ABIresearch

Global Cybersecurity Index

Cadre conceptuel

Les technologies de l'information et de la communication (TIC) sont l'élément moteur de l'évolution des sociétés modernes. Elles sous-tendent aussi bien la croissance sociale, économique et politique des individus que celle des organisations et des gouvernements. De nos jours, les TIC sont non seulement omniprésentes, mais aussi essentielles au progrès. Les puces électroniques, les communications de machine à machine, les services en nuage et beaucoup d'autres technologies font progresser les sociétés en réseau de nouvelle génération. La technologie numérique et la connectivité Internet sont systématiquement intégrées dans tous les segments des secteurs privé et public parce qu'elles présentent des avantages substantiels: productivité, rapidité, réduction des coûts et flexibilité. C'est pourquoi les TIC sont progressivement utilisées sur de nouvelles plates-formes comme les systèmes RFID dans le commerce de détail et les dispositifs télématiques pour les véhicules. Mais elles sont avant tout utilisées pour moderniser des infrastructures critiques, notamment les réseaux énergétiques, les réseaux de transport et les systèmes de soins de santé.

La cybersécurité est essentielle pour maintenir un modèle fiable sur le plan technologique. Les perturbations de l'approvisionnement en électricité ou les défaillances des systèmes financiers dues à des interférences avec des réseaux TIC sont une réalité et constituent des menaces pour la sécurité nationale. Les agents malveillants en ligne sont nombreux, organisés et leurs motivations sont très diverses: politiques, criminelles, terroristes ou hacktivistes. Les outils à leur disposition gagnent en sophistication et en complexité au fil du temps et avec l'expérience, tandis que le nombre croissant des plates-formes connectées contribue à multiplier les vecteurs d'attaque. Nous ne reviendrons jamais à une époque où les choses étaient plus simples. La cybersécurité doit faire partie intégrante du progrès technologique.

Malheureusement, elle n'a pas encore trouvé sa place au cœur de nombreuses stratégies technologiques nationales et industrielles. Malgré les efforts importants mis en œuvre dans le domaine de la cybersécurité, ils n'en restent pas moins éclectiques et dispersés. Les écarts dans le taux de pénétration d'Internet, les développements technologiques, la dynamique du secteur privé et les stratégies gouvernementales font que la cybersécurité se fonde sur une approche ascendante. Cela n'est pas surprenant étant donné les disparités qui existent entre les différents Etats, les secteurs public et privé et entre les différents secteurs industriels.

Toutefois, l'introduction d'une culture globale de la cybersécurité bénéficierait davantage d'une approche descendante. Le partage des informations et la coopération sont essentiels pour faire face aux menaces transfrontalières. Ces éléments nécessitent une certaine organisation dans toute une gamme de disciplines, juridiques, techniques et éducatives. Même si certains pays ou secteurs ont élaboré et adopté un cadre de cybersécurité extrêmement efficace, il est rare qu'il soit connu au-delà.

Le principal écueil est que la cybersécurité est une question sensible, aussi bien du point de vue du gouvernement que du secteur privé. Toute admission de vulnérabilité pourra être considérée comme une faiblesse. Cela constitue un obstacle à la discussion et au partage d'informations sur les menaces et les bonnes pratiques. Or, "la sécurité par l'obscurité" n'est pas un modèle de défense viable contre les cybermenaces modernes. La solution consiste à mettre en œuvre des mécanismes de cybersécurité à tous les niveaux de la société. Cependant, cette solution suscite peu d'enthousiasme, soit en raison des coûts qu'elle implique, soit par pure méconnaissance de la question. Pour remédier à cette situation, une première étape consisterait à comparer les capacités des différents Etats en matière de cybersécurité et à publier un classement efficace de leur statut. Un système de classement révélerait toute lacune et encouragerait les Etats à intensifier leurs efforts en matière de cybersécurité. Ce n'est qu'en effectuant des comparaisons que l'on pourra véritablement évaluer la valeur exacte des capacités d'une nation en matière de cybersécurité.

Le projet sur l'Indice de cybersécurité dans le monde (GCI) vise à évaluer avec précision le niveau de développement de chaque pays en matière de cybersécurité. L'objectif ultime est d'encourager une culture mondiale de la cybersécurité et de l'intégrer au cœur même des technologies de l'information et de la communication. Le projet a été lancé par l'Union internationale des télécommunications (UIT) et une entreprise du secteur privé, ABI Research. Le projet sur le GCI se base sur la mission actuelle de l'UIT et les projets et activités associés du Bureau de développement des télécommunications de l'UIT (BDT).

En tant que coordonnateur principal de la grande orientation C5 du SMSI (Sommet mondial sur la société de l'information), l'UIT a pour responsabilité d'aider les parties prenantes à établir la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC) aux niveaux national, régional et international. La mission de l'UIT en matière de cybersécurité bénéficie en outre du soutien de la Résolution 69, qui appelle à la "Création d'équipes nationales d'intervention en cas d'incident informatique en particulier pour les pays en développement, et coopération entre ces équipes" adoptée lors de la cinquième Conférence mondiale de développement des télécommunications (CMDT-10), et par la Résolution 130 (Guadalajara, 2010) intitulée "Renforcement du rôle de l'UIT dans l'instauration de la confiance de la sécurité dans l'utilisation des technologies de l'information et de la communication". Dans ce contexte, le Programme mondial cybersécurité (GCA) a été lancé par le Secrétaire général de l'UIT pour servir de cadre de coopération internationale multi-parties prenantes en vue de créer une société de l'information plus sûre et plus sécurisée. Ce programme porte sur les cinq domaines de travail suivants:

- Cadre juridique

- Mesures techniques
- Structures organisationnelles
- Renforcement des capacités
- Coopération.

Ces cinq domaines d'activités formeront la base des indicateurs du GCI. Ces cinq indicateurs sont essentiels pour évaluer les capacités nationales en matière de cybersécurité parce qu'ils constituent les éléments de base d'une culture nationale. La cybersécurité possède un champ d'application qui recoupe toutes les industries et tous les secteurs, aussi bien verticalement qu'horizontalement. Par conséquent, l'élaboration de capacités nationales exige des investissements par les acteurs politiques, économiques et sociaux. Pour cela, on peut faire appel aux services du maintien de l'ordre et aux Ministères de la justice, aux établissements scolaires et aux Ministères de l'éducation, aux opérateurs du secteur privé et aux développeurs de technologie, aux partenariats public-privé et à la coopération entre Etats.

L'objectif à long terme est d'encourager l'adoption et l'intégration de la cybersécurité à l'échelle mondiale. Une comparaison des stratégies de cybersécurité nationales indiquera quels Etats sont les mieux notés dans certains domaines et mettra en exergue des stratégies moins connues mais qui donnent néanmoins d'excellents résultats. Cela pourra également favoriser le partage des informations sur le déploiement de la cybersécurité pour les Etats à différents niveaux de développement. En mesurant le niveau de préparation à la cybersécurité dans divers domaines, l'indice permettra aux Etats d'évaluer leur position sur une échelle de développement et d'identifier dans quels domaines des améliorations sont nécessaires et le chemin qui leur reste à parcourir pour mettre en œuvre un niveau de cybersécurité adéquat. Tous les Etats évoluant vers un environnement plus numérisé et plus connecté, l'adoption de la cybersécurité en amont permettra de déployer une infrastructure plus sûre et plus résiliente à long terme.

Le projet GCI unira les efforts du BDT – en particulier de la division cybersécurité et applications TIC (CYB) – et d'ABI Research. CYB sera l'interlocuteur principal et le responsable du projet, tandis qu'ABI Research apportera ses compétences fondamentales en matière de développement de stratégies, de veille concurrentielle, de planification commerciale, d'évaluation de la technologie et d'analyse comparative sectorielle pour la réalisation du projet. ABI Research est un bureau d'études de marché spécialiste des prévisions quantitatives et de l'analyse de paramètres et tendances clés des marchés technologiques. ABI Research propose au secteur de la technologie ses compétences uniques en matière d'analyse des tendances et de collecte de données concrètes, actualisées et exploitables. Il mettra cette expertise au service de l'élaboration et de la production d'un indice fiable. Dans le cadre de cet accord, l'UIT et ABI Research cherchent à:

- identifier des paramètres de performance;
- élaborer une méthode de classement mondial;
- effectuer des recherches et collecter des données sur les capacités des Etats en matière de cybersécurité;

- communiquer et rester en contact avec les Etats et les organisations pertinentes;
- identifier et saisir les données pertinentes dans l'indice;
- publier un indice de cybersécurité dans le monde.

Catégories et indicateurs de performance

L'indice GCI permettra de mesurer les capacités nationales en matière de développement de la cybersécurité et d'établir un classement des pays sur la base de ses résultats. Cet outil de référence composite regroupant plusieurs indicateurs analyse le processus de développement de la cybersécurité en fonction de cinq catégories principales, elles-mêmes subdivisées en sous-groupes d'indicateurs (voir ci-après). Les pays seront classés par rapport à la norme de référence fournie pour chaque catégorie.

1. Cadre juridique

La législation constitue une mesure cruciale de la capacité à proposer un cadre harmonisé fournissant aux différentes entités une base réglementaire commune en matière d'interdiction de conduites criminelles spécifiées ou d'obligations réglementaires minimales. Les mesures juridiques permettent également aux pays de définir les mécanismes de base de la réponse aux infractions: enquêtes et poursuites en cas de délits et imposition de sanctions pour non-respect ou violation de la loi. Le cadre juridique fixe les normes générales minimales de comportement applicables à tous, qui rendent possible la consolidation des capacités en matière de cybersécurité. Le but final est que tous les Etats mettent en place une législation permettant d'harmoniser les pratiques au niveau supranational et disposent 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 relatifs à la cybersécurité et à la cybercriminalité. Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

A. Législation pénale

On entend par législation anti-cybercriminalité l'ensemble des lois couvrant l'accès, l'ingérence et l'interception illicites (sans en avoir le droit) en rapport avec le matériel informatique, les systèmes et les données. La législation peut relever d'un des trois niveaux suivants: aucune, partielle ou exhaustive. "Législation partielle" correspond à la simple insertion d'une mention en rapport avec l'informatique dans une loi ou un code pénal existant(e), se limitant à étendre au cyberespace les notions de fraude ou de contrefaçon ou bien de surveillance et de vol, par exemple. "Législation exhaustive" correspond à la promulgation d'une loi spéciale portant sur des aspects spécifiques de la criminalité informatique (par exemple, loi britannique de 1990 sur l'usage abusif de l'informatique). Cette catégorie peut comprendre la législation partielle si la jurisprudence est abondante. Veuillez préciser les types de loi et de réglementation ainsi que leur absence ou bien leur caractère partiel ou exhaustif.

B. Réglementation et conformité

On entend par réglementation relative à la cybersécurité la législation couvrant la protection des données, la notification des infractions et les obligations en matière de certification/normalisation. La réglementation peut relever de l'un des trois niveaux suivants: aucune, partielle ou exhaustive. "Réglementation partielle" correspond à l'insertion d'une mention en rapport avec l'informatique dans une loi pénale ou civile existante ou nouvelle, de

façon que ladite loi s'applique au cyberespace dans une réglementation sans relation spécifique ou exclusive avec la cybersécurité (par exemple, Directive 95/46/CE de l'UE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données). "Réglementation exhaustive" correspond à la promulgation d'une loi ou d'une directive spéciale exigeant spécifiquement le respect de la cybersécurité (par exemple, Loi fédérale américaine de 2002 sur la gestion de la sécurité des informations). Veuillez préciser les types de loi et de réglementation, ainsi que leur absence ou bien leur caractère partiel ou exhaustif.

2. Mesures techniques

La technologie constitue la première ligne de défense contre les cybermenaces et les agents malveillants en ligne. Sans mesures techniques adéquates et sans capacité de détection et de réponse aux cyberattaques, les Etats et leurs entités demeurent vulnérables aux cybermenaces. L'adoption et le succès des TIC ne sont véritablement possibles que dans un climat de confiance et de sécurité. Les Etats doivent donc être capables d'élaborer des stratégies visant à la mise en place de critères de sécurité minimaux reconnus ainsi que de programmes d'accréditation des logiciels et des systèmes. Ces efforts doivent être appuyés par la création d'une entité nationale spécialisée dans la gestion des cyberincidents au niveau du pays, comportant au minimum un organisme public responsable et un cadre national de veille, d'alerte et de réponse aux incidents.

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'Etat. Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

A. Centres de veille, d'alerte et de réponse aux incidents informatiques (CERT/CIRT/CSRIT)

Création de centres de veille, d'alerte et de réponse aux incidents informatiques de type CIRT (équipe d'intervention en cas d'incident informatique), CERT (équipe d'intervention d'urgence en cas d'incident informatique) ou CSIRT (équipe d'intervention en cas d'incident relatif à la sécurité informatique), capables d'identifier les cybermenaces, de les prévenir, d'y répondre, de les gérer et de renforcer la sécurité du cyberespace dans le pays. L'Etat doit associer cette capacité à la collecte de ses propres renseignements et ne pas se fier entièrement au signalement de seconde main des incidents de sécurité par les membres du CIRT ou d'autres sources. Veuillez préciser le nom et le nombre des centres CERT ou CSIRT nationaux ou sectoriels* approuvés et indiquer s'ils sont ou non légalement mandatés. Le classement du niveau de développement dépendra de l'existence ou de l'absence de centres nationaux et d'un mandat légal.

B. Normes

Cet indicateur mesure l'existence d'un ou plusieurs cadres approuvés (ou ratifiés) par le gouvernement concernant l'application des normes internationales en matière de cybersécurité dans le secteur public (administrations) et dans l'infrastructure vitale (même si elle est gérée par le secteur privé). Les normes concernées sont, entre autre, 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. Veuillez préciser les éventuels cadres nationaux (et sectoriels) d'application des normes internationales en matière de cybersécurité approuvés officiellement.

C. Certification

Cet indicateur mesure l'existence d'un ou plusieurs cadres approuvés (ou ratifiés) par le gouvernement concernant la certification et l'accréditation d'organismes nationaux (administrations) et de professionnels du secteur public sur la base de normes internationales en matière de cybersécurité. Ces certifications, accréditations et normes sont, entre autre, 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), (pas de suggestion) Certification, 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), etc. Veuillez préciser les éventuels cadres nationaux (et sectoriels) de certification et d'accréditation des organismes nationaux et des professionnels du secteur public approuvés officiellement.

3. Structures organisationnelles

La mise en œuvre d'une initiative nationale, quelle qu'elle soit, requiert des mesures organisationnelles et procédurales. L'Etat doit fixer un objectif stratégique général donnant lieu à l'établissement d'un plan complet de mise en œuvre, d'exécution et de mesure. Des structures telles que des agences nationales doivent être constituées pour appliquer la stratégie et évaluer la réussite ou l'échec du plan. En l'absence d'une stratégie nationale, d'un modèle de gouvernance et d'un organisme de supervision, les efforts menés dans les différents secteurs et domaines d'activité restent disparates et isolés, contrecarrant toute tentative d'harmonisation nationale du développement des capacités en matière de cybersécurité.

Les critères de mesure des structures organisationnelles sont l'existence et le nombre des institutions et des stratégies organisant le développement de la cybersécurité au niveau national. La création de structures organisationnelles efficaces est nécessaire pour sensibiliser à la cybersécurité, lutter contre la cybercriminalité et promouvoir le rôle de veille, d'alerte et de réponse aux incidents, dans la mesure où elles permettent de coordonner les initiatives nouvelles et existantes au niveau intersectoriel et transfrontalier, ainsi qu'entre les différents organismes. Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

A. Politique

L'élaboration d'une politique de promotion de la cybersécurité est reconnue comme une priorité majeure. La stratégie nationale de sécurité des réseaux et des systèmes d'information doit assurer la résilience et la fiabilité de l'infrastructure informatique et viser à garantir la sécurité des citoyens, protéger les ressources physiques et intellectuelles des citoyens, des organisations et de l'Etat, empêcher les cyberattaques contre les infrastructures vitales, limiter les dégâts dus aux cyberattaques et raccourcir les délais de rétablissement. Les politiques en matière de stratégies nationales de cybersécurité ou de plans nationaux pour la protection des infrastructures informatiques sont celles officiellement définies et approuvées par les Etats. Elles peuvent comprendre les engagements suivants: désigner clairement des responsables de la cybersécurité à tous les niveaux de gouvernement (local, régional et fédéral ou national) dotés de rôles et de responsabilités clairement définis, s'engager clairement dans une

cybersécurité publique et transparente et encourager la participation du secteur privé et les partenariats public-privé dans le cadre des initiatives de promotion de la cybersécurité placées sous l'égide des pouvoirs publics. Veuillez préciser toutes les stratégies nationales ou sectorielles officielles en matière de cybersécurité.

B. Feuille de route relative à la gouvernance

En général, la feuille de route relative à la gouvernance de la cybersécurité est définie par la stratégie/politique nationale en matière de cybersécurité et désigne les principales parties prenantes. L'élaboration d'un cadre politique national constitue une priorité majeure en vue de l'élaboration d'une gouvernance de haut niveau en matière de cybersécurité. Le cadre politique national doit tenir compte des besoins relatifs à la protection de l'infrastructure informatique nationale vitale. Il doit également encourager le partage d'informations au sein du secteur public ainsi qu'entre le secteur public et le secteur privé. Il convient que la gouvernance en matière de cybersécurité s'appuie sur un cadre national abordant les défis et d'autres questions relatives à la sécurité des informations et des réseaux au niveau national, susceptible de comprendre: stratégie et politique nationales, fondements juridiques de la transposition de la législation relative à la sécurité aux environnements en réseau et en ligne, participation de toutes les parties prenantes, élaboration d'une culture de la cybersécurité, procédures de riposte aux violations de sécurité dans les TIC et de gestion des incidents (signalement, partage d'informations, gestion des alertes, collaboration entre le corps judiciaire et les forces de l'ordre), mise en œuvre efficace de la politique nationale en matière de cybersécurité, contrôle, évaluation, validation et optimisation des programmes de cybersécurité. Veuillez préciser les éventuelles feuilles de route nationales ou sectorielles officielles en matière de gouvernance de la cybersécurité.

C. Organisme responsable

L'organisme responsable de la mise en œuvre de la stratégie/politique nationale en matière de cybersécurité peut comprendre des comités permanents, des groupes de travail officiels, des conseils consultatifs et des centres interdisciplinaires. La plupart des organismes nationaux seront directement responsables des systèmes de veille et d'alerte ainsi que de réponse aux incidents, mais aussi de l'élaboration des structures organisationnelles requises pour coordonner les réponses aux cyberattaques. Veuillez préciser les éventuels organismes nationaux ou sectoriels officiels en charge de la cybersécurité.

D. Evaluations comparatives nationales

Cet indicateur mesure l'existence d'exercices d'évaluation comparative nationaux ou sectoriels officiels ou d'un référentiel servant à mesurer le développement de la cybersécurité. Par exemple, une norme de cybersécurité nationale (référentiel CSN) basée sur la norme ISO/CEI 27002-2005 peut aider les Etats à répondre à des exigences spécifiées en matière de cybersécurité. Ce référentiel comporte cinq domaines: stratégies et politiques en matière de cybersécurité nationale, structures organisationnelles de cybersécurité nationale, mise en œuvre de la cybersécurité nationale, coordination nationale, activités de sensibilisation à la cybersécurité. Veuillez préciser les éventuels exercices d'évaluation comparative nationaux ou sectoriels officiels ou le référentiel servant à mesurer le développement de la cybersécurité.

4. Renforcement des capacités

Le renforcement des capacités est intrinsèque aux trois premières catégories de mesure (juridique, technique et organisationnelle). Comprendre la technologie, le risque et les implications peut faciliter l'élaboration d'une meilleure législation, de meilleures politiques et stratégies ainsi qu'une meilleure distribution des divers rôles et responsabilités. La cybersécurité est un domaine relativement nouveau, guère plus âgé qu'Internet lui-même. Elle est abordée le plus souvent sous l'angle de la technologie. Pourtant, elle présente de nombreuses implications socioéconomiques et politiques. Le renforcement des capacités humaines et institutionnelles est nécessaire pour améliorer les connaissances et le savoir-faire dans tous les secteurs, appliquer les solutions les mieux adaptées et promouvoir un niveau de compétence optimal chez les professionnels.

Le renforcement des capacités est intrinsèque aux trois premières catégories de mesure (juridique, technique et organisationnelle). Comprendre la technologie, le risque et les implications peut faciliter l'élaboration d'une meilleure législation, de meilleures politiques et stratégies ainsi qu'une meilleure distribution des divers rôles et responsabilités. La cybersécurité est un domaine relativement nouveau, guère plus âgé qu'Internet lui-même. Elle est abordée le plus souvent sous l'angle de la technologie. Pourtant, elle présente de nombreuses implications socio-économiques et politiques. Le renforcement des capacités humaines et institutionnelles est nécessaire pour améliorer les connaissances et le savoir-faire dans tous les secteurs, appliquer les solutions les mieux adaptées et promouvoir un niveau de compétence optimal chez les professionnels.

A. Normalisation

La normalisation constitue un bon indicateur du niveau de maturité d'une technologie et l'apparition de nouvelles normes dans des domaines clés souligne l'importance vitale de ces instruments. Bien que la cybersécurité ait toujours relevé de la sécurité nationale et fait l'objet d'un traitement différent selon les pays, des normes reconnues par tous facilitent les approches communes. Les normes concernées sont, entre autre, 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. Veuillez préciser les éventuels programmes/projets nationaux ou sectoriels officiels de recherche et développement axés sur les normes, les bonnes pratiques et les lignes directrices en matière de cybersécurité applicables au secteur privé ou public.

B. Développement des compétences des ressources humaines

Le développement des compétences des ressources humaines doit comprendre les efforts déployés par les Etats pour promouvoir des campagnes de publicité à grande échelle visant à toucher le plus grand nombre de personnes possible, mais aussi s'appuyer sur les ONG, les institutions, les organisations, les FSI, les bibliothèques, les organisations du commerce locales, les centres communautaires, les revendeurs d'informatique, les collèges, les programmes d'éducation pour adultes, les écoles et les organisations parents-enseignants pour faire passer les messages relatifs à un comportement sûr en ligne. Concrètement, il peut s'agir de la création de portails et de sites web de sensibilisation, de la diffusion de matériel pédagogique à l'intention des enseignants/formateurs et de la création de cours de formation professionnelle et de programmes éducatifs (ou de mesures incitatives à leur création). Veuillez préciser les éventuels programmes éducatifs et professionnels nationaux ou sectoriels officiels de

sensibilisation du grand public (par exemple, jour, semaine ou mois de sensibilisation nationale à la cybersécurité), promotion de cours sur la cybersécurité dans l'enseignement supérieur (technique, sciences sociales, etc.) et promotion de la certification des professionnels dans le secteur public ou privé.

C. Certification professionnelle

Les critères de mesure de cet indicateur de performance peuvent être le nombre de professionnels du secteur public certifiés conformément aux normes internationales en matière de programmes de certification, dont, entre autre: 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), (pas de suggestion) Certification, 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), (Professional Risk Managers International Association), PMP (Project Management Institute), etc. Veuillez préciser le nombre de professionnels du secteur public certifiés dans le cadre de programmes de certification reconnus sur le plan international.

D. Certification des organismes

Les critères de mesure de cet indicateur de performance peuvent être le nombre d'organismes du secteur public et d'administrations certifiés conformément à des normes internationales. Les normes concernées sont, entre autre, 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. Veuillez préciser le nombre d'administrations et d'organismes du secteur public certifiés conformément à des normes internationales.

5. Coopération internationale

La cybersécurité requérant des informations en provenance de tous les secteurs et de toutes les disciplines, elle doit faire l'objet d'une approche multipartite. Parce qu'elle renforce le dialogue et la coordination, la coopération permet d'élargir le champ d'application de la cybersécurité. Le partage d'informations, déjà difficile entre différentes disciplines et entre opérateurs du secteur privé, l'est encore plus au niveau international. Cependant, le problème de la cybercriminalité est planétaire et ignore les frontières ou les distinctions sectorielles. La coopération permet de partager les informations sur les menaces, les scénarios d'attaques et les bonnes pratiques en matière de réponse et de protection. Des initiatives de coopération élargies peuvent permettre de renforcer considérablement les capacités en matière de cybersécurité, de prévenir la répétition et la persistance des menaces en ligne et d'améliorer les enquêtes, les arrestations et les poursuites à l'encontre des agents malveillants.

Les critères de mesure de la coopération nationale et internationale peuvent être l'existence et le nombre de partenariats, de cadres coopératifs et de réseaux de partage d'informations. Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

A. Coopération entre Etats

La coopération entre Etats fait référence à tout partenariat national ou sectoriel officiel ayant pour objet le partage des ressources en matière de cybersécurité avec d'autres Etats (partenariats bilatéraux ou multilatéraux de coopération ou d'échange d'informations, d'expertise, de technologie et/ou de ressources). Elle comprend aussi des initiatives régionales telles que (entre autre) celles mises en œuvre par l'Union européenne, le Conseil de l'Europe, le G8, l'APEC (Asian Pacific Economic Cooperation), l'OEA (Organisation des Etats américains), l'ANASE (Association des nations de l'Asie du Sud-Est), la Ligue arabe, l'Union africaine, la SCO (Shanghai Cooperation Organization) et les NOG (Network Operations Groups, Groupes opérationnels de réseaux), etc. Veuillez préciser les éventuels partenariats nationaux ou sectoriels officiels de partage des ressources relatives à la cybersécurité avec d'autres Etats.

B. Coopération entre organismes

On entend par coopération entre organismes tout programme national ou sectoriel officiel de partage des ressources en matière de cybersécurité (personnel, processus, outils) au sein du secteur public (partenariats officiels en vue de la coopération ou du partage d'informations, d'expertise, de technologie et/ou de ressources entre départements et organismes, par exemple). Elle comprend des initiatives et des programmes entre différents secteurs (forces de l'ordre, armée, santé, transport, énergie, gestion des déchets et de l'eau, etc.) ainsi qu'au sein des départements/ministères (autorités fédérales/locales, ressources humaines, service informatique, relations publiques, etc.). Veuillez préciser les éventuels programmes nationaux ou sectoriels officiels de partage des ressources en matière de cybersécurité au sein du secteur public.

C. Partenariats public-privé

On entend par partenariats public-privé (PPP) les initiatives associant le secteur public et le secteur privé. Les critères de mesure de cet indicateur de performance peuvent être le nombre de PPP nationaux ou sectoriels officiels de partage des ressources en matière de cybersécurité (personnel, processus, outils) entre le secteur public et le secteur privé (partenariats officiels pour la coopération ou l'échange d'informations, d'expertise, de technologie et/ou de ressources, par exemple). Veuillez préciser les éventuels programmes nationaux ou sectoriels officiels de partage des ressources en matière de cybersécurité entre le secteur public et le secteur privé.

D. Coopération internationale

Cet indicateur de performance mesure la participation officielle à des plates-formes et des forums internationaux sur la cybersécurité. Ces initiatives de coopération comprennent, entre autre, celles menées par l'Assemblée générale des Nations Unies, l'Union internationale des télécommunications (UIT), Interpol/Europol, l'Organisation pour la coopération et le développement économiques (OCDE), l'Office des Nations Unies contre la drogue et le crime (UNODC), l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI), l'ICANN (Internet Corporation for Assigned Names and Numbers), l'Organisation internationale de normalisation (ISO), la Commission électrotechnique internationale (CEI), l'IETF (Internet Engineering Task Force), FIRST (Forum for Incident Response and Security Teams). Veuillez préciser les éventuelles participations officielles à des plateformes et des forums régionaux et/ou internationaux sur la cybersécurité.

Méthodologie

Le modèle statistique utilisé se basera sur une analyse multicritères. Cette analyse établit des préférences entre différentes options par rapport à un ensemble explicite d'objectifs identifiés, pour lesquels il existe des critères mesurables établis pour évaluer le degré d'accomplissement des objectifs. Un modèle additif d'évaluation linéaire simple sera appliqué. La matrice de performances de l'analyse multicritères décrit les options et chaque colonne décrit la performance des options par rapport à chaque critère. L'évaluation individuelle de la performance est numérique.

La notation comparative se basera sur les indicateurs ci-dessous, auxquels la même pondération sera appliquée (à noter que la pondération de certaines sous-catégories sera effectuée à un niveau supérieur étant donné que certains indicateurs contiennent plus de sous-groupes). 0 points sont alloués lorsqu'il n'y a aucune activité ; 1 point est alloué pour une action partielle et 2 points pour une action plus exhaustive. Nombre de points total pour chaque catégorie:

1. Cadre juridique	**4**
A. Législation pénale	2
B. Réglementation et conformité	2
2. Mesures techniques	**6**
A. Centres de veille, d'alerte et de réponse aux incidents informatiques (CERT/CIRT/CSRIT)	2
B. Normes	2
C. Certification	2
3. Structures organisationnelles	**8**
A. Politique	2
B. Feuille de route relative à la gouvernance	2
C. Organisme responsable	2
D. Evaluations comparatives nationales	2
4. Renforcement des capacités	**8**
A. Normalisation	2
B. Développement des compétences des ressources humaines	2
C. Certification professionnelle	2
D. Certification des organismes	2
5. Coopération internationale	**8**
A. Coopération entre Etats	2
B. Coopération entre organismes	2
C. Partenariats public-privé	2
D. Coopération internationale	2

Notation:

x_{qc} Valeur de l'indicateur individuel q pour le pays c, où q = 1,...,Q et c = 1,...,M.

I_{qc} Valeur normalisée de l'indicateur individuel q pour le pays c

CI_c Valeur de l'indicateur composite pour le pays c

Le critère de référence utilisé sera le score du pays hypothétique qui obtiendra le plus grand nombre de points total (34) concernant son degré de préparation. L'indice composite résultant ira de zéro (niveau de préparation le plus bas) à 1 (critère de référence):

$$CI_c = \frac{I_{qc}}{34}$$

La technique de normalisation sera basée sur une méthode de classement:

$I_{qc} = Rang\ (x_{qc})$

Le classement ainsi obtenu sera catalogué par niveaux pour permettre aux pays de déterminer les domaines à améliorer et développer afin de remplir les critères minimums qui leur permettront de passer au niveau suivant:

Niveau 1: Niveau élevé de préparation à la cybersécurité	**Minimum 29 points**
Juridique	Minimum 3 points
Technique	Minimum 5 points
Organisation	Minimum 7 points
Capacité	Minimum 7 points
Coopération	Minimum 7 points
Niveau 2: Niveau intermédiaire de préparation à la cybersécurité	**17-29 points**
Juridique	2-3 points
Technique	3-5 points
Organisation	4-7 points
Capacité	4-7 points
Coopération	4-7 points
Niveau 3: Faible niveau de préparation à la cybersécurité	**Moins de 17 points**
Juridique	Moins de 2 points
Technique	Moins de 3 points
Organisation	Moins de 4 points
Capacité	Moins de 4 points
Coopération	Moins de 4 points

Impact

L'objectif à long terme du GCI est d'encourager l'adoption et l'intégration de la cybersécurité à l'échelle mondiale. Une comparaison des stratégies de cybersécurité nationales indiquera quels Etats sont les mieux classés dans certains domaines et mettra en exergue des stratégies moins connues mais qui donnent néanmoins d'excellents résultats. Cela pourra également favoriser le partage des informations sur le déploiement de la cybersécurité pour les Etats à différents niveaux de développement. En mesurant le niveau de préparation à la cybersécurité dans divers domaines, l'indice permettra aux Etats d'évaluer leur position sur une échelle de développement et d'identifier dans quels domaines des améliorations sont nécessaires et le chemin qui leur reste à parcourir pour mettre en œuvre un niveau de cybersécurité adéquat. Tous les Etats évoluant vers un environnement plus numérisé et connecté, l'adoption de la cybersécurité en amont permettra de déployer une infrastructure plus sûre et plus résiliente.