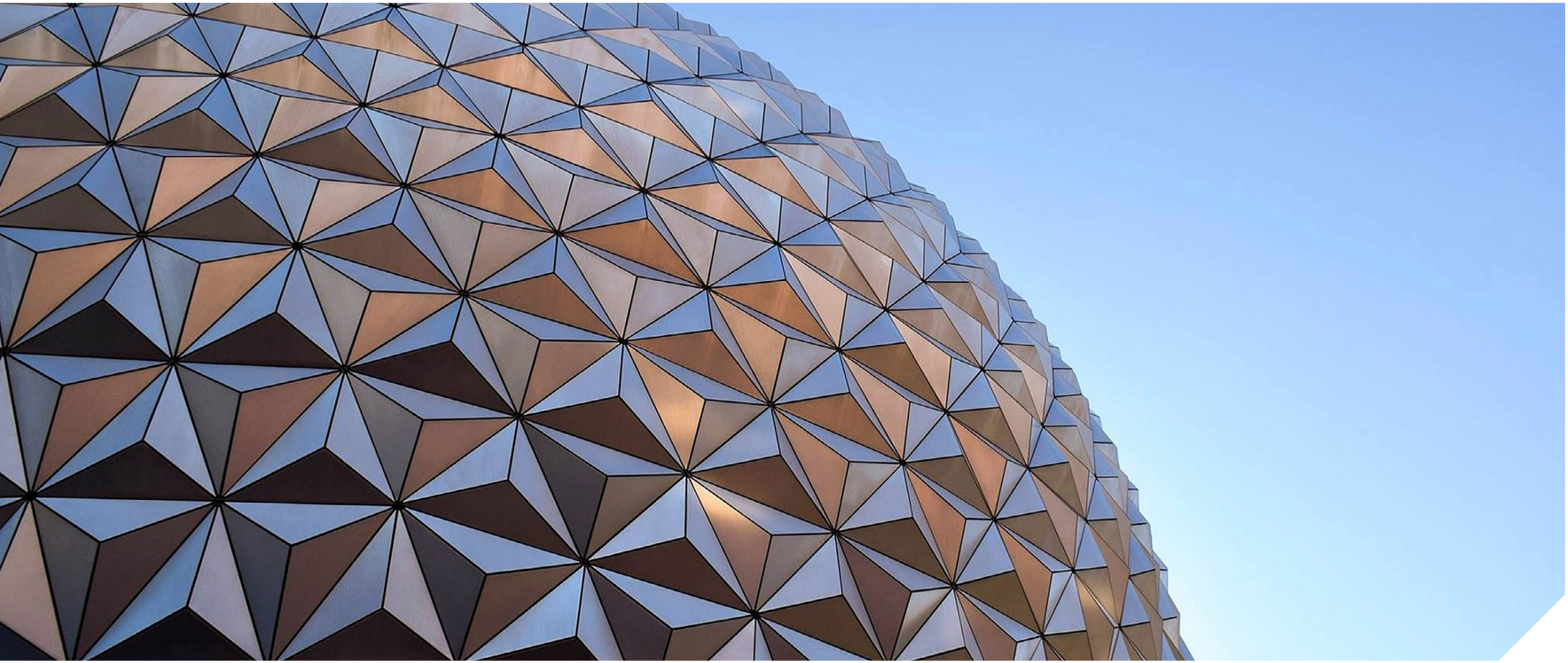
Global
Cyber Security
Capacity Centre



Modèle de Maturité de la Capacité de Cybersécurité pour les Nations (CMM)

Édition 2021

Résumé

Les économies du monde entier continuent de se développer en dépendant de plus en plus de la technologie. Si nous ne veillons pas à ce que des capacités de cybersécurité existent dans l'ensemble du cyberespace, nous créerons inévitablement des cyberghettos. Dans de tels environnements, les cybermenaces peuvent devenir monnaie courante et les cyberattaques peuvent être facilement lancées. L'aptitude des pays à réagir et à accroître leurs capacités face à l'évolution des menaces — qu'elles soient dues aux tendances de l'utilisation des technologies, au climat sociopolitique ou à l'évolution de l'écosystème des acteurs de la menace — n'a jamais été aussi importante.

Le modèle de maturité de la capacité de cybersécurité pour les nations (CMM, Cybersecurity Capacity Maturity Model for Nations) aide les nations à comprendre ce qui fonctionne, ce qui ne fonctionne pas ainsi que le pourquoi, dans tous les domaines des capacités nationales en matière de cybersécurité. C'est important pour que les gouvernements et les entreprises puissent adopter des politiques et faire des investissements susceptibles d'améliorer considérablement la sûreté et la sécurité dans le cyberespace, tout en respectant les droits de l'homme, tels que la vie privée et la liberté d'expression.

Depuis 2015, le Centre mondial des capacités en matière de cybersécurité (GCSCC, Global Cyber Security Capacity Centre) a activement promu le CMM dans tous les secteurs, afin d'alimenter la conversation autour des capacités nationales en matière de cybersécurité et de contribuer à améliorer la technologie mondiale. L'adoption du CMM qui en a résulté par diverses parties prenantes internationales majeures, et la réalisation de plus de 120 examens du CMM dans plus de 85 pays, démontre l'impact positif de la recherche, soutient les auto-évaluations des gouvernements et informe sur le développement d'outils et de ressources du secteur.

Poussé par l'évolution du paysage des menaces et des pratiques de cybersécurité correspondantes, le GCSCC a mené une révision du CMM, la première à être réalisée depuis la publication de l'édition 2016. Pour produire cette édition 2021, le GCSCC a entrepris un exercice de coopération mondiale visant à extraire et synthétiser les dernières connaissances de la communauté. Le GCSCC a élaboré des propositions de changement basées sur les enseignements tirés des déploiements du CMM, et a entrepris une série de consultations en ligne et hors ligne avec des experts, pour valider les résultats et discuter des changements. Les personnes consultées comprennent le groupe consultatif d'experts du GCSCC, les partenaires stratégiques, régionaux et de mise en œuvre du GCSCC, ainsi que d'autres experts issus du monde universitaire, d'organisations internationales et régionales, de gouvernements, du secteur privé et de la société civile. Sur la base de leur contribution, des indicateurs pour chaque *aspect* ont été identifiés, conçus, affinés et validés.

Les acteurs du monde entier, qu'il s'agisse d'individus ou d'États-nations, doivent veiller à ce que le cyberespace et les systèmes qui en dépendent soient résistants aux attaques croissantes. L'*édition 2021 du CMM* et son déploiement continueront de contribuer aux efforts visant à atteindre cette résilience, non seulement en acquérant une compréhension plus approfondie de la capacité en matière de cybersécurité internationale, mais aussi en augmentant l'investissement effectif dans les capacités nationales en matière de cybersécurité sur la base d'une analyse rigoureuse des données recueillies lors du déploiement du modèle. Les lacunes critiques dans tous les domaines de la cybersécurité internationale seront identifiées et comblées par des contre-mesures évolutives et efficaces, en coopération avec des partenaires internationaux de la communauté mondiale de la cybersécurité.

Sommaire

Une évaluation nationale de la cybersécurité avec le CMM

L'examen du CMM d'un pays implique la collecte de données par une équipe de chercheurs qui mènent des consultations avec les parties prenantes dans le pays et des recherches documentaires. Le résultat est un rapport fondé sur des preuves qui :

- permet d'évaluer la maturité de la capacité d'un pays en matière de cybersécurité ;
- détaille un ensemble pragmatique d'actions visant à contribuer à combler les lacunes en matière de maturité des capacités de cybersécurité ; et
- identifie les priorités en matière d'investissement et de renforcement des capacités futures, sur la base des besoins spécifiques d'un pays.

Selon une étude indépendante commandée par *UK Foreign and Commonwealth Office (FCDO, le Bureau des Affaires étrangères, du Commonwealth et du Développement du Royaume-Uni)*, les avantages d'un examen du CMM pour un pays sont nombreux et comprennent notamment :

- une sensibilisation accrue à la cybersécurité et un renforcement des capacités, ainsi qu'une plus grande coopération au sein du gouvernement ;
- la mise en réseau et la coopération avec les entreprises et la Société au sens large ;
- le renforcement de la crédibilité interne des objectifs de la cybersécurité au sein des gouvernements ;
- une aide à définir les rôles et les responsabilités au sein des gouvernements ;
- une mise à disposition des preuves pour augmenter le financement du renforcement des capacités en matière de cybersécurité ; et
- une base pour l'élaboration de stratégies et de politiques nationales.

Il est important qu'un pays puisse prouver ses réalisations en matière de cybersécurité et le CMM définit ce que doivent être ces preuves et ce qu'elles démontrent. Cette collecte de preuves est en soi un processus multipartite, impliquant un large éventail de sources et d'organisations. Les discussions peuvent être importantes pour résoudre les divergences d'opinions. Le pays qui entreprend l'examen décidera si ces discussions peuvent être efficaces si elles sont menées à distance (et en ligne), ou si elles nécessitent des réunions en présentiel.

