Programme de cybersécurité UIT-D

Indice mondial de cybersécurité – cinquième édition

Version définitive du questionnaire révisé

Table des matières

Cinquième édition de l'Indice mondial de cybersécurité – Historique et définitions

Questionnaire révisé relatif à la cinquième édition de l'Indice mondial de cybersécurité (GCIv5), y compris les mesures correspondantes associées aux précédentes éditions de l'Indice mondial de cybersécurité, définitions des principaux termes et logique sous-tendant les indicateurs et le cadre

Légende

Code-[NUMÉRO D'ÉDITION] – le code de la question/section est le numéro d'édition correspondant

Justification-[NUMÉRO D'ÉDITION] – Toute explication relative à la logique ou au contexte portant sur une question de l'édition correspondante

Indicateurs liés à l'Indice mondial de cybersécurité par pilier

Mesures juridiques

Justification-GCIv5: La législation constitue une mesure cruciale pour fournir un cadre harmonisé permettant aux différentes entités de s'appuyer sur des bases législatives et réglementaires communes, qu'il s'agisse de l'interdiction de certains actes délictueux ou d'obligations réglementaires minimales. Les cadres juridiques décrivent les rôles, les devoirs et les responsabilités des différentes parties prenantes. On peut considérer que la législation sur la cybersécurité pose cinq questions fondamentales: "1) Que sécurisons-nous? 2) Où sécurisons-nous et qui?; 3) Comment sécurisons-nous?; 4) Quand sécurisons-nous? et 5) Pourquoi sécurisons-nous?[1]". La sécurité des données est une partie importante de la cybersécurité, mais n'en est pas la seule composante, car la cybersécurité touche aussi les systèmes sur lesquels les données sont stockées et les réseaux sur lesquels les données sont transmises [2].

Les mesures juridiques permettent à un pays de mettre en place les mécanismes d'intervention essentiels en cas de violation: en enquêtant sur les infractions et en engageant des poursuites contre leurs auteurs, et en sanctionnant le fait de ne pas respecter la loi ou de l'enfreindre. Les lois protègent la sécurité générale, garantissent les droits des citoyens en cas d'atteinte par autrui et assurent une protection contre l'utilisation des technologies les plus récentes à des fins illicites. Un cadre législatif fixe les normes de comportement élémentaires applicables dans tous les domaines et à chacun, sur lesquelles peut s'appuyer la création de nouvelles capacités de cybersécurité. En dernière analyse, l'objectif est que les pays puissent mettre en place une législation adéquate afin de pouvoir harmoniser les pratiques au niveau supranational et disposer d'un cadre de mesures interopérables facilitant la lutte internationale contre la cybercriminalité.

Les critères de mesure du cadre juridique peuvent être l'existence et le nombre d'institutions et de cadres juridiques favorisant la cybersécurité et luttant contre la cybercriminalité. Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

1 Lois relatives à la cybercriminalité

Code-GCIv5: Juridique1

Justification-GCIv5: Les lois contre la cybercriminalité visent l'accès, l'ingérence et l'interception illicites (sans en avoir le droit) de matériel informatique, de systèmes et de données. La législation peut prendre les formes suivantes: droit matériel et/ou procédural, droit public et/ou privé, *common law*, droit jurisprudentiel, droit écrit, droit administratif ou autres formes de droit applicables.

---

1 https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022.

2 https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022.

1.1 Lois sur les comportements en ligne non autorisés

Code-GCIv5: Juridique1.1

Justification-GCIv5: Divers comportements en ligne peuvent nuire à la sécurité des activités en ligne et à la confiance qu'elles inspirent. Certains de ces comportements ont été cités dans des instruments internationaux tels que la Convention de 2011 du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest). Les dispositions de la législation en vigueur visant ces comportements peuvent comporter des directives claires sur la répression des infractions, permettre d'y voir clair sur le plan judiciaire et prévoir des compensations pour les personnes victimes de tels comportements.

1.1.1 Une législation sur l'accès illégal aux appareils, aux systèmes informatiques et aux données est-elle en vigueur dans votre pays?

Code-GCIv5: Juridique1.1.1

Justification-GCIv5: Divers comportements en ligne peuvent nuire à la sécurité des activités en ligne et à la confiance qu'elles inspirent. On peut notamment combattre ces comportements par l'intermédiaire de la législation. L'objectif de cette question est de déterminer si le pays répondant au questionnaire relatif à l'Indice GCI applique une législation visant expressément à combattre l'accès illégal aux dispositifs, aux systèmes informatiques et aux données, lequel peut porter atteinte à la vie privée, à la propriété ou à la dignité de la personne, entre autres préjudices ou dommages. Un point entier ne peut être attribué s'il s'agit de lois dont l'adoption est prévue, de projets de loi ou de lois qui ne sont pas actuellement en vigueur.

1.1.2 Une législation sur les interventions illicites sur des dispositifs, des données ou des systèmes informatiques (par introduction, altération ou suppression) est-elle en vigueur dans votre pays?

Code-GCIv5: Juridique1.1.2

Justification-GCIv5: Divers comportements en ligne peuvent nuire à la sécurité des activités en ligne et à la confiance qu'elles inspirent. On peut notamment combattre ces comportements par l'intermédiaire de la législation. L'objectif de cette question est de déterminer si le pays répondant au questionnaire relatif au GCI s'est doté d'une législation visant expressément à combattre les interventions illicites sur des dispositifs, des données ou des systèmes informatiques (par introduction, altération ou suppression). Un point entier ne peut être attribué s'il s'agit de lois dont l'adoption est prévue, de projets de loi ou de lois qui ne sont pas actuellement en vigueur.

1.1.3 Une législation relative à l'interception illicite des dispositifs, des données et des systèmes informatiques est-elle en vigueur dans votre pays?

Code-GCIv5: Juridique1.1.3

Justification-GCIv5: Divers comportements en ligne peuvent nuire à la sécurité des activités en ligne et à la confiance qu'elles inspirent. On peut notamment combattre ces comportements par l'intermédiaire de la législation. L'objectif de cette question est de déterminer si le pays répondant au questionnaire relatif au GCI s'est doté d'une législation visant expressément à combattre l'interception illicite des dispositifs, des données et des systèmes informatiques. Un point entier ne peut être attribué s'il s'agit de lois dont l'adoption est prévue, de projets de loi ou de lois qui ne sont pas actuellement en vigueur.

1.1.4 Votre pays dispose-t-il d'une règle juridique de fond sur l'identité en ligne?

Code-GCIv5: Juridique1.1.4

Justification-GCIv5: Les personnes doivent pouvoir s'identifier en ligne par des moyens fiables et dignes de confiance pour accomplir un nombre croissant d'activités en ligne. Qu'elles soient consacrées aux activités en ligne ou fassent partie d'autres lois portant sur l'identité, notamment, les lois contribuent à établir le fondement juridique de l'utilisation et de la gestion de l'identité en ligne, ainsi que des comportements en la matière.

1.2 Votre pays applique-t-il une législation relative à la falsification informatique (piratage/atteinte aux droits d'auteur)?

Code-GCIv5: Juridique1.2

Justification-GCIv5: Dans l'écosystème numérique, la confiance est fondamentale. La falsification informatique porte atteinte à cette confiance. Elle englobe la saisie, la modification, l'effacement ou la suppression de données informatiques délibérés et en l'absence de droit, produisant des données non authentiques avec l'intention qu'elles soient prises en compte ou utilisées à des fins juridiques comme si elles étaient authentiques, que les données soient ou non directement lisibles et intelligibles[3]. C'est le cas, par exemple, si un auteur modifie un courrier électronique authentique émanant d'une institution financière puis envoie la version modifiée à un certain nombre de destinataires (pratique également appelée "hameçonnage"). Dans certaines approches nationales, les données informatiques originales doivent se rapporter à des documents destinés à créer des obligations juridiques contraignantes. Dans d'autres il est seulement exigé que l'auteur de l'infraction ait l'intention que la version modifiée découlant de son acte soit prise en compte ou suivie d'effet en ce qui concerne les obligations juridiques[4].

1.3 Lois sur la sécurité en ligne

Code-GCIv5: Juridique1.3

Justification-GCIv5: Sachant que les comportements antisociaux affaiblissent les activités en ligne, car ils réduisent le sentiment de sécurité des utilisateurs et des communautés, la réglementation de certains de ces comportements est mesurée ci-après. Cette réglementation doit souvent associer judicieusement les droits de l'homme à d'autres valeurs notamment reconnues dans les Pactes internationaux relatifs aux droits de l'homme adoptés par l'ONU. Veuillez noter qu'il n'est pas nécessaire que les dispositions de ces lois indiquent explicitement qu'elles s'appliquent à des cas numériques/en ligne, mais que les organes judiciaires du pays considèrent que ces lois sont applicables aux cas numériques/en ligne.

---

[3] https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html.

[4] http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime_questionnaires/Member_State_questionnaire.xls.

1.3.1 Existe-t-il, dans votre pays, une législation en vigueur applicable aux contenus en ligne à caractère raciste ou xénophobe?

Code-GCIv5: Juridique1.3.1

Justification-GCIv5: Les contenus en ligne à caractère raciste ou xénophobe ont d'importants effets négatifs sur les communautés virtuelles, notamment en réduisant la diversité et en avivant les divisions, et peuvent porter préjudice à des individus. La législation en vigueur visant à combattre le racisme et la xénophobie devrait être claire, pour que les individus puissent facilement la comprendre et la respecter. Une législation ne portant pas expressément sur les technologies sera acceptée. La législation peut être acceptée s'il n'est pas précisé que ses dispositions s'appliquent aux contenus en ligne à caractère raciste ou xénophobes mais qu'il existe des mentions légales associées, des éléments fournis par des amici curiae, une jurisprudence, des poursuites antérieures ou d'autres documents appropriés démontrant l'applicabilité de cette législation aux situations en ligne.

1.3.2 Une législation applicable au harcèlement et aux abus en ligne visant à porter atteinte à la dignité et à l'intégrité des personnes est-elle en vigueur dans votre pays?

Code-GCIv5: Juridique1.3.2

Justification-GCIv5: Le harcèlement et les abus en ligne visant à porter atteinte à la dignité et à l'intégrité des personnes peuvent avoir d'importants effets négatifs sur leurs victimes, en particulier lorsqu'ils ont lieu en ligne. La législation en vigueur oriente les forces de l'ordre sur les cas dans lesquels des mesures doivent être prises et les autorités judiciaires sur la manière de traiter les affaires, fournit des orientations sur les compensations que peuvent recevoir les personnes touchées et, à terme, contribue à la confiance et à la sécurité en ligne. Une législation ne portant pas expressément sur les technologies sera acceptée. La législation peut être acceptée s'il n'est pas précisé que ses dispositions s'appliquent au harcèlement et abus en ligne ou aux contenus xénophobes mais qu'il existe des mentions légales associées, des éléments fournis par des amici curiae, une jurisprudence, des poursuites antérieures ou d'autres documents appropriés démontrant l'applicabilité de cette législation aux situations en ligne.

2 Réglementation relative à la cybersécurité

Code-GCIv5: Juridique2

Justification-GCIv2: On entend par réglementation relative à la cybersécurité les règles régissant la protection des données et la notification des infractions et les obligations en matière de certification/normalisation, la protection des données, la notification des infractions, les obligations relatives à la certification/normalisation dans le domaine de la cybersécurité, la mise en œuvre des mesures de cybersécurité, les obligations en matière d'audits de cybersécurité, la protection de la vie privée, la protection en ligne des enfants, les signatures numériques et les transactions électroniques, et la responsabilité des fournisseurs de services Internet. Les règlements sont souvent le cadre d'application des lois, dont ils précisent les modalités d'application. Les pays peuvent s'engager plus vigoureusement en faveur de la cybersécurité en adoptant des réglementations claires, cohérentes, applicables et adapté aux réalités actuelles.

2.1 Existe-t-il dans votre pays une ou des réglementation(s) relative(s) à la protection des données personnelles?

Code-GCIv5: Juridique2.1

***Justification-GCIv5*:** La réglementation des données personnelles renforce la gestion des données en soulignant les responsabilités des détenteurs des données et les droits des individus. Elle peut comporter des directives prévoyant que les détenteurs de données soient tenus responsables de la façon dont ils utilisent les données personnelles et garantissant que les organisations n'utilisent pas les données collectées de façon abusive.

2.2 Existe-t-il dans votre pays une ou des réglementation(s) relative(s) à la protection de la vie privée?

Code-GCIv5: Juridique2.2

Justification-GCIv5: Les réglementations sur la protection de la vie privée garantissent la protection des données personnelles, les organisations sont transparentes dans la façon dont elles utilisent les données et les individus ont le droit d'accéder à leurs données personnelles et de les corriger. La réglementation peut interdire aux organisations de vendre ou de partager des données personnelles sans le consentement de la personne concernée. La protection de la vie privée peut garantir aux individus la possibilité d'exercer un contrôle sur leurs données personnelles. L'utilisation abusive des données à caractère personnel peut contribuer à la cybercriminalité et à l'érosion de la confiance dans les technologies numériques.

2.3 Existe-t-il dans votre pays une ou des réglementation(s) relative(s) à la notification de violations de données/d'incidents s'appliquant aux intervenants du secteur privé?

Code-GCIv5: Juridique2.3

Justification-GCIv5: Une violation de données peut avoir des conséquences préjudiciables pour les particuliers, les entreprises et les gouvernements, en rendant possibles la fraude financière et le vol d'identité, avoir des répercussions malheureuses sur la réputation et aboutir à des sanctions contre les détenteurs des données. Une réglementation efficace peut notamment prévoir des notifications des violations de données et exiger des intervenants qu'ils préviennent dans les meilleurs délais les particuliers, les entreprises et les gouvernements des violations de données. De telles dispositions permettraient aux particuliers, aux entreprises et aux gouvernements de faire le nécessaire pour se protéger des dommages pouvant découler d'une violation de données. Les règlements sur la notification des violations de données peuvent encourager les bonnes pratiques en matière de gestion des données, exiger la notification dans les meilleurs délais et permettre aux personnes lésées de lancer une procédure de recours.

2.4 Dans votre pays, existe-t-il une réglementation (ou plus) traitant des obligations en matière d'audits de cybersécurité imposées à l'administration centrale, aux ministères ou à leurs sous-traitants?

Code-GCIv5: Juridique2.4

Justification-GCIv5: Les règlements concernant les obligations en matière d'audits de cybersécurité peuvent favoriser la détection des risques pour la cybersécurité et promouvoir de bonnes pratiques de cybersécurité en encourageant les organismes, les départements et les

sous-traitants à repérer et corriger les points faibles de leurs systèmes. En outre, ils peuvent encourager les organismes, les départements et les sous-traitants à adopter des pratiques optimales dans le domaine de la cybersécurité et à respecter les normes internationales.

2.5 Dans votre pays, existe-t-il une réglementation (ou plus) traitant des normes de cybersécurité applicables aux acteurs du secteur public national?

Code-GCIv5: Juridique2.5

Justification-GCIv5: Les acteurs du secteur public sont souvent la cible de cyberattaques. Il importe donc que ces acteurs utilisent de solides dispositifs de protection de la cybersécurité pour assurer leur protection et celle des citoyens. L'application d'un règlement relatif aux normes de cybersécurité applicables aux acteurs du secteur public national peut contribuer au renforcement de la protection de ces acteurs contre les cyberattaques et garantir qu'ils adoptent les bonnes pratiques dans le domaine de la cybersécurité. Ces normes sont notamment, sans toutefois s'y limiter, les suivantes: connaissance de la sécurité dans le nuage informatique (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Conseil de l'Europe), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), PRMIA (Professional Risk Managers International Association), PMP (Project Management Institute), ainsi que les conditions découlant des normes ISO/IEC 27001-Management de la sécurité de l'information, ISO 28000 – Management de la sûreté de la chaîne d'approvisionnement et ISA 62443-ISA 62443-Sécurité pour les systèmes d'automatisation et de contrôle industriels (Security for Industrial Automation and Control Systems), entre autres.

