OEA) et Banque mondiale. L'indice CRI continue d'avoir des incidences à l'échelle mondiale et Melissa Hathaway, chercheuse principale, a sensibilisé davantage les dirigeants du monde entier à ces questions. Régulièrement invitée à des manifestations et des discussions internationales de haut niveau et citée dans de nombreuses publications internationales, Melissa Hathaway continue de sensibiliser les dirigeants nationaux à l'intérêt pratique de l'utilisation de l'indice CRI 2.0 comme outil de planification/d'évaluation comparative ainsi qu'à la nécessité de garantir la participation de diverses parties prenantes aux efforts et processus nationaux dans le domaine de la cybersécurité et d'accroître les fonds alloués au renforcement des capacités de cybersécurité.
Quels sont les avantages d'une évaluation?	L'évaluation à l'aide de l'indice CRI 2.0 peut aider les pays à déterminer l'écart entre leur niveau de préparation en matière de cybersécurité et les cybercapacités nationales dont ils ont besoin pour forger leur avenir numérique. L'outil peut également être utilisé pour évaluer où se situe un pays sur la courbe de maturité du point de vue de l'ensemble des pouvoirs publics et à l'échelle de la nation tout entière. Pris ensemble, ces indicateurs peuvent aider les gouvernements à évaluer et harmoniser leurs initiatives en matière de sécurité numérique et nationale. Grâce aux données recueillies, l'indice CRI peut également mettre en évidence les bonnes pratiques que les pays peuvent mettre en œuvre pour faciliter et contribuer à stimuler les efforts de préparation à la lutte contre la cybercriminalité dans les différents secteurs d'activité. L 'indice CRI 2.0 met en avant les outils que les dirigeants nationaux peuvent exploiter, notamment les politiques, les lois, la réglementation, les normes, les effets de levier sur les marchés et d'autres initiatives qu'ils peuvent prendre, afin de protéger la valeur de leurs investissements numériques et de lutter contre l'érosion économique actuelle créée par la cyberinsécurité. Cette évaluation peut aider les dirigeants nationaux à reconnaître que pour tirer pleinement parti de l'économie numérique en termes de croissance économique, d'augmentation de la productivité et d'efficacité, de renforcement des compétences et d'amélioration de l'accès aux activités et à l'information commerciales, il est nécessaire d'harmoniser les stratégies de développement économique et les priorités liées à la sécurité nationale. L'évaluation montre comment les TIC peuvent favoriser la croissance économique, mais uniquement si les politiques, les processus et les technologies appropriés sont mis en place pour protéger et sécuriser les cyberinfrastructures et les cyberservices dont dépendent l'avenir et la croissance numériques d'un pays.
Avez-vous recours à un processus de calcul de la pondération?	Oui. Dans notre base de données interne, nous attribuons une note de 5.0 aux indicateurs pleinement opérationnels, de 3.0 aux indicateurs partiellement opérationnels et de 1.0 lorsque certains éléments sont classés ou que les éléments de preuve démontrant leur existence ou leur mise en œuvre sont insuffisants. Le calcul de la pondération n'est utilisé que pour créer des graphiques radar et d'autres éléments visuels, mais pas pour établir un classement entre les pays.

Adoptez-vous un mécanisme de notation et/ou de classement dans votre évaluation?	L'indice CRI 2.0 fournit une note de maturité pour chaque élément essentiel, mais n'établit pas de classement entre les pays.

Détails

À quelles questions essentielles l'outil peut-il contribuer à répondre?	• Les objectifs à court terme et à long terme du pays, notamment sa stratégie numérique, ses politiques industrielles, ses objectifs économiques et ses priorités en matière de sécurité nationale, sont-ils en phase avec sa stratégie nationale de cybersécurité? • Quels types de cybermenaces pourraient nuire à ces objectifs ou en compromettre la réalisation? • Quelles sont les secteurs dépendants du numérique les plus essentiels du pays (entreprises, services, infrastructures et actifs, par exemple) qui, s'ils étaient mis à mal, auraient de graves conséquences sur l'économie et la sécurité nationale? • Existe-t-il des chaînes de responsabilité claires pour garantir que les objectifs du pays sont atteints et que les mesures de réduction des risques sont mises en œuvre? • Les considérations de cybersécurité et de résilience ont-elles été au cœur du processus de planification? • Quelles mesures le pays peut-il prendre pour renforcer sa résilience numérique? L'indice CRI 2.0 peut également servir de référence aux pays pour mettre en évidence l'écart entre leur situation actuelle en matière de cybersécurité et les cybercapacités nationales nécessaires pour remédier aux insuffisances et appuyer les priorités futures du pays dans les domaines de l'économie et de la sécurité. Les responsables des pouvoirs publics peuvent utiliser l'indice CRI 2.0 pour faciliter et contribuer à promouvoir les efforts de préparation à la lutte contre la cybercriminalité dans les différents secteurs d'activité, de façon à accorder en permanence l'attention voulue aux liens entre leur stratégie numérique et industrielle et leurs priorités en matière de sécurité nationale.
À quel stade du cycle de vie de la stratégie l'évaluation doit-elle être effectuée?	La méthodologie CRI devrait faire partie intégrante de l'ensemble du cycle de vie de la stratégie et son outil d'évaluation peut être utilisé avant et/ou après l'élaboration d'une stratégie nationale de cybersécurité, y compris pendant le lancement/l'inventaire et l'analyse/l'élaboration de la stratégie/la mise en œuvre/le suivi et l'évaluation/la mise à jour de la stratégie.
Comment l'évaluation contribue-t-elle à harmoniser d'autres activités?	L'indice CRI 2.0 établit un lien entre la croissance et le développement économiques et les politiques de sécurité nationale, de sorte qu'il peut aider les pays à mieux faire correspondre leur stratégie nationale de cybersécurité et leurs stratégies numérique et de croissance.
Quel est le rôle de l'évaluation dans le processus de mise en correspondance avec le GFCE?	L'indice 2.0 peut corroborer ou compléter d'autres outils d'évaluation proposés par la communauté du GFCE, notamment le Modèle CMM de l'Université d'Oxford et l'Indice GCI de l'UIT

Quelles études de cas ou références sont disponibles concernant les avantages de l'outil?	En plus de tous les pays et organisations internationales énumérés ci-dessus qui ont utilisé le CRI pour orienter leurs politiques et stratégies, la méthodologie reposant sur l'indice CRI a été citée ou utilisée dans un grand nombre d'articles, d'allocutions, de séances d'information, de rapports et de publications connexes. Ainsi, l'OEA et la BID ont eu recours à la méthodologie et à la base de données CRI 2.0 pour corroborer et valider leur rapport international sur les capacités et le niveau de préparation des pays membres en matière de cybersécurité (Cybersecurity: Are We Ready in Latin America and the Caribbean? – "Cybersécurité: sommes-nous prêts en Amérique latine et dans les Caraïbes?"). L'équipe du CRI a collaboré activement avec l'UIT pour échanger des données, harmoniser les efforts, accroître l'efficacité et contribuer à deux des projets phares de l'UIT en matière de cybersécurité, à savoir l'élaboration de la deuxième version de l'Indice mondial de cybersécurité (GCI) de l'UIT et l'établissement du Guide pour l'élaboration d'une stratégie nationale de cybersécurité, placé sous la direction de l'UIT et faisant intervenir plusieurs partenaires. On trouvera d'autres articles faisant référence à l'indice CRI 2.0 sous la rubrique "Cyber readiness in the News": https://www.potomacinstitute.org/academic-centers/cyber-readiness-index
Quels sont les mécanismes propres à garantir l'indépendance, l'impartialité et la neutralité de vos résultats?	Les rapports de pays sont établis sur la base de données provenant de sources primaires et validés de manière indépendante par notre équipe d'experts.

Modèle de maturité des capacités en matière de cybersécurité pour les nations (CMM)

Centre mondial des capacités de cybersécurité (GCSCC), Université d'Oxford, et partenaires

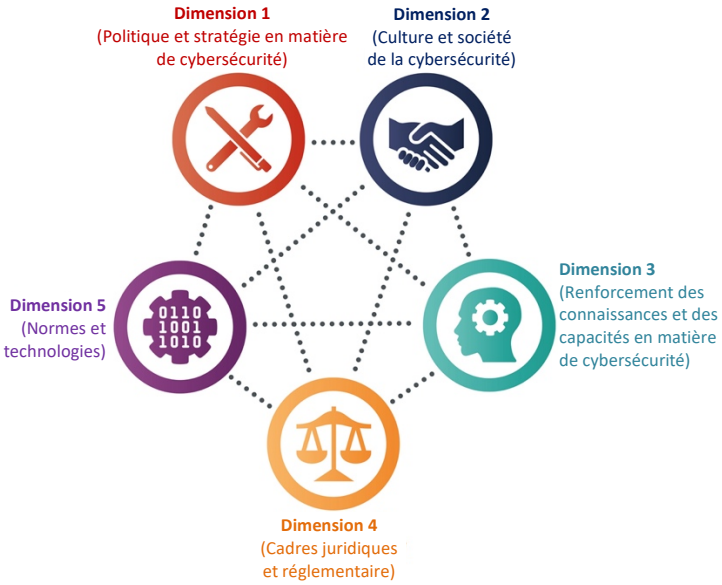
Le modèle de maturité des capacités en matière de cybersécurité pour les nations (CMM), élaboré par le Centre mondial des capacités de cybersécurité (GCSCC) de l'Université d'Oxford, vise à évaluer les capacités nationales de cybersécurité selon cinq dimensions, de façon à permettre aux pays de s'auto-évaluer, de mieux planifier les investissements et les stratégies nationales de cybersécurité et de fixer des priorités en matière de renforcement des capacités. Depuis 2015, plus de 110 examens CMM ont été effectués dans plus de 80 pays.

Le Centre GCSCC et ses partenaires définissent les capacités de cybersécurité au sens large, afin de tenir compte des facteurs politiques, stratégiques, sociaux et culturels, de l'éducation et de la formation, de la législation et de la réglementation ainsi que des cybertechnologies et des normes. Conformément à cette définition, les travaux de recherche sont pluridisciplinaires et abordent les capacités de cybersécurité dans toutes leurs dimensions, selon plusieurs points de vue des milieux universitaires.

Le modèle CMM a été élaboré en vue d'étudier les divers aspects du renforcement des capacités à travers et au sein de toutes ces dimensions et les types d'activités qui peuvent fournir et accroître les capacités, de déterminer s'il existe de bonnes pratiques, les conditions dans lesquelles il faudrait procéder à un renforcement des capacités et la façon dont les dimensions sont liées et dépendent les unes des autres pour obtenir de bons résultats. Dans cette optique, le modèle CMM sert également de cadre pour comparer les capacités en matière de cybersécurité entre les différents pays et au fil du temps. Sa méthodologie permet de recueillir les points de vue des différents acteurs et groupes de parties prenantes, afin de donner une vue d'ensemble des capacités de cybersécurité de chaque pays.

Vue d'ensemble

Dernière date de mise à jour de l'outil	Mars 2021
Quel est le nom de l'outil d'évaluation?	Modèle de maturité des capacités en matière de cybersécurité pour les nations (CMM), édition de2021
Quel est le nom de l'organisation qui gère l'outil?	Centre mondial des capacités de cybersécurité (GCSCC) Centre océanien de cybersécurité (OCSC) Centre des capacité de cybersécurité pour l'Afrique australe (C3SA)
Quels sont les responsables de la mise en œuvre des évaluations?	Centre mondial des capacités de cybersécurité (GCSCC) Centre océanien de cybersécurité (OCSC), Centre des capacité de cybersécurité pour l'Afrique australe (C3SA) Organisation des États américains (OEA), Banque mondiale, NRD Cyber Security Partenaires de la mise en œuvre: Union internationale des télécommunications (UIT), Forum mondial sur la cyberexpertise (GFCE), Organisation des télécommunications du Commonwealth (CTO), Centre d'information sur les réseaux de la région Asie-Pacifique (APNIC), Télécommunauté Asie-Pacifique (APT), Institut norvégien des affaires internationales (NUPI), Agence allemande pour la coopération internationale GmbH (GIZ), Allemagne.

Veuillez fournir des liens vers l'outil et toute information supplémentaire	https://gcscc.ox.ac.uk/the-cmm
Qui faut-il contacter pour discuter de l'organisation d'une évaluation?	GCSCC, monde, Mme Carolin Weisser Harris: carolin.weisser@cs.ox.ac.uk OCSC, région Océanie, M. James Boorman: james.boorman@ocsc.com.au C3SA, région Afrique, Mme Nthabiseng Pule: npule@researchictafrica.net
Couverture géographique	Mondiale
Qui peut utiliser l'outil?	Tout le monde. Le CMM est un document accessible au public. Pour procéder à un examen du modèle CMM, il est recommandé de collaborer avec l'un des responsables de la mise en œuvre connaissant bien la méthodologie CMM.
Quels sont les thèmes ou les sujets abordés?	Le modèle CMM envisage les capacités de cybersécurité sous l'angle des cinq dimensions essentielles au renforcement des capacités de cybersécurité d'un pays, à savoir:  **Dimension 1 (*Politique et stratégie en matière de cybersécurité*)**: capacité du pays à élaborer et à mettre en œuvre une stratégie de cybersécurité, et à renforcer sa résilience en matière de cybersécurité, en améliorant ses capacités d'intervention en cas d'incident, de cyberdéfense et de protection des infrastructures essentielles. Cette dimension concerne l'efficacité de la stratégie et des politiques aux fins de la mise en place de capacités nationales de cybersécurité, tout en maintenant les avantages d'un cyberespace vital pour les pouvoirs publics, les entreprises internationales et la société en général.

	Dimension 2 (*Culture et société de la cybersécurité*): passe en revue les éléments importants d'une culture responsable en matière de cybersécurité, par exemple la compréhension des risques liés à la cybercriminalité dans la société, le niveau de confiance dans les services Internet, l'administration publique en ligne et les services de commerce électronique, et la compréhension par les utilisateurs de la protection des données personnelles en ligne. En outre, cette dimension traite de la possibilité d'utiliser les mécanismes de signalement comme des moyens permettant aux utilisateurs de signaler les cas de cybercriminalité. Cette dimension porte aussi sur le rôle que jouent les médias et les réseaux sociaux en forgeant les valeurs, les attitudes et les comportements en matière de cybersécurité. **Dimension 3 (*Renforcement des connaissances et des capacités en matière de cybersécurité*)** traite de la disponibilité, de la qualité et de l'adoption de programmes destinés aux différents groupes de parties prenantes, notamment les pouvoirs publics, le secteur privé et la population dans son ensemble, et concerne les programmes de sensibilisation à la cybersécurité, les programmes éducatifs formels en matière de cybersécurité et les programmes de formation professionnelle. **Dimension 4 (*Cadres juridiques et réglementaire*)**: traite de la capacité des pouvoirs publics à élaborer et à adopter des législations nationales se rapportant directement et indirectement à la cybersécurité, l'accent étant mis en particulier sur les prescriptions réglementaires en matière de cybersécurité, la législation relative à la cybercriminalité et les lois connexes. La capacité à faire appliquer ces lois est examinée sous l'angle des capacités des organismes chargés de l'application de la loi et des poursuites judiciaires, des organismes de régulation et des tribunaux. En outre, cette dimension tient compte de questions telles que les cadres de coopération formels et informels pour lutter contre la cybercriminalité. **Dimension 5 (*Normes et technologies*)**: porte sur l'utilisation efficace et généralisée des technologies de cybersécurité pour protéger les personnes, les organisations et les infrastructures nationales. Cette dimension traite plus particulièrement de la mise en œuvre des normes et des bonnes pratiques en matière de cybersécurité, du déploiement des processus et des mesures de contrôle, ainsi que de la mise au point de technologies et de produits pour réduire les risques liés à la cybersécurité.
Quels sont les thèmes ou sujets traités par le GFCE?	Politiques générales et stratégie ☒ Stratégies ☒ Évaluations ☒ Mesures de renforcement de la confiance et normes ☒ Cyberdiplomatie ☐ Le droit international dans le cyberespace Gestion des incidents et protection des infrastructures essentielles de l'information ☒ Intervention en cas d'incident de sécurité informatique ☒ Examen et analyse des incidents ☒ Exercices de cybersécurité ☒ Protection des infrastructures essentielles de l'information

	Cybercriminalité ☒ Cadres juridiques/Droit de la cybercriminalité ☒ Application de la loi dans le cyberespace ☒ Formation en matière de cybercriminalité ☒ Prévention de la cybercriminalité Culture et compétences ☒ Sensibilisation à la cybersécurité ☒ Éducation et formation ☒ Perfectionnement de la main-d'œuvre Normes ☒ Normes internationales et/ou nationales
Types d'indicateurs	Indicateurs qualitatifs
Combien d'indicateurs sont utilisés et comment sont-ils appliqués?	Le modèle CMM comprend environ 600 indicateurs permettant d'évaluer la maturité au regard de cinq dimensions essentielles pour le renforcement des capacités de cybersécurité d'un pays: *politique et stratégie en matière de cybersécurité, culture et société de la cybersécurité, renforcement des connaissances et des capacités en matière de cybersécurité, cadres juridiques et réglementaire et normes et technologies*. Chaque **dimension** du modèle CMM est constituée d'un ensemble de **facteurs**, qui décrivent et définissent ce que signifie posséder des capacités nationales en matière de cybersécurité. La plupart des facteurs recouvrent plusieurs **aspects**. Chaque facteur/aspect comporte une série **d'indicateurs** pour cinq **stades** de maturité: *stade de démarrage, stade de formation, stade établi, stade stratégique, stade dynamique*. Ces indicateurs décrivent les étapes et les mesures à prendre pour atteindre ou maintenir un stade de maturité donné dans la hiérarchie aspect/facteur/dimension. Pour qu'un pays puisse démontrer sa maturité, telle qu'évaluée au regard d'un aspect/facteur donné, chaque indicateur doit être étayé par des éléments concrets, sans quoi le pays ne pourra être considéré comme ayant progressé vers l'étape suivante.
Méthodologie − Quel type d'évaluation est utilisé?	Le déploiement du modèle CMM est un processus à plusieurs étapes qui associe plusieurs parties prenantes, et comprend trois étapes principales: 1) Contextualisation de la recherche documentaire effectuée par l'équipe chargée de la mise en œuvre. 2) Discussions au sein de groupe spécialisés dans le pays pendant trois à quatre jours en présence des principales parties prenantes, par exemple des établissements universitaires, des représentants de la justice pénale, des forces de l'ordre, des informaticiens et des représentants d'entités du secteur public, des propriétaires d'infrastructures essentielles, des décideurs, des informaticiens des pouvoirs publics et du secteur privé (y compris des institutions financières), des sociétés de télécommunication, des représentants du secteur bancaire ainsi que de la société civile et des partenaires internationaux.

	3) Elaboration d'un rapport détaillé sur le modèle CMM décrivant le contexte de la cybersécurité dans le pays, présentant brièvement les résultats pour chaque facteur et aspect du modèle CMM, indiquant les niveaux de maturité concernant les capacités de cybersécurité et contenant des recommandations destinées à permettre au pays de renforcer ses capacités de cybersécurité. Ce rapport est examiné par le Comité technique du GCSCC et soumis au gouvernement pour observations. Pour plus de précisions, voir le site: https://gcscc.ox.ac.uk/cmm-review-process
Méthode de collecte de données primaires	• Groupes spécialisés modifiés (collecte principale de données primaires) • Questionnaires et enquêtes (études régionales de l'OEA) • Entretiens (facultatifs pour obtenir des éléments de preuve supplémentaires)
Procédez-vous à la collecte de données secondaires?	Oui (dans le cadre des recherches documentaires effectuées avant/après les travaux des groupes spécialisés CMM) • Informations provenant de sources libres • Documents non publiés • Documents et dossiers • Questionnaires et enquêtes
Quels mécanismes adoptez-vous pour garantir l'exactitude des données recueillies?	• Chacune des discussions des groupes spécialisés CCM se rapporte à une ou plusieurs dimensions, ce qui permet de recueillir au moins deux fois des éléments de preuve au regard de chaque dimension. Cela permet également de procéder à une triangulation et à la collecte de différentes réponses à la même question auprès de différentes parties prenantes. • les réunions des groupes spécialisés CCM, si ceux-ci donnent leur l'assentiment préalable, sont enregistrées, et certains responsables de la mise en œuvre utilisent des transcriptions rendues anonymes des réunions pour analyser les réponses aux questions pour l'ensemble des données de l'examen. • La recherche documentaire confirme les données des groupes spécialisés CCM. • Le rapport CCM fait l'objet d'un examen par les pairs au sein du Comité technique du GCSCC et est soumis au gouvernement pour observations. • Certains responsables de la mise en œuvre utilisent l'outil de codage de champ structuré (SFC), qui leur permet de saisir et de coder les réponses issues des recherches documentaires et des groupes spécialisés CCM et de valider les indicateurs à chaque étape du processus d'examen. Les méthodes évoluent avec la mise en œuvre de l'outil SFC, ce qui témoigne de la volonté constante d'améliorer les méthodologies d'examen du modèle CCM.
Quels sont les principaux résultats de l'évaluation?	Rapport reposant sur des éléments factuels qui est soumis aux pouvoirs publics
Format de présentation des résultats de l'évaluation	• Rapport écrit comprenant des recommandations (PDF) • Présentation du résumé analytique au pays hôte (facultatif) • Atelier de validation avec le pays hôte et les principales parties prenantes (facultatif) • Outil de visualisation (OEA: https://www.cybersecurityobservatory.org)

Les résultats de l'évaluation peuvent-ils être publiés?	Oui. La transmission et/ou la publication du rapport, en totalité ou en partie, est laissée à la discrétion des pouvoirs publics.
Dans l'affirmative, comment peut-on accéder aux rapports précédents?	Tous les examens CMM, y compris les liens vers les rapports publiés, se trouvent sur les sites web suivants: • https://gcscc.ox.ac.uk/cmm-reviews • https://cybilportal.org/tools/portal-of-cybersecurity-capacity-maturity-model-cmm-review-reports/ (Pour en savoir plus sur l'état d'avancement du rapport, consultez le portail Cybil en recherchant "CMM + nom du pays")
Quels sont les éléments qui attestent de résultats concrets?	Les conclusions d'une évaluation indépendante d'un échantillon de déploiements du modèle CMM en février 2020 sont les suivantes: • L'examen CMM a permis d'accroître la sensibilisation à la cybersécurité et le renforcement des capacités. • L'examen CMM a contribué à une plus grande collaboration au sein des gouvernements. • Les pays ont indiqué que le modèle CMM avait servi de base à l'élaboration de leur stratégie et de leur politique (Macédoine du Nord, Lituanie et Géorgie par exemple). • L'examen CMM a renforcé la crédibilité interne de la stratégie de cybersécurité au sein des gouvernements. • L'examen CMM a permis de définir les rôles et les responsabilités au sein des gouvernements et de mobiliser davantage de fonds en faveur du renforcement des capacités de cybersécurité. • L'examen CMM a contribué à l'instauration de contacts en réseau et à la collaboration avec des entreprises et la société en général. L'examen CMM a été mené plus de 120 fois, avec des déploiements CMM dans plus de 85 pays, en collaboration avec des gouvernements nationaux dans toutes les régions du monde. On citera en particulier: • Deux études régionales (2016 et 2020) effectuées par l'Organisation des États américains (OEA). • Plus de 25 examens menés en collaboration avec la Banque mondiale et l'Agence coréenne de l'Internet et de la sécurité (KISA) dans le cadre de leurs programmes mondiaux relatifs aux capacités en matière de cybersécurité (phases I et II) et des évaluations des capacités nationales de cybersécurité (CMM) pour le Commonwealth et le portefeuille de programmes de la CEDEAO. • Équipe d'intervention en cas d'urgence informatique (CERT) et évaluation des capacités dans la région du Pacifique avec l'UIT, l'APT, l'APNIC et d'autres partenaires. • Renforcement des capacités de cybersécurité dans les pays du Commonwealth avec l'OTC. Les données provenant des examens CMM ont été utilisées pour les articles universitaires suivants:

	• Creese, S., Shillair, R., Bada, M., Reisdorf, B. C., Roberts, T. et Dutton, W. H. (2019). "The Cybersecurity Capacity of Nations", pp. 165-179 in Graham, M. and Dutton, W. H. (eds), Society and the Internet: How Networks of Information and Communication are Changing our Lives, 2nd edition. Oxford: Oxford University Press. • Dutton, W. H., Creese, S., Shillair, R. et Bada, M. (2019). "Cyber Security Capacity: Does It Matter?". Journal of Information Policy, 9: 280-306. doi:10.5325/jinfopoli.9.2019.0280. • Creese, S., Dutton, W. H., Esteve-González, P. et Shillair, R. (2021). "Cybersecurity Capacity Building: Cross-National Benefits and International Divides". Ce document sera présenté à la conférence CRPT Conference, Washington D.C., février 2021. Disponible sur le site du SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658350.
Quels sont les avantages d'une évaluation?	L'objectif d'un examen CMM est de recueillir des données sur les capacités d'un pays en matière de cybersécurité et de déterminer, parmi les cinq stades de maturité en matière de cybersécurité, celui que le pays a atteint au regard des dimensions du modèle CMM. Les données sont utilisées pour élaborer un rapport fondé sur des données factuelles, qui est soumis aux pouvoirs publics et est assorti de recommandations visant à: • évaluer la maturité des capacité de cybersécurité d'un pays; • présenter un ensemble pragmatique de mesures destinées à réduire et à éliminer les disparités concernant la maturité des capacités de cybersécurité; • définir les priorités en matière d'investissements et de renforcement des capacités futures; et • procéder à des analyses de rentabilité concernant les investissements et les améliorations correspondantes à apporter à la mise en œuvre de la cybersécurité au niveau national.
Avez-vous recours à un processus de calcul de la pondération?	Non.
Adoptez-vous un mécanisme de notation et/ou de classement dans votre évaluation?	Oui – Une notation de la maturité est effectuée, mais pas de classement. Le modèle CMM comprend cinq stades de maturité allant du stade du démarrage au stade dynamique. Le stade de démarrage suppose une approche ponctuelle des capacités, tandis que le stade dynamique représente une approche stratégique et la capacité de s'adapter à l'évolution de l'environnement. Le fait qu'un pays se trouve à un certain stade signifie qu'il a atteint un certain niveau de maturité des capacités de cybersécurité. Le modèle CMM propose les éléments de preuve qui seraient nécessaires pour déterminer qu'un certain stade de maturité a été atteint pour tel ou tel facteur/aspect. Pour atteindre un niveau de maturité dans une dimension du modèle CMM, il doit avoir été satisfait à tous les indicateurs correspondant à un facteur/aspect de cette dimension. Le modèle CMM indique donc directement les domaines qui doivent être développés davantage afin d'atteindre le stade de maturité suivant et les données à fournir pour prouver que ce niveau de maturité des capacités a été atteint.

Détails

À quelles questions essentielles l'outil peut-il contribuer à répondre?	• Quelles sont les capacités de cybersécurité existantes dans un pays? • Quelles sont les lacunes existantes en matière de cybersécurité dans un pays? • Quel est l'état d'avancement de la mise en œuvre des stratégies et des politiques? • Quels sont les acteurs concernés et quels sont les rôles et responsabilités? • Quelles mesures un pays peut-il prendre pour améliorer sa cybersécurité?
À quel stade du cycle de vie de la stratégie l'évaluation doit-elle être effectuée?	Lancement/Bilan et analyse/Suivi et évaluation
Comment l'évaluation contribue-t-elle à harmoniser d'autres activités?	Étant donné que les groupes spécialisés CMM rassemblent en un même lieu un large éventail de parties prenantes au niveau national ainsi que des partenaires internationaux (dans la mesure du possible), les examens CMM se prêtent bien à une coordination avec d'autres activités avant ou après le processus et en parallèle. Le groupes spécialisés CMM − de par leur forme − permettent également de recueillir des contributions pendant la réunion aux fins d'autres évaluations, le cas échéant.
Quel est le rôle de l'évaluation dans le processus de mise en correspondance avec le GFCE?	Les examens des capacités de cybersécurité, conjointement avec les examens nationaux des capacités d'intervention en cas d'incident et les évaluations nationales des risques, constituent la première activité du programme du GFCE s'inscrivant dans le processus d'élaboration d'une stratégie nationale et font partie de la phase de lancement. Grâce à son approche multipartite, son exhaustivité et sa transparence, l'examen CMM permet de réunir les différentes parties prenantes d'un pays, ainsi que les bailleurs de fonds et les responsables de la mise en œuvre, et de fournir une base commune sur laquelle planifier et mettre en œuvre des activités de renforcement des capacités de cybersécurité.
Quelles études de cas ou références sont disponibles concernant les avantages de l'outil?	Etudes de cas CMM: Macédoine du Nord, Ghana, Samoa, Géorgie et rapports régionaux de l'OEA: https://gcscc.ox.ac.uk/case-studies. Étude de cas du Sénégal: Réunion annuelle du GFCE à Singapour, "*National Stratégies. Interviews Behind the Cover*": https://thegfce.org/national-strategies-interviews-behind-the-cover. Banque mondiale: Programme mondial de renforcement des capacités en matière de cybersécurité. Enseignements tirés et recommandations visant à renforcer le programme https://cybilportal.org/publications/global-cybersecurity-capacity-program-lessons-learned-and-recommendations-towards-strengthening-the-program/. La cybersécurité dans les États insulaires du Pacifique: https://t.co/smxYhtrqBz?amp=1.
Quels sont les mécanismes propres à garantir l'indépendance, l'impartialité et la neutralité de vos résultats?	La plupart des responsables de la mise en œuvre sont des instituts de recherche et ont reçu l'autorisation éthique de leurs Bureaux de recherche respectifs pour recueillir les données relatives à cette évaluation. Chaque rapport CMM est validé par le Comité technique du GCSCC, qui comprend des universitaires reconnus et des experts en cybersécurité.

Veuillez ajouter toute information supplémentaire	Façon dont les examens CMM contribuent à la recherche sur le renforcement des capacités de cybersécurité: https://gcscc.ox.ac.uk/our-approach. Rapport OEA/BID sur la cybersécurité (2020): Risques, progrès et perspectives dans la région Amérique latine et Caraïbes: https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean. Rapport OEA/BID sur la cybersécurité (2016): Sommes-nous prêts dans la région Amérique latine et Caraïbes?: https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean. GFCE – Évaluer les capacités nationales en matière de cybersécurité à l'aide d'un modèle de maturité https://thegfce.org/wp-content/uploads/2020/04/Assessnationalcybersecuritycapacityusingamaturitymodel.pdf. Initiative GFCE: Faire progresser la cybersécurité au Sénégal et en Afrique de l'Ouest: https://cybilportal.org/projects/progressing-cybersecurity-in-senegal-and-west-africa-gfce-initiative/. Initiative GFCE: Évaluer et développer les capacités en matière de cybersécurité https://cybilportal.org/projects/assessing-and-developing-cybersecurity-capability-gfce-initiative/.

Cadre pour l'élaboration et la mise en œuvre d'une stratégie de cybersécurité (CSDI)

MITRE Corporation

Le cadre pour l'élaboration et la mise en œuvre d'une stratégie de cybersécurité comprend un modèle en quatre étapes permettant 1) d'appréhender le contexte national des cyberrisques/possibilités; 2) d'évaluer les capacités actuelles dans huit catégories essentielles ainsi que les bases stratégiques ("capacité à renforcer les capacités"); 3) de définir et de classer par ordre de priorité les objectifs et les investissements stratégiques en fonction des lacunes recensées sur le plan des capacités; et 4) d'élaborer des feuilles de route pour la mise en œuvre, afin de garantir la viabilité à long terme.

Vue d'ensemble

Dernière date de mise à jour de l'outil	Septembre 2020
Quel est le nom de l'outil d'évaluation?	Cadre pour l'élaboration et la mise en œuvre d'une stratégie de cybersécurité (CSDI)
Quel est le nom de l'organisation qui gère l'outil?	MITRE Corporation
Quels sont les responsables de la mise en œuvre des évaluations?	MITRE Corporation
Veuillez fournir des liens vers l'outil et toute information supplémentaire.	https://cybilportal.org/tools/national-cyber-strategy-development-implementation-framework/
Qui faut-il contacter pour discuter de l'organisation d'une évaluation?	Gary Bundy: gbundy@mitre.org Cynthia Wright: cawright@mitre.org Johanna Vazzana: jvazzana@mitre.org
Couverture géographique	Régionale, nationale ou au niveau de l'organisation
Qui peut utiliser l'outil?	Tout le monde

Quels sont les thèmes ou sujets traités?	Les huit catégories évaluées sont les suivantes: 1) Droit civil, réglementation et responsabilité 2) Politique et normes 3) Mobilisation de ressources tenant compte des risques 4) Résilience des activités 5) Intervention en cas d'incident 6) Prévention de la cybercriminalité et poursuites judiciaires 7) Perfectionnement du personnel qualifié en matière de cybersécurité 8) Sensibilisation du public et culture de la cybersécurité. Dans chacune de ces catégories, la participation de plusieurs parties prenantes et les partenariats sont considérés comme des facteurs essentiels, et les méthodes de mise en œuvre pour le perfectionnement du personnel, en particulier, sont axées sur l'établissement de partenariats efficaces entre le secteur public et le secteur privé. Les bases stratégiques sont également prises en compte dans les évaluations, les plus importants de ces facteurs étant l'engagement des hauts responsables et la participation des parties prenantes.
Quels sont les thèmes ou sujets traités par le GFCE?	Politiques générales et stratégie ☒ Stratégies ☒ Évaluations ☐ Mesures de renforcement de la confiance et normes ☐ Cyberdiplomatie ☐ Le droit international dans le cyberespace Gestion des incidents et protection des infrastructures essentielles de l'information ☒ Équipes nationales d'intervention en cas d'incident de sécurité informatique ☐ Examen et analyse des incidents ☐ Exercices de cybersécurité ☒ Protection des infrastructures essentielles de l'information Cybercriminalité ☒ Cadres juridiques/Droit de la cybercriminalité ☒ Application de la loi dans le cyberespace ☒ Formation en matière de cybercriminalité ☒ Prévention de la cybercriminalité Culture et compétences ☒ Sensibilisation à la cybersécurité ☒ Éducation et formation ☒ Perfectionnement de la main-d'œuvre Normes ☒ Normes internationales et/ou nationales

Types d'indicateurs	Les indicateurs sont avant tout qualitatifs et portent principalement sur les mécanismes de gouvernance, les politiques générales, les processus et la mobilisation de ressources. En général, ils ne présentent pas un caractère particulièrement technique (c'est-à-dire qu'ils ne sont pas axés sur telle ou telle architecture de réseau ou sur des tests de systèmes pratiques).
Combien d'indicateurs sont utilisés et comment sont-ils appliqués	Plus de 100 indicateurs, regroupés dans les différents catégories de capacités concernées, sont utilisés.
Méthodologie – Quel type d'évaluation est utilisé?	Analyses fondées sur la recherche et enquêtes /entretiens avec les parties prenantes.
Méthode de collecte de données primaires	• Informations provenant de sources libres • Entretiens • Questionnaires et enquêtes • Documents et dossiers
Procédez-vous à la collecte de données secondaires?	Ateliers pour les parties prenantes
Quels mécanismes adoptez-vous pour garantir l'exactitude des données recueillies?	• Examen de la qualité en interne • Les questionnaires sont gérés par un groupe de parties prenantes aussi diversifié que possible, afin d'élargir les perspectives/de valider les idées • Enquête avec notation automatisée des réponses
Quels sont les principaux résultats de l'évaluation?	On associe les résultats d'un ensemble de travaux de recherche en accès libre, d'une analyse des menaces/possibilités, d'une évaluation correctement gérée et d'entretiens de suivi, de façon à obtenir un "diagramme radar" intuitif destiné à faciliter l'établissement d'un ordre de priorité entre les objectifs et les investissements en fonction des risques dans les huit catégories précitées, et à élaborer un rapport détaillé contenant des recommandations classées par ordre de priorité.
Format de présentation des résultats de l'évaluation	• Rapport • Outil de visualisation
Les résultats de l'évaluation peuvent-ils être publiés?	Oui, avec l'approbation de l'entité requérante.
Comment accéder aux rapports précédents?	Une demande doit être adressée au gouvernement ou à l'organisation faisant l'objet de l'évaluation.

Quels sont les éléments qui attestent de résultats concrets?	Dans chaque pays avec lequel MITRE entretient des relations durables, le gouvernement et/ou les organisations faisant l'objet de l'évaluation ont apporté des modifications aux objectifs stratégiques, aux structures/mécanismes de gouvernance, aux processus de coordination opérationnelle, aux communications et processus d'intervention en cas d'incident, aux méthodes de perfectionnement du personnel et/ou aux thèmes du programme de sensibilisation du public, afin de tenir compte des priorités identifiées dans le cadre de leur participation.
Quels sont les avantages d'une évaluation?	Les pays, organisations et/ou organismes d'assistance faisant l'objet de l'évaluation se font une idée plus précise du contexte stratégique des risques/possibilités qui est le leur ainsi que des leviers, des besoins et des lacunes en termes de capacités, sous une forme qui facilite un aspect essentiel de l'investissement dans les capacités, à savoir la hiérarchisation des priorités. Grâce à des ateliers de suivi sur l'élaboration et la mise en œuvre de stratégies, ils mettent en évidence les rôles et responsabilités des principales parties prenantes, les bonnes pratiques en matière de gouvernance, les possibilités de partenariat, les stratégies de mobilisation de ressources, les insuffisances et les ambiguïtés des textes législatifs et des politiques générales, ainsi que les exigences de base (conditions préalables), compte tenu des spécificités de leur contexte lié aux menaces et de leurs besoins en matière de renforcement des capacités. En outre, étant donné que l'évaluation privilégie une approche mobilisant l'ensemble des services de l'État ou engageant l'ensemble de l'organisation et que les ateliers sont organisés à l'aide d'outils participatifs éprouvés reposant sur la pensée créative, elle favorise la participation et l'adhésion des parties prenantes, ce qui est essentiel pour l'efficacité de la mise en œuvre.
Avez-vous recours à un processus de calcul de la pondération?	Les catégories de capacités ont la même importance lors de l'évaluation. Cependant, certaines catégories seront plus importantes que d'autres pour certains pays/organisations faisant l'objet de l'évaluation, en fonction de leur contexte stratégique, de leurs capacités actuelles et de leurs ressources humaines/financières. Cette approche vise plus particulièrement à recenser les catégories qui devraient donner lieu à une pondération plus importante pour chaque entité faisant l'objet de l'évaluation, en fonction de leurs besoins spécifiques en matière de risques/possibilités.
Adoptez-vous un mécanisme de notation et/ou de classement dans votre évaluation?	Le diagramme radar (outil de sortie auquel vient s'ajouter une analyse détaillée et un rapport contenant des recommandations) qui est élaboré utilise une échelle à quatre niveaux. Cependant, il ne s'agit pas d'un modèle de maturité: les insuffisances en matière de capacités sont évaluées dans le contexte de l'objectif final recherché par le pays ou l'organisation, et non sur la base d'un ensemble objectif de critères. Cette approche permet de faire en sorte que les pays/organisations ne recherchent pas des indicateurs qui sont moins importants pour leur contexte de menace stratégique, et permet aux responsables de la mise en œuvre de contribuer à adapter les stratégies d'investissement aux besoins présentant le plus d'intérêt pour les objectifs économiques et de sécurité.

Détails

À quelles questions essentielles l'outil peut-il contribuer à répondre?	• Quelle est notre situation en termes de cybermenaces/possibilités? • Compte tenu de cette situation, quels sont nos objectifs s'agissant du renforcement et de la sécurisation des capacités et services TIC/de cybersécurité/numériques? • Quelles sont les parties prenantes dans cet espace, et quel est leur rôle? • Quelles sont nos lacunes en matière de capacités au regard de nos objectifs stratégiques? • Compte tenu de ces lacunes, quelles mesures devrions-nous prendre en priorité? • Quels objectifs pourraient nous aider à atteindre nos buts prioritaires? • Comment pourrions-nous concevoir des initiatives pour les atteindre? • Parmi les diverses initiatives que nous pourrions prendre, quelles sont celles qui offrent le meilleur retour sur investissement en termes de résultats et de faisabilité? • Quelles ressources peuvent être utilisées? • Qui sont nos partenaires potentiels pour la mise en œuvre des initiatives retenues? • Comment élaborer et exécuter une feuille de route relative à la mise en œuvre? • Comment pouvons-nous accroître l'adhésion des parties prenantes et le soutien du public?
À quel stade du cycle de vie de la stratégie l'évaluation doit-elle être effectuée?	Lancement/Bilan et analyse/Élaboration de la stratégie/Mise en œuvre
Comment l'évaluation contribue-t-elle à harmoniser d'autres activités?	Cette approche, qui privilégie une perspective mobilisant l'ensemble des services de l'État ou de l'organisation dans un contexte de menaces et de possibilités bien défini, fournit aux parties prenantes un cadre commun permettant de définir, de classer par ordre de priorité, de financer et de poursuivre des objectifs communs. En différenciant les lacunes en matière de capacités en fonction de grandes catégories, elle aide les entités à privilégier les catégories les plus importantes pour elles, tout en mettant en évidence d'autres catégories dans lesquelles des possibilités de renforcement des capacités peuvent se présenter, par exemple les ressources des programmes d'assistance susceptibles d'accroître les capacités sans détourner les ressources internes, qui sont limitées. Enfin, comme cette approche s'inscrit dans un cadre multi- parties prenantes, elle permet de mettre l'accent sur la communication, l'échange d'informations et la transparence des processus, autant d'éléments qui garantissent que les parties prenantes et les partenaires connaissent bien les priorités essentielles et les activités en cours (et y adhèrent).
Quel est le rôle de l'évaluation dans le processus de mise en correspondance avec le GFCE?	L'évaluation clarifie les besoins prioritaires, les contacts avec les parties prenantes, les autres programmes en cours/disponibles et les ressources humaines et financières disponibles.

Quelles études de cas ou références sont disponibles concernant les avantages de l'outil?	A ce jour, toutes les évaluations ont été effectuées pour le compte de pays/d'organisations qui en avaient fait la demande, ou à la demande du Département d'État des États-Unis. Aucune évaluation n'a été publiée, bien que les Gouvernements du Botswana, du Ghana, de l'Ukraine et de l'Équateur aient publiquement exprimé leur satisfaction à l'occasion d'allocutions publiques, de communiqués sur les réseaux sociaux et/ou de sommets intergouvernementaux. Le meilleur gage de reconnaissance est sans doute le fait que les administrations fédérales des États-Unis et les pays partenaires continuent de nous demander de leur transmettre nos recommandations en matière d'assistance, de les utiliser et d'y donner suite, et que le nombre de pays avec lesquels nous collaborons directement est passé de trois à plus de vingt-quatre au cours des quatre années d'utilisation de ce cadre; de plus, chaque pays sollicite activement nos conseils et notre assistance. Au niveau régional, le nombre de pays avec lesquels nous collaborons est supérieur à 90 et ne cesse de croître, et de nouvelles demandes d'assistance spécifiques nous sont soumises à l'issue de chaque collaboration.
Quels sont les mécanismes propres à garantir l'indépendance, l'impartialité et la neutralité de vos résultats?	MITRE est une organisation de recherche-développement financée par le gouvernement fédéral, qui applique des exigences très strictes en matière de contrôle de la qualité interne ainsi qu'une charte publique en vertu de laquelle elle s'engage expressément à fournir un service impartial, sans conflit d'intérêts et dans le sens de l'intérêt général.
Veuillez ajouter toute information supplémentaire	Ce cadre a été élaboré sous l'égide du Bureau du coordonnateur pour les questions de cybersécurité du Département d'État des États-Unis, et a été amélioré dans le cadre d'engagements bilatéraux et régionaux sous la direction du Département d'État. L'utilisation de cette évaluation hors du cadre des engagements placés sous la direction du Département d'État des États-Unis ne signifie pas nécessairement qu'elle bénéficie de l'appui du le Gouvernement des États-Unis ou va dans le sens de ses politiques. Cependant, les valeurs des États-Unis que sont la liberté d'information, la détermination à œuvrer en faveur d'un Internet libre et ouvert, la primauté du droit et les droits de l'homme sont implicites dans notre modèle et nos recommandations.

Indice mondial de cybersécurité (GCI)

Union internationale des télécommunications (UIT)

L'Indice mondial de cybersécurité (GCI) a pour but d'aider les pays à recenser les domaines dans lesquels des améliorations pourraient être apportées en matière de cybersécurité, de les inciter à agir pour améliorer leur classement à cet égard et d'augmenter par là même le niveau de cybersécurité dans le monde. Le champ d'application et le cadre de l'indice GCI sont définis dans la Résolution 130 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires de l'UIT, qui porte sur le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des TIC. Le questionnaire du GCI, à partir duquel sont définis des indicateurs, des sous-indicateurs et des micro-indicateurs, est créé et approuvé dans le cadre d'une consultation menée au titre de la Question 3/2(Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité parmi les membres de l'UIT) de la Commission d'études 2 du Secteur du développement des télécommunications de l'UIT (UIT-D). L'enquête est administrée au moyen d'une plate-forme en ligne permettant de recueillir les éléments de preuve nécessaires.

La quatrième itération du questionnaire GCI (2019-2020) mesure 20 indicateurs généraux au moyen de 82 questions. Les 20 indicateurs s'articulent autour des cinq piliers du Programme mondial cybersécurité (GCA), à savoir: *cadre juridique, mesures techniques, mesures organisationnelles, renforcement des capacités et mesures en matière de coopération*. Le questionnaire GCIv4 et la documentation pertinente relative à l'indice GCI ont été soumis par le Bureau de développement des télécommunications de l'UIT (BDT) à la Commission d'études 2 de l'UIT-D en octobre 2019, avant le lancement de l'enquête. En mars 2020, le BDT a rendu compte à la Commission d'études 2 de l'état des réponses au questionnaire, a informé les membres des prochaines étapes du processus d'analyse des données et a précisé que pour l'élaboration des coefficients de pondération, il serait fait appel à un groupe d'experts constitué dans le cadre d'un processus de consultation ouvert auprès des États Membres de l'UIT, des Membres du Secteur et des partenaires du BDT. En octobre 2020, le groupe d'experts chargé de la pondération a formulé des recommandations relatives à la pondération pour les indicateurs, sous-indicateurs et micro-indicateurs GCIv4, et a proposé d'apporter des modifications au questionnaire GCI pour les itérations futures. La vérification des réponses au questionnaire est en cours, aux fins de validation finale par les pays ayant soumis des réponses. Le rapport final devrait être publié en 2021.

Vue d'ensemble

Dernière date de mise à jour de l'outil	La dernière mise à jour de la publication a été effectuée en mars 2019. Nous procédons actuellement à la collecte des données et à la vérification des données soumises pour le rapport GCIv4.
Quel est le nom de l'outil d'évaluation?	Indice mondial de cybersécurité (ICG)
Quel est le nom de l'organisation qui gère l'outil?	Union internationale des télécommunications (UIT)
Quels sont les responsables de la mise en œuvre des évaluations?	Union internationale des télécommunications (UIT)

Veuillez fournir des liens vers l'outil et toute information supplémentaire	• Site web de l'UIT: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global- cybersecurity-index.aspx. • Portail Cybil: https://cybilportal.org/projects/itu-global-cybersecurity-index-gci- programme/.
Qui faut-il contacter pour discuter de l'organisation d'une évaluation?	Équipe chargée de l'indice GCI: gci@itu.int
Couverture géographique	Mondiale
Qui peut utiliser l'outil?	• États Membres: ministères/organismes • Organismes de cybersécurité/décideurs • Établissements universitaires • Experts en cybersécurité • Toute personne intéressée La participation aux travaux de l'UIT peut être exigée pour les universités et les organisations qui souhaitent collaborer concernant l'indice GCI.
Quels sont les thèmes ou les sujets abordés?	Les thèmes de l'indice GCI sont les suivants: **Cadre juridique:** • Règle juridique de fond en matière de cybercriminalité • Réglementation relative à la cybersécurité **Mesures techniques:** • Équipes d'intervention nationales/gouvernementales en cas d'incident (CERT/CIRT/CSRIT) • Équipes CIRT/CSIRT/CERT sectorielles • Cadre national pour la mise en œuvre des normes en matière de cybersécurité • Protection en ligne des enfants (COP) **Mesures organisationnelles:** • Stratégies nationales en matière de cybersécurité (NCS) • Organismes responsables/nationaux • Indicateurs relatifs à la cybersécurité **Mesures relatives au renforcement des capacités:** • Campagnes de sensibilisation du public à la cybersécurité • Formation à l'intention des professionnels de la cybersécurité • Programmes d'études nationaux et programmes universitaires • Programmes de recherche-développement en matière de cybersécurité • Secteur de la cybersécurité à l'échelle nationale • Mécanismes incitatifs du gouvernement visant à encourager le renforcement des capacités en matière de cybersécurité **Mesures relatives à la coopération:** • Accords bilatéraux • Participation à des mécanismes internationaux (forums) • Accords multilatéraux • Partenariats secteur public-secteur privé

<table>
<tr><td></td><td>

- Partenariats interorganismes

Pour une description complète de chaque mesure, veuillez consulter les rapports publiés à l'adresse suivante: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
</td></tr>
<tr><td>Quels sont les thèmes ou sujets traités par le GFCE?</td><td>

Politiques générales et stratégie

☒ Stratégies

☒ Évaluations

☒ Mesures de renforcement de la confiance et normes

☒ Cyberdiplomatie

☒ Le droit international dans le cyberespace

Gestion des incidents et protection des infrastructures essentielles de l'information

☒ Intervention en cas d'incident de sécurité informatique

☒ Examen et analyse des incidents

☒ Exercices de cybersécurité

☒ protection des infrastructures essentielles de l'information

Cybercriminalité

☒ Cadres juridiques/Droit de la cybercriminalité

☒ Application de la loi dans le cyberespace

☒ Formation en matière de cybercriminalité

☒ Prévention de la cybercriminalité

Culture et compétences

☒ Sensibilisation à la cybersécurité

☒ Éducation et formation

☒ Perfectionnement de la main-d'œuvre

Normes

☒ Normes internationales et/ou nationales
</td></tr>
<tr><td>Types d'indicateurs</td><td>La collecte des données GCI est qualitative et un système binaire est utilisé pour évaluer l'existence ou l'absence d'une activité, d'un service ou d'une mesure donné.</td></tr>
<tr><td>Combien d'indicateurs sont utilisés et comment sont-ils appliqués?</td><td>L'indice GCI ne suit pas une série d'indicateurs préétablis. À chaque itération, le questionnaire est modifié et révisé compte tenu des observations reçues de la part des coordonnateurs des pays et des membres. Le nombre d'indicateurs peut donc diminuer ou augmenter, et il n'y a pas un nombre fixe d'indicateurs pour chaque thème., Voir par exemple le tableau ci-dessous, qui indique le nombre d'indicateurs dans chaque itération effectuée à ce jour.
<table>
<tr><th>GCIv1</th><th>GCIv2</th><th>GCIv3</th><th>GCIv4</th></tr>
<tr><td>17 indicateurs avec 17 questions principales</td><td>25 indicateurs avec 157 questions</td><td>25 indicateurs avec 50 questions principales</td><td>20 indicateurs avec 82 questions principales</td></tr>
</table>
</td></tr>
</table>

Méthodologie – Quel type d'évaluation est utilisé?	L'indice GCI utilise des méthodes d'évaluation primaires et secondaires. L'équipe chargée de l'indice GCI recueille des données pour les pays qui ne participent pas et leur communique les résultats pour approbation, et vérifie et valide les réponses soumises par les coordonnateurs des États Membres de l'UIT
Méthode de collecte de données primaires	• Informations provenant de sources libres • Documents non publiés • Questionnaires et enquêtes • Documents et dossiers
Procédez-vous à la collecte de données secondaires?	Oui. Des données secondaires sont recueillies pour les pays qui répondent au questionnaire GCI, les différentes étapes étant les suivantes: • L'UIT procède à des vérifications, en identifiant les réponses manquantes, les documents justificatifs et les liens, et en utilisant les informations provenant de sources libres, des documents non publiés, des questionnaires et des enquêtes, ainsi que des documents et des dossiers accessibles au public. • Les réponses vérifiées sont renvoyées au coordonnateur national, qui améliore au besoin la précision des réponses. • L'UIT valide les modifications finales apportées par le coordonnateur national et renvoie le document à chaque coordonnateur pour approbation finale. • Les réponses au questionnaire ainsi validées sont ensuite utilisées aux fins de l'analyse, de la notation et du classement.
Quels mécanismes adoptez-vous pour garantir l'exactitude des données recueillies?	Les coordonnateurs GCI désignés par les ministères ont généralement suivi une formation ou possèdent des compétences spécialisées dans le domaine de la cybersécurité et occupent des postes liés à la cybersécurité au sein des différents ministères. En outre, les liens et les documents pertinents demandés et validés proviennent des sites web publics officiels des gouvernements, et il arrive que des documents officiels confidentiels soient fournis. Nous faisons appel à des experts chargés de la validation possédant une expérience dans les domaines liés à la cybersécurité, qui doivent mener à bien le processus de vérification plusieurs fois pour chaque pays et contacter les pays jusqu'à ce qu'ils obtiennent une confirmation finale pour garantir l'exactitude des données.
Format de présentation des résultats de l'évaluation	Rapport
Les résultats de l'évaluation peuvent-ils être publiés?	Oui, les résultats peuvent être publiés. L'indice GCI est un produit en accès libre qui vise à sensibiliser l'opinion à l'échelle mondiale. Tous les rapports précédents peuvent être consultés à l'adresse: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
Comment accéder aux rapports précédents?	Les rapports précédents sont accessibles et peuvent être téléchargés à l'adresse: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Quels sont les éléments qui attestent de résultats concrets?	La participation grandissante des États Membres au processus GCI témoigne de l'intérêt sans cesse croissant que suscite l'indice: **GCIv1 (2015)** / **GCIv2 (2017)** / **GCIv3 (2018)** / **GCIv4 (2019-2020)** 105 pays / 134 pays / 155 pays / Actuellement 163 pays De nombreux pays demandent à l'UIT de les aider à concevoir leur approche en matière de cybersécurité, notamment en élaborant des stratégies nationales et en améliorant les stratégies existantes, en mettant sur pied des CERT et en menant des activités de renforcement des capacités. Les pays ayant obtenu une note faible ou moyenne (sur la base de plages de notation qui sont maintenues constantes dans le temps) ont pu bénéficier d'interventions ciblées, ce qui a entraîné une diminution régulière du nombre de ces pays.
Quels sont les avantages d'une évaluation?	Les évaluations permettent d'identifier les lacunes concernant le développement de la cybersécurité dans les pays et les régions, et d'accroître la sensibilisation à la cybersécurité dans le monde. Elles permettent également d'identifier les pays qui ont le plus besoin d'une assistance pour améliorer leur situation en matière de cybersécurité. Grâce aux données recueillies, la GCI met en évidence les pratiques que les États Membres peuvent suivre et qui sont adaptées à leur environnement national, encourage l'adoption de bonnes pratiques et favorise une culture mondiale de la cybersécurité.
Avez-vous recours à un processus de calcul de la pondération?	Oui. La pondération des indicateurs dans le cadre de l'indice GCI est évaluée par les membres du groupe d'experts sur l'Indice GCI, en fonction de l'importance de l'indicateur au regard des cinq piliers du Programme GCA, de sa pertinence par rapport aux principaux objectifs et au cadre conceptuel de l'Indice GCI, ainsi que de la disponibilité et de la qualité des données. Le groupe d'experts formule des recommandations impartiales sur la pondération à l'issue de la réunion du groupe d'experts chargé de la pondération qui est organisée pour chaque itération de l'Indice GCI.
Adoptez-vous un mécanisme de notation et/ou de classement dans votre évaluation?	Oui. La moyenne des coefficients de pondération des indicateurs de chaque expert est calculée afin d'obtenir le coefficient de pondération final de chaque indicateur. Grâce à une fonction appliquée, un pays ayant répondu OUI avec pièce justificative à l'appui se voit attribuer la note maximale pour l'indicateur, tandis qu'un pays qui ne fournit pas d'éléments de preuve ou répond NON obtient une note égale à zéro pour cet indicateur. Les notes globales sont normalisées et classées.

Détails

À quelles questions essentielles l'outil peut-il contribuer à répondre?	• Quelles sont les tendances mondiales actuelles et la nature des politiques en matière de cybersécurité? • Comment les États Membres peuvent-ils identifier les points forts et les points faibles des mesures de cybersécurité qu'ils ont adoptées? • Quels sont les niveaux d'engagement des pays en matière de cybersécurité, et quels pays proposent des bonnes pratiques dans ce domaine?

<table>
<tr><td>À quel stade du cycle de vie de la stratégie l'évaluation doit-elle être effectuée?</td><td>Lancement/Bilan et analyse/Élaboration de la stratégie/Mise en œuvre/Suivi et évaluation</td></tr>
<tr><td>Comment l'évaluation contribue-t-elle à harmoniser d'autres activités?</td><td>L'évaluation de l'indice GCI permet de déterminer les points forts ou les points faibles des engagements pris par les États Membres en matière de cybersécurité, afin de définir les domaines dans lesquels ils peuvent avoir besoin d'une assistance supplémentaire concernant le renforcement des capacités, ou dans lesquels ils sont en mesure d'apporter un appui à d'autres États Membres. Ainsi, grâce à l'évaluation GCI, l'UIT peut identifier les besoins d'éducation en matière de cybersécurité dans les systèmes éducatifs des membres.
<table>
<tr><th>Année</th><th>Note élevée</th><th>Note moyenne</th><th>Note faible</th></tr>
<tr><td>2018-2019</td><td>54</td><td>53</td><td>87</td></tr>
<tr><td>2016-2017</td><td>30</td><td>60</td><td>104</td></tr>
<tr><td>2014-2015</td><td>19</td><td>52</td><td>122</td></tr>
</table></td></tr>
<tr><td>Quelles études de cas ou références sont disponibles concernant les avantages de l'outil?</td><td>Chaque année, de nombreux pays demandent une assistance en vue de la mise en place d'équipes CERT et de stratégies nationales de cybersécurité à la suite de l'évaluation, des notes et du classement GCI.
Par exemple:
Le Bénin a mis en œuvre une stratégie de cybersécurité suite aux activités de sensibilisation menées dans le cadre de l'indice GCI: https://news.itu.int/benin-launches-a-new-national-cybersecurity-strategy/.
La République du Congo a adopté la loi sur la cybersécurité et la loi sur la cybercriminalité: https://postetelecom.gouv.cg/le-senat-adopte-a-lunanimite-la-creation-de-lagence-nationale-de-securite-des-systemes-dinformation/.
En 2018, des progrès ont été accomplis dans les pays ci-après en ce qui concerne les engagements en matière de cybersécurité, tels qu'ils ont été communiqués dans le cadre des évaluations de l'indice GCI:
Bénin, Estonie, Pologne, Zimbabwe, Zambie, Égypte, Afrique du Sud et Eswatini (élaboration de lois sur la cybercriminalité);
Ouganda (rédaction d'une législation sur la protection des données et de la vie privée);
Australie, Botswana, Canada, République tchèque, Danemark, Japon, Jordanie, Pays-Bas, Espagne, Samoa, Singapour et Luxembourg, (mise à jour des stratégies nationales en matière de cybersécurité (NCS)); et
Cameroun, Malawi, Tanzanie et Zimbabwe, élaboration de stratégies nationales en matière de cybersécurité (NCS).
Articles dans les médias consacrés à l'indice GCI: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.</td></tr>
<tr><td>Quels sont les mécanismes propres à garantir l'indépendance, l'impartialité et la neutralité de vos résultats?</td><td>Les soumissions concernant l'indice GCI sont validées de manière indépendante par notre équipe.
Un groupe d'experts indépendants donne son avis sur les coefficients de pondération des indicateurs dans le modèle, aucun expert ne pouvant à lui seul modifier de manière significative ces coefficients.</td></tr>
</table>

Cadre d'évaluation des capacités nationales (CECN)

Agence de l'Union européenne pour la cybersécurité (ENISA)

Le principal objectif du *cadre d'évaluation des capacités nationales* (CECN) est de créer un outil d'autoévaluation destiné à aider les États Membres de l'UE à mesurer le niveau de maturité de leurs capacités de cybersécurité. Dans cette optique, l'ENISA a utilisé comme point de départ les objectifs stratégiques des stratégies nationales de cybersécurité (SNCS) des États Membres de l'UE. Étant donné que les capacités de cybersécurité sont les principaux instruments utilisés par les pays pour atteindre les objectifs de leurs SNCS, le CECN comprend des questions portant sur cinq niveaux de maturité, compte tenu de 17 objectifs stratégiques inclus dans la plupart des SNCS des pays européens. Le cadre présente une vue simple et représentative du niveau de maturité de l'État Membre en matière de cybersécurité à trois niveaux différents: au niveau des objectifs, au niveau des groupes et au niveau global.

Vue d'ensemble

Dernière date de mise à jour de l'outil	2 décembre 2020
Quel est le nom de l'outil d'évaluation?	Cadre d'évaluation des capacités nationales (CECN)
Quel est le nom de l'organisation qui gère l'outil?	Agence de l'Union européenne pour la cybersécurité (ENISA)
Quels sont les responsables de la mise en œuvre des évaluations?	États Membres de l'UE
Veuillez fournir des liens vers l'outil et toute information supplémentaire.	https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework Le CECN sera disponible sous la forme d'un outil en ligne en 2021.
Qui faut-il contacter pour discuter de l'organisation d'une évaluation?	Agence de l'Union européenne pour la cybersécurité (ENISA)
Couverture géographique	Union européenne/monde
Qui peut utiliser l'outil?	Le CECN s'adresse aux décideurs, aux experts et aux représentants des pouvoirs publics responsables de la conception, de la mise en œuvre et de l'évaluation des SNCS et – de manière générale – des capacités de cybersécurité, ou participant à ces activités. En outre, les conclusions entérinées dans le document publié peuvent s'avérer utiles pour les experts et les chercheurs dans le domaine des politiques de cybersécurité à l'échelle nationale ou européenne.

Quels sont les thèmes ou les sujets abordés?	Le modèle conceptuel du cadre d'autoévaluation comprend 17 objectifs stratégiques tirés des stratégies nationales sur la cybersécurité des États Membres de l'UE et s'articule autour de quatre groupes principaux. Chacun de ces groupes couvre un domaine thématique clé pour le renforcement des capacités de cybersécurité et contient différents objectifs. Chaque objectif est ensuite évalué à l'aide de questions portant sur différents niveaux de maturité. Les groupes de questions ont trait aux sujets suivants: **I) Gouvernance et normes en matière de cybersécurité** 1) Élaborer des plans d'urgence cybernétique nationaux 2) Établir des mesures de sécurité de base 3) Sécuriser l'identité numérique et instaurer la confiance dans les services publics numériques Ce groupe traite des aspects de la planification à prendre en compte pour que l'État Membre soit prêt à faire face aux cyberattaques ainsi que les normes à élaborer pour protéger les États Membres et l'identité numérique. **II) Renforcement des capacités et sensibilisation** 4) Organiser des exercices de cybersécurité 5) Établir une capacité de réponse aux incidents 6) Sensibiliser les utilisateurs 7) Renforcer les programmes de formation et d'enseignement 8) Encourager la recherche-développement 9) Inciter le secteur privé à investir dans des mesures de sécurité 10) Améliorer la cybersécurité de la chaîne d'approvisionnement Ce groupe évalue la capacité des États Membres à sensibiliser l'opinion aux risques et aux menaces en matière de cybersécurité et à la manière d'y faire face. En outre, cette dimension évalue la capacité du pays à renforcer en permanence ses capacités de cybersécurité et à accroître le niveau général des connaissances et des compétences dans ce domaine. **III) Législation et réglementation** 11) Protéger les infrastructures essentielles de l'information, les opérateurs fournissant des services essentiels (OES) et les fournisseurs de services numériques(DSP) 12) Lutter contre la cybercriminalité 13) Mettre en place des mécanismes de signalement des incidents 14) Renforcer la protection de la vie privée et des données Ce groupe mesure la capacité des États Membres à mettre en place les instruments juridiques et réglementaires nécessaires pour lutter contre la montée de la cybercriminalité et pour tenir compte d'impératifs juridiques tels que le signalement des incidents, les questions de respect de la vie privée et la protection des infrastructures essentielles de l'information(CIIP). **IV) Coopération** 15) Établir un partenariat public-privé 16) Institutionnaliser la coopération entre les organismes publics 17) Participer à la coopération internationale Ce groupe évalue la coopération et le partage d'informations entre les différents groupes de parties prenantes à l'échelle nationale et internationale.

Quels sont les thèmes ou les sujets abordés par le GFCE?	Politiques générales et stratégie ☒ Stratégies ☒ Évaluations ☒ Mesures de renforcement de la confiance et normes ☒ Cyberdiplomatie ☐ Le droit international dans le cyberespace Gestion des incidents et protection des infrastructures essentielles de l'information ☒ Intervention en cas d'incident de sécurité informatique ☒ Examen et analyse des incidents ☒ Exercices de cybersécurité ☒ Protection des infrastructures essentielles de l'information Cybercriminalité ☒ Cadres juridiques/législation sur la cybercriminalité ☒ Application de la loi dans le cyberespace ☒ Formation en matière de cybercriminalité ☒ Prévention de la cybercriminalité Culture et compétences ☒ Sensibilisation à la cybersécurité ☒ Éducation et formation ☒ Perfectionnement de la main-d'œuvre Normes ☒ Normes internationales et/ou nationales
Types d'indicateurs	Le cadre comprend des indicateurs qualitatifs qui reposent sur deux niveaux: niveau stratégique et niveau opérationnel. Pour chaque objectif inclus dans le cadre d'autoévaluation, il existe une série d'indicateurs répartis entre les cinq niveaux de maturité. Chaque indicateur est fondé sur une question dichotomique (oui/non). L'indicateur peut être un élément nécessaire ou accessoire.
Combien d'indicateurs sont utilisés et comment sont-ils appliqués	Le modèle fournit un score reposant sur la valeur de deux paramètres: ***le niveau de maturité*** et ***le taux de couverture***. Chacun de ces paramètres peut être calculé à différents niveaux: i) par objectif, ii) par groupe d'objectifs ou iii) globalement. De plus, pour s'adapter aux spécificités des États Membres, tout en permettant une vue d'ensemble cohérente, le score est calculé à partir de deux échantillons différents au niveau des groupes et au niveau global: • **Scores généraux**: un échantillon complet couvrant tous les objectifs inclus dans le groupe ou dans le cadre général (de 1 à 17). • **Scores spécifiques**: un échantillon spécifique couvrant uniquement les objectifs sélectionnés par l'État Membre (correspondant généralement aux objectifs présents dans la SNCS du pays concerné) au sein du groupe ou du cadre général.

	Pour chaque groupe, un tableau présente l'ensemble des indicateurs sous forme de questions représentatives d'un niveau de maturité donné. Le questionnaire est l'instrument principal de l'autoévaluation. Pour chaque objectif, il y a deux séries d'indicateurs: • une série de questions génériques sur la maturité de la stratégie (9 questions génériques), notées de "a" à "c" pour chaque niveau de maturité, répétées pour chaque objectif; et • une série de questions sur la capacité de cybersécurité (319 questions sur la capacité de cybersécurité), numérotées de "1" à "10" pour chaque niveau de maturité, propres au domaine couvert par l'objectif.
Méthodologie – Quel type d'évaluation est utilisé?	**Niveaux de maturité**: Échelle de maturité à cinq niveaux **Attributs**: Basé sur quatre dimensions/groupes portant sur différents domaines pour renforcer les capacités en matière de cybersécurité **Méthode d'évaluation**: Auto-évaluation **Affichage des résultats**: Présentation des résultats à différents niveaux de granularité
Méthode de collecte de données primaires	• Anticiper les activités de coordination pour recueillir les données et les regrouper. • Identifier un organisme central chargé de réaliser l'autoévaluation à l'échelle nationale. • Utiliser l'exercice d'évaluation comme moyen de partager et de communiquer sur les sujets de cybersécurité. • utiliser la SNCS comme cadre pour sélectionner les objectifs soumis à l'évaluation. Lorsque la portée de la SNCS évolue, assurez-vous que l'interprétation du score reste cohérente avec l'évolution de la SNCS. Le cycle de vie de la SNCS s'étend sur plusieurs années.
Procédez-vous à la collecte de données secondaires?	Lorsque vous remplissez le questionnaire d'autoévaluation, gardez à l'esprit que l'objectif est d'apporter un appui aux États Membres concernant le renforcement des capacités de cybersécurité
Quels mécanismes adoptez-vous pour garantir l'exactitude des données recueillies?	L'État Membre/pays de l'UE qui procède à l'évaluation doit veiller à l'exactitude des données pour tirer parti des résultats du cadre.
Quels sont les principaux résultats de l'évaluation?	Les résultats de l'évaluation sont présentés à trois niveaux différents: au niveau des objectifs, au niveau des groupes et au niveau global. Le pays fait l'objet d'une évaluation et reçoit un résultat final générique qui prend en compte tous les objectifs de chaque groupe, et un résultat final spécifique qui ne tient compte que des objectifs retenus que le pays souhaite évaluer. En outre, le CECN fournit un taux de couverture. Le taux de couverture est calculé comme la **proportion** entre le **nombre total de questions** au sein de l'objectif et le **nombre de questions pour lesquelles la réponse est positive**. Le taux de couverture est exprimé en pourcentage.
Format de présentation des résultats de l'évaluation	Rapport Visualisation à partir de l'outil en ligne (travaux futurs de l'ENISA)

Les résultats de l'évaluation peuvent-ils être publiés?	Les résultats de l'évaluation ne sont publiés que si l'État Membre décide de le faire de sa propre initiative.
Comment accéder aux rapports précédents?	L'État Membre est en mesure de suivre sa progression dans le temps sur la base de réévaluations.
Quels sont les éléments qui attestent de résultats concrets?	Au total, près de 20 États Membres ont participé à l'élaboration du cadre et la quasi-totalité des États Membres ont participé à l'atelier de validation au cours duquel le cadre a été présenté et longuement examiné. Plus précisément, le cadre devrait permettre aux États Membres: • de procéder à une évaluation de leurs capacités nationales en matière de cybersécurité; • de mieux faire connaître le niveau de maturité du pays; • de recenser les domaines à améliorer; et • de renforcer les capacités en matière de cybersécurité.
Quels sont les avantages d'une évaluation?	Le CECN est un outil qui aide les États Membres: • à obtenir des informations utiles pour l'élaboration d'une stratégie à long terme (bonnes pratiques, lignes directrices par exemple); • à identifier les éléments manquants dans leur SNCS; • à renforcer leurs capacités en matière de cybersécurité; • à étayer le bien-fondé de l'action politique; • à acquérir de la crédibilité vis-à-vis du grand public et des partenaires internationaux; • à renforcer leur rayonnement et à améliorer leur image publique en tant qu'organisation transparente; • à anticiper les défis de demain; • à recenser les enseignements tirés et les bonnes pratiques; • à fournir une base de référence sur les capacités de cybersécurité à l'échelle de l'UE pour faciliter les discussions; et • à évaluer les capacités nationales en matière de cybersécurité.
Avez-vous recours à un processus de calcul de la pondération?	L'État Membre de l'UE peut afficher les résultats de l'évaluation en présentant le niveau de maturité des capacités de cybersécurité du pays, d'un groupe d'objectifs, voire d'un seul objectif. Tous les objectifs évalués ont la même pertinence dans le cadre d'évaluation. Ils ont donc la même importance. Il en va de même pour les indicateurs déployés dans ce cadre.
Adoptez-vous un mécanisme de notation et/ou de classement dans votre évaluation?	Le CECN vise à mesurer les capacités des États Membres en matière de cybersécurité au regard des 17 objectifs. Toutefois, l'État Membre peut choisir les objectifs qu'il souhaite évaluer et n'évaluer qu'un sous-ensemble des 17 objectifs.

Indice national de cybersécurité (NCSI)

e-Governance Academy (eGA)

L'*Indice national de cybersécurité* (NCSI) est un indice mondial qui permet de mesurer la capacité des pays de prévenir les cybermenaces et de gérer les cyberincidents. L'indice NCSI constitue également une base de données contenant des éléments de preuve accessibles au public et un outil de renforcement des capacités nationales en matière de cybersécurité.

L'indice NCSI porte essentiellement sur les aspects mesurables de la cybersécurité mise en œuvre par le gouvernement central:

1) **Législation en vigueur** – Textes de loi, règlementation, arrêtés, etc.
2) **Unités établies** – Organisations, départements, etc. existants.
3) **Cadres de coopération** – Comités, groupes de travail, etc.
4) **Résultats** – Politiques, exercices, technologies, sites web, programmes, etc.

Depuis 2016, 160 pays ont fait l'objet d'une évaluation à l'aide de l'indice NCSI. La collecte, l'examen et la publication des données constituent un processus continu dans le cadre de l'indice NCSI. L'indice NCSI ne donne pas lieu à la publication d'itérations annuelles. Lorsque de nouvelles données probantes sont fournies, elles sont évaluées; si elles sont fondées, le classement fait immédiatement l'objet des modifications nécessaires. La méthodologie NCSI a été élaborée en 2016 et mise à jour en 2018. Actuellement, elle est en cours de révision et la nouvelle itération sera publiée au plus tard en 2022.

Vue d'ensemble

Dernière date de mise à jour de l'outil	Les données fournies par les pays au titre de l'indice NCSI sont constamment mises à jour, ce qui signifie que l'indice lui-même est actualisé en permanence.
Quel est le nom de l'outil d'évaluation?	Indice national de cybersécurité (NCSI)
Quel est le nom de l'organisation qui gère l'outil?	e-Governance Academy
Quels sont les responsables de la mise en œuvre des évaluations?	• e-Governance Academy • Entités et institutions s'occupant de la cybersécurité des pays classés
Veuillez fournir des liens vers l'outil et toute information supplémentaire	Portail Cybil: https://cybilportal.org/projects/national-cybersecurity-index/
Qui faut-il contacter pour discuter de l'organisation d'une évaluation?	Mme Epp Maaten: epp.maaten@ega.ee M. Radu Serrano: radu.serrano@ega.ee Mme Merle Maigre: merle.maigre@ega.ee Équipe chargée de l'indice NCSI: ncsi@ega.ee
Couverture géographique	Mondiale

Qui peut utiliser l'outil?	• Ministères/organismes nationaux • Organismes de cybersécurité/décideurs • Établissements universitaires • Experts en cybersécurité • Toute personne intéressée Pour collaborer à la collecte de données nationales pour l'indice NCSI, il suffit de contacter l'équipe chargée de l'indice NCSI.
Quels sont les thèmes ou les sujets abordés?	**1 Élaboration de la politique de cybersécurité:** 1.1 Unité des politiques en matière de cybersécurité 1.2 Cadre de coordination de la politique de cybersécurité 1.3 Stratégie de cybersécurité 1.4 Plan de mise en œuvre de la stratégie de cybersécurité **2 Analyse des cybermenaces et informations sur les cybermenaces:** 2.1 Unité d'analyse des cybermenaces 2.2 Des rapports publics sur les cybermenaces sont publiés chaque année 2.3 Site web sur la cybersécurité et la sécurité **3 Éducation et perfectionnement professionnel:** 3.1 Compétences en matière de cybersécurité dans l'enseignement primaire ou secondaire 3.2 Programme de cybersécurité (niveau licence) 3.3 Programme de cybersécurité (niveau master) 3.4 Programme de cybersécurité (niveau doctorat) 3.5 Association professionnelle de cybersécurité **4 Contribution à la cybersécurité dans le monde:** 4.1 Convention sur la cybercriminalité 4.2 Représentation dans les cadres de coopération internationale 4.3 Organisation internationale de cybersécurité accueillie par le pays 4.4 Renforcement des capacités de cybersécurité pour d'autres pays **5 Protection des services numériques:** 5.1 Responsabilité des fournisseurs de services numériques en matière de cybersécurité 5.2 Normes de cybersécurité pour le secteur public 5.3 Autorité de surveillance compétente **6 Protection des services essentiels:** 6.1 Les opérateurs de services essentiels sont identifiés 6.2 Exigences de cybersécurité pour les opérateurs de services essentiels 6.3 Autorité de surveillance compétente 6.4 Suivi régulier des mesures de sécurité **7 Identification électronique et services de confiance:** 7.1 Identifiant unique permanent 7.2 Exigences relatives aux cryptosystèmes 7.3 Identification électronique

	7.4 Signature électronique 7.5 Horodatage 7.6 Service d'envoi recommandé électronique 7.7 Autorité de surveillance compétente **8 Protection des données personnelles:** 8.1 Législation sur la protection des données personnelles 8.2 Autorité chargée de la protection des données personnelles **9 Intervention en cas de cyberincident:** 9.1 Unité d'urgence en cas de cyberincident 9.2 Responsabilité en matière d'établissement de rapports 9.3 Point de contact unique pour la coordination internationale **10 Gestion des cybercrises:** 10.1 Plan de gestion des cybercrises 10.2 Exercice de gestion des cybercrises au niveau national 10.3 Participation à des exercices internationaux de cybercrise 10.4 Appui opérationnel apporté par des bénévoles dans les cybercrises **11 Lutte contre la cybercriminalité:** 11.1 la cybercriminalité est sanctionnée pénalement 11.2 Unité de lutte contre la cybercriminalité 11.3 Unité de criminalistique numérique 11.4 Point de contact 24 heures sur 24 et 7 jours sur 7 pour la cybercriminalité internationale
	12 Cyberopérations militaires: 12.1 Unité chargée des cyberopérations 12.2 Exercice de cyberopérations 12.3 Participation à des cyberexercices internationaux
Quels sont les thèmes ou sujets traités par le GFCE?	Politiques générales et stratégie ☒ Stratégies ☒ Évaluations ☐ Mesures de renforcement de la confiance et normes ☒ Cyberdiplomatie ☐ Le droit international dans le cyberespace Gestion des incidents et protection des infrastructures essentielles de l'information ☒ Intervention en cas d'incident de sécurité informatique ☒ Examen et analyse des incidents ☒ Exercices de cybersécurité ☒ Protection des infrastructures essentielles de l'information Cybercriminalité ☒ Cadres juridiques/Droit de la cybercriminalité ☒ Application de la loi dans le cyberespace ☐ Formation en matière de cybercriminalité ☒ Prévention de la cybercriminalité

	Culture et compétences ☒ Sensibilisation à la cybersécurité ☒ Éducation et formation ☒ Perfectionnement de la main-d'œuvre Normes ☒ Normes internationales et nationales
Types d'indicateurs	La collecte de données concernant l'indice NCSI est qualitative et un système de valeurs est utilisé pour déterminer s'il existe un texte de loi, une unité spécialisée, un cadre de coopération officiel et/ou un résultat spécifique.
Combien d'indicateurs sont utilisés et comment sont-ils appliqués	Il existe un total de 46 indicateurs (qui se présentent sous la forme des thèmes et sujets susmentionnés). Les indicateurs eux-mêmes sont subdivisés en 12 capacités. Chaque indicateur a une valeur, qui indique l'importance relative de l'indicateur dans l'indice, et un critère, qui explique quel type de données peut être soumis comme élément de preuve. Pour obtenir une valeur positive pour un critère, des éléments de preuve doivent être fournis sous la forme de données. Si les données fournies répondent à tous les aspects du critère, elles seront acceptées comme éléments de preuve suffisants.
Méthodologie – Quel type d'évaluation est utilisé	L'évaluation de chaque pays est saisie et mise à jour dans l'indice NCSI au cas par cas. Une fois que l'évaluation d'un pays a été saisie/mise à jour, l'indice NCSI l'affiche dans un classement comparatif mondial.
Méthode de collecte de données primaires	• Informations provenant de sources libres • Documents et dossiers • Législation et autres documents officiels • Sites web officiels
Procédez-vous à la collecte de données secondaires?	Oui. L'indice NCSI n'est pas un indice statique, de sorte que les données sont recueillies en permanence tout au long de l'année. • Informations provenant de sources libres • Documents et dossiers • Législation et autres documents officiels • Sites web officiels
Quels mécanismes adoptez-vous pour garantir l'exactitude des données recueillies?	Tous les éléments de preuve doivent être des informations publiques et accessibles au public. Seules les données officielles peuvent être considérées comme des éléments de preuve. Les éléments de preuve/références acceptés sont les suivants: textes de loi, documents officiels et sites web officiels. Lorsque la collecte des données est terminée, les informations fournies sont examinées par au moins deux experts de l'indice NCSI. Après examen, l'ensemble des données est publié sur le site web du NCSI.
Quels sont les principaux résultats de l'évaluation?	• Informations mises à jour sur la page du pays (pour les pays existants figurant dans l'indice NCSI) • Pages consacrées à des pays (pour les pays qui n'ont pas encore été inclus dans l'indice NCSI) • Classement de l'indice NCSI (qui est actualisé chaque fois que la page d'un pays est mise à jour)

Format de présentation des résultats de l'évaluation	• Site web • Outil de visualisation (avec possibilité de comparer des ensembles de données passés ou actuels pour un seul pays ou entre pays) • Possibilité de télécharger une page consacrée à un pays au format PDF
Les résultats de l'évaluation peuvent-ils être publiés?	Oui, toujours.
Comment accéder aux rapports précédents?	Pour une page consacrée à un pays donné, l'indice NCSI indique la date à laquelle les informations sur le pays ont été mises à jour. En principe, la page consacrée au pays présente les dernières informations disponibles. Le visiteur du site peut consulter les informations d'une mise à jour précédente en choisissant une date de mise à jour donnée dans un menu déroulant intitulé "Choisissez une version".
Quels sont les éléments qui attestent de résultats concrets?	• La participation croissante des pays à l'indice NCSI témoigne de l'intérêt sans cesse grandissant que suscite cet indice. Différents pays ont demandé des évaluations individuelles distinctes détaillées sur la base de l'indice NCSI, afin de déterminer l'état actuel de la cybersécurité au niveau national et de l'améliorer. • Des chercheurs universitaires ont eu recours à l'outil pour examiner une ou plusieurs études de cas.
Quels sont les avantages d'une évaluation?	Les pays peuvent déterminer leur niveau de préparation en matière de prévention des cybermenaces. L'indice NCSI, qui permet de comparer les données entre les pays et de scinder les notes en indicateurs, favorise une approche transnationale de la cybersécurité fondée sur la participation, dans le cadre de laquelle les bonnes pratiques sont échangées entre plusieurs pays.
Avez-vous recours à un processus de calcul de la pondération?	Non.
Adoptez-vous un mécanisme de notation et/ou de classement dans votre évaluation?	Oui – pour les indicateurs, pour la note NCSI (pays), pour le niveau de développement numérique (DDL) et pour la différence (entre la note NCSI et le DDL). • Chaque indicateur a une valeur, qui indique l'importance relative de l'indicateur dans l'indice. Les valeurs sont attribuées par le groupe d'experts en fonction des considérations suivantes: 1 point – Texte de loi régissant un domaine donné 2-3 points – Unité spécialisée 2 points – Cadre officiel de coopération 1-3 points – Résultat/produit. • La note NCSI indique le pourcentage obtenu par le pays par rapport à la valeur maximale des indicateurs. La note maximale NCSI est toujours 100 (100%), que des indicateurs soient ou non ajoutés ou supprimés. • Outre la note NCSI, le tableau de l'indice indique également le niveau de développement numérique (DDL). Le DDL est calculé en fonction de l'indice de développement des TIC (IDI) et de l'indice de préparation des réseaux (NRI). Le DDL est le pourcentage moyen que le pays a obtenu par rapport à la valeur maximale des deux indices.

	La différence correspond à la relation entre la note NCSI et le DDL. Un résultat positif indique que le développement de la cybersécurité du pays est en phase avec le développement numérique ou est bien avancé. Un résultat négatif signifie que la société numérique du pays est plus avancée que sa cybersécurité nationale.

Détails

À quelles questions essentielles l'outil peut-il contribuer à répondre?	• Quel est le niveau de préparation de mon pays face à une cyberattaque/cybermenace? • Quelles sont les lacunes de mon pays en termes de protection contre les cybermenaces? • Quelles sont les institutions compétentes pour accomplir cette tâche? • Comment pouvons-nous améliorer encore notre niveau de préparation face à l'évolution des cybermenaces? • Quelles bonnes pratiques en vigueur dans le monde pouvons-nous adapter et/ou mettre en œuvre?
À quel stade du cycle de vie de la stratégie l'évaluation doit-elle être effectuée?	L'évaluation (analyse par pays) peut être effectuée à n'importe quel stade du cycle de vie de la stratégie, afin que l'indice NCSI soit aussi à jour que possible. Toutefois, pour chaque pays, il est recommandé de procéder à cette évaluation lors de la ou des phases de "lancement", de "bilan et analyse" ou de "suivi et évaluation".
Comment l'évaluation contribue-t-elle à harmoniser d'autres activités?	L'indice NCSI permet de recenser les points forts et les points faibles du niveau de préparation d'un pays en ce qui concerne la prévention des cybermenaces, et indique les domaines dans lesquels le pays pourrait avoir besoin d'un appui supplémentaire pour renforcer ses capacités, ou ceux dans lesquels il pourrait apporter son appui à d'autres pays. Les pages consacrées au pays au titre de l'indice NCSI énumèrent également les bonnes pratiques nationales susceptibles d'être adaptées/mises en œuvre par d'autres pays, avec ou sans l'aide de bailleurs de fonds, d'organisations internationales, etc.
Quel est le rôle l'évaluation dans le processus de mise en correspondance du GFCE?	Étant donné que l'indice NCSI présente des informations accessibles au public, les bailleurs de fonds et les responsables de la mise en œuvre peuvent identifier les atouts et les faiblesses d'un pays et, partant, établir un dialogue avec ces pays pour leur proposer de renforcer leurs cybercapacités ou de mener des activités et d'apporter des améliorations analogues, en fonction des besoins.
Quelles études de cas ou références sont disponibles concernant les avantages de l'outil?	Situation Review: Safety and Security of Cyberspace and e-Democracy in the Eastern Partnership Countries (2017), e-Governance Academy
Quels sont les mécanismes propres à garantir l'indépendance, l'impartialité et la neutralité de vos résultats?	Les soumissions des pays contribuant à l'indice NCSI sont validées de manière indépendante par notre équipe.

Veuillez ajouter toute information supplémentaire	**Manuel:** • National Cyber Security in Practice (2020), e-Governance Academy **Podcast/article:** • What should governments do to secure their national cyberspace? (2020), e-Governance Academy • NCSI – How prepared is your country for a cyberattack? (2020), e-Governance Academy • What is cyber hygiene? (2020), e-Governance Academy **Article:** • 160 Countries in the NCSI: Barriers, Lessons Learnt, and Interesting Facts (2020), e-Governance Academy.

Vue d'ensemble des outils

	Lutter contre la cybercriminalité: Outil de renforcement des capacités	La cybermaturité dans la région Asie-Pacifique	CRI	CMM	CSDI	GCI	CECN	NCSI
Politiques générales et stratégie								
Stratégies	●	●	●	●	●	●	●	●
Évaluations	●	●	●	●	●	●	●	●
Mesures de renforcement de la confiance et normes		●	●	●		●	●	
Cyberdiplomatie		●	●	●		●	●	●
Le droit international dans le cyberespace	●	●	●					
Gestion des incidents et protection des infrastructures essentielles de l'information (CIIP)								
Intervention en cas d'incident de sécurité informatique	●	●	●	●	●	●	●	●
Examen et analyse des incidents			●	●		●	●	●
Exercices de cybersécurité			●	●		●	●	●
Protection des infrastructures essentielles de l'information	●	●	●	●	●	●	●	●
Cybercriminalité								
Cadres juridiques/ Droit de la cybercriminalité	●	●	●	●	●	●	●	●
Application de la loi dans le cyberespace	●	●	●	●	●	●	●	●
Formation en matière de cybercriminalité	●		●	●	●	●	●	
Prévention de la cybercriminalité	●		●	●	●	●	●	●

Culture et compétences								
Sensibilisation à la cybersécurité	●	●	●	●	●	●	●	●
Éducation et formation	●	●	●	●	●	●	●	●
Perfectionnement de la main-d'œuvre	●	●	●	●	●	●	●	●
Normes								
Normes internationales ou nationales			●	●	●	●	●	●