Pour plus d'informations sur la méthodologie et le processus d'examen du CMM et sur les rapports exemplaires du CMM, consultez le site: https://gcscc.ox.ac.uk/the-cmm

Les dimensions de la capacité nationale en matière de cybersécurité

Le CMM considère que la cybersécurité comprend cinq *dimensions* qui, ensemble, constituent l'étendue de la capacité nationale dont un pays a besoin pour être efficace en matière de cybersécurité :

1. **Développer une politique et une stratégie de cybersécurité ;**
2. **Encourager une culture responsable de la cybersécurité au sein de la Société ;**
3. **Renforcer les connaissances et les capacités en matière de cybersécurité ;**
4. **Créer des cadres juridiques et réglementaires efficaces ; et**
5. **Maîtriser les risques grâce aux normes et aux technologies.**

***La 1ère dimension :* Politique et stratégie en matière de cybersécurité** examine la capacité du pays à élaborer et à mettre en œuvre une stratégie de cybersécurité, et à renforcer sa résilience en matière de cybersécurité en améliorant ses capacités de réponse aux incidents, de cyberdéfense et de protection des infrastructures critiques (IC). Cette *dimension* examine l'efficacité de la stratégie et de la politique dans la mise en place d'une capacité nationale de cybersécurité, tout en maintenant les avantages d'un cyberespace vital pour le gouvernement, les entreprises internationales et la société en général.

***La 2e dimension :* Culture et Société de la cybersécurité** passe en revue les éléments importants d'une culture de cybersécurité responsable, tels que la compréhension des risques liés à la cybercriminalité dans la Société, le niveau de confiance dans les services Internet, l'administration en ligne et les services de commerce électronique, et la compréhension par les utilisateurs de la protection des informations personnelles en ligne. En outre, cette *dimension* explore l'existence de mécanismes de signalement fonctionnant comme des canaux permettant aux utilisateurs de signaler la cybercriminalité. En outre, cette *dimension* examine le rôle des médias et des réseaux sociaux dans la formation des valeurs, des attitudes et des comportements en matière de cybersécurité.

***La 3e dimension :* Renforcer les connaissances et les capacités en matière de cybersécurité** rexamine la disponibilité, la qualité et l'adoption de programmes destinés aux différents groupes de parties prenantes, notamment le gouvernement, le secteur privé et la population dans son ensemble, et concerne les programmes de sensibilisation à la cybersécurité, les programmes éducatifs formels en matière de cybersécurité et les programmes de formation professionnelle.

***La 4e dimension :* Cadres juridiques et réglementaire** examine la capacité des pouvoirs publics à concevoir et à promulguer des lois nationales ayant un rapport direct et indirect avec la cybersécurité, en mettant l'accent en particulier sur les exigences réglementaires en matière de cybersécurité, les lois relatives à la cybercriminalité et les lois connexes. La capacité à faire appliquer ces lois est examinée par le biais des capacités des services répressifs, des poursuites judiciaires, des organismes de réglementation et des tribunaux. En outre, cette *dimension* observe des questions telles que les cadres de coopération formels et informels pour lutter contre la cybercriminalité.

***La 5e dimension :* Normes et technologies** porte sur l'utilisation efficace et généralisée des technologies de cybersécurité pour protéger les personnes, les organisations et les infrastructures nationales. Cette *dimension* examine spécifiquement la mise en œuvre de normes et de bonnes pratiques en matière de cybersécurité, le déploiement de processus et de contrôles, ainsi que le développement de technologies et de produits afin de réduire les risques liés à la cybersécurité.

Le CMM définit cinq stades de maturité pour toutes les *dimensions* : démarrage, formation, établi, stratégie et dynamique. Ces stades correspondent aux éléments suivants : développement initial de la capacité, implémentation, leadership mondial et capacité à anticiper et à se préparer aux besoins futurs en matière de cybersécurité.

Il convient de noter qu'il existe des relations entre les *dimensions* ; par exemple, pour être efficace dans un domaine, il faut souvent répondre à des exigences dans d'autres domaines. Il est également vrai que les ressources sont limitées et que les priorités en matière de renforcement des capacités sont susceptibles d'exiger une réponse qui pourrait couvrir plusieurs *dimensions*. Par conséquent, une activité de test de performance examine un pays par rapport à l'ensemble du CMM et à travers toutes les *dimensions*, permettant une considération holistique de la capacité nationale.

[1] Pour qu'un pays atteigne un niveau de maturité mis en œuvre sous *l'aspect* « Initiatives des pouvoirs publics » du *facteur* 3.1 « Sensibilisation à la cybersécurité », l'une des conditions à remplir est que le contenu du programme national coordonné de sensibilisation à la cybersécurité comporte des liens explicites avec la stratégie nationale en matière de cybersécurité. De même, pour qu'un pays atteigne un niveau de maturité mis en œuvre sous l'*aspect* « Administration » du *facteur* 3.2 Éducation à la cybersécurité, les priorités en matière d'éducation à la cybersécurité résultant du processus de consultation. multipartite doivent être reflétées dans la stratégie nationale de cybersécurité.

La structure du CMM

Dimension :

les cinq *dimensions* couvrent l'ensemble des capacités nationales en matière de cybersécurité évaluées par le CMM. Chaque *dimension* est constituée d'une série de *facteurs*, qui reflètent les capacités essentielles requises pour la réaliser. Ensemble, ils représentent les différents « objectifs » à travers lesquelles les capacités nationales en matière de cybersécurité peuvent être démontrées et analysées ;

Facteur :

au sein des cinq *dimensions*, les *facteurs* décrivent ce que signifie posséder des capacités nationales en matière de cybersécurité. Ce sont les éléments essentiels de la capacité nationale, qui sont ensuite mesurés pour *stade d*e maturité. La liste complète des *facteurs* vise à intégrer de manière holistique tous les besoins d'une nation en matière de capacités nationales en matière de cybersécurité. La plupart des *facteurs* sont composés d'un certain nombre d'*aspects* qui structurent les *indicateurs* du *facteur* en parties plus concises (qui sont directement liées à la collecte et à la mesure des preuves). Cependant, certains *facteurs*, dont la portée est plus limitée, n'ont pas d'*aspects* spécifiques ;

Aspect :

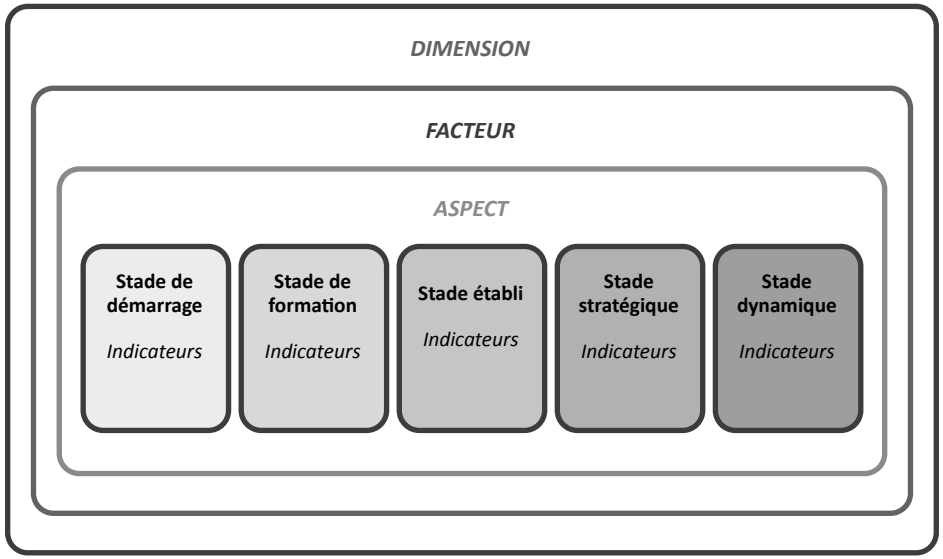
lorsqu'un *facteur* possède plusieurs composantes, il s'agit d'*aspects*. Les *aspects* sont une méthode d'organisation permettant de diviser les *indicateurs* en groupes plus petits, plus faciles à comprendre. Le nombre d'*aspects* dépend des thèmes qui émergent du contenu du *facteur* et de la complexité globale du *facteur* ;

Stade :

Les *stades* définissent le degré de progression d'un pays par rapport à un certain *facteur* ou aspect des capacités nationales en matière de cybersécurité. Le CMM comprend cinq *stades* distincts: démarrage, formation, établi, stratégique, dynamique (voir page 8). L'examen du CMM permettra d'évaluer un pays par rapport à ces *stades*, en tenant compte des capacités nationales en matière de cybersécurité existantes, à partir desquelles un pays peut s'améliorer ou décliner en fonction des mesures prises (ou non). Pour chaque stade, il existe un certain nombre d'*indicateurs* qu'un pays doit remplir pour avoir atteint ce stade.

Indicateur :

Les *indicateurs* représentent la partie la plus fondamentale de la structure du CMM. Chaque *indicateur* décrit les stades, les actions ou les blocs de construction qui sont indicatifs d'un *stade de* maturité spécifique. Pour atteindre un stade *de* maturité, un pays devra se convaincre qu'il peut prouver chacun de ces *indicateurs*. Afin d'élever le niveau de maturité des capacités nationales en matière de cybersécurité d'un pays, tous les *indicateurs* d'un stade particulier devront avoir été atteints. La plupart de ces *indicateurs* sont de nature binaire, c'est-à-dire que le pays peut soit prouver qu'il a rempli les critères de l'*indicateur*, soit ne peut pas fournir cette preuve.