2.6 Dans votre pays, existe-t-il une réglementation (ou plus) traitant de l'utilisation de la signature numérique et des transactions électroniques dans les services et les applications de l'administration publique (administration publique en ligne)?

Code-GCIv5: Juridique2.6

Justification-GCIv5: Les États utilisent de plus en plus la signature numérique et les transactions électroniques dans leurs services et applications. Ce passage aux systèmes électroniques a des avantages, notamment une efficacité et une sécurité accrues. Toutefois, si une réglementation adéquate n'est pas adoptée, ces systèmes risquent de ne pas être utilisés efficacement ou de manière sécurisée.

Grâce à la réglementation, les citoyens n'ont pas à douter que leurs données soient sécurisées ou que les systèmes publics soient efficaces et fiables.

2.7 Dans votre pays, existe-t-il une réglementation (ou plus) traitant des communications non sollicitées, également connues sous le nom de spams?

Code-GCIv5: Juridique2.7

Justification-GCIv5: En réglementant les communications non sollicitées, les pays peuvent rendre les activités de tous en ligne plus sûres et plus agréables. Les règlements en la matière aident à protéger les citoyens des effets préjudiciables du spam et empêchent les spammeurs de profiter d'autrui.

2.8 Dans votre pays, existe-t-il une réglementation (ou plus) traitant de l'identification et de la protection des infrastructures essentielles de l'information au niveau national?

Code-GCIv5: Juridique2.8

Justification-GCIv5: En déterminant quelles sont les infrastructures nationales essentielles et en les protégeant, un pays peut maîtriser les risques liés à la cybersécurité. Une réglementation visant à protéger les infrastructures nationales essentielles aide un pays à planifier les mesures à prendre en réaction à une catastrophe ou une agression importantes, en lui permettant de réagir rapidement et efficacement à une catastrophe ou une attaque importantes. Un pays a aussi besoin de disposer d'un plan de relèvement à la suite d'importantes catastrophes ou attaques.

2.9 Dans votre pays, existe-t-il une réglementation (ou plus) traitant de la protection en ligne des enfants?

Code-GCIv5: Juridique2.9

Justification-GCIv5: Assurer la protection en ligne des enfants au moyen d'une réglementations adaptée permet aux organismes et acteurs concernés de prendre des dispositions et d'appliquer des prescriptions et des règles précisément définies pour maîtriser et combattre les infractions commises en ligne/la cybercriminalité visant des enfants et des jeunes. Il est indispensable que ces règles soient mises en œuvre par une grande variété de parties prenantes de tous les secteurs et toutes les catégories de la société, des opérateurs du secteur aux parties prenantes chargées de la répression des infractions et à la société civile, dont l'action collective devrait favoriser la réalisation d'un environnement numérique sûr et sécurisé pour les enfants et les jeunes.

Mesures techniques

Justification-GCIv5: La technologie est le premier rempart contre les cybermenaces et les agents malveillants en ligne. En l'absence de mesures adéquates et de techniques et de capacités de détection des cyberattaques et de réaction, les pays et leurs entités respectives restent vulnérables face aux cybermenaces. L'arrivée des TIC et leur succès ne peuvent véritablement porter leurs fruits que dans un climat de confiance et de sécurité. Il faut donc que les pays soient en mesure d'élaborer des stratégies visant à mettre en place des critères de sécurité et des mécanismes d'accréditation minimaux acceptés pour les applications et les systèmes logiciels. Ces efforts doivent s'accompagner de la création d'une entité nationale principalement chargée du traitement des incidents informatiques au niveau national avec, au strict minimum, un organisme gouvernemental responsable et un cadre national d'accompagnement fournissant des moyens de surveillance, d'alerte et de réaction.

Les critères d'évaluation des mesures techniques peuvent être l'existence et le nombre d'institutions et de cadres techniques en rapport avec la cybersécurité approuvés ou créés par l'État. Le sous-groupe est composé des indicateurs de performance suivants:

1 Équipes CERT/CIRT/CSIRT ou SOC nationaux

Code-GCIv5: Tech1

Justification-GCIv5: Des mécanismes et des structures institutionnelles efficaces au niveau national sont nécessaires pour détecter, prévenir, réagir et atténuer les cybermenaces et les incidents. Les équipes d'intervention en cas d'incident informatique (CIRT), ainsi que les équipes de réponse aux incidents de sécurité informatique (CSIRTS), les équipes d'intervention en cas d'urgence informatique (CERT) et les centres d'opérations de sécurité (SOC)[5] sont responsables de la protection et de la détection des incidents de cybersécurité et de la réponse à ces incidents, et peuvent améliorer la capacité d'un pays à gérer ces incidents. Les CIRT ou les SOC peuvent: servir à construire une base de connaissances qui renforcera la mise en œuvre par le pays d'une stratégie nationale de cybersécurité, ainsi que d'une approche pour la protection des infrastructures d'information critiques; encourager la création d'une culture et d'un écosystème nationaux de cybersécurité, ainsi que les initiatives de sensibilisation connexes; contribuer au développement de plates-formes nationales connexes de cybersécurité, telles que les services d'administration en ligne, les cadres nationaux de gestion de l'identité et de l'accès; et permettre au pays de développer et d'améliorer ses capacités de coordination et de réponse aux incidents.

1.1 Existe-t-il, dans votre pays, une équipe CIRT/CSIRT/CERT ou des SOC pleinement opérationnels au niveau national ou gouvernemental?

Code-GCIv5: Tech1.1

Justification-GCIv5: L'équipe d'intervention en cas d'incident informatique (CIRT), ainsi que l'équipe de réponse aux incidents de sécurité informatique (CSIRTS), l'équipe d'intervention en cas d'urgence informatique (CERT) et les centres d'opérations de sécurité (SOC) sont responsables de la protection et de la détection des incidents de cybersécurité et de la réponse à ces incidents. Une équipe CIRT/CSIRT/CERT et un centre SOC sont considérés comme pleinement opérationnels si les conditions suivantes sont remplies:

---

[5] https://ieeexplore.ieee.org/document/9296846.

- Structure organisationnelle définie et approuvée.
- Personnel formé et qualifié.
- Installations sécurisées mises en place (les mesures nécessaires sont prises pour protéger les installations des menaces physiques et environnementales).
- Processus et procédures détaillés élaborés et mis en œuvre pour ses activités.
- Adoption et mise en œuvre de la technologie requise pour ses activités.
- Processus mis en œuvre pour permettre les interactions avec les principaux intervenants et partenaires.
- Prestation des services à ses clients de manière efficace et efficiente.

Les étapes initiales de la mise en place d'une équipe CIRT sont notamment l'évaluation (mesurer l'état de préparation en prévision de la création de l'équipe CIRT et préparer les parties prenantes à assurer la participation nécessaire), la conception (préparer le dossier technique détaillé sur l'équipe CIRT) et le processus d'établissement (mise en place de l'infrastructure, des relations avec les parties prenantes et la clientèle, établissement de processus de mandat, mise en place des services, lancement des opérations et demande d'adhésion à une association internationale).

1.2 Activités des équipes CIRT/CSIRT/CERT ou des centres SOC nationaux

Code-GCIv5: Tech1.2

Justification-GCIv5: Les équipes d'intervention en cas d'incident informatique (CIRT), les équipes de réponse aux incidents de sécurité informatique (CSIRTS), les équipes d'intervention en cas d'urgence informatique (CERT) et les centres d'opérations de sécurité (SOC) sont responsables de la protection et de la détection des incidents de cybersécurité et de la réponse à ces incidents. Ils jouent un rôle central dans le signalement de ces incidents. En outre, ils fournissent des informations et une assistance technique qui aident les organisations à prévenir et atténuer les incidents de sécurité informatique et réagir à ces incidents. Une équipe CIRT ou un centre SOC nationaux réalisent aussi des travaux de recherche sur les problèmes de cybersécurité et élaborent des documents, dont des directives, sur les bonnes pratiques en cas d'incident de sécurité informatique.

1.2.1 L'équipe CIRT/CSIRT/CERT ou le centre SOC nationaux ou gouvernementaux de votre pays élaborent-ils et mettent-ils en œuvre des activités de sensibilisation à la cybersécurité?

Code-GCIv5: Tech1.2.1

Justification-GCIv5: Les CIRT ou SOC nationaux peuvent jouer un rôle important en menant des campagnes de sensibilisation à la cybersécurité. En tant qu'organes centraux de coordination, ils peuvent être davantage mis en avant dans le traitement des cybermenaces actuelles et émergentes, des défis en matière de cybersécurité, des vulnérabilités, ainsi que dans l'analyse des grandes tendances dans le domaine de la cybersécurité, la réalisation de progrès technologiques en matière de cybersécurité et l'établissement de bonnes pratiques en matière de détection des menaces informatiques et de réaction face à ces menaces. Pour renforcer la culture de la cybersécurité et promouvoir la connaissance des mesures de cybersécurité, ainsi que des bonnes pratiques et des comportements à adopter, les équipes CIRT/CSIRT/CERT ou les centres SOC devraient concevoir, exécuter ou coordonner des initiatives et des activités de sensibilisation à la cybersécurité adaptées aux différentes parties prenantes et fondées sur les informations recueillies sur l'évolution des menaces, les grandes tendances en matière de cybersécurité et les bonnes pratiques.

1.2.2 Les équipes CIRT/CSIRT/CERT ou le centre SOC nationaux ou gouvernementaux de votre pays organisent-ils régulièrement des exercices de cybersécurité (cyberexercices)?

Code-GCIv5: Tech1.2.2

Justification-GCIv5: Les exercices de cybersécurité sont des activités planifiées, au cours desquelles une organisation simule une cyberperturbation afin de renforcer ou de tester ses capacités de prévention, de détection, d'atténuation ou de traitement des perturbations, ou de rétablissement après une perturbation. Menés régulièrement et en association avec les parties prenantes, ces exercices constituent une mesure anticipative d'amélioration de la préparation et de la résilience en matière de cybersécurité. Les équipes CIRT/CSIRT/CERT ou les centres SOC devraient périodiquement concevoir et mener des exercices de gestion des incidents/crises informatiques, avec la participation de toute entité publique ou privée concernée du pays, afin de tester leurs capacités de réaction aux incidents.

1.2.3 Les équipes CIRT/CSIRT/CERT ou le centre SOC nationaux ou gouvernementaux de votre pays émettent-ils des mises en garde de cybersécurité publiques?

Code-GCIv5: Tech1.2.3

Justification-GCIv5: Les mises en garde de cybersécurité publiques permettent de tenir les organismes et les ministères informés des menaces potentielles à la cybersécurité et de prendre des précautions en conséquence. De plus, ces mises en garde peuvent contribuer à la mise en œuvre de réponses coordonnées aux menaces pesant sur la cybersécurité.

1.3 L'équipe CIRT/CSIRT/CERT et le centre SOC nationaux ou gouvernementaux sont-ils membres de FIRST et/ou figurent-ils sur la liste TF-CSIRT?

Code-GCIv5: Tech1.3

Justification-GCIv5: Les équipes CIRT et les centres SOC nationaux rattachés à FIRST bénéficient de l'apport d'un réseau mondial d'équipes CIRT, d'activités de formations et de ressources, des compétences du personnel de FIRST et de possibilités de collaborer et de partager des bonnes pratiques. Les conditions d'admission à FIRST supposent une participation active des pays. L'état actuel de de la liste TF-CSIRT sera pris en compte aux fins de cette question.

1.4 L'équipe CIRT/CSIRT/CERT et le centre SOC nationaux ou gouvernementaux cités dans la question 1.3 sont-ils membres d'une équipe CIRT régionale (telle que APCERT, PACSON, AFRICA CERT, ENSIA, OCI ou OEA)?

Code-GCIv5: Tech1.4

Justification-GCIv5: L'appartenance à une équipe CIRT régionale désigne toute relation officielle ou régulière avec tout autre groupe régional CIRT. L'appartenance à une équipe CIRT ou CERT régionale présente de nombreux avantages, dont la possibilité d'échanger des connaissances et des données d'expérience, ces équipes peuvent souvent partager des connaissances et des expériences liées à un contexte national.

2 Équipes CERT/CIRT/CSIRT ou centres SOC sectoriels

Code-GCIv5: Tech2

Justification-GCIv5: Une équipe CERT/CIRT/CSIRT ou un centre SOC sectoriels sont au service de clients travaillant dans des secteurs donnés, comme le secteur financier, le monde universitaire,

l'énergie, la santé, les télécommunications, les services publics ou les infrastructures critiques. Une équipe CIRT ou un centre SOC sectoriels travaille pour ses clients en utilisant des renseignements et des services se rapportant aux menaces qui sont spécialisés et adaptés à ses besoins particuliers. Un pays peut avoir la même équipe CIRT ou le même centre SOC sectoriels qu'un autre pays, car une équipe CIRT ou un centre SOC sectoriels travaillent pour des clients évoluant dans un secteur donné et leurs activités se déroulent dans plusieurs pays. Aux fins du présent indicateur, les équipes CIRT militaires ne sont pas acceptées.

2.1 Existe-t-il, dans votre pays, une équipe CERT/CIRT/CSIRT ou un centre SOC sectoriels?

Code-GCIv5: Tech2.1

Justification-GCIv5: Une équipe CERT/CIRT/CSIRT ou un centre SOC sectoriels sont au service de clients travaillant dans des secteurs donnés, comme le secteur financier, le monde universitaire, l'énergie, la santé, les télécommunications, les services publics ou les infrastructures critiques. Une équipe CIRT ou un centre SOC sectoriels travaille pour ses clients en utilisant des renseignements et des services se rapportant aux menaces qui sont spécialisés et adaptés à ses besoins particuliers. Un pays peut avoir la même équipe CIRT ou le même SOC sectoriels qu'un autre pays, car une équipe CIRT ou un centre SOC sectoriels travaillent pour des clients évoluant dans un secteur donné et leurs activités se déroulent dans plusieurs pays. Aux fins du présent indicateur, les équipes CIRT militaires ne sont pas acceptées. Une équipe CERT/CIRT/CSIRT ou un centre SOC sectoriels sont considérés comme pleinement opérationnels si les conditions suivantes sont remplies:

- Structure organisationnelle définie et approuvée.
- Personnel formé et qualifié.
- Installations sécurisées mises en place (les mesures nécessaires sont prises pour protéger les installations des menaces physiques et environnementales).
- Processus et procédures détaillés élaborés et mis en œuvre pour ses activités.
- Adoption et mise en œuvre de la technologie requise pour ses activités.
- Processus mis en œuvre pour permettre les interactions avec les principaux intervenants et partenaires.
- Prestation des services à ses clients de manière efficace et efficiente.

La mise en place d'équipes CIRT sectorielles peut être partielle si certaines des activités suivantes ont été menées: évaluation (mesure de l'état de préparation en prévision de la création de l'équipe CIRT sectorielle et préparation des parties prenantes à assurer la participation nécessaire), conception (préparation du dossier technique détaillé sur l'équipe CIRT) et processus d'établissement (mise en place de l'infrastructure, des relations avec les parties prenantes et la clientèle, établissement de processus de mandat, mise en place des services, lancement des opérations et demande d'adhésion à une association internationale).

2.2 Activités des équipes CERT/CIRT/CSIRT et des centres SOC sectoriels

Code-GCIv5: Tech2.2

Justification-GCIv5: Les équipes d'intervention en cas d'incident informatique (CIRT), ainsi que les équipes de réponse aux incidents de sécurité informatique (CSIRTS), les équipes d'intervention en cas d'urgence informatique (CERT) sectorielles et les centre d'opérations de sécurité (SOC) sectoriels sont responsables de la protection et de la détection des incidents de cybersécurité et de la réponse à ces incidents.

L'équipe CIRT ou le centre SOC sectoriels jouent un rôle central dans le signalement des incidents de cybersécurité. En outre, ils fournissent des informations et une assistance technique qui aident les organisations du secteur à prévenir et atténuer les incidents de sécurité informatique et réagir à ces incidents. Une équipe CIRT ou un centre SOC sectoriels réalisent aussi des travaux de recherche sur les problèmes de cybersécurité et élaborent des documents, dont des directives, sur les bonnes pratiques en cas d'incident de sécurité informatique.

2.2.1 Les équipes CIRT, CSIRT et CERT sectorielles ou les centre SOC sectoriels élaborent-ils et mettent-ils en œuvre des activités de sensibilisation à la cybersécurité concernant un secteur?

Code-GCIv5: Tech2.2.1

Justification-GCIv5: Les CIRT ou les centres SOC sectoriels peuvent jouer un rôle important en menant des campagnes de sensibilisation à la cybersécurité adaptées à un secteur en particulier. En tant qu'organes centraux de coordination, ils connaissent les tendances du domaine de la cybersécurité qui présentent une importance pour les parties prenantes. En fonction des menaces globales et propres à un secteur, les équipes CIRT sectorielles peuvent aider à concevoir et exécuter des activités de sensibilisation adaptées aux groupes de parties prenantes de différents secteurs pour améliorer les comportements en matière de cybersécurité.

2.2.2 Les équipes CIRT, CSIRT et CERT sectorielles ou les centres SOC sectoriels participent-ils régulièrement à des exercices de cybersécurité (Cyberexercices)?

Code-GCIv5: Tech2.2.2

Justification-GCIv5: Les exercices de cybersécurité sont des activités planifiées, au cours desquelles une organisation simule une cyberperturbation afin de renforcer ou de tester ses capacités de prévention, de détection, d'atténuation ou de traitement des perturbations, ou de rétablissement après une perturbation. La participation de CIRT sectorielles à des exercices de cybersécurité nationaux représente une mesure anticipative d'amélioration des capacités globales en matière de cybersécurité.

2.2.3 Les équipes CIRT, CSIRT et CERT sectorielles ou les centres SOC sectoriels transmettent-ils à leurs clients des renseignements sur des incidents concernant des secteurs donnés?

Code-GCIv5: Tech2.2.3

Justification-GCIv5: La communication de renseignements pertinents sur les menaces pesant sur certains secteurs peut permettre aux opérateurs de ces secteurs de mieux connaître les menaces et les vulnérabilités qui présentent une importance dans leur secteur d'améliorer les délais et l'efficacité des interventions en cas d'incident. En outre, cela peut contribuer au renforcement de la coordination de la réponse de l'ensemble des services publics, du secteur privé et de la population aux incidents de cybersécurité.

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

Code-GCIv5: Tech3

Justification-GCIv5: Les cadres nationaux pour la mise en œuvre des normes de cybersécurité supposent l'existence d'un ou plusieurs cadres approuvés (ou entérinés) par le gouvernement concernant la certification et l'accréditation de professionnels sur la base de normes internationalement reconnues en matière de cybersécurité. Ces normes sont notamment, sans

toutefois s'y limiter, les suivantes: Connaissance de la sécurité dans le nuage informatique (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK et Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Conseil de l'Europe), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), PRMIA (Professional Risk Managers International Association), PMP (Project Management Institute), ainsi que les conditions découlant des normes ISO/IEC 27001-Management de la sécurité de l'information, ISO 28000 – Management de la sûreté de la chaîne d'approvisionnement et ISA 62443-ISA 62443-Sécurité pour les systèmes d'automatisation et de contrôle industriels (Security for Industrial Automation and Control Systems), entre autres.

3.1 Votre gouvernement dispose-t-il d'un cadre aux fins de la mise en œuvre/l'adoption de normes de cybersécurité nationalement ou internationalement reconnues?

Code-GCIv5: Tech3.1

Justification-GCIv5: Les cadres nationaux pour la mise en œuvre des normes de cybersécurité supposent l'existence d'un ou plusieurs cadres approuvés (ou entérinés) par le gouvernement concernant la certification et l'accréditation de professionnels sur la base de normes internationalement reconnues en matière de cybersécurité. Un cadre pourrait définir un plan ou une feuille de route pour la mise en œuvre/l'adoption de normes et préciser quelles parties prenantes seront amenées à participer, les processus qui seront utilisés pour les mises à jour futures et les autres méthodes qui guideront la mise en œuvre.

Ces normes sont notamment, sans toutefois s'y limiter, les suivantes: connaissance de la sécurité dans le nuage informatique (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Conseil de l'Europe), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), PRMIA (Professional Risk Managers International Association), PMP (Project Management Institute), ainsi que les conditions découlant des normes ISO/IEC 27001-Management de la sécurité de l'information, ISO 28000 – Management de la sûreté de la chaîne d'approvisionnement et ISA 62443-ISA 62443-Sécurité pour les systèmes d'automatisation et de contrôle industriels (Security for Industrial Automation and Control Systems), entre autres.

3.2 Les infrastructures critiques sont-elles prises en compte dans le cadre relatif à la mise en œuvre/l'adoption de normes de cybersécurité nationalement ou internationalement reconnues?

Code-GCIv5: Tech3.2

Justification-GCIv5: Pour améliorer la protection et la résilience des infrastructures critiques et les aider à réduire leurs vulnérabilités et à gérer efficacement les risques, il est essentiel que ces

infrastructures soient prises en compte dans tout cadre relatif à la mise en œuvre/l'adoption de normes de cybersécurité nationalement ou internationalement reconnues.

Mesures organisationnelles

Justification-GCIv5: Des mesures organisationnelles sont nécessaires à la bonne mise en œuvre du dispositif national de cybersécurité. Les objectifs stratégiques doivent être établis par le gouvernement et assortis d'un plan complet de mise en œuvre, d'exécution et de mesure. Des structures de gouvernance doivent être créées et habilitées à appliquer le dispositif de cybersécurité, à suivre cette application et à en évaluer les résultats. Sans un réseau organisationnel bien défini de partenaires, les efforts de l'industrie, de la société civile et du monde universitaire dans différents secteurs et industries deviennent disparates et disjoints, ce qui va à l'encontre des efforts visant à atteindre une harmonisation nationale en termes de développement des capacités de cybersécurité.

Les critères de mesure des structures organisationnelles peuvent être l'existence et le nombre d'institutions et de stratégies organisant le développement de la cybersécurité au niveau national. La création de structures organisationnelles efficaces est nécessaire pour promouvoir le développement de la cybersécurité, lutter contre la cybercriminalité et promouvoir le rôle des moyens de surveillance, d'alerte et de réaction afin d'assurer la coordination intrainstitutionnelle, intersectorielle et transfrontalière entre les initiatives nouvelles et existantes. Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

1 Stratégie nationale de cybersécurité

Code-GCIv5: Org1

Justification-GCIv5: Une stratégie nationale de cybersécurité crée un cadre d'allocation des ressources[6] consacrées à la définition des objectifs nationaux de cybersécurité et permet d'attribuer en priorité des ressources à la réalisation de ces objectifs, qui visent l'amélioration de la sécurité et de la résilience d'un pays[7]. Elle permet aussi au gouvernement de coopérer avec toutes les parties prenantes concernées au niveau national. En outre, une stratégie nationale de cybersécurité peut contribuer à promouvoir l'innovation et à protéger la vie privée et les libertés civiles. Une telle stratégie devrait définir clairement les objectifs nationaux en matière de cybersécurité et la structure d'encadrement de leur réalisation[8].

1.1 Existe-t-il, dans votre pays une stratégie ou une politique nationale de cybersécurité, qu'il s'agisse d'un document autonome ou d'une partie d'un autre document?

Code-GCIv5: Org1.1

Justification-GCIv5: Il ne fait aucun doute que la cybersécurité est un enjeu capital pour toutes les nations. Une stratégie nationale de cybersécurité crée un cadre pour l'affectation de ressources à la protection des infrastructures essentielles d'un pays. Elle permet également à l'État de collaborer avec le secteur privé pour repérer et atténuer les cybermenaces. En outre, une stratégie nationale de cybersécurité peut contribuer à promouvoir l'innovation et à protéger la vie privée et les libertés civiles.

---

6 https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained.

7 https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

8 https://ncsguide.org/the-guide/.

1.2 Priorités de la stratégie nationale de cybersécurité

Code-GCIv5: Org1.2

Justification-GCIv5: Une stratégie nationale comportant des priorités permet de mener une action concertée face aux cyberrisques. Comme chaque pays est confronté à des défis différents en matière de cybersécurité, se concentrer sur des domaines particuliers de la cybersécurité aide les pays à répartir les ressources selon les priorités et à assurer la coordination des interventions face aux cybermenaces. La plupart des guides relatifs à l'élaboration d'une stratégie nationale de cybersécurité peuvent privilégier différentes priorités, comme dans le cas du document intitulé "Élaboration d'une stratégie nationale de cybersécurité" [9]. Dans certaines stratégies, les domaines prioritaires peuvent aussi se référer à des "domaines d'action" [10]. Les Questions 1.2.1. à 1.2.4 comprennent les domaines prioritaires qui pourraient être traités dans le cadre de la stratégie nationale de cybersécurité d'un pays. Toutefois, les pays peuvent avoir d'autres domaines prioritaires.

1.2.1 La stratégie nationale de cybersécurité de votre pays prévoit-elle la protection des infrastructures critiques nationales?

Code-GCIv5: Org1.2.1

Justification-GCIv5: Les infrastructures critiques nationales vont du réseau électrique et des réseaux d'alimentation en eau aux réseaux de transport et aux institutions financières. Si l'une d'entre elles venait à s'effondrer, le pays sombrerait dans le chaos. C'est pourquoi il est si important qu'une stratégie nationale de cybersécurité comprenne un plan garantissant la bonne protection de ces infrastructures essentielles au maintien de l'ordre et de la sécurité publics, importantes pour l'économie d'un pays et d'une importance capitale pour la sûreté nationale.

1.2.2 La stratégie nationale de cybersécurité de votre pays intègre-t-elle des principes de gestion du cycle de vie en faisant régulièrement l'objet d'un suivi, d'évaluations et de mises à jour?

Code-GCIv5: Org1.2.3

Justification-GCIv5: La stratégie nationale de cybersécurité d'un pays devrait intégrer les principes de gestion du cycle de vie[11] et faire régulièrement l'objet d'un suivi, d'évaluations et de mises à jour, afin qu'elle reste efficace et pertinente. Cela permet de recenser les risques associés à une stratégie donnée et de s'y attaquer et, au besoin, de modifier la stratégie pour tenir compte de l'évolution du contexte. L'approche de gestion du cycle de vie permet également de faire participer tous les intervenants à l'élaboration et à la mise en œuvre de la stratégie, et de s'assurer que toutes les parties prenantes travaillent vers le même objectif. Enfin, appliquer les principes de gestion du cycle de vie permet de surveiller la mise en œuvre de la stratégie et d'évaluer les résultats obtenus. Le cas échéant, la trajectoire peut être rapidement corrigée pour que la stratégie conserve sa pertinence et son efficacité.

---

9 http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf.

10 https://ncsguide.org/the-guide/.

11 https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

1.2.3 La stratégie nationale de cybersécurité de votre pays prévoit-elle un mécanisme garantissant la consultation régulière des experts et des parties prenantes en cybersécurité?

Code-GCIv5: Org1.2.4

Justification-GCIv5: La situation dans le domaine de la cybersécurité étant en constante évolution, il importe de mettre en place un mécanisme garantissant des mises à jour régulières de la stratégie nationale de cybersécurité. Les experts en cybersécurité peuvent fournir de précieuses informations sur les dernières menaces en date, ainsi que sur les meilleures manières de les écarter. Les parties prenantes, notamment les entreprises et les citoyens, doivent également être consultées dans le cadre de l'application de la stratégie nationale de cybersécurité afin que les politiques appliquées soient plus efficaces. Elles peuvent formuler des observations sur le fonctionnement de la stratégie et proposer des améliorations. Le fait de consulter les experts et les parties prenantes permet d'adapter la stratégie nationale de cybersécurité aux besoins du pays.

1.2.4 Dans votre pays, un plan d'action ou une feuille de route ont-ils été définis aux fins de la mise en œuvre de la stratégie nationale de cybersécurité?

Code-GCIv5: Org1.2.5

Justification-GCIv5: Un plan d'action ou une feuille de route élaborés pour appuyer l'application d'une stratégie de cybersécurité sont des éléments essentiels de la protection de l'infrastructure numérique et des citoyens d'un pays. En l'absence de plan, il est difficile d'affecter les ressources et de mesurer les progrès, ce qui peut nuire à l'efficacité et provoquer des disparités dans l'application. Un plan d'action ou une feuille de route bien définis peuvent aider à informer tous les intervenants de leurs rôles et responsabilités respectives dans l'application de la stratégie, et contribuer à l'élaboration d'un plan réalisable et réaliste. Ils peuvent également faciliter le suivi et l'évaluation des effets de la stratégie au fil du temps, ainsi que les ajustements nécessaires.

2 Organisme responsable

Code-GCIv5: Org2

Justification-GCIv5: On entend par "organisme responsable" une autorité compétente chargée de gérer la cybersécurité. Cette autorité devrait être un chef de file (qu'il s'agisse d'une personne ou d'une entité), disposer de responsabilités élevées et être solidement implantée au plus haut niveau de l'État afin de pouvoir formuler des orientations, coordonner l'action menée et surveiller la mise en œuvre des activités et des programmes de cybersécurité. L'autorité nationale compétente devrait aussi être une entité de gestion, qui définit et explicite les rôles, les responsabilités, les processus, les droits de décision et les tâches requises, afin que le dispositif de cybersécurité fonctionne efficacement.

2.1 Existe-t-il, dans votre pays, un organisme ou un ministère responsable de la cybersécurité au niveau national?

Code-GCIv5: Org2.1

Justification-GCIv5: Un organisme national ou un ministère responsable de la cybersécurité au niveau national peut favoriser une gestion cohérente des menaces à la cybersécurité et l'adoption à titre anticipatif de mesures de cybersécurité. Cet organisme ou ce ministère devraient associer leur action à celle menée par d'autres administrations, le secteur privé, la société civile et d'autres

acteurs concernés aux fins de l'élaboration et de l'application d'une stratégie nationale de cybersécurité.

2.2 Dans votre pays, existe-t-il un organisme ou un ministère responsable de la cybersécurité dans le cadre de la protection des infrastructures critiques nationales?

Code-GCIv5: Org2.2

Justification-GCIv5: Un organisme ou un ministère responsable des infrastructures critiques à l'échelle nationale contribue à la résilience et à la poursuite des opérations. Les infrastructures critiques peuvent comprendre des services essentiels comme l'eau, l'électricité et les télécommunications, qui sont indispensables au fonctionnement de la société. Un organisme national ou un ministère responsable des infrastructures critiques peut aider à prévenir ou à atténuer ces perturbations en travaillant avec les parties prenantes concernées.

2.3 Dans votre pays, existe-t-il un organisme, un ministère, un groupe de travail ou un autre organe chargé de superviser le renforcement des capacités nationales en matière de cybersécurité?

Code-GCIv5: Org2.3

Justification-GCIv5: Une démarche coordonnée et globale du renforcement des compétences et des capacités nécessaires dans le domaine de la cybersécurité peut réduire la probabilité d'incidents de cybersécurité et améliorer la résilience. La cybersécurité est une question multidimensionnelle qui nécessite la coordination et la coopération de nombreux organismes gouvernementaux et entités du secteur privé.

2.4 Dans votre pays, la coordination des initiatives et des activités de protection en ligne des enfants relève-t-elle de la responsabilité d'un organisme, ministère, groupe de travail ou organe?

Code-GCIv5: Org2.5

Justification-GCIv5: La coordination de l'action des parties prenantes et des groupes cibles, et la supervision des activités contribuent beaucoup à la complémentarité des interventions portant sur la protection en ligne des enfants. La responsabilité de la coordination, au niveau national, des initiatives et activités de protection en ligne des enfants peut soit être confiée à un organisme autonome, à un ministère, à un groupe de travail ou à un autre organe, soit faire partie d'un ensemble de responsabilités plus large confiées l'un de ces intervenants.

3 Indicateurs relatifs à la cybersécurité

Code-GCIv5: Org3

Justification-GCIv5: Les indicateurs relatifs à la cybersécurité comprennent tout exercice d'analyse comparative ou référentiel national ou sectoriel officiellement reconnu, utilisé pour mesurer le développement de la cybersécurité, les stratégies d'évaluation des risques, les audits de

cybersécurité et d'autres outils et activités, afin de noter ou évaluer la performance découlant d'améliorations à venir. À titre d'exemple, la norme ISO/IEC 27004[12] porte sur les mesures relatives au management de la sécurité de l'information.

3.1 Des audits de cybersécurité sont-ils menés au niveau national?

Code-GCIv5: Org3.1

Justification-GCIv5: Les audits de cybersécurité peuvent être menés au niveau national en raison de problèmes de sécurité ou conformément à des dispositions règlementaires ou à d'autres documents d'orientation. S'il existe une réglementation relative aux audits de cybersécurité, il faut mener efficacement les audits de la cybersécurité au niveau national. Les vérifications réalisées à ce titre peuvent donner lieu à l'élaboration de rapports d'audit, de résumés, d'exposés, de notes de service ou d'autres documents comparables.

Un audit de cybersécurité donne lieu au recensement des vulnérabilités potentielles. Une fois qu'elles ont été repérées, ces vulnérabilités peuvent être évaluées et classées par ordre de priorité afin de déterminer quel niveau de risque elles représentent pour l'organisation. Tout une gamme d'outils peut être utilisée pour évaluer ces vulnérabilités, y compris les scanners de vulnérabilités, les tests d'intrusion et les exercices d'"équipe rouge". Chacun de ces outils comportant des lacunes et des points forts particuliers, il importe de choisir un outil adapté à l'objectif visé. Une fois que les vulnérabilités sont connues, déterminer le niveau de risque qu'elles posent pour l'organisation est une étape importante.

3.2 Existe-t-il des méthodes ou des outils de mesure qui permettent d'évaluer les risques de cybersécurité au niveau national?

Code-GCIv5: Org3.2

Justification-GCIv5: Les outils de mesure qui permettent d'évaluer les risques de cybersécurité au niveau national changent en fonction des pays et devraient être adaptés aux menaces et aux capacités, ainsi qu'aux problèmes propres à chaque pays. L'adaptation à la situation nationale peut être assurée en utilisant différentes méthodes, dont celles fondées sur les facteurs d'impact, les facteurs de probabilité et les valeurs des actifs. L'utilisation de ces mesures permet de déterminer le niveau et la gravité du risque posé par chaque vulnérabilité et de prendre les mesures correctives requises[13]. La norme ISO/IEC 27004[14] décrit des techniques de sécurité qui peuvent être utilisées pour surveiller, mesurer, analyser et évaluer les risques liés à la cybersécurité.

---

[12] https://www.iso.org/standard/64120.html.

[13] https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

[14] https://www.iso.org/fr/standard/64120.html.

3.3 Existe-t-il des méthodes de mesure permettant d'évaluer le niveau de développement de la cybersécurité au niveau national à l'aide d'outils tels que le Modèle de maturité des capacités en matière de cybersécurité, l'Indice de préparation à la lutte contre la cybercriminalité, ou de tout autre outil d'évaluation adéquat?

Code-GCIv5: Org3.3

Justification-GCIv5: L'évaluation du niveau de développement de la cybersécurité peut permettre aux pays de déterminer le degré de maturité et de fiabilité de leurs infrastructures de cybersécurité; quant aux mesures d'évaluation à proprement parler, elles peuvent varier d'un pays à l'autre. Parmi les outils couramment utilisés pour évaluer le niveau de développement de la cybersécurité à l'échelle nationale, figure le Modèle de maturité des capacités en matière de cybersécurité[15], l'Indice de préparation à la lutte contre la cybercriminalité[16] et toute autre mesure effectuée par un pays. Aux fins de la présente question, la participation des pays à l'Indice mondial de cybersécurité élaboré par l'UIT ne figure pas parmi les outils d'évaluation.

4 Stratégies et initiatives de protection en ligne des enfants

Code-GCIv5: Org4

Justification-GCIv5: "Protection en ligne des enfants" est le terme général désignant les stratégies et initiatives conçues pour protéger les enfants contre les préjudices et de l'exploitation lorsqu'ils utilisent Internet. Il peut notamment s'agir de faire en sorte que les enfants utilisent des logiciels et des outils de filtrage adaptés à leur âge et d'apprendre aux parents et aux enfants à rester en la sécurité lorsqu'ils sont en ligne. Il existe différentes stratégies et initiatives de protection en ligne des enfants, en général spécialement adaptées aux besoins particuliers des enfants du pays cible.

4.1 Existe-t-il, dans votre pays, une stratégie nationale de protection en ligne des enfants associée aux initiatives actuelles en la matière?

Code-GCIv5: Org4.1

Justification-GCIv5: Il est recommandé, dans les Lignes directrices relatives à la protection en ligne des enfants, d'adopter une stratégie globale susceptible de protéger les enfants dans le cyberenvironnement qui soit exclusivement consacrée à cette question étant donné qu'elle devrait traiter de domaines tels que la santé, le bien-être et le développement des connaissances des enfants. Lorsqu'une stratégie de protection en ligne des enfants est intégrée à un autre dispositif, elle est rarement globale et souvent uniquement axée sur les abus sexuels sur mineurs ou la pédopornographie.

---

[15] https://gcscc.ox.ac.uk/cmm-2021-edition.

[16] https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

4.2 Des capacités et des mécanismes publics de signalement, quels qu'ils soient, ont-ils été mis en place dans votre pays, au niveau national, pour aider à protéger les enfants dans le cyberenvironnement?

Code-GCIv5: Org4.2

Justification-GCIv5: Les mécanismes de signalement mis à la disposition du grand public pour identifier, pister et assurer le suivi des problèmes auxquels sont exposés les enfants dans le cyberenvironnement permettent aux particuliers de déterminer l'existence de tels problèmes et de les signaler. Ces mécanismes peuvent comporter des capacités techniques telles que l'avertissement de contenu. Les équipes CIRT et les autorités de police peuvent proposer des mécanismes de signalement. Idéalement, il faudrait que différents systèmes, tels que des services nationaux d'aide téléphonique et des portails en ligne donnant accès à des systèmes d'orientation et de soutien, soient disponibles.

Mesures relatives au renforcement des capacités

Justification-GCIv5: Le renforcement des capacités est intégré aux mesures juridiques, techniques et organisationnelles prévues au titre de l'Indice mondial de cybersécurité élaboré par l'UIT; c'est l'un des moteurs du développement numérique. Les programmes de renforcement des capacités visent à renforcer les compétences, les connaissances et la confiance au niveau local et, par ricochet, à combler le déficit de compétences et créer un écosystème technologique plus inclusif. En outre, la capacité de fournir des services numériques inclusifs dépend de plus en plus de l'existence d'une main-d'œuvre qualifiée. Les cadres de renforcement des capacités dans le cadre de la promotion de la cybersécurité peuvent comprendre des activités de sensibilisation et les critères de mesure peuvent être l'existence et le nombre de programmes de recherche et de développement, de programmes d'éducation et de formation, et de professionnels certifiés, ainsi que d'organismes publics.

1 Campagnes de sensibilisation du public à la cybersécurité

Code-GCIv5: Devcapacités1

Justification-GCIv5: Les campagnes de sensibilisation du public à la cybersécurité ont pour principal objectif l'adoption de comportements sécurisés en ligne. Afin d'obtenir une véritable évolution des comportements, ces campagnes doivent convaincre les gens que les informations présentées sont pertinentes, les aider à comprendre comment réagir et les persuader d'accepter de réagir en fonction d'autres priorités[17]. Les campagnes de sensibilisation se heurtent à de nombreux problèmes, en particulier parce qu'elles exigent des efforts et des compétences considérables et qu'"il est rare que la peur produise une évolution des comportements"[18]. Lorsqu'elles sont ciblées, les campagnes de sensibilisation permettent de moduler les interventions pour relever ces défis plus efficacement.

1.1 Votre gouvernement a-t-il élaboré des campagnes de sensibilisation du public ciblant spécifiquement les micro-entreprises et petites et moyennes entreprises?

Code-GCIv5: Devcapacités1.1

Justification-GCIv5: Les micro-entreprises et petites et moyennes entreprises sont un élément essentiel de l'économie d'un pays et doivent être conscientes des menaces à la cybersécurité susceptibles d'avoir un impact sur leurs entreprises. Elles doivent surmonter des difficultés particulières pour améliorer la cybersécurité, notamment l'insuffisance des ressources et de compétences techniques. Les interventions ciblées peuvent s'attaquer à ces problèmes spécifiques et être conçues en priorité pour maximiser leur apport aux micro-entreprises et petites et moyennes entreprises. Les campagnes de sensibilisation à la cybersécurité, en particulier celles qui s'adressent aux petites et moyennes entreprises, peuvent leur communiquer des informations sur les mesures à prendre pour se protéger contre les cyberattaques et pour réagir en cas d'attaque.

---

[17] Rogers, R.W. Attitude change and information integration in fear appeals. Psychological Reports, 56, (1985) 183–188
Witte, K. Message and conceptual confounds in fear appeals: The role of threat, fear and efficacy. The Southern Communication Journal, 58(2), (1993) 147-155.
https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8.

[18] https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8.

1.2 Votre gouvernement mène-t-il des campagnes de sensibilisation du public s'adressant particulièrement au secteur privé?

Code-GCIv5: Devcapacités1.2

Justification-GCIv5: Tout opérateur privé doit faire face à des problèmes de cybersécurité. Indépendamment des besoins particuliers des micro-entreprises et petites et moyennes entreprises, les campagnes de sensibilisation du public sur les risques de cybersécurité touchant le secteur privé peuvent contribuer à améliorer les comportements.

1.3 Votre gouvernement mène-t-il des campagnes de sensibilisation du public s'adressant expressément aux organismes publics aux niveaux local, municipal et national, ainsi qu'aux employés du secteur public?

Code-GCIv5: Devcapacités1.3

Justification-GCIv5: Les campagnes de sensibilisation à la cybersécurité présentent un intérêt pour les organismes publics. Elles sont spécialement conçues pour toucher les travailleurs du secteur public et fournissent des informations importantes sur la façon de protéger les données sensibles et les infrastructures critiques.

1.4 Votre gouvernement mène-t-il des campagnes de sensibilisation du public s'adressant spécialement à la société civile?

Code-GCIv5: Devcapacités1.4

Justification-GCIv5: Les organisations de la société civile peuvent être la cible de cyberattaques. Ces attaques peuvent prendre la forme de cyberharcèlement ou de vol de données ou d'informations financières. Il importe que les organisations de la société civile prennent conscience de ces risques et s'en protègent. Pour cela, elles doivent notamment assurer la formation de leur personnel et utiliser de mots de passe sûrs et des logiciels antivirus à jour. Les pays peuvent aider à mettre ces organisations, dont ils ne sauraient se passer, à l'abri des actes nuisibles en les informant des moyens de défendre en toute sécurité leur organisation et leur réseau, ainsi que les données des citoyens.

1.5 Votre gouvernement mène-t-il des campagnes de sensibilisation du public ciblant la population en général?

Code-GCIv5: Devcapacités1.5

Justification-GCIv5: La cybersécurité n'est pas utile qu'aux entreprises et aux gouvernements. Les citoyens sont les plus vulnérables face à la cybercriminalité mais sont souvent dépourvus des connaissances et outils nécessaires à leur protection. Les cybercriminels cherchent en permanence de nouveaux moyens de commettre des vols de données, d'argent ou d'identité. Ils atteignent leur objectif en piratant des systèmes informatiques, en volant des mots de passe ou en créant de faux sites web. Au niveau national, les États peuvent sensibiliser les citoyens à ce risque pour les protéger. Ils peuvent apprendre aux citoyens à se protéger en utilisant des mots de passe solides, à faire preuve de prudence lors de l'ouverture de courriels et à ne jamais fournir de renseignements personnels en ligne. Les citoyens doivent aussi pouvoir repérer les indices d'une tentative d'escroquerie ou d'hameçonnage. Les gouvernements devraient s'employer résolument à informer tous les citoyens des problèmes de cybersécurité et prier instamment chacun d'entre eux de prendre les mesures nécessaires pour se protéger en ligne.

1.6 Votre gouvernement mène-t-il des campagnes de sensibilisation du public spécialement adressées aux personnes âgées (vieillards)?

Code-GCIv5: Devcapacités1.6

Justification-GCIv5: Au fur et à mesure que notre population vieillit, le nombre de personnes âgées utilisant Internet et des appareils électroniques augmente. Malheureusement, elles constituent une cible de choix pour les cybercriminels. La vulnérabilité accrue des aînés face aux cybermenaces a plusieurs raisons: ils peuvent ne pas être suffisamment conscients des dangers liés à l'utilisation d'Internet, ne pas avoir les compétences techniques nécessaires pour se protéger, risquer davantage de tomber dans le piège d'escroqueries et moins enclins à signaler un délit informatique.

Pour cette raison, les gouvernements informent les personnes âgées des questions relatives à la cybersécurité afin qu'elles puissent rester en sécurité dans le cyberenvironnement et sachent protéger leurs renseignements personnels.

1.7 Votre gouvernement mène-t-il des campagnes de sensibilisation du public ciblant expressément les personnes ayant des besoins particuliers, notamment les personnes handicapées?

Code-GCIv5: Devcapacités1.7

Justification-GCIv5: La prise en compte du handicap remplaçant de plus en plus souvent le modèle médical par un autre fondé sur les droits humains, les capacités et la sécurité des personnes handicapées peuvent être renforcées grâce à l'élimination des obstacles sociétaux auxquels se heurtent les personnes ayant des besoins particuliers, notamment dans l'architecture, les moyens de communication, les comportements et les structures sociales[19]. Par ailleurs, la nécessité de mener des activités de sensibilisation et de formation à la cybersécurité expressément conçues pour les personnes handicapées a augmenté. Les personnes handicapées sont plus vulnérables aux cyberattaques pour un certain nombre de raisons, dont leur connaissance plus superficielle de la technologie, ainsi que le fait qu'elles dépendent de l'aide d'autrui et hésitent à demander de l'aide. Il est donc indispensable de leur dispenser une formation et de les sensibiliser, et les gouvernements doivent s'assurer que tous les membres de la société récoltent les avantages de l'action menée dans le domaine de la cybersécurité. La prise en compte des besoins de cette partie de la population dans les campagnes de sensibilisation du public a une forte incidence sur l'inclusivité et l'efficacité du développement des capacités en matière de cybersécurité.

1.8 Votre gouvernement mène-t-il des campagnes de sensibilisation du public s'adressant expressément aux parents, aux éducateurs et aux enfants dans le cadre des mesures de protection en ligne des enfants?

Code-GCIv5: Devcapacités1.8

Justification-GCIv5: L'État devrait encourager la conception de campagnes de sensibilisation du public s'adressant expressément aux parents et aux éducateurs pour qu'ils puissent enrichir leur connaissance des risques et des dangers auxquels les enfants et les jeunes sont exposés et renforcer leur capacité de surmonter les obstacles à la protection en ligne des enfants.

---

[19] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e777?rskey=sn89T4&result=201&prd=MPIL#.

1.9 Votre gouvernement mène-t-il expressément des campagnes de sensibilisation du public à l'intention des enfants dans le cadre de son action pour la protection en ligne des enfants?

Code-GCIv5: Devcapacités1.9

Justification-GCIv5: Étant donné qu'ils passent de plus en plus de temps en ligne, les enfants sont vulnérables. Ils sont particulièrement vulnérables face aux cybermenaces, car leur connaissance des dangers peut être insuffisante et ils peuvent avoir une connaissance et une expérience de la cybersécurité moins importantes que celles d'un adulte. Les gouvernements devraient encourager l'élaboration de campagnes de sensibilisation du public conçues pour les enfants afin d'aider ceux-ci à acquérir des connaissances sur les différents risques qui existent dans le cyberenvironnement et à mieux repérer et atténuer ces risques, et afin de promouvoir des comportements responsables en ligne.

2 Formation à l'intention des professionnels de la cybersécurité

Code-GCIv5: Devcapacités2

Justification-GCIv5: La formation professionnelle compétences peut contribuer à la constitution d'une main-d'œuvre compétente et adaptée aux réalités de la cybersécurité. Pour former une main-d'œuvre pouvant travailler dans la cybersécurité, il faut en permanence assurer son adaptation aux changements et évolutions qui interviennent dans ce domaine.

2.1 Votre gouvernement élabore-t-il ou finance-t-il des cours à l'intention des professionnels de la cybersécurité?

Code-GCIv5: Devcapacités2.1

Justification-GCIv5: De plus en plus d'entreprises transfèrent leurs activités en ligne et la demande de professionnels de la cybersécurité n'a jamais été aussi forte. Mais il arrive trop souvent que ces professionnels n'aient pas suivi la formation nécessaire pour pouvoir protéger leurs employeurs contre les cyberattaques. La formation en cybersécurité est importante pour plusieurs raisons, notamment parce qu'elle aide les professionnels de la cybersécurité à acquérir des bases solides dans ce domaine, leur montre comment mettre en pratique leurs connaissances, leur permet de rester informés des tendances et évolutions les plus récentes, et les aide à acquérir les compétences nécessaires pour sécuriser les réseaux et les données de leur organisation.

2.2 Existe-t-il, dans votre pays, des programmes d'accréditation des professionnels de la cybersécurité reconnus au niveau national ou international?

Code-GCIv5: Devcapacités2.2

Justification-GCIv5: Les programmes d'accréditation dans le domaine de la cybersécurité permettent de faire en sorte que le niveau exigé des professionnels de la cybersécurité soit élevé. Cela peut aider à améliorer la qualité globale des prestations des professionnels de la cybersécurité et à protéger les particuliers et les organisations d'éventuels préjudices. En outre, les pays peuvent développer la confiance entre les professionnels de la cybersécurité et leurs clients. S'il existe un programme d'accréditation universellement reconnu, il peut être plus facile à toutes les parties concernées d'accorder leur confiance aux professionnels avec lesquels elles travaillent au vu de leurs qualifications.

2.3 Programmes d'études/de formation sectoriels nationaux pour les professionnels dans le domaine de la cybersécurité

Code-GCIv5: Devcapacités2.3

Justification-GCIv5: Dans un pays, les professionnels de différents secteurs peuvent participer à des programmes/suivre des cours sur la cybersécurité qui traiteront des problèmes et des situations spécifiques que rencontrent ces professionnels dans leur travail et qui auront pour objectif de transmettre aux participants des compétences adaptées à leurs besoins.

2.3.1 Votre gouvernement élabore-t-il ou soutient-il des formations ou des programmes éducatifs portant sur la cybersécurité destinés aux organismes chargés de l'application de la loi à l'échelle nationale?

Code-GCIv5: Devcapacités2.3.1

Justification-GCIv5: Les membres des services de maintien de l'ordre, notamment les policiers et les agents des services de police, jouent un rôle essentiel dans la protection de notre pays contre les cyberattaques. Ils peuvent aider à repérer les cybercrimes et à enquêter sur la cybercriminalité, et aider des entreprises et d'autres entités à améliorer leur dispositif de cybersécurité. Il faut que ces services possèdent les connaissances et les outils nécessaires pour répondre à ces menaces de plus en plus importantes. Une formation sur la cybersécurité peut les aider à mieux comprendre les menaces les plus récentes, à reconnaître les activités malveillantes et à protéger leurs réseaux.

2.3.2 Votre gouvernement élabore-t-il ou soutient-il des formations ou des programmes éducatifs portant sur la cybersécurité destinés au personnel judiciaire au niveau national?

Code-GCIv5: Devcapacités2.3.2

Justification-GCIv5: Le personnel judiciaire de chaque pays joue un rôle essentiel en garantissant la sécurité et la sûreté de son pays et doivent disposer des connaissances et des outils nécessaires pour faire face aux menaces de cybersécurité. Au moment de la planification des formations nationales portant sur la cybersécurité, il faut prévoir une formation sur la cybersécurité à l'intention du personnel judiciaire et des autres professionnels du domaine juridique, et des formations professionnelles et techniques pouvant être organisées de manière récurrente à l'intention des juges, avocats, conseillers juridiques, magistrats, auxiliaires juridiques ainsi que de toute autre professionnel dans le domaine juridique ou dans le domaine de l'application de la loi.

2.3.3 Votre gouvernement élabore-t-il ou soutient-il des formations ou des programmes éducatifs portant sur la cybersécurité destinés aux micro-entreprises et petites et moyennes entreprises? [CETTE QUESTION NE SERA PAS NOTÉE]

Code-GCIv5: Devcapacités2.3.3

Justification-GCIv5: Les micro-entreprises et petites et moyennes entreprises ont besoin de formations en cybersécurité, car elles détiennent une grande quantité de données sensibles, qui peuvent être volées ou compromises en cas de cyberattaque. En outre, elles n'ont souvent pas conscience des risques découlant de l'utilisation de la technologie et n'ont pas nécessairement les outils ou les ressources nécessaires pour protéger leurs données. La formation en cybersécurité peut aider ces entreprises à comprendre les risques qu'entraîne l'utilisation de la technologie et les mesures à prendre pour protéger leurs données. Elle peut aussi les aider à repérer les activités

suspectes et à réagir en cas de cyberattaque. En fournissant aux micro-entreprises et petites et moyennes entreprises les outils et les connaissances dont elles ont besoin pour protéger leurs données, les États contribuent à protéger leur propre développement économique.

2.3.4 Votre gouvernement élabore-t-il ou soutient-il des formations ou des programmes éducatifs portant sur la cybersécurité destinés au secteur privé en général?

Code-GCIv5: Devcapacités2.3.4

Justification-GCIv5: Le secteur privé doit faire face à des cyberrisques dont la portée, l'ampleur et la complexité sont croissantes et qui ont une incidence sur les finances, la réputation et les biens des entreprises. La technologie n'étant qu'une composante de la cybersécurité, l'application de politiques et de programmes visant à modifier le comportement des personnes dans le secteur privé peut améliorer la résilience et réduire les cyberrisques.

2.3.5 Votre gouvernement élabore-t-il ou soutient-il des formations ou des programmes éducatifs portant sur la cybersécurité destinés aux membres du secteur public ou de l'administration en général?

Code-GCIv5: Devcapacités2.3.5

Justification-GCIv5: Le secteur public fournit des services essentiels aux citoyens et aux entreprises. Pour fournir des services en toute sécurité, les intervenants du secteur public doivent bien comprendre la cybersécurité et la manière de se protéger et de protéger les citoyens contre les menaces numériques. Il peut être utile aux représentants du secteur public et du gouvernement ne travaillant pas dans le système judiciaire ni dans les forces de l'ordre de suivre des cours et des formations en cybersécurité.

2.3.6 Votre gouvernement élabore-t-il ou soutient-il des formations ou des programmes éducatifs portant sur la cybersécurité destinés aux opérateurs des secteurs des finances, de la santé, des télécommunications, des transports et/ou de l'énergie?

Code-GCIv5: Devcapacités2.3.6

Justification-GCIv5: Les préoccupations en matière de cybersécurité varient souvent d'un secteur à l'autre. Compte tenu des rôles essentiels des secteurs des finances, de la santé, des télécommunications, des transports et de l'énergie, des formations ciblées pour ces opérateurs peuvent améliorer le dispositif global de cybersécurité d'un pays.

2.3.7 Votre gouvernement élabore-t-il ou soutient-il des formations ou des programmes éducatifs portant sur la cybersécurité destinés aux jeunes?

Code-GCIv5: Devcapacités2.3.8

Justification-GCIv5: Généralement, les gouvernements interviennent pour corriger les externalités négatives du marché et soutenir des groupes qui, autrement, n'auraient qu'un accès restreint aux services de base. En ce qui concerne le développement par l'État de programmes éducatifs et de formations en cybersécurité, ainsi que le soutien de l'État à ces activités, leur rendement peut ne pas être suffisamment élevé pour inciter le secteur privé à participer. Le soutien de l'État peut notamment prendre la forme de subventions financières, de soutien aux études, de soutien à l'apprentissage. Les jeunes qui envisagent une carrière dans la cybersécurité peuvent avoir particulièrement besoin d'un tel soutien, car ils n'ont pas les capitaux nécessaires pour financer leurs études.

2.3.8 Votre gouvernement élabore-t-il ou soutient-il des formations ou des programmes éducatifs portant sur la cybersécurité destinés aux éducateurs, notamment des programmes éducatifs de protection en ligne des enfants?

Code-GCIv5: Devcapacités2.3.9

Justification-GCIv5: La fonction des éducateurs et leur rôle dans l'éducation des enfants et des jeunes leur permet d'inculquer à ces derniers des comportements positifs en matière de cybersécurité. En proposant aux éducateurs une formation à la cybersécurité portant notamment sur la protection en ligne des enfants, les pays démontrent qu'ils œuvrent pour la cybersécurité à long terme en accordant leur soutien aux éducateurs, qui travaillent avec la prochaine génération d'internautes au moment où elle découvre le cyberenvironnement.

3 Programmes pédagogiques sur la cybersécurité intégrés aux programmes universitaires nationaux

Code-GCIv5: Devcapacités3

Justification-GCIv5: Pour améliorer les capacités de la population en cybersécurité, intégrer aux programmes scolaires nationaux les principes qui sont au cœur de la cybersécurité peut enseigner aux élèves de tous âges à mieux gérer les risques de cybersécurité.

3.1 Votre gouvernement élabore-t-il ou soutient-il des programmes éducatifs sur la cybersécurité intégrés aux programmes de l'enseignement primaire?

Code-GCIv5: Devcapacités3.1

Justification-GCIv5: Dans l'enseignement primaire (niveau 1 de la CITE), les enfants entament leur scolarité et, généralement, apprennent la lecture, l'écriture et les mathématiques[20]. Introduire des activités destinées à l'acquisition des principes de base d'un comportement sûr dans le cyberenvironnement peut les aider à avoir conscience de ces questions tout au long de leur vie. Toutefois, comme les enfants du primaire n'ont parfois pas encore le sens critique et l'autonomie nécessaires pour évaluer en toute indépendance les risques de cybersécurité, ils sont exposés à des risques particuliers[21]. Les activités menées pourraient notamment porter sur la protection en ligne des enfants.

3.2 Votre gouvernement élabore-t-il ou prend-il en charge des programmes pédagogiques portant sur la cybersécurité intégrés aux programmes d'études de l'enseignement secondaire?

Code-GCIv5: Devcapacités3.2

Justification-GCIv5: Les élèves de l'enseignement secondaire étudiant dans des programmes scolaires des niveaux 2 et 3 de la CITE, suivent souvent des enseignements dont "l'objectif est d'établir la base d'un apprentissage tout au long de la vie et d'un développement humain que les systèmes éducatifs pourront enrichir par de nouvelles possibilités d'éducation", puis des

---

[20] https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-fr.pdf.

[21] https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity/.

enseignements "conçus pour compléter l'enseignement secondaire et préparer à l'enseignement supérieur, et/ou pour enseigner des compétences pertinentes pour exercer un emploi"[22]. Commencer à étudier la cybersécurité à ce niveau peut non seulement aider à enseigner aux élèves des compétences qui les aideront à être plus en sécurité dans le cyberenvironnement, mais aussi éveiller chez eux un intérêt qui peut les mener à une carrière dans la technologie et la cybersécurité.

3.3 Votre gouvernement élabore-t-il ou soutient-il des programmes éducatifs sur la cybersécurité intégrés aux programmes d'études de l'enseignement supérieur?

Code-GCIv5: Devcapacités3.3

Justification-GCIv5: Les étudiants de l'enseignement postsecondaire (niveaux 5 à 8 de la CITE) ont souvent rempli leur obligation scolaire. Les programmes de l'enseignement postsecondaire peuvent comprendre des cours conçus pour enseigner aux participants des connaissances, des aptitudes et des compétences professionnelles (niveau 5 de la CITE); enseigner aux participants des connaissances, aptitudes et compétences académiques et/ou professionnelles intermédiaires conduisant à un premier diplôme ou une certification équivalente (niveau 6 de la CITE); enseigner aux participants des connaissances, aptitudes et compétences académiques et/ou professionnelles conduisant à un deuxième diplôme ou une certification équivalente, telle qu'un diplôme équivalent à un master (niveau 7 de la CITE); ou destinés à l'obtention d'une certification de chercheur hautement qualifié, de niveau doctorat ou équivalent (niveau 8 de la CITE)[23]. Étudier la cybersécurité à ces niveaux d'éducation peut aboutir à la constitution d'une main-d'œuvre sensibilisée et compétente en matière de cybersécurité, et promouvoir le développement des capacités de recherche et développement.

4 Programmes de recherche-développement portant sur la cybersécurité

Code-GCIv5: Devcapacités4

Justification-GCIv5: La recherche-développement dans les secteurs public, privé et universitaire peut soutenir les efforts de cybersécurité en développant les capacités humaines, en créant de nouvelles techniques et de nouveaux produits et en améliorant la compréhension des risques et des mesures d'atténuation. La recherche-développement peut produire des solutions techniques ou non techniques.

4.1 Dans votre pays, les opérateurs privés du secteur exercent-ils des activités de recherche-développement portant sur la cybersécurité?

Code-GCIv5: Devcapacités4.1

Justification-GCIv5: Le fait que le secteur privé mène des activités de recherche-développement démontre qu'il veut à la fois d'investir dans la croissance et l'innovation dans le domaine de la cybersécurité et améliorer les solutions de cybersécurité disponibles sur le marché.

---

22 https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-fr.pdf.

23 https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-fr.pdf.

4.2 Des opérateurs du secteur public national de votre pays mènent-ils des activités de recherche-développement portant sur la cybersécurité?

Code-GCIv5: Devcapacités5.2

Justification-GCIv5: La participation active des opérateurs publics aux activités de recherche-développement portant sur la cybersécurité peut contribuer à une meilleure identification et correction des vulnérabilités de l'infrastructure de cybersécurité d'un pays. Elle peut aussi faciliter l'élaboration de solutions de cybersécurité pouvant être utilisées pour protéger les infrastructures critiques d'un pays. Les activités de recherche-développement du secteur public portant sur la cybersécurité peuvent également préparer aux cyberattaques. Aux fins de la réponse à la présente question, les opérateurs publics du secteur devraient faire partie du gouvernement central et non d'un État ou d'une administration locale.

4.3 Les établissements d'enseignement supérieur de votre pays mènent-ils des activités de recherche-développement sur la cybersécurité?

Code-GCIv5: Devcapacités5.3

Justification-GCIv5: Le monde universitaire a un rôle essentiel à jouer dans la recherche-développement sur la cybersécurité. Il participe à la recherche de pointe et au renouvellement des modes de pensée, forme les générations futures de professionnels et fait le lien avec les secteurs privé et public.

4.4 Existe-t-il, dans votre pays, des programmes ou initiatives visant à évaluer la cybersécurité des produits TIC, tels que les systèmes de labélisation ou de certification?

Code-GCIv5: Devcapacités4.2

Justification-GCIv5: Les systèmes de certification et de labélisation permettant d'évaluer la cybersécurité des produits TIC peuvent contribuer à inciter les fabricants à promouvoir des normes de cybersécurité plus exigeantes, assurer la transparence et simplifier le choix de produits par les consommateurs. Les pays peuvent appliquer différents types de systèmes en fonction de leur situation et de leurs besoins nationaux.

5 Secteur national de la cybersécurité

Code-GCIv5: Devcapacités5

Justification-GCIv5: Le développement d'un secteur national de la cybersécurité et le soutien à ce secteur peuvent à la fois améliorer la capacité nationale de résoudre les problèmes en matière de cybersécurité et de concevoir de meilleures solutions à ces problèmes et conduire à une gestion anticipative de la cybersécurité.

5.1 Existe-t-il un secteur local de la cybersécurité dans votre pays?

Code-GCIv5: Devcapacités5.1

Justification-GCIv5: Un environnement économique, politique et social favorable au développement de la cybersécurité facilitera la croissance du secteur privé autour de cette activité. Les campagnes de sensibilisation, le développement des compétences des ressources humaines, le renforcement des capacités et les mesures incitatives du gouvernement soutiendront le marché des produits et services liés à la cybersécurité. L'existence d'un secteur d'activité local axé sur la

cybersécurité atteste d'un tel environnement et encouragera la croissance du marché de la cyberassurance et de jeunes entreprises spécialisées dans ce domaine.

5.2 Existe-t-il, dans votre pays, des organisations ou des associations qui œuvrent pour le développement du secteur national de la cybersécurité?

Code-GCIv5: Devcapacités5.4

Justification-GCIv5: Un secteur de la cybersécurité actif et mobilisé peut tirer parti des activités d'organisations et d'associations si elle encourage l'échange de connaissances, le développement des aptitudes, l'accès aux investissements et au financement, notamment. Ces organisations et associations peuvent être soutenues par le secteur ou obtenir le soutien d'organismes nationaux ou d'autres organismes.

6 Mécanismes incitatifs publics

Code-GCIv5: Devcapacités6

Justification-GCIv5: L'investissement dans la sécurité peut avoir des externalités positives qui ne sont pas prises en compte par ceux qui investissent ou déploient des efforts. Pour remédier, le cas échéant, au sous-investissement ou à l'insuffisance des efforts dans le domaine de la cybersécurité, les États peuvent intervenir par des mesures susceptibles d'encourager l'amélioration de la cybersécurité, notamment le financement, la réglementation ou d'autres mécanismes. Ces mesures de soutien peuvent produire une amélioration du niveau de la cybersécurité dans un pays supérieure à celle qui se produirait en l'absence de soutien.

6.1 Des mécanismes incitatifs publics ont-ils été mis en place pour encourager le renforcement des capacités dans le domaine de la cybersécurité?

Code-GCIv5: Devcapacités6.1

Justification-GCIv5: Les mécanismes incitatifs publics peuvent encourager le développement de capacités de cybersécurité, notamment la réalisation d'études, la participation à la formation continue ou l'élaboration de nouveaux programmes de renforcement des capacités, les mécanismes incitatifs tels que les subventions, les bourses d'études, le soutien financier, les prêts et les possibilités d'emploi.

6.2 Existe-t-il des mécanismes incitatifs publics pour la mise en place ou la poursuite du développement de l'industrie de la cybersécurité?

Code-GCIv5: Devcapacités6.2

Justification-GCIv5: Compte tenu des caractéristiques de biens informationnels tels que la cybersécurité, il peut y avoir des monopoles[24]. Pour favoriser l'apparition d'idées et de pratiques nouvelles dans les organisations nouvelles et existantes, et encourager différents acteurs et parties prenantes à participer à la cybersécurité, les gouvernements peuvent offrir des incitations telles que des aides monétaires, des mesures d'allégement fiscal ou de réduction des frais, des

[24] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf.

avantages sur le plan de la réputation, des conditions contractuelles avantageuses ou des mesures visant à inciter les entreprises, les organisations et les particuliers à participer à un écosystème de cybersécurité.

6.3 Existe-t-il, dans votre pays, des mécanismes incitatifs publics qui encouragent les activités de recherche-développement dans le domaine de la cybersécurité?

Code-GCIv5: Devcapacités6.3

Justification-GCIv5: Les mécanismes incitatifs publics sont utiles lorsque les mécanismes du marché ne produisent pas les résultats souhaités. Comme les avantages des activités de recherche-développement sur la cybersécurité peuvent avoir des externalités positives pour l'ensemble de la société, les États peuvent notamment encourager ces activités en les subventionnant, en créant des mécanismes de prêt, en instaurant des conditions propices à l'activité commerciale et aux affaires, en proposant des contrats et en soutenant les activités universitaires.

Mesures relatives à la coopération

Justification-GCIv5: Étant donné que la cybersécurité nécessite des informations émanant de tous les secteurs et de toutes les disciplines, elle doit faire l'objet d'une approche multipartite. Parce qu'elle renforce le dialogue et la coordination, la coopération permet d'élargir le champ d'application de la cybersécurité. Des initiatives de coopération de plus grande ampleur peuvent permettre de constituer des capacités de cybersécurité beaucoup plus fortes et, ainsi, contribuer à dissuader les menaces en ligne répétées et persistantes, et rendre plus efficaces les enquêtes sur les agents malveillants, ainsi que leur arrestation et les procédures judiciaires les visant.

La coopération nationale et internationale peut être mesurée en se référant à l'existence et au nombre de partenariats, de cadres de coopération et de réseaux de partage d'information.

1 Accords de cybersécurité bilatéraux

Code-GCIv5: Coop1

Justification-GCIv5: Les accords bilatéraux (ou accords entre deux parties) désignent toute forme de partenariat officiel, national ou sectoriel, visant à partager des ressources relatives à la cybersécurité avec un autre État ou une organisation intergouvernementale régionale (échange d'informations, de compétences, d'informations sur la politique, de technologies et d'autres ressources) afin d'éviter les cyberconflits transnationaux. La mesure de cet indicateur prend aussi en compte du caractère juridiquement contraignant de l'accord ou du fait qu'il soit en attente de ratification. Les ressources peuvent désigner le partage de professionnels (détachements, placements ou autres affectations temporaires d'employés), d'installations, d'équipement et d'autres outils et services.

1.1 Accord bilatéral ou accords bilatéraux de cybersécurité avec d'autres pays

Code-GCIv5: Coop1.1

Justification-GCIv5: Les accords bilatéraux (ou accords entre deux parties) désignent toute forme de partenariat national officiel visant à partager des ressources relatives à la cybersécurité avec un autre État (échange d'informations, de compétences, d'informations sur la politique, de technologies et d'autres ressources). Le partage de connaissances et de compétences entre des pays peut contribuer à la constitution de solides capacités de réaction aux incidents, ainsi qu'à l'élaboration à titre anticipatif de mesures visant à lutter contre les risques de cybersécurité.

1.1.1 Des mesures de partage d'informations dans le domaine de la cybersécurité sont-elles prises dans votre pays au titre d'accords bilatéraux avec d'autres pays?

Code-GCIv5: Coop1.1.1

Justification-GCIv5: Les accords de cybersécurité prévoyant un partage d'informations sont associés à de plus grandes contributions des pays à la cybersécurité, car ces mesures facilitent la prise en compte des risques potentiels, la réalisation d'évaluations des menaces et l'adoption de mesures de coopération dans le domaine de la cybersécurité.

1.1.2 Des mesures de renforcement des capacités dans le domaine de la cybersécurité sont-elles prises dans votre pays au titre d'accords bilatéraux avec d'autres pays?

Code-GCIv5: Coop1.1.2

Justification-GCIv5: Les accords qui favorisent le développement bilatéral des capacités dans le domaine de la cybersécurité renforcent le potentiel des pays à parer les cyberrisques à titre anticipatif grâce au partage des bonnes pratiques, à l'amélioration des compétences du personnel, à l'intensification de la collaboration et des activités de sensibilisation, ainsi qu'à l'élaboration et l'application de procédures opérationnelles dans le domaine de la cybersécurité.

1.2 Accord(s) de cybersécurité avec des organisations internationales et régionales

Code-GCIv5: Coop1.2

Justification-GCIv5: Compte tenu de l'importance des organisations intergouvernementales régionales, les pays concluent de plus en plus d'accords de coopération dans le domaine de la cybersécurité visant la transmission transfrontalière des actifs de cybersécurité, notamment par l'échange d'informations, de compétences, de technologies et d'autres ressources, soit par à titre individuel, soit en tant que membres d'une organisation intergouvernementale régionale, avec d'autres organisations intergouvernementales régionales, dont l'Union européenne, l'Association des nations de l'Asie du Sud-Est (ASEAN), la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), l'Organisation des États américains (OEA) et l'Union africaine (UA).

1.2.1 Le partage d'informations sur la cybersécurité est-il prévu dans des accords bilatéraux avec d'autres organisations régionales et internationales auxquels est partie votre pays ou l'organisation intergouvernementale régionale dont il est membre?

Code-GCIv5: Coop1.2.1

Justification-GCIv5: Les accords de cybersécurité prévoyant un partage d'information sont associés à de plus grandes contributions des pays à la cybersécurité, car ces mesures facilitent la prise en compte des risques potentiels, le partage de données sur la réalisation d'évaluations des menaces et l'adoption de mesures de coopération dans le domaine de la cybersécurité.

1.2.2 Le renforcement des capacités en matière de cybersécurité est-il prévu dans des accords bilatéraux avec d'autres organisations régionales et internationales auxquels est partie votre pays ou l'organisation intergouvernementale régionale dont il est membre?

Code-GCIv5: Coop1.2.2

Justification-GCIv5: Les accords de cybersécurité bilatéraux qui traitent du renforcement des capacités dans le domaine de la cybersécurité entre les pays et l'organisation intergouvernementale régionale peuvent renforcer les capacités dans ce domaine grâce au partage des bonnes pratiques, à l'amélioration des compétences du personnel, à l'intensification de la collaboration et des activités de sensibilisation, ainsi qu'à l'élaboration et l'application de procédures opérationnelles dans le domaine de la cybersécurité.

2 Accords de cybersécurité multilatéraux avec d'autres pays

Code-GCIv5: Coop2

Justification-GCIv5: La participation à des accords multilatéraux écrits suppose un accord sur les définitions et paramètres essentiels en matière de cybersécurité et un programme commun des avancées dans le domaine de la cybersécurité. Ces accords peuvent aussi favoriser l'instauration de mesures de renforcement de la confiance par l'intermédiaire de la création de mécanismes de rétroaction positive visant l'instauration de relations pacifiques.

2.1 Votre pays est-il partie à un accord multilatéral de cybersécurité prévoyant notamment le partage d'informations dans le domaine de la cybersécurité?

Code-GCIv5: Coop2.1.1

Justification-GCIv5: Les accords de cybersécurité prévoyant un partage d'information sont associés à de plus grandes contributions des pays à la cybersécurité, car ces accords facilitent la prise en compte des risques potentiels, le partage de données sur la réalisation d'évaluations des menaces et l'adoption de mesures de coopération dans le domaine de la cybersécurité.

2.2 Votre pays est-il partie à un accord multilatéral de cybersécurité prévoyant notamment des échanges dans le domaine du renforcement des capacités?

Code-GCIv5: Coop2.1.2

Justification-GCIv5: La participation à des accords multilatéraux écrits prévoyant notamment le renforcement des capacités peut favoriser le renforcement des capacités dans les pays où les dispositifs de cybersécurité sont plus faibles et soutenir les mesures de renforcement de la confiance.

3 Traités d'entraide judiciaire[25] dans le domaine de la cybersécurité

Code-GCIv5: Coop3

***Justification* – GCIv5:** Compte tenu du caractère transnational de la cybersécurité, les interventions face à des menaces ayant une incidence sur la souveraineté d'un État tiers nécessitent des mécanismes de coopération clairs, en particulier pour les questions judiciaires. L'entraide judiciaire entre pays, notamment les traités d'entraide judiciaire, peut aller de la signification de documents et la transmission de preuves à l'assistance en matière d'enquête, entre autres formes d'assistance[26].

---

[25] https://www.unodc.org/e4j/en/organized-crime/module-11/key-issues/mutual-legal-assistance.html.

[26] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL.

3.1 Votre pays participe-t-il à des traités d'entraide judiciaire dans le domaine de la cybersécurité au titre d'accords bilatéraux ou multilatéraux avec d'autres pays ou organisations régionales ou intergouvernementales?

Code-GCIv5: Coop3.1

Justification-GCIv5: Compte tenu du caractère transnational de la cybersécurité, les interventions face à des menaces ayant une incidence sur la souveraineté d'un État tiers nécessitent des mécanismes de coopération clairs, en particulier pour les questions judiciaires. L'entraide judiciaire entre pays, notamment les traités d'entraide judiciaire, peut aller de la signification de documents et la transmission de preuves à l'assistance en matière d'enquête, entre autres formes d'assistance[27].

4 Partenariats public-privé

Code-GCIv5: Coop4

Justification-GCIv5: Les partenariats public-privé s'inscrivent dans une tendance motivée à la fois par des éléments idéologiques et par la volonté d'optimisation des fonds[28]. En particulier dans le domaine de la cybersécurité, où les innovations récentes sont souvent issues du secteur privé, la participation à des partenariats public-privé peut aider les États à bénéficier plus rapidement de ces innovations, qui sont susceptibles d'améliorer la cybersécurité. Toutefois, un certain nombre de défis est associé aux partenariats public-privé, notamment les problèmes d'agent principal, la gestion des coûts externes, la complexité de la négociation des contrats, la souplesse des contrats et la réalisation d'évaluations efficaces[29].

4.1 Votre pays participe-t-il à des partenariats public-privé pour la cybersécurité avec des entreprises nationales?

Code-GCIv5: Coop4.1

Justification-GCIv5: En raison des effets de réseau qui font partie intégrante des partenariats public-privé avec les entreprises nationales, ces partenariats peuvent faciliter la construction d'un écosystème national de cybersécurité et, ainsi, permettre aux acteurs nationaux du secteur privé de développer et étendre leurs compétences, leurs systèmes et leurs services.

---

27 https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL.

28 https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page5.

29 https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page66.

4.2 Votre pays participe-t-il à des partenariats public-privé pour la cybersécurité mis en œuvre au niveau national avec des entreprises étrangères?

Code-GCIv5: Coop4.2

Justification-GCIv5: En tant que bien informationnel, la cybersécurité est soumise aux effets de réseau et aux gains de compétences spécialisées liés à l'échelle[30]. Les intervenants internationaux ayant acquis des compétences spécialisées en matière de cybersécurité dans différentes sortes de contextes ou de parcours nationaux peuvent offrir des prestations supplémentaires aux États qui souhaitent renforcer la cybersécurité nationale. Les États qui participent à des partenariats public-privé avec des intervenants étrangers peuvent mettre leurs compétences spécialisées au service de la croissance et de la sécurité nationale.

5 Partenariats interorganismes

Code-GCIv5: Coop5

Justification-GCIv5: Tout partenariat national officiel entre différents organismes publics à l'intérieur d'un pays peut améliorer la capacité d'ajustement de l'État face aux risques de cybersécurité risques de cybersécurité. Il peut s'agir de partenariats en faveur du partage d'informations ou de ressources entre les ministères, les départements, les programmes et d'autres institutions du secteur public. Dans la présente section, les partenariats interorganismes entre des organismes situés dans différents pays ou entre différentes organisations intergouvernementales ne sont pas pris en compte.

5.1 Existe-t-il, dans votre pays, des processus de coordination interorganismes portant spécifiquement sur la cybersécurité entre différents organes gouvernementaux nationaux?

Code-GCIv5: Coop5.1

Justification-GCIv5: Tout partenariat national officiel entre différents organismes publics à l'intérieur d'un pays peut améliorer la capacité d'ajustement de l'État face aux risques de cybersécurité. Il peut s'agir de partenariats en faveur du partage d'informations ou de ressources entre les ministères, les départements, les programmes et d'autres institutions du secteur public. Dans la présente section, les partenariats interorganismes entre des organismes situés dans différents pays ou entre différentes organisations intergouvernementales ne sont pas pris en compte.

---

[30] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf.

Définitions

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
Monde universitaire		Le monde du savoir universitaire	Oxford English Dictionary		Tech2; Devcapacités4.1.3; Devcapacités6.2
Établissements d'enseignement supérieur		Institutions faisant partie du monde du savoir universitaire	Oxford English Dictionary		Devcapacités4.1.3
Accord		Engagements réciproques conclus par écrit entre des États ou d'autres parties et régi par le droit international, qu'ils soient consignés dans un instrument unique ou dans deux ou plusieurs instruments connexes	D'après la Convention de Vienne sur le droit des traités		
Accords bilatéraux		Accords conclus par écrit entre deux parties, notamment des États, des organismes régionaux ou des organisations, signés par les décideurs concernés	Deuxième édition de l'Indice GCI		Coop1; Coop1.1; Coop1.1.1; Coop1.1.2; Coop1.1.3
Développement des capacités		Le renforcement des capacités est un processus de changement. Il est souvent assimilé au recrutement de personnel supplémentaire, à des activités de formation et à des ateliers. Bien que la formation individuelle et les ateliers puissent être mis en œuvre dans le cadre d'un plan global de développement des capacités, ces activités ne sauraient suffire. En effet, le fait qu'une personne suive des activités de formation ne garantit pas que cette formation sera ensuite mise à profit dans un environnement professionnel. Le renforcement des capacités doit être plus large et prévoir des mesures d'amélioration des systèmes de santé de nature à augmenter le rendement et assurer la durabilité. Une évaluation du fonctionnement actuel du système et des domaines dans lesquels une aide est nécessaire devrait être menée. Les mesures à prendre pourraient être les suivantes: élaborer et	PNUD https://www.undp-capacitydevelopment-health.org/en/capacities/		Org2.3; Devcapacités1; Devcapacités6.1; Coop1.1.2

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		mettre en œuvre des systèmes d'information sanitaire, former le personnel à l'analyse des données, élaborer des politiques et des procédures pour une gestion financière rigoureuse ou améliorer l'approvisionnement et la distribution des principaux produits de santé.			
Protection en ligne des enfants	COP	La protection en ligne des enfants (COP) vise à protéger les enfants et les jeunes contre les menaces et les risques qu'ils peuvent rencontrer en ligne. Le concept de la protection en ligne des enfants englobe l'adoption d'une approche holistique de la construction d'espaces numériques sûrs, adaptés à l'âge, inclusifs et participatifs pour les enfants et les jeunes, caractérisée par: • la réponse, le soutien et l'auto-assistance face à la menace; • la prévention des préjudices; • un équilibre dynamique entre assurer la protection et offrir aux enfants la possibilité d'être des citoyens numériques; • défendre les droits et les responsabilités des enfants et de la société.	https://www.itu-cop-guidelines.com/		Juridique1.3.3; Tech1.2.4 Tech4; Org1.3; Org2.4; Devcapacités1.6
Infrastructures critiques (voir aussi: infrastructures critiques nationales)		Systèmes, services et fonctions essentiels dont la perturbation ou la destruction affaiblirait les secteurs de la santé et de la sécurité publiques, du commerce et de la sûreté nationale, isolément ou non.	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf	Sont notamment mais non exclusivement concernés: les systèmes de défense, la banque et la finance, les télécommunications, les transports, la santé et l'énergie.	Tech1.2
Infrastructures essentielles de l'information	CII	Biens et actifs, réseaux, services et installations matériels et numériques dont la perturbation ou la destruction pèserait lourdement sur la santé, la sécurité et le bien-être économique des citoyens, et	INTERNATIONAL CIIP HANDBOOK 2008/2009	Sont notamment mais non exclusivement concernés: les centraux téléphoniques, les points d'échange Internet, les	

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		nuirait à l'efficacité du de l'administration du pays touché.		réseaux sans fil et les satellites.	
Lois relatives à la cybercriminalité		Les lois relatives à la cybercriminalité énoncent les règles de conduite et les normes de comportement applicables à l'utilisation d'Internet, des ordinateurs et des technologies numériques connexes, ainsi qu'aux actions de la population, de l'État et des organisations privées; les règles d'administration de la preuve et le règlement de la procédure pénale, ainsi que d'autres questions de justice pénale concernant le cyberenvironnement; et la réglementation.	https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html		Juridique1
Obligations en matière d'audits de cybersécurité		Un audit de sécurité est une évaluation systématique et périodique de la sécurité du système d'information. Généralement, pareil audit comprend une évaluation de la sécurité de la configuration et de l'environnement physiques du système, des logiciels, des processus de traitement de l'information et des pratiques d'utilisation.	Quatrième édition de l'Indice GCI		Juridique2.3n
Écosystème de cybersécurité		Ensemble d'opérateurs en marge et à l'intérieur du secteur de la cybersécurité, dont les rôles et responsabilités évoluent de concert	D'après James Moore, *The Death of Competition, 1996*	Par exemple, des professionnels dans les domaines du droit, de la technique, des affaires et de l'élaboration des politiques, dont les activités relatives aux problèmes de cybersécurité se complètent.	Devcapacités5.1, Devcapacités6.2
Résilience en matière de cybersécurité		Un plan national de résilience en matière de cybersécurité permet au pays de résister aux conséquences d'une catastrophe, de les atténuer, de s'y adapter et de se rétablir rapidement et efficacement des conséquences d'une catastrophe (d'origine naturelle ou anthropique), notamment grâce à la préservation et à la restauration de ses	https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/website/web-fg-ssc-0090-r7-technical_report_on_ICT_infrastruc		Tech1.3

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		fonctions et services essentiels en s'appuyant sur des services extérieurs.	ture_for_resilience_security.doc		
Traités et accords de cybersécurité		Traité ou accord entre deux pays, organisations ou autres groupes portant spécifiquement sur la cybersécurité	https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478		
Violation de données notification		Les lois ou règlements en matière de signalement des infractions imposent à l'entité victime d'une infraction d'en informer les autorités, les clients et autres parties, et de prendre des mesures en vue de remédier aux dommages causés. Ces lois sont généralement promulguées en réponse au nombre croissant d'infractions perpétrées contre les bases de données de consommateurs, qui contiennent des informations d'identification personnelle.	Deuxième édition de l'Indice GCI		Juridique2.2
Accès illégal		L'accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un système d'information. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.	Deuxième édition de l'Indice GCI		Juridique1.1.1
Interception illégale		L'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques.	Deuxième édition de l'Indice GCI		Juridique1.1.3

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
Atteinte à l'intégrité des données		"Le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques" et "l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration ou la suppression de données informatiques".	Deuxième édition de l'Indice GCI		Juridique1.1.2
Notification en cas d'incident		Notification par une équipe d'intervention en cas d'incident informatique ou par d'autres intervenant aux parties concernées par un incident de cybersécurité.			Juridique2.2
Partenariats/ accords interorganismes		Tout partenariat national officiel entre différents organismes publics à l'intérieur d'un pays peut améliorer la capacité d'ajustement de l'État face aux risques de cybersécurité. Il peut s'agir de partenariats en faveur du partage d'informations ou de ressources entre les ministères, les départements, les programmes et d'autres institutions du secteur public. Dans la présente section, les partenariats interorganismes entre des organismes situés dans différents pays ou entre différentes organisations intergouvernementales ne sont pas pris en compte.	Deuxième édition de l'Indice GCI		Coop5
Processus de coordination interorganismes		Coordination sur certaines questions entre deux organismes gouvernementaux ou plus afin de contribuer à la réalisation d'activités et d'objectifs harmonisés.			Coop5.1
Micro-entreprises et petites et moyennes entreprises	MPME	La définition des micro-entreprises et petites et moyennes entreprises peut varier selon les pays. Les définitions recensées par le SME Finance Forum devraient être utilisées dans la mesure du possible.		https://www.smefinanceforum.org/data-sites/msme-country-indicators	Devcapacités1.1; Devcapacités2.3.3

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
Accords multilatéral		Les accords multilatéraux (accords entre au moins trois parties) désignent toute forme de programme officiellement reconnu, national ou sectoriel, visant à partager des informations ou des ressources relatives à la cybersécurité avec plusieurs autres États ou organisations internationales (coopération ou échange d'informations, de compétences spécialisées, de technologies et d'autres ressources). Il peut aussi s'agir de la ratification d'accords internationaux relatifs à la cybersécurité, tels que la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel et la Convention sur la cybercriminalité (Convention de Budapest).	Deuxième édition de l'Indice GCI		Coop3; Coop3.1.1; Coop3.1.2
Infrastructures critiques nationales (Voir aussi: infrastructures critiques)		Systèmes, services et fonctions essentiels dont la perturbation ou la destruction affaiblirait les secteurs de la santé et de la sécurité publiques, du commerce et de la sûreté nationale, isolément ou non.	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf		Juridique2.7; Org1.1.1
CIRT nationale		Les CIRT (équipes d'intervention en cas d'incident informatique), CERT (équipes d'intervention en cas d'urgence informatique) et CSIRT (équipes de réponse aux incidents de sécurité informatique) sont des entités organisationnelles qui ont pour mission de coordonner et d'appuyer les interventions en cas d'évènements ou d'incidents en matière de sécurité informatique au niveau national. Elles doivent être capables d'identifier les cybermenaces, de les prévenir, d'y répondre et de les gérer, ainsi que de renforcer la sécurité du cyberenvironnement dans le pays. Outre cette capacité, elles doivent pouvoir collecter elles-mêmes des renseignements afin de ne pas devoir compter sur des signalements de seconde main d'incidents de sécurité faits par les clients de la	Deuxième édition de l'Indice GCI		

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		CIRT ou d'autres sources. Elles peuvent être militaires ou civiles.			
Abus en ligne					Juridique1.3.2
Cyberharcèle-ment		Messages envoyés par courrier électronique, par messagerie instantanée ou via des sites Internet de dénigrement afin d'intimider ou de harceler un individu ou un groupe d'individus par le biais d'attaques personnelles.	Quatrième édition de l'Indice GCI		Juridique1.3.2
Sécurité en ligne		Fait d'accroître au maximum la sécurité sur Internet pour se prémunir contre les différents risques pour les informations privées et personnelles ou les informations liées à la propriété, et d'améliorer la capacité des utilisateurs à se protéger eux-mêmes contre la cybercriminalité.	Quatrième édition de l'Indice GCI		Juridique1.3
Personnes ayant des besoins particuliers		Exigences particulières dues à un handicap physique ou à des difficultés d'apprentissage ou de comportement, etc. (en particulier dans les contextes éducatifs).	Oxford English Dictionary	"special needs, n. and adj.". Site Web du Oxford English Dictionary, juin 2021, Oxford University Press. https://www.oed.com/view/Entry/253889?redirectedFrom=special+needs (page consultée le 30 août 2021).	
Protection des données personnelles		On entend par "données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable. La protection des données personnelles est le processus visant à préserver les données personnelles.	https://gdpr-info.eu/issues/personal-data/ Définition figurant dans le Règlement général sur la protection des données (RGPD)	La norme non contraignante UIT-T X.1058 | ISO/CEI 29151 représente un précieux point de référence pour les gouvernements et l'industrie qui intensifient leurs efforts visant à garantir la protection des données personnelles. La norme X.1058 énonce les objectifs des contrôles de protection des données,	Juridique2.1a

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
				précise les contrôles à mettre en œuvre et fournit des lignes directrices à cette fin. La manière dont les modalités de ces contrôles peuvent répondre aux obligations relatives à la protection des données personnelles recensées dans des évaluations des risques et des études d'impact réalisées par des organisations est présentée dans cette norme.	
Politique		Les politiques sont des règles, des principes, des lignes directrices ou des structures adoptés ou élaborés par une organisation ou un pays afin d'atteindre des objectifs à long terme. Elles sont généralement définies par écrit et faciles à comprendre. Les politiques sont formulées pour guider et influencer toutes les décisions importantes devant être prises dans l'organisation et faire en sorte que toutes les activités respectent un ensemble de limites établies.	Nouveau		Org1.1
Enseignement post-secondaire non-supérieur (niveau 4 de la CITE)	CITE, niveau 4	L'enseignement post-secondaire non-supérieur fournit des expériences d'apprentissage qui viennent compléter l'enseignement secondaire et préparent à l'entrée sur le marché du travail ainsi qu'à l'enseignement supérieur. Il vise l'acquisition individuelle de connaissances, aptitudes et compétences dont le niveau de complexité est inférieur à celui de l'enseignement supérieur. Les programmes du niveau 4 de la CITE, ou "enseignement post-secondaire non-supérieur", sont généralement conçus pour fournir aux individus qui ont achevé le niveau 3 de la CITE des certifications exigées pour	https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-fr.pdf	Cartographies de la CITE	Devcapacités3.4n

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		accéder à l'enseignement supérieur ou à l'emploi lorsque leur certification de niveau 3 de la CITE ne leur donne pas cet accès.			
Enseignement primaire (Niveau 1 de la CITE)		Les programmes du niveau 1 de la CITE, ou "enseignement primaire", sont généralement conçus pour donner aux élèves des aptitudes fondamentales en lecture, écriture et mathématiques (c'est-à-dire l'alphabétisme et le calcul) et établir une base solide pour l'apprentissage et la compréhension des connaissances de base, le développement personnel et social et la préparation au premier cycle de l'enseignement secondaire. Il vise un apprentissage avec un niveau de complexité de base et peu ou pas de spécialisation. L'âge est normalement le seul critère d'admission dans ce niveau. L'âge habituel ou légal d'admission n'est généralement ni inférieur à 5 ans, ni supérieur à 7 ans.	https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-fr.pdf	Cartographies de la CITE	Devcapacités3.1
Protection de la vie privée		La protection de la vie privée sur Internet renvoie au niveau de confidentialité et de sécurité des données personnelles publiées en ligne. C'est un terme général qui désigne une grande diversité de facteurs, techniques et technologies utilisées pour protéger les données, les communications et les préférences à caractère sensible et privé. La loi sur la protection des données est un exemple de législation de ce type.	Deuxième édition de l'Indice GCI		Juridique2.1b
Partenariat entre secteur public et secteur privé (partenariat public-privé)	PPP	Un contrat à long terme entre une partie privée et une entité publique, visant la fourniture d'un bien ou d'un service public, au titre duquel la partie privée assume un risque important et la responsabilité de la direction, et la rémunération dépend de la performance. NOTE: En l'absence de définition juridique officielle, les partenariats public-privé sont souvent caractérisés par leur fonction. Le Secrétaire général de l'ONU a	https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships		

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		suggéré deux typologies.11 La première compte cinq grandes fonctions: a) dialogue sur les mesures à prendre, p. ex. Groupe d'étude des technologies de l'information et des communications, Commission internationale des grands barrages, Alliance Gavi; b) activités de plaidoyer, p. ex. partenariat d'ONUSIDA avec les médias pour sensibiliser à la question du VIH/sida; c) mobilisation de fonds privés, p. ex. Fondation pour les Nations Unies et Fonds des Nations Unies pour les partenariats internationaux, projet pour l'investissement étranger (CNUCED et Chambre de commerce internationale); d) information et apprentissage, p. ex. projets conjoints de recherche et de formation; et e) exécution opérationnelle, p. ex. Initiative Premiers sur le terrain (ONU-LM Ericsson), projet d'immatriculation des réfugiés (ONU-Microsoft) (ONU, orientations 18 à 32).12 La seconde compte quatre fonctions: a) partenariats de plaidoyer, p. ex. Alliance mondiale pour l'amélioration de la nutrition, partenariat mondial entre le secteur public et le secteur privé pour le lavage des mains au savon; b) partenariats pour la définition de normes et de critères, p. ex. Global Reporting Initiative, projet "Who Cares Wins" sur la responsabilité des entreprises dans les industries financières; c) partage des ressources et des compétences, p. ex. programme logistique"Moving the World" (Programme alimentaire mondial – TNT); d) mobilisation des marchés en faveur du développement, p. ex. initiative de production de beurre de karité (UNIFEM-L'Occitane), projet de composants automobiles en Inde (ONUDI-FIAT) (Assemblée générale des Nations Unies, "Rapport du Secrétaire général sur le renforcement de la coopération entre l'Organisation des Nations Unies et tous les	https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1084?rskey=CTIBOr&result=1&prd=MPIL		

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		partenaires concernés, en particulier le secteur privé" *[10 août 2005]* 5).13 Les lignes directrices de l'ONU distinguent plusieurs modalités de coopération, ainsi que les dispositions juridiques types correspondant à chacune de ces modalités ou les désignent simplement comme des projets entre le secteur public et le secteur privé. Cet indicateur de résultat peut être mesuré au moyen du nombre de partenariats public-privé nationaux ou sectoriels officiellement reconnus pour le partage d'informations (renseignements sur les menaces) sur la cybersécurité et d'actifs de cybersécurité (personnes, processus, outils) (autrement dit des partenariats officiels pour la coopération ou l'échange d'information, de compétences, de technologies et/ou de ressources), que ce soit à l'échelle nationale ou internationale.			
Règlementation		Règle ou principe régissant les comportements ou les pratiques; en particulier, un acte de cette nature établi et imposé par une autorité.	Oxford English Dictionary	"regulation, n. and adj.". Site Web du Oxford English Dictionary, juin 2021. Oxford University Press. https://www.oed.com/view/Entry/161427?redirectedFrom=regulation (page consultée le 30 août 2021).	Juridique2, Juridique2.1, Juridique2.2
Recherche et développement	R&D	La recherche et le développement expérimental (r-d) englobent les activités créatives et systématiques entreprises en vue d'accroître la somme des connaissances – y compris la connaissance de l'humanité, de la culture et de la société – et de concevoir de nouvelles applications à partir des connaissances disponibles. L'expression "recherche et développement" (r-d) englobe trois types d'activité: la recherche fondamentale, la recherche appliquée et le développement expérimental. Pour être considérée	Organisation de coopération et de développement économiques (OCDE), 2015, Manuel de Frascati 2015 Lignes directrices pour le recueil et la communication		Devcapacités4.1; Devcapacités4.1.1; Devcapacités4.1.2; Devcapacités4.1.3

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		comme relevant de la r-d, une activité doit remplir cinq critères de base. L'activité considérée doit comporter un élément: • de nouveauté; • de créativité; • d'incertitude et être; • systématique; • transférable et/ou reproductible.	des données sur la recherche et le développement expérimental http://uis.unesco.org/en/glossary-term/research-and-experimentaldevelopment-rd		
Enseignement secondaire (niveaux 2 et 3 de la CITE)	Niveaux 2 et 3 de la CITE	Les programmes du niveau 2 de la CITE, ou "premier cycle de l'enseignement secondaire", sont généralement destinés à compléter les acquis scolaires du niveau 1 de la CITE. Dans la plupart des cas, l'objectif est d'établir la base d'un apprentissage tout au long de la vie et d'un développement humain que les systèmes éducatifs pourront enrichir par de nouvelles possibilités d'éducation. Certains systèmes éducatifs peuvent déjà offrir des programmes d'enseignement professionnel du niveau 2 de la CITE afin d'enseigner des compétences pertinentes pour le marché du travail. Les programmes du niveau 3 de la CITE, ou "deuxième cycle du secondaire", sont généralement conçus pour compléter l'enseignement secondaire et préparer à l'enseignement supérieur, et/ou pour enseigner des compétences pertinentes pour exercer un emploi. Le niveau 3 de la CITE commence après 8 à 11 ans d'enseignement depuis le début du niveau 1 de la CITE.	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	Devcapacités3.2
Enseignement supérieur	Niveaux 5 à 8 de la CITE	Les programmes du niveau 5 de la CITE, ou "enseignement supérieur de cycle court", sont conçus principalement pour enseigner aux participants des	https://uis.unesco.org/sites/default/files/documents	Cartographies de la CITE	Devcapacités3.3

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
(niveaux 5 à 8 de la CITE)		connaissances, aptitudes et compétences professionnelles. Habituellement, ils sont fondés sur la pratique, professionnellement spécifiques et ils préparent les étudiants à entrer sur le marché du travail. Toutefois, ces programmes peuvent aussi représenter une passerelle vers d'autres programmes de l'enseignement supérieur. Les programmes du niveau 6 de la CITE, ou "licence ou équivalent", sont souvent destinés à enseigner aux participants des connaissances, aptitudes et compétences académiques et/ou professionnelles intermédiaires conduisant à un premier diplôme ou une certification équivalente. Les programmes du niveau 7 de la CITE, ou "niveau master ou équivalent", sont souvent destinés à enseigner aux participants des connaissances, aptitudes et compétences académiques et/ou professionnelles conduisant à un deuxième diplôme ou une certification équivalente. Les programmes du niveau 8 de la CITE, ou "niveau doctorat ou équivalent", sont principalement destinés à l'obtention d'une certification de chercheur hautement qualifié. Les programmes de ce niveau de la CITE sont donc consacrés à des études approfondies et à des travaux de recherche originaux et sont dispensés presqu'exclusivement par des établissements d'enseignement supérieur orientés vers la recherche, comme des universités par exemple. Les programmes de doctorat existent aussi bien dans des domaines académiques que professionnels.	/international-standard-classification-of-education-isced-2011-fr.pdf		
Xénophobie		Hostilité ou préjugés manifestés à l'égard des personnes, cultures et coutumes étrangères ou perçues comme telles.	Oxford English Dictionary	"xenophobia, n.". Site Web du Oxford English Dictionary, juin 2021. Oxford University Press. https://www.oed.com/view/E	Juridique1.3.1

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
				ntry/230996?redirectedFrom=xenophobia (page consultée le 30 août 2021).	
Initiatives nationales		Activités menées au niveau national pour remédier à une préoccupation spécifique de manière systématique	Deuxième édition de l'Indice GCI	Les initiatives nationales sont généralement conçues pour remédier à un sujet de préoccupation particulier de l'organisation. Elles peuvent notamment porter sur les droits de l'homme, l'éducation ou l'environnement. Il peut s'agir de cibles ou d'objectifs attribués à un ou plusieurs membres par l'intermédiaire de l'interface "créer un projet".	
Falsification informatique		La falsification informatique passe par l'usurpation de l'identité d'individus, d'autorités, d'organismes et d'autres entités légitimes en ligne à des fins frauduleuses.	https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html#:~:text=Computer%2Drelated%20forgery%20involves%20impersonation,entities%20online%20for%20fraudulent%20purposes		Juridique1.2
Communica-tions électroniques		Une communication électronique, telle qu'un courriel, un SMS, un réseau social ou un appel téléphonique, non sollicitée par le destinataire. Le spam désigne de	Deuxième édition de l'Indice GCI		Juridique2.7

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
non sollicitées ou spam		telles communications non sollicitées, envoyées en masse.			
Signature numérique		Une signature numérique est une technique mathématique qui sert à valider l'authenticité et l'intégrité d'un message, d'un logiciel ou d'un document numérique.	Deuxième édition de l'Indice GCI		Juridique2.6
Transaction électronique		Une transaction électronique désigne la vente ou l'achat de biens ou de services entre entreprises, ménages, individus, États et autres organismes publics ou privés, sur des réseaux informatisés. Les lois sur le commerce, les signatures et les transactions électroniques sont autant d'exemples de ce type de législation, qui peut prévoir des réglementations relatives à l'institution d'un contrôleur des autorités de certification.	Deuxième édition de l'Indice GCI		
Normes de cybersécurité		Existence d'un ou plusieurs cadres approuvés (ou ratifiés) par le gouvernement concernant l'application des normes internationalement reconnues en matière de cybersécurité dans le secteur public (administrations publiques) et dans l'infrastructure critique (même si elle est gérée par le secteur privé). Les normes concernées sont, entre autres, celles élaborées par les organismes suivants: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc. La réglementation relative à la certification/normalisation en matière de cybersécurité impose aux entités exerçant leurs activités sur le territoire du pays de satisfaire à certaines exigences minimales en la matière. Ces exigences peuvent varier en fonction du secteur d'activité. Les normes concernées sont, entre autres, celles élaborées par les organismes suivants: ISO, UIT IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG,		Définition figurant dans la quatrième édition de l'Indice GCI et la deuxième édition de l'Indice GCI	Juridique2.5

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.			
Exercices de cybersécurité (tels que les cyberexercices)		Il s'agit d'une activité planifiée au cours de laquelle une organisation simule une cyberperturbation afin de renforcer ou de tester ses capacités de prévention, de détection, d'atténuation ou de traitement des perturbations, ou de rétablissement après une perturbation.	Quatrième édition de l'Indice GCI		Tech1.2.2
Cyberexercice		Un cyberexercice est une manifestation annuelle consistant à simuler des cyberattaques, des incidents liés à la sécurité de l'information ou d'autres types de dysfonctionnements, en vue de tester les cybercapacités d'une organisation, qu'il s'agisse de détecter un incident de sécurité ou d'intervenir comme il se doit et d'atténuer autant que possible les conséquences d'un tel dysfonctionnement. Un cyberexercice permet aux participants de valider les politiques, des plans, des procédures, des processus et des capacités de préparation, de prévention, d'intervention, de rétablissement et de continuité des activités.	Définition de l'UIT	https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx	Tech1.2.2
Mises en garde concernant la cybersécurité		Orientations des équipes CIRT: informations communiquées au grand public au sujet des nouvelles cybermenaces et des mesures recommandées.	Quatrième édition de l'Indice GCI		Tech1.2.3
Affiliation au FIRST		Membre titulaire ou agent de liaison du Forum des équipes d'intervention et de sécurité en cas d'incident (FIRST). www.first.org	Quatrième édition de l'Indice GCI		Tech1.3
Affiliation à des équipes CIRT/CERT/ CSIRT régionales		Relation, officielle ou non, avec n'importe quelle autre équipe CERT, au sein du pays ou non, dans le cadre d'un groupe régional de CERT. Parmi les équipes CERT régionales, on peut citer APCERT, AFRICACERT, EGC, OIC et OAS.	Quatrième édition de l'Indice GCI		Tech1.4

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
Équipes CIRT/CSIRT/ CERT sectorielles		Une équipe CIRT/CSIRT/CERT sectorielle est une entité qui intervient en cas d'incident relatif à la sécurité informatique ou à la cybersécurité touchant un secteur d'activité spécifique. Les équipes CERT sectorielles sont généralement créées pour des secteurs essentiels, tels que la santé, les services publics, l'enseignement supérieur, les services d'urgence et le secteur financier. Si l'équipe CERT gouvernementale est au service du secteur public, une équipe CERT sectorielle fournit ses services aux parties prenantes d'un seul secteur d'activité.	Deuxième édition de l'Indice GCI		Tech2.1
Coopération internationale dans le domaine de la cybersécurité		Collaboration entre deux ou plusieurs États, organismes nationaux, organes de contrôle, équipes CIRT nationales, organisations de la société civile ou universités.			Org1.8
Dispositifs et fonctionnalités de signalement		Il s'agit notamment de lignes d'assistance nationales et de lignes d'assistance connectées au système international de lignes d'assistance. Ces lignes doivent être reliées à des systèmes d'orientation et de soutien.			Org4.3
Campagnes de sensibilisation du public à la cybersécurité		La sensibilisation du public comprend les efforts déployés pour promouvoir des campagnes visant à toucher autant de personnes que possible, mais aussi à recourir à des ONG, des institutions, des organisations, des fournisseurs de services Internet, des bibliothèques, des organisations du commerce locales, des centres communautaires, des lycées, des programmes de formation pour adultes, des écoles et des organisations parents-enseignants, afin de faire passer les messages relatifs à un comportement sécurisé en ligne. Il peut s'agir de la création de portails et de sites Internet de sensibilisation, de la distribution de matériel pédagogique et d'autres activités pertinentes.	Quatrième édition de l'Indice GCI		Devcapacités1.

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
Service sécurité production	SOC	On entend par "service sécurité production" (SOC) une unité organisationnelle opérant au cœur de toutes les opérations de sécurité. Le SOC n'est généralement pas considéré comme une entité ou un système distinct, mais plutôt comme une structure complexe servant à gérer et améliorer le dispositif de sécurité global d'une organisation. Sa fonction est de détecter, analyser et répondre aux menaces et aux incidents de cybersécurité en utilisant des personnes, des processus et des technologies. Ces activités peuvent être formalisées en sept dimensions ou domaines fonctionnels d'un SOC. Bien que leur rôle essentiel dans la sécurité des entreprises soit largement admis, les SOC sont toujours considérés comme un mécanisme de défense passif et réactif. "Équipe d'intervention en cas d'incident informatique" (CSIRT) est souvent utilisé à la place de SOC, bien qu'une équipe CSIRT privilégie la réponse après une attaque. Une équipe CSIRT est une unité organisationnelle chargée de coordonner et de soutenir la réponse à un incident de sécurité informatique. Elle est considérée comme une équipe indépendante ou faisant partie d'un SOC. Le centre d'exploitation de réseau (NOC) supervise l'identification, l'enquête, le classement selon un rang de priorité, le renvoi au niveau supérieur et le règlement des problèmes. Cependant, dans les NOC, les problèmes traités sont différents, car les centres se concentrent sur les incidents qui compromettent le rendement et la disponibilité du réseau d'une organisation. Comme des incidents peuvent se produire sur tous les systèmes et pas seulement sur les réseaux, il est dans l'intérêt des organisations que les équipes NOC et SOC travaillent ensemble. Un Centre d'exploitation de réseau (NOC) "Centre de	https://ieeexplore.ieee.org/document/9296846		

Terme ou expression	Abréviation	Définition	Source	Exemples	Questions à consulter (quatrième édition de l'Indice GCI)
		renseignement de sécurité" a été utilisé pour la première fois en 2017 pour désigner le successeur des SOC. L'objectif du centre de renseignement de sécurité est de fournir une vision plus globale et intégrée qu'un centre SOC; il peut visualiser et gérer entièrement le renseignement de sécurité en un seul endroit. Il associe donc plusieurs technologies (dont la gestion des connaissances en sécurité de l'information et le traitement des mégadonnées). La gestion des informations et des événements de sécurité (SIEM) fait partie intégrante de nombreux SOC afin de prendre en compte une grande partie des exigences technologiques. Elle est responsable de la collecte centralisée des données relatives à la sécurité. Ainsi, elle déploie des capacités d'analyse de sécurité en corrélant les événements de journal. D'autres fonctionnalités permettent d'enrichir avec des données contextuelles, de normaliser des données hétérogènes, de générer des rapports et d'alerter. Pour permettre l'échange d'informations sur les menaces, la SIEM fournit une connexion aux plates-formes d'échange de renseignements sur les cybermenaces, et il fait participer des analystes de la sécurité humaine en offrant des capacités d'analyse visuelle de la sécurité. Il comporte des capacités de gestion des journaux des données d'événement par stockage à long terme.			

_____