Les stades de la capacité nationale en matière de cybersécurité

Les *stades* définissent le degré de progression d'un pays par rapport à un certain *facteur* ou *aspect des* capacités nationales en matière de cybersécurité (voir page 6). L'examen du CMM permet de comparer un pays à ces *stades* et de déterminer les capacités nationales en matière de cybersécurité.

Stade de démarrage :

lors de ce stade, soit la maturité en matière de cybersécurité n'existe pas, soit elle est de nature très embryonnaire. Il peut y avoir des discussions initiales sur le renforcement des capacités en matière de cybersécurité, mais aucune action concrète n'a été prise. Il peut y avoir une absence de preuves observables lors de ce stade ;

Stade de formation :

certaines caractéristiques de l'*aspect* ont commencé à se développer et à être formulées, mais peuvent être désorganisées, mal définies, simplement nouvelles ou non systématiques. Cependant, les preuves de cette activité peuvent être clairement démontrées ;

Stade établi:

les *indicateurs* de l'aspect sont en place, et les preuves montrent qu'ils fonctionnent. Il n'y a cependant pas de réflexion approfondie sur l'allocation relative des ressources. Peu de décisions de compromis ont été prises concernant l'investissement relatif dans les différents éléments de l'*aspect*. Mais l'*aspect* est fonctionnel et défini ;

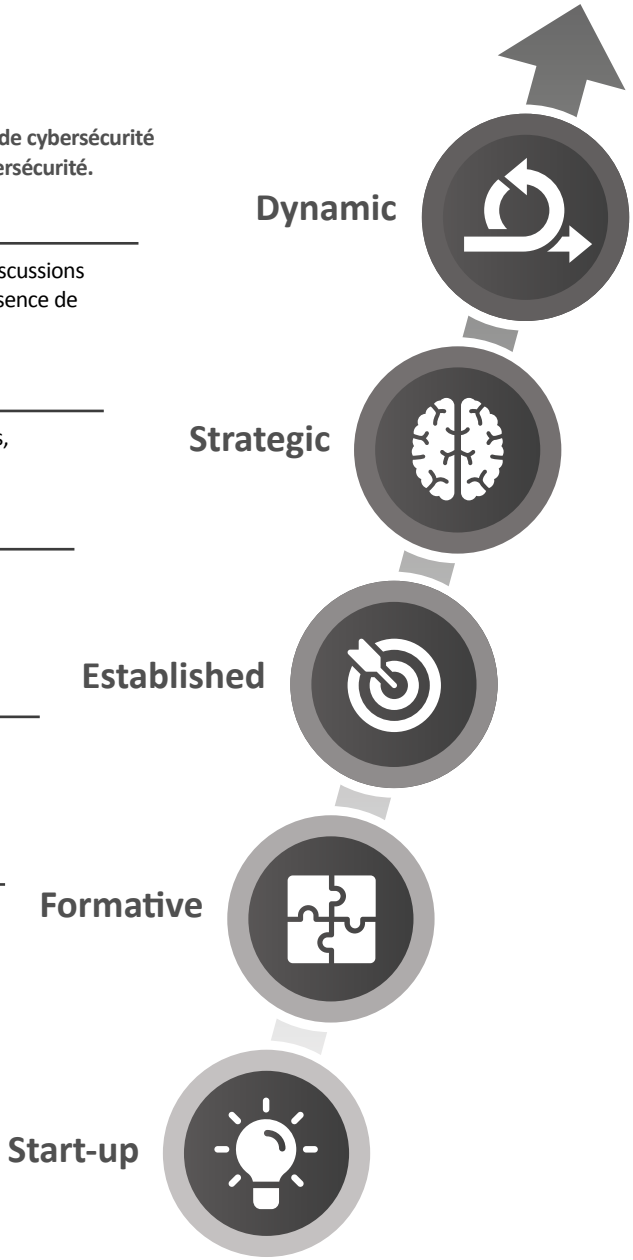
Stade stratégique :

des choix ont été faits quant aux parties de l'*aspect qui* sont importantes et à celles qui le sont moins pour l'organisation ou la nation concernée. Le stade stratégique reflète le fait que ces choix ont été faits, en fonction des circonstances particulières de la nation ou de l'organisation ; et

Stade dynamique :

lors de ce stade, *il* existe des mécanismes clairs permettant de modifier la stratégie nationale en fonction des circonstances, telles que la technologie de l'environnement de la menace, un conflit mondial ou un changement important dans un domaine de préoccupation (par exemple, la cybercriminalité ou la vie privée). Il existe également des preuves d'un leadership mondial sur les questions de cybersécurité. Les secteurs clés, du moins, ont conçu des méthodes permettant de modifier les stratégies à tout moment de leur développement. La prise de décision rapide, la réaffectation des ressources et l'attention constante portée à l'évolution de l'environnement sont des caractéristiques de ce stade.

Le CMM permet de comparer les capacités nationales actuelles en matière de cybersécurité. Comprendre les exigences pour atteindre des niveaux de capacité plus élevés indiquera directement les domaines dans lesquels il faut investir davantage, et la manière de prouver ces niveaux de capacité. Le CMM peut également servir à élaborer des analyses de rentabilité pour les investissements et les améliorations de performance attendues. En combinant un examen du CMM avec des évaluations nationales des risques et des stratégies sociales et économiques, il est possible de mieux hiérarchiser les améliorations à apporter aux capacités.



1ère Dimension : Politique et stratégie en matière de cybersécurité

Cette *dimension* explore la capacité du pays à élaborer et à mettre en œuvre une stratégie de cybersécurité et à renforcer sa résilience en matière de cybersécurité en améliorant ses capacités de réponse aux incidents, de cyberdéfense et de protection des infrastructures critiques. Cette *dimension* examine l'efficacité de la stratégie et de la politique dans la mise en place d'une capacité nationale de cybersécurité, tout en maintenant les avantages d'un cyberespace vital pour le gouvernement, les entreprises internationales et la société en général.

Facteur
D 1.1 : Stratégie nationale de cybersécurité

La stratégie en matière de cybersécurité est essentielle à l'intégration d'un programme de cybersécurité dans l'ensemble du gouvernement, car elle permet de donner la priorité à la cybersécurité en tant que domaine d'action important, de déterminer les responsabilités et les mandats des principaux acteurs gouvernementaux et non gouvernementaux en matière de cybersécurité et d'orienter l'affectation des ressources vers les questions et les priorités émergentes et existantes en matière de cybersécurité.
> Navigate to Factor

Aspects

- **Élaboration de la stratégie :** cet *aspect* concerne l'élaboration d'une stratégie nationale, la répartition des pouvoirs de mise en œuvre entre les secteurs et la société civile, et une compréhension des risques et des menaces en matière de cybersécurité au niveau national, ce qui favorise le renforcement des capacités au niveau national ;
- **Contenu :** Cet *aspect* concerne le contenu de la stratégie nationale de cybersécurité et s'il est explicitement lié aux risques, priorités et objectifs nationaux tels que la sécurité nationale, la sensibilisation du public, l'atténuation de la cybercriminalité, la capacité de réponse aux incidents et la protection des infrastructures nationales critiques ;
- **Mise en œuvre et examen :** cet *aspect* concerne l'existence d'un programme global de coordination de la cybersécurité, comprenant un propriétaire ou un organisme de coordination ministériel doté d'un budget consolidé ; et
- **Engagement international :** cet *aspect* examine dans quelle mesure le pays est conscient de l'existence de discussions internationales sur la politique de cybersécurité, et comment les débats internationaux sur la politique de cybersécurité et les questions connexes affectent les intérêts du pays et son statut international. standing.

Facteur
D 1.2 : Réponse aux incidents et gestion de crise

Ce *facteur* traite de la capacité du gouvernement à identifier et à déterminer les caractéristiques des incidents de niveau national de manière systématique. Il examine également la capacité du gouvernement à organiser, coordonner et rendre opérationnelle la réponse aux incidents, et si la cybersécurité a été intégrée dans le cadre national de gestion de crise.
> Navigate to Factor

Aspects

- **Identification et catégorisation des incidents :** cet *aspect* identifie si des mécanismes internes sont en place pour identifier et catégoriser les incidents ;
- **Organisation :** cet *aspect* traite de l'existence d'un organisme central mandaté pour recueillir les informations sur les incidents, et de sa relation avec les secteurs public et privé pour la réponse aux incidents au niveau national ; et
- **Intégration de la cybersécurité dans la gestion nationale des crises :** cet *aspect* examine dans quelle mesure la cybersécurité est intégrée dans le cadre de la gestion nationale des crises.

Facteur

D 1.3 : Protection des infrastructures critiques (IC)

Ce *facteur* étudie la capacité du gouvernement à identifier les actifs des IC, les exigences réglementaires spécifiques à la cybersécurité des IC, et la mise en œuvre de bonnes pratiques de cybersécurité par les opérateurs d'IC.
> Navigate to Factor

Aspects

- **Identification :** cet *aspect* concerne l'existence d'une liste générale des actifs, secteurs et opérateurs d'infrastructures critiques, ainsi qu'un audit régulier des actifs d'infrastructures critiques ;
- **Exigences réglementaires :** cet *aspect* traite de l'existence d'exigences réglementaires spécifiques à la cybersécurité des IC ; et
- **Pratiques opérationnelles :** cet *aspect* examine si les opérateurs d'infrastructures critiques mettent en œuvre des normes industrielles reconnues, et l'existence d'accords de coopération entre et au sein des secteurs.

Facteur

D 1.4 : La cybersécurité dans la défense et la sécurité nationale

Ce *facteur* examine si le gouvernement a la capacité de concevoir et de mettre en œuvre une stratégie de cybersécurité au sein de la sécurité nationale et de la défense. Il examine également le niveau des capacités nationales en matière de cybersécurité au sein de l'établissement de sécurité nationale et de défense, ainsi que les accords de coopération en matière de cybersécurité entre les entités civiles et de défense.
> Navigate to Factor

Aspects

- **Stratégie de cybersécurité des forces de défense :** cet *aspect* porte sur l'existence d'une stratégie de soutien à la cybersécurité au sein de la sécurité nationale et de la défense, et si elle est soutenue par les autorités juridiques appropriées et la doctrine opérationnelle et les règles d'engagement pertinentes ;
- **Capacités nationales en matière de cybersécurité des forces de défense :** cet *aspect* examine le niveau des capacités nationales en matière de cybersécurité et les structures organisationnelles au sein de l'établissement de sécurité nationale ; et
- **Coordination de la défense civile :** cet *aspect* examine la coopération en matière de cybersécurité entre les entités civiles et de défense, ainsi que l'existence de ressources adéquates.

Facteur - D 1.1 : Stratégie nationale de cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Développement de la stratégie	Il n'existe pas de stratégie nationale de cybersécurité, bien que les processus de planification pour l'élaboration d'une stratégie aient peut-être commencé. Des conseils peuvent avoir été demandés à des partenaires internationaux.	Les processus d'élaboration de la stratégie ont été lancés. Une ébauche de stratégie nationale en matière de cybersécurité a été élaborée. Des processus de consultation ont été convenus pour les principaux groupes de parties prenantes, notamment le secteur privé, la société civile et les partenaires internationaux	Une stratégie nationale de cybersécurité a été publiée. Une évaluation du risque de cybersécurité nationale spécifique à chaque pays a été réalisée. La stratégie reflète les besoins et les rôles des parties prenantes concernées au sein du gouvernement (national et infranational), des entreprises et de la société civile. Un programme de mise en œuvre est en place et couvre le champ d'application de la stratégie. Des mécanismes sont en place pour permettre aux « propriétaires » de la stratégie de contrôler la réalisation des résultats, de traiter les problèmes de mise en œuvre et de maintenir l'alignement de la stratégie.	Des processus de révision et de renouvellement de la stratégie sont en place. Les risques émergents en matière de cybersécurité sont régulièrement évalués et utilisés pour mettre à jour la stratégie et le plan de mise en œuvre. L'impact de la stratégie sur la réduction des risques et des dommages est compris et utilisé pour informer les décisions de financement et de priorité.	La stratégie nationale de cybersécurité et le plan de mise en œuvre sont tous deux revus de manière proactive afin de tenir compte des évolutions stratégiques plus larges du pays (politiques, économiques, sociales, techniques, juridiques et environnementales). Le pays est une autorité reconnue au sein de la communauté internationale et soutient le développement de stratégies nationales et mondiales en matière de cybersécurité. Les considérations relatives à la cybersécurité sont intégrées dans d'autres stratégies et programmes de mise en œuvre pertinents au niveau national.
Contenu	Il peut exister diverses politiques et stratégies nationales faisant référence à la cybersécurité, mais elles ne sont pas exhaustives et rien ne prouve qu'elles reflètent les priorités et les circonstances nationales spécifiques.	Il existe un contenu qui reflète les priorités et les circonstances propres à chaque pays. Des liens existent entre la stratégie (ou le projet de stratégie) et des priorités telles que la sécurité nationale, la stratégie numérique et le développement économique, mais ils sont généralement au coup par coup et manquent de détails. La stratégie (ou le projet de stratégie) définit les principaux résultats par rapport auxquels le succès peut être évalué.	Le contenu de la stratégie nationale de cybersécurité est basé sur une évaluation complète des risques qui comprend des liens explicites avec des politiques et stratégies économiques et politiques plus larges au niveau national. Le contenu comprend des actions visant à sensibiliser le public et les entreprises, à atténuer la cybercriminalité, à établir une capacité de réponse aux incidents, à promouvoir le partenariat public-privé et à protéger les infrastructures critiques et l'économie au sens large. La manière dont la stratégie nationale de cybersécurité pourrait intégrer ou soutenir des objectifs politiques en ligne plus larges, tels que la protection des enfants, la promotion des droits de l'homme, la promotion de l'égalité, de la diversité et de l'inclusion, et la gestion de la désinformation a été examinée.	Le contenu tient compte de l'impact sur le risque de cybersécurité des technologies émergentes et de leur utilisation au sein des infrastructures critiques, l'économie au sens large et la société. Les résultats définis dans la stratégie sont spécifiques et mesurables. Des paramètres ont été définis pour permettre aux parties prenantes d'évaluer l'efficacité de la stratégie en matière de réduction des dommages. Une réflexion a été menée sur la manière dont les résultats bénéfiques de la stratégie peuvent être maintenus au-delà de la durée de vie de la stratégie, y compris la manière dont le maintien des nouvelles capacités sera financé.	Le contenu tient compte de l'impact de développements plus larges sur le risque de cybersécurité (politique, économique, social, technique, juridique et environnemental). Le contenu de la stratégie nationale de cybersécurité favorise et encourage la coopération bilatérale et multilatérale entre les pays afin de garantir un cyberespace sûr, résilient et fiable.

Facteur - D 1.1 : Stratégie nationale de cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Mise en œuvre et révision	Aucun programme national global de mise en œuvre de la cybersécurité n'a été élaboré.	de mise en œuvre de la cybersécurité est en cours d'élaboration avec la participation des acteurs concernés, notamment le secteur privé et la société civile. Les actions du programme ont été attribuées à des « responsables » spécifiques, mais la disponibilité des ressources adéquates n'a pas encore été confirmée. Les mécanismes d'examen des processus sont limités ou ne sont pas systématiques.	Un plan de mise en œuvre détaillé a été publié, comprenant des actions, des entités responsables et des budgets de ressources. Le plan de mise en œuvre implique les parties prenantes concernées au sein du gouvernement et d'autres secteurs. Un organisme de coordination a été désigné. Cet organisme dispose d'une autorité suffisante pour veiller à ce que les « responsables » des actions soient tenus de rendre des comptes. Les ressources nécessaires à la réalisation des actions du programme ont été identifiées et sont en place. Les déficits budgétaires sont identifiés et transmis à l'autorité compétente. Des processus de révision du programme et des paramètres sont en place pour permettre de mesurer les progrès et de transmettre les risques, les problèmes et les dépendances à l'autorité compétente. Ces processus sont financés de manière adéquate.	Des mesures axées sur les résultats sont utilisées pour surveiller l'impact du programme sur la réduction des risques (et d'autres objectifs stratégiques pertinents). Il existe des preuves que ces mesures sont utilisées pour affiner les plans d'action. Les paramètres (tant ceux qui concernent les progrès que ceux axés sur les résultats) proviennent d'un large éventail de sources gouvernementales, non gouvernementales et internationales. Il existe une supervision et/ou une garantie indépendante du programme.	Des mécanismes sont en place pour apporter des modifications plus profondes au programme en cas de changements importants des circonstances (politiques, économiques, sociales, techniques, juridiques et environnementales). Le programme contribue au développement mondial de mesures axées sur les résultats et à leur application.
Engagement international	La connaissance des principaux débats internationaux relatifs à la politique de cybersécurité (tels que les normes de cybersécurité, l'entraide judiciaire mutuelle, la gouvernance de l'Internet, la souveraineté des données, la protection des données) est limitée. Le pays peut bénéficier des réseaux de collaboration opérationnelle régionaux/internationaux, mais ne s'y engage pas activement.	Le pays est conscient de l'existence de discussions internationales sur la politique de cybersécurité et les questions connexes. Le pays peut, à l'occasion, participer à des discussions régionales ou internationales sur des questions liées à la cybersécurité, mais ne joue généralement pas un rôle actif. Le pays peut participer à la collaboration opérationnelle et aux organes politiques pertinents (tels que FIRST*, les organes régionaux de CERT**, le FGI*** ou le GGE**** des Nations unies), mais il joue principalement un rôle passif.	Une évaluation a été faite sur la manière dont les débats internationaux sur la politique de cybersécurité et les questions connexes affectent les intérêts et la position internationale du pays. Des objectifs d'engagement spécifiques ont été définis en conséquence. De multiples parties prenantes ont été impliquées dans ce processus. Le pays participe activement aux instances et forums internationaux pertinents, soit directement, soit par l'intermédiaire d'organes représentatifs. Leurs voix sont entendues et ont un impact. Le pays contribue activement à la collaboration opérationnelle régionale/internationale et aux organes politiques.	Le pays s'emploie activement à créer des communautés d'intérêt internationales autour d'objectifs politiques spécifiques en matière de cybersécurité et à promouvoir leur adoption. Le pays apporte une contribution importante aux organes opérationnels régionaux/internationaux et participe activement au renforcement des capacités dans les pays tiers.	Le pays est un acteur de premier plan dans la recherche d'un consensus, la promotion de l'inclusivité et l'orientation des débats internationaux sur les principales questions de politique de cybersécurité. Le pays se concentre sur l'avenir, voit les questions émergentes (autour des nouvelles technologies ou des nouveaux types de menaces) et lance de nouveaux débats internationaux autour des questions clés. Le pays participe activement à la création de nouveaux mécanismes de collaboration régionale/internationale.

*Forum des équipes de réponse aux incidents et de sécurité ** Computer Emergency Response Team (Équipe d'intervention en cas d'urgence informatique)
*** Forum sur la gouvernance de l'Internet **** Le groupe d'experts gouvernementaux des Nations Unies

Facteur - D 1.2 : Réponse aux incidents et gestion de crise

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Identification et catégorisation des incidents	Il n'existe aucun processus d'identification et de catégorisation des incidents au niveau national.	Certaines organisations et certains secteurs disposent de mécanismes internes pour identifier et classer les incidents qui relèvent de leur compétence. Un processus d'identification des incidents au niveau national est en cours d'élaboration. Il n'y a pas de registre central en place, mais des arrangements au coup par coup existent pour traiter les événements les plus importants.	La plupart des grandes organisations disposent de mécanismes internes pour identifier et classer les incidents. Il existe un registre central des incidents de cybersécurité au niveau national et un processus de remontée rapide des incidents, du niveau organisationnel au niveau national, est en place. Les incidents nationaux individuels sont classés en fonction de leur gravité et les ressources sont allouées en conséquence.	Les enseignements tirés des incidents survenus au niveau national sont systématiquement analysés afin d'en tirer des enseignements et d'éclairer la politique et la stratégie de cybersécurité au sens large.	Les critères de classement des incidents sont suffisamment souples pour tenir compte de l'évolution rapide de l'environnement technologique ou des menaces sous-jacentes. Le pays contribue aux meilleures pratiques internationales en matière d'identification et de catégorisation des incidents.
Organisation	Il n'existe aucune organisation pour la réponse aux cyberincidents au niveau national. Quelques organisations peuvent avoir mis en place des mécanismes internes de réponse à la cybersécurité, mais la coordination est minimale.	Une CERT* nationale peut exister, mais ne dispose pas de ressources et de compétences suffisantes. Les processus de gestion des incidents sont encore en cours de développement. Certaines organisations des secteurs public et privé ont mis en place des mécanismes internes de réponse à la cybersécurité, mais la coordination avec la CERT nationale n'est pas systématique. Le rôle des organismes infranationaux n'est pas clair. La coopération bilatérale avec les partenaires internationaux est limitée ou au coup par coup.	Un organisme national de réponse aux incidents a été créé. Il dispose des ressources, des compétences, des processus documentés et des autorisations légales nécessaires pour faire face à l'ensemble des scénarios de cyberincidents auxquels le pays est susceptible d'être confronté (y compris les capacités en dehors des heures de travail, le cas échéant). Des relations et des protocoles sont en place pour permettre la coordination de la gestion des incidents entre l'organisme national et d'autres éléments des secteurs public et privé. Le rôle des organismes infranationaux dans la réponse aux incidents est clair et des mécanismes sont en place pour permettre la coordination entre les niveaux national et infranational. Il existe un partage régulier d'informations sur les menaces et les vulnérabilités, ainsi que de bonnes pratiques opérationnelles entre l'organisme national et un large éventail d'organisations des secteurs public et privé, ainsi que des partenaires internationaux.	L'organisme national entreprend un large éventail d'activités d'engagement telles que la convocation de communautés d'intérêts, l'organisation d'exercices intersectoriels et la promotion des meilleures pratiques en matière de cybersécurité. L'organisme national innove pour fournir une gamme de services supplémentaires qui améliorent la capacité du pays à prévenir, détecter, répondre et se remettre des menaces. L'organisme national est largement reconnu comme une voix faisant autorité en matière de cybersécurité dans le pays. L'efficacité de l'organisme national dans la réduction des cyberisques et des dommages est régulièrement évaluée et comparée aux bonnes pratiques internationales.	La réponse opérationnelle globale du gouvernement s'adapte aux changements de l'environnement technique et des menaces sous-jacentes. Le pays contribue aux meilleures pratiques internationales sur la manière d'organiser les réponses opérationnelles aux menaces de cybersécurité.

* Computer Emergency Response Team (Équipe d'intervention en cas d'urgence informatique)

Facteur - D 1.2 : Réponse aux incidents et gestion de crise

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Intégration de la cybersécurité dans la gestion nationale des crises	Il n'existe aucun cadre pour la gestion des crises au niveau national. La cybersécurité n'a pas été considérée comme un scénario de crise potentielle au niveau national. Les capacités de communication d'urgence sont limitées.	Un cadre national de gestion des crises est en cours d'élaboration et une organisation spécifique a été chargée de diriger la réponse aux crises au niveau national. La cybersécurité a été reconnue comme pertinente pour la gestion des crises nationales, à la fois comme un facteur à part entière et comme un élément d'autres scénarios de crise. Un programme d'exercices est en cours d'élaboration et comprend des scénarios basés sur la cybersécurité. Des capacités de communication d'urgence sont en place, mais elles peuvent ne pas être bien intégrées ou manquer de résilience face à la cyberperturbation.	La cybersécurité est pleinement intégrée au cadre national de gestion des crises et l'organisation responsable de la gestion des crises est équipée pour faire face à toute une série de scénarios liés à la cybersécurité. Le rôle d'une autorité de gestion des cyberincidents dans le processus de gestion de crise est bien défini et établi, et les seuils d'escalade sont parfaitement compris. Des scénarios nationaux de gestion de crise comportant des éléments de cybersécurité sont régulièrement pratiqués. Les systèmes de communication d'urgence font régulièrement l'objet de tests de cyberrésilience dans le cadre d'une série de scénarios liés à la cybersécurité.	Les enseignements tirés des exercices de cybercrise sont utilisés pour alimenter à la fois la politique nationale de gestion des crises et la stratégie nationale de cybersécurité et son plan de mise en œuvre. La planification et l'exercice de crise internationale avec des partenaires existent et incluent régulièrement la cybersécurité comme élément. La résilience des communications d'urgence a été mise à l'épreuve dans un large éventail de scénarios potentiels.	Le pays contribue au débat sur l'intégration de la cybersécurité dans la gestion des crises nationales et internationales. Les capacités de communication d'urgence sont capables de fonctionner au-delà des frontières du pays afin de soutenir les pays tiers et les réponses aux crises mondiales.

Facteur - D 1.3 : Protection des infrastructures critiques (IC)

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Identification	Il peut y avoir une certaine appréciation de ce qui constitue un actif d'IC, mais aucune catégorisation formelle des actifs d'IC n'a été produite.	Une liste d'actifs, de secteurs et d'opérateurs d'IC généraux a été créée.	La liste des actifs de l'IC a été formalisée et comprend une série d'organisations appropriées des secteurs public et privé. Des opérateurs spécifiques ont été identifiés et sont au courant de leur statut. La liste est tenue à jour pour refléter les changements des circonstances du pays. Des dépendances transfrontalières ont été identifiées.	La liste des actifs d'IC s'adapte aux changements stratégiques de l'environnement technique, social et économique sous-jacent. Les interdépendances entre les secteurs sont gérées. Les dépendances transfrontalières sont gérées.	Il existe une certaine souplesse dans le processus d'identification des actifs d'IC pour tenir compte des changements rapides de l'environnement technologique ou des menaces sous-jacentes. Le pays participe activement à l'identification et à la hiérarchisation des actifs mondiaux en matière d'infrastructures critiques. Les dépendances intersectorielles et transfrontalières sont atténuées.
Exigences réglementaires	Il n'existe pas d'exigences réglementaires spécifiques à la cybersécurité des IC.	La nécessité de normes de base pour régir les actifs des IC est reconnue, mais celles-ci ne sont pas explicitement prescrites par la réglementation. Les organismes de réglementation du secteur n'évaluent pas systématiquement la conformité des exploitants d'IC.	Les exploitants d'infrastructures critiques sont tenus de respecter des normes de cybersécurité appropriées (soit sous la forme d'une cyberréglementation spécifique, soit dans le cadre d'exigences réglementaires plus larges). Des exigences obligatoires en matière de notification des violations et de divulgation des vulnérabilités sont en place. Des processus formels sont en place pour évaluer la conformité des opérateurs d'IC aux normes réglementaires et à la divulgation des incidents et des vulnérabilités.	Des approches novatrices de la supervision réglementaire sont en cours d'élaboration afin d'améliorer la cybersécurité des infrastructures critiques tout en facilitant la prestation de services efficaces et efficients dans ce domaine. Le pays promeut les meilleures pratiques en matière de réglementation au niveau international.	Les cadres réglementaires sont suffisamment souples pour s'adapter aux changements rapides de l'environnement technologique ou des menaces sous-jacentes. Le pays participe activement à l'établissement d'approches réglementaires visant à garantir l'IC mondiale.
Pratique opérationnelle	A few CI operators may be implementing good cybersecurity practices, but this is inconsistent.	Many CI operators are implementing good cybersecurity practice. There is some self-assessment against recognised industry standards. Some informal arrangements exist for collaboration across and within sectors.	CI operators are consistently implementing recognised industry standards and the effectiveness of their cybersecurity controls are regularly assessed. Mechanisms are in place for operators to share threat and vulnerability information, best practices and lessons learned from incidents and near misses. CI operators participate fully in national incident response and crisis management planning and exercising. Mechanisms are in place for public authorities to provide information and other practical support to CI operators, both pre- and post- incident.	There is extensive collaboration among CI operators and with public authorities to develop strategies that enhance collective cybersecurity. The resilience of the critical infrastructure ecosystem as a whole has been assessed against a range of scenarios, and measures are in place to address systemic risks to the economy and society.	The country and its CI operators are contributing to the international debate on global critical infrastructure resilience. Experts from the regulators and CI operators are recognised internationally for their contribution to addressing global infrastructure protection challenges.

Facteur - D 1.4 : La cybersécurité dans la défense et la sécurité nationale

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Stratégie de cybersécurité des forces de défense	L'impact potentiel de la cybersécurité sur la sécurité nationale et la défense a peut-être été envisagé, mais n'a pas été formellement formulé.	L'impact potentiel de la cybersécurité sur la sécurité nationale et la défense a été évalué et une stratégie pour faire face à ces risques est en cours d'élaboration. Cette analyse porte notamment sur les risques qui pèsent sur la capacité des forces armées et des autres moyens de sécurité nationale du pays à fonctionner dans un cyberenvironnement contesté.	Une stratégie de cybersécurité pour la sécurité nationale et la défense a été officiellement adoptée (de manière autonome ou dans le cadre d'un document plus large). La stratégie est soutenue par les autorités judiciaires appropriées ainsi que par la doctrine opérationnelle et les règles d'engagement pertinentes. Celles-ci sont conformes au droit humanitaire international. La dépendance des entités militaires et de sécurité nationale à l'égard de la cybersécurité d'autres parties de l'infrastructure nationale critique est comprise et traitée dans la stratégie de cybersécurité de la défense. Les considérations relatives à la cybersécurité alimentent d'autres éléments de la stratégie de sécurité nationale et de défense, le cas échéant.	La stratégie de défense comprend des considérations appropriées de dissuasion. L'establishment de la défense et de la sécurité nationale du pays (ainsi que d'autres parties prenantes) est activement engagé dans le débat mondial sur le droit humanitaire international et les normes de comportement en rapport avec les conflits dans le cyberespace. La stratégie déclaratoire et la doctrine publiée peuvent en faire partie.	La stratégie et la doctrine ne sont pas statiques, mais s'adaptent à l'évolution des capacités et à l'environnement géopolitique et technique des menaces. La stratégie est conçue pour promouvoir la stabilité dans le cyberespace. Elle comprend des mesures visant à prévoir et à influencer les stratégies et les actions et réactions des alliés et adversaires potentiels.
Capacités nationales en matière de cybersécurité des forces de défense	Les capacités spécialisées en matière de cybersécurité au sein de l'establishment de la sécurité nationale sont limitées.	Les besoins en capacités spécialisées en matière de cybersécurité sont compris et les structures organisationnelles pertinentes ont été définies. Des mesures initiales ont été prises pour les mettre en place.	Les capacités et les structures organisationnelles sont en place et ont été testées. Les ressources sont fournies par le biais de l'estimation militaire nationale ou d'un processus équivalent. La doctrine opérationnelle et les règles d'engagement sont pleinement intégrées à la formation. Des ressources spécialisées en matière de renseignement sont utilisées pour fournir un soutien et sont dotées de ressources appropriées. Des mécanismes visant à faciliter la collaboration avec les alliés sont en place et ont été testés.	Des capacités pertinentes de dissuasion et de défense/résilience sont en place et font partie de la stratégie de défense du pays en matière de cybersécurité. La cybersécurité fait partie intégrante de la formation opérationnelle et de la formation au commandement au sein des forces armées du pays.	Les capacités de cybersécurité de la défense sont en mesure de soutenir les réponses multilatérales aux défis communs de sécurité nationale.

Facteur - D 1.4 : La cybersécurité dans la défense et la sécurité nationale

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Coordination de la protection civile	La collaboration en matière de cybersécurité entre les entités civiles et de défense est limitée.	Une collaboration informelle sur la cybersécurité entre les entités civiles et de défense peut exister, mais n'a pas été formalisée. Les entités de défense n'ont pas été formellement dotées des ressources nécessaires pour entreprendre ce travail.	La collaboration en matière de cybersécurité entre les entités civiles et de défense existe et a été formalisée. Les rôles respectifs ont été définis dans le cadre des procédures de gestion de crise du pays. Les ressources nécessaires au sein de la communauté de la défense et de la sécurité nationale, pour soutenir les autorités civiles et les autorités chargées des ICont été formellement évaluées et attribuées. Des mécanismes formels sont en place pour déterminer les dépendances de la cybersécurité militaire/sécurité nationale à l'égard des infrastructures civiles et des infrastructures critiques. La capacité des opérateurs d'infrastructures civiles et d'infrastructures critiques à fournir ces services a été assurée.	La collaboration de la défense civile en matière de cybersécurité est intégrée dans la planification stratégique des deux secteurs et conçue pour faire face à une série de scénarios de crise futurs. Des mécanismes sont en place pour permettre à la communauté de la défense et de la sécurité nationale de s'appuyer sur les compétences et les capacités de l'économie et de la société au sens large. (Par exemple, par le biais d'une cyberforce de réserve officielle)	Le pays mène le débat international sur les meilleures pratiques en matière de collaboration intergouvernementale entre civils et militaires dans le domaine de la cybersécurité.

2e dimension : Culture et Société de la cybersécurité

Cette *dimension* passe en revue les éléments importants d'une culture de cybersécurité responsable, tels que la compréhension des risques liés à la cybercriminalité dans la société, le niveau de confiance dans les services Internet, l'administration en ligne et les services de commerce électronique, et la compréhension par les utilisateurs de la protection des informations personnelles en ligne. En outre, cette *dimension* explore l'existence de mécanismes de signalement fonctionnant comme des canaux permettant aux utilisateurs de signaler la cybercriminalité. En outre, cette *dimension* examine le rôle des médias et des réseaux sociaux dans la formation des valeurs, des attitudes et des comportements en matière de cybersécurité.

Facteur
D 2.1 : L'état d'esprit en matière de cybersécurité

Ce *facteur* évalue le degré de priorité et d'intégration de la cybersécurité dans les valeurs, les attitudes et les pratiques des pouvoirs publics, du secteur privé et des utilisateurs dans l'ensemble de la société. L'état d'esprit en matière de cybersécurité consiste en des valeurs, des attitudes et des pratiques — y compris les habitudes des utilisateurs individuels, des experts et d'autres acteurs — dans l'écosystème de la cybersécurité, qui renforcent la capacité des utilisateurs à se protéger en ligne.
> Navigate to Factor

Aspects

- **Sensibilisation aux risques :** cet *aspect* examine si les internautes évaluent de manière critique ce qu'ils voient ou reçoivent en ligne ;
- **Priorité de la sécurité :** cet *aspect* examine dans quelle mesure le gouvernement, le secteur privé et les utilisateurs font de la cybersécurité une priorité ; et
- **Pratiques :** cet *aspect* examine si le gouvernement, le secteur privé et les utilisateurs suivent des pratiques sûres en matière de cybersécurité.

Facteur
D 2.2 : Confiance dans les services en ligne

Ce *facteur* passe en revue les compétences critiques, la gestion de la désinformation, le niveau de confiance des utilisateurs dans l'utilisation des services en ligne en général, et des services d'administration en ligne et de commerce électronique en particulier.
> Navigate to Factor

Aspects

- **Culture et compétences numériques :** cet *aspect* examine si les internautes évaluent de manière critique ce qu'ils voient ou reçoivent en ligne ;
- **Confiance des utilisateurs dans la recherche et l'information en ligne :** cet *aspect* examine si les utilisateurs ont confiance dans l'utilisation sécurisée de l'internet sur la base d'indicateurs de légitimité des sites internet ;
- **Désinformation :** cet *aspect* examine l'existence d'outils et de ressources pour lutter contre la désinformation en ligne ;
- **Confiance des utilisateurs dans les services gouvernementaux en ligne :** cet *aspect* examine lorsque des services gouvernementaux en ligne sont offerts, si la confiance existe dans la prestation sécurisée de ces services, et si des efforts sont en place pour promouvoir cette confiance dans l'application des mesures de sécurité ; et
- **Confiance des utilisateurs dans les services de commerce électronique :** cet *aspect* examine si les services de commerce électronique sont proposés et établis dans un environnement sécurisé et si les utilisateurs leur font confiance.

Facteur
D 2.3 : Compréhension par les utilisateurs de la protection des informations personnelles en ligne

Ce *facteur* cherche à savoir si les internautes et les parties prenantes des secteurs public et privé reconnaissent et comprennent l'importance de la protection des informations personnelles en ligne, et s'ils sont sensibles à leur droit à la vie privée.
> Navigate to Factor

Aspects

- **Protection des informations personnelles en ligne :** (comme ci-dessus)

Facteur
D 2.4 : Mécanismes de rapport

Ce *facteur* explore l'existence de mécanismes de signalement qui fonctionnent comme des canaux permettant aux utilisateurs de signaler les délits liés à l'internet tels que la fraude en ligne, le cyberharcèlement, la maltraitance des enfants en ligne, l'usurpation d'identité, les atteintes à la vie privée et à la sécurité, et d'autres incidents.
> Navigate to Factor

Aspects

- **Mécanismes de rapport :** (comme ci-dessus)

Facteur
D 2.5 : Médias et plateformes en ligne

Ce *facteur* vise à déterminer si la cybersécurité est un sujet de discussion courant dans les médias grand public, et un sujet de discussion large sur les médias sociaux. En outre, ce *facteur* examine le rôle des médias dans la transmission d'informations sur la cybersécurité au public, façonnant ainsi leurs valeurs, attitudes et comportements en ligne en matière de cybersécurité.
> Navigate to Factor

Aspects

- **Médias et réseaux sociaux :** (comme ci-dessus)

Facteur - D 2.1 : L'état d'esprit en matière de cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Prise de conscience des risques	Le gouvernement est peu ou pas sensibilisé aux risques liés à la cybersécurité. Le secteur privé est peu ou pas sensibilisé aux risques liés à la cybersécurité. Les utilisateurs ont un niveau de sensibilisation minimal ou nul aux risques de cybersécurité.	Les principales agences gouvernementales ont un niveau minimal de sensibilisation aux risques de cybersécurité. Les grandes entreprises privées ont un niveau minimal de sensibilisation aux risques de cybersécurité. Une proportion limitée d'internautes est consciente des risques liés à la cybersécurité.	La plupart des agences gouvernementales sont largement conscientes des risques liés à la cybersécurité. La plupart des entreprises privées sont largement conscientes des risques liés à la cybersécurité. Un nombre croissant d'internautes au sein de la société est conscient des risques de cybersécurité.	Les agences gouvernementales à tous les niveaux sont conscientes des risques de cybersécurité et anticipent de manière proactive les nouveaux risques. Les acteurs du secteur privé à tous les niveaux sont pleinement conscients des risques liés à la cybersécurité et anticipent les nouveaux risques. Les utilisateurs sont pleinement conscients des risques de cybersécurité et essaient d'anticiper les nouveaux risques.	Les agences gouvernementales à tous les niveaux sont pleinement conscientes des risques de cybersécurité et les utilisent pour mettre à jour les politiques de cybersécurité et les pratiques opérationnelles. La plupart des acteurs du secteur privé, à tous les niveaux, atténuent les risques de cybersécurité et les utilisent pour mettre à jour les politiques de cybersécurité et les pratiques opérationnelles. La plupart des utilisateurs identifient et anticipent les risques de cybersécurité et tentent d'adapter leur comportement.
Priorité à la sécurité	Le gouvernement ne reconnaît pas ou peu la nécessité de donner la priorité à la cybersécurité. Les acteurs du secteur privé ne reconnaissent pas ou peu la nécessité d'accorder la priorité à la cybersécurité. Les utilisateurs ne reconnaissent pas ou peu la nécessité de donner la priorité à la cybersécurité. Il n'existe pas d'enquêtes ou de mesures permettant de documenter la cybersécurité au sein du gouvernement, du secteur privé ou parmi les utilisateurs.	Les principales agences gouvernementales et entreprises privées reconnaissent la nécessité de donner la priorité à la cybersécurité. Les entreprises privées reconnaissent la nécessité de donner la priorité à la cybersécurité. Une proportion limitée d'internautes reconnaît la nécessité de donner la priorité à la cybersécurité. Les enquêtes et les mesures visant à évaluer les connaissances en matière de cybersécurité au sein de la nation sont limitées ou au coup par coup.	La plupart des agences gouvernementales, à tous les niveaux, font de la cybersécurité une priorité. La plupart des entreprises privées, à tous les niveaux, font de la cybersécurité une priorité. Un nombre croissant d'internautes au sein de la société font de la cybersécurité une priorité. Des enquêtes et des mesures permettant d'évaluer la connaissance de la cybersécurité au sein de la nation sont disponibles.	Les organismes publics à tous les niveaux hiérarchisent et réévaluent régulièrement les priorités en matière de cybersécurité en fonction de l'évolution des menaces pesant sur la population. La plupart des acteurs du secteur privé à tous les niveaux hiérarchisent et réévaluent régulièrement les priorités en matière de cybersécurité en fonction de l'évolution des menaces pesant sur la population. La plupart des utilisateurs accordent systématiquement la priorité à la cybersécurité et cherchent à prendre des mesures proactives pour améliorer la cybersécurité. Des enquêtes et des mesures sont régulièrement menées et rendues publiques dans les domaines du gouvernement, des entreprises et de l'industrie, ainsi qu'auprès des utilisateurs.	Les agences gouvernementales à tous les niveaux ont l'habitude, comme une évidence, de donner la priorité à la cybersécurité. Les acteurs du secteur privé à tous les niveaux ont l'habitude de donner la priorité à la cybersécurité, comme une évidence. Les utilisateurs ont l'habitude de donner la priorité à la cybersécurité et de prendre des mesures pour améliorer leur sécurité en ligne. Les résultats d'enquêtes et des mesures sont utilisés pour affiner les politiques de cybersécurité, informer les pratiques opérationnelles et les initiatives liées aux TI au sein de la nation.

Facteur - D 2.1 : L'état d'esprit en matière de cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Pratiques	The government agencies do not follow safe cybersecurity practices. Private sector companies do not follow safe cybersecurity practices. In this country, very few Internet users follow safe cybersecurity practices or take protective measures to ensure their security.	Leading government agencies follow safe cybersecurity practices. Leading private firms follow safe cybersecurity practices. A limited but growing proportion of Internet users know or follow safe cybersecurity practices.	Most government agencies at all levels follow safe cybersecurity practices. Most private firms at all levels follow safe cybersecurity practices. Most Internet users within this country know and follow safe cybersecurity practices	Government agencies across all levels routinely follow safe cybersecurity practices. Most private sector actors, (including SMEs) across all levels routinely follow safe cybersecurity practices. Most users know and routinely follow safe cybersecurity practices.	Government agencies at all levels habitually follow and also develop safe cybersecurity practices. Private sector actors at all levels habitually follow and develop safe cybersecurity practices. Nearly all users know and habitually follow safe cybersecurity practices as a matter of course.

Facteur - D 2.2 : Confiance dans les services en ligne

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Culture et compétences numériques	Très peu d'internautes dans ce pays évaluent de manière critique ce qu'ils voient ou reçoivent en ligne. Les internautes ne croient généralement pas ou ne considèrent même pas qu'ils ont la capacité d'utiliser l'internet et de se protéger en ligne. Aucun programme n'est disponible pour soutenir les compétences numériques et médiatiques.	Une proportion limitée, mais croissante d'internautes évalue de manière critique ce qu'ils voient ou reçoivent en ligne. Une proportion limitée pense avoir la capacité d'utiliser l'internet et de se protéger en ligne. Un ou plusieurs programmes sont en cours d'élaboration pour soutenir les compétences numériques et médiatiques.	La plupart des internautes évaluent de manière critique ce qu'ils voient ou reçoivent en ligne, en se basant sur l'identification des risques éventuels. La plupart des internautes comprennent comment et agissent pour se protéger des fausses informations en ligne, par exemple en effectuant une recherche. Des programmes ont été élaborés pour soutenir les compétences en matière d'éducation numérique et médiatique.	La plupart des internautes évaluent de manière critique ce qu'ils voient ou reçoivent en ligne, en se basant sur l'identification des risques éventuels. La plupart des internautes reconnaissent les informations douteuses en ligne et prennent des mesures pour les ignorer ou en vérifier la validité. Des efforts sont en cours pour coordonner les programmes qui soutiennent les compétences en matière d'internet, de numérique et de médias entre les fournisseurs de plateformes internet, les régulateurs et la société civile.	Presque tous les internautes évaluent habituellement le risque lié à l'utilisation des services en ligne, y compris les changements dans l'environnement technique et de cybersécurité. Les internautes adaptent continuellement leur comportement en fonction de leur évaluation de la qualité des informations qu'ils reçoivent. Les fournisseurs de plateformes internet, les régulateurs et la société civile développent en collaboration des programmes visant à soutenir les compétences en matière d'internet, de numérique et de médias.
Confiance des utilisateurs dans la recherche et l'information en ligne	La plupart des internautes n'ont aucune confiance ou une confiance aveugle dans les sites internet et dans ce qu'ils voient ou reçoivent en ligne. Très peu d'internautes se sentent en confiance pour utiliser l'Internet. Il n'existe pas d'enquêtes ou d'autres mesures permettant d'évaluer la confiance des utilisateurs en ligne.	Seule une proportion limitée d'utilisateurs a suffisamment confiance dans son utilisation de l'internet. Une proportion limitée d'utilisateurs de l'internet se sent en confiance pour l'utiliser. Les enquêtes et les mesures permettant d'évaluer la confiance des utilisateurs en ligne sont limitées ou au coup par coup.	Une proportion croissante d'utilisateurs a suffisamment confiance pour utiliser l'internet en toute sécurité et reconnait les indicateurs de sites et de sources d'information légitimes. Un nombre croissant d'utilisateurs se sent en confiance pour utiliser l'internet. Des enquêtes et des paramètres permettant d'évaluer la confiance des utilisateurs en ligne sont en place et bénéficient d'un financement adéquat.	La plupart des utilisateurs ont acquis un certain niveau de confiance dans l'utilisation sûre de l'internet et reconnaissent les indicateurs de sites et de sources d'information légitimes. La plupart des utilisateurs de l'internet se sentent confiants dans l'utilisation de l'internet, pensent pouvoir reconnaître les sites web problématiques ou non légitimes (y compris les tentatives de mimétisme) et vérifier les informations à l'aide d'outils tels que les options de recherche. Des enquêtes et des mesures visant à évaluer la confiance des utilisateurs en ligne sont régulièrement réalisées.	Presque tous les utilisateurs pensent qu'ils peuvent utiliser l'internet en toute sécurité à des fins diverses et qu'ils peuvent aider les autres à l'utiliser en toute sécurité. Presque tous les utilisateurs de l'internet se sentent en confiance pour utiliser l'internet et trouver du contenu valable. Les enquêtes et les mesures ont une forte réputation dans la région ou dans le monde et façonnent le développement des mesures dans d'autres nations.

Facteur - D 2.2 : Confiance dans les services en ligne

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Désinformation	Les fournisseurs de plateformes Internet n'abordent pas les questions de désinformation, comme la mésinformation, dans ce pays. La société civile et les autres acteurs non gouvernementaux ne disposent pas des outils et des ressources nécessaires pour lutter contre la désinformation en ligne, notamment en dénonçant les campagnes de mésinformation. Les agences et acteurs gouvernementaux n'ont pas abordé la désinformation en ligne.	Les fournisseurs de plateformes Internet développent des approches pour répondre aux problèmes de désinformation dans ce pays. Le développement d'outils et de ressources pour lutter contre la désinformation a été initié par des acteurs majeurs de la société civile et des organisations non gouvernementales. Des programmes et initiatives gouvernementaux visant à lutter contre la désinformation sont en cours d'élaboration, mais ils impliquent un filtrage et des efforts limités pour informer les internautes.	Les fournisseurs de plateformes Internet ont mis en place un certain nombre d'approches pour lutter contre la désinformation ; celles-ci respectent la liberté d'expression et les autres droits de l'homme en ligne. Les acteurs de la société civile ont développé des outils et des ressources pour lutter contre la désinformation en ligne. Les programmes et initiatives gouvernementaux visant à renforcer la préparation du public contre la désinformation en ligne se limitent à la sensibilisation, mais évitent la censure ou le filtrage des informations.	Les fournisseurs de plateformes Internet ont mis en place des politiques et des pratiques pour lutter contre la désinformation ; celles-ci respectent la liberté d'expression et les autres droits de l'homme en ligne. Les efforts conjoints des acteurs de la société civile sont en place et sont régulièrement utilisés pour lutter contre la désinformation en ligne de manière à respecter la liberté d'expression et les autres droits de l'homme en ligne. Les enquêtes axées sur les résultats sont utilisées pour affiner les programmes et les initiatives visant à responsabiliser les utilisateurs et à renforcer la compréhension du public face à une éventuelle désinformation en ligne.	Les fournisseurs de plateformes Internet ont mis en place des politiques et des pratiques pour lutter contre la désinformation de manière innovante, tout en respectant la liberté d'expression et les autres droits de l'homme en ligne. Les efforts conjoints des acteurs de la société civile sont examinés de manière proactive afin de tenir compte des développements stratégiques plus larges liés à la désinformation et à la sensibilisation. Le pays soutient l'élaboration de plans d'action et de lignes directrices nationaux/régionaux/internationaux pour lutter contre la désinformation de manière à protéger un internet ouvert et à responsabiliser les utilisateurs.
La confiance des utilisateurs dans les services d'administration en ligne	Le gouvernement offre un nombre très limité de services électroniques, voire aucun, et n'a pas fait la promotion publique de leur sécurité. En règle générale, le public n'utilise pas de services administratifs en ligne importants. Il n'existe pas d'enquêtes ou de mesures montrant la confiance des internautes dans les services administratifs en ligne. Il y a un manque d'informations sur la sécurité de l'administration en ligne et les failles de sécurité.	Le gouvernement a commencé à mettre en place un ensemble de services électroniques de base, pour lesquels il reconnaît la nécessité d'appliquer des mesures de sécurité afin d'établir la confiance dans leur utilisation. Un nombre limité d'adeptes précoces ont confiance dans l'utilisation sécurisée des services d'administration en ligne. Les mesures permettant d'évaluer la confiance des utilisateurs dans les services administratifs en ligne sont limitées au coup par coup. Les autorités publiques élaborent des informations sur les initiatives et les violations de la vie privée et de la sécurité au coup par coup.	Les principaux services administratifs en ligne ont été développés et ont généré un grand nombre d'utilisateurs. Un nombre important et croissant d'internautes ont confiance dans l'utilisation des services administratifs en ligne. Des enquêtes et des mesures permettant d'évaluer la confiance des utilisateurs dans les services administratifs en ligne sont en place et bénéficient d'un financement adéquat. Les autorités publiques publient des informations et des mises à jour sur leurs atteintes à la vie privée et à la sécurité, ainsi que sur des initiatives telles qu'un « paramétrage par défaut favorable au respect de la vie privée ».	Les services administratifs en ligne sont devenus le mode dominant (par défaut) de prestation de services d'information gouvernementaux. La majorité des internautes de ce pays ont confiance dans l'utilisation sécurisée des services administratifs en ligne et y ont recours. Des enquêtes et des mesures visant à évaluer la confiance des utilisateurs dans les services administratifs en ligne sont régulièrement réalisées. Les autorités publiques coordonnent, publient et informent les utilisateurs sur les initiatives et les atteintes à la vie privée et à la sécurité.	Les services administratifs en ligne de ce pays sont reconnus au niveau régional ou international. Les internautes ont confiance dans le fait que les services administratifs en ligne sont examinés, améliorés et étendus de manière proactive afin de renforcer leur sécurité. Les enquêtes axées sur les résultats sont utilisées pour examiner les services administratifs en ligne et évaluer la gestion du contenu en ligne. Le pays est un chef de file en matière d'information des utilisateurs sur les atteintes à la vie privée et à la sécurité, les initiatives et autres problèmes actuels et futurs.

Facteur - D 2.2 : Confiance dans les services en ligne

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
La confiance des utilisateurs dans les services de commerce électronique	Les services de commerce électronique ne sont pas proposés. Les internautes n'ont pas la confiance nécessaire pour utiliser les services de commerce électronique disponibles. Il n'existe pas d'enquêtes ou de mesures pour montrer la confiance des internautes dans les services de commerce électronique. La nécessité d'initiatives en matière de sécurité pour les services de commerce électronique est peu ou pas reconnue .	Les services de commerce électronique sont fournis dans une mesure limitée. Un nombre limité d'adeptes précoces ont confiance dans l'utilisation sécurisée des services de commerce électronique. Les mesures permettant d'évaluer la confiance des utilisateurs dans les services de commerce électronique sont limitées ou au coup par coup. Le secteur privé reconnaît la nécessité d'appliquer des mesures de sécurité pour établir la confiance dans les services de commerce électronique.	Les services de commerce électronique sont entièrement établis par de multiples parties prenantes dans un environnement sécurisé. Un nombre important et croissant d'internautes ont confiance dans l'utilisation sécurisée des services de commerce électronique. Des enquêtes et des mesures visant à évaluer la confiance des utilisateurs dans les services de commerce électronique sont en place et financées de manière adéquate. Des solutions de sécurité fiables sont à jour et disponibles, par exemple pour les systèmes de paiement. Des systèmes de certification et des marques de confiance pour les services de commerce électronique sont en place.	Les services de commerce électronique sont désormais largement acceptés comme une pratique sûre pour les consommateurs. La majorité des utilisateurs ont confiance dans l'utilisation sécurisée des services de commerce électronique et y ont recours. Des enquêtes et des mesures visant à évaluer la confiance des utilisateurs dans les services de commerce électronique sont régulièrement réalisées. Les parties prenantes investissent dans l'amélioration des fonctionnalités des services de commerce électronique, la protection des informations personnelles et la mise en place de mécanismes de retour d'information pour les utilisateurs.	Les services de commerce électronique dans ce pays sont reconnus au niveau régional ou international. Les internautes ont confiance dans le fait que les services de commerce électronique sont examinés de manière proactive, améliorées et étendues pour renforcer leur sécurité. Les enquêtes axées sur les résultats sont utilisées pour examiner et améliorer les services de commerce électronique afin de promouvoir des systèmes transparents, dignes de confiance et sûrs. Les conditions générales fournies par les services de commerce électronique sont claires et facilement compréhensibles pour tous les utilisateurs.

Facteur - D 2.3 : Compréhension par les utilisateurs de la protection des renseignements personnels en ligne

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Informations personnelles et protection des données	Les utilisateurs et les parties prenantes des secteurs public et privé n'ont pas ou peu de connaissances sur la manière dont les informations personnelles sont traitées en ligne, et ils ne pensent pas que des mesures adéquates sont en place pour protéger leurs informations personnelles en ligne. La protection des informations personnelles en ligne n'est pas ou peu discutée. Les normes de protection de la vie privée ne sont pas en place pour encadrer les pratiques de l'internet et des médias sociaux.	Les utilisateurs et les parties prenantes des secteurs public et privé peuvent avoir des connaissances générales sur la manière dont les informations personnelles sont traitées en ligne et peuvent adopter de bonnes pratiques (proactives) en matière de cybersécurité pour protéger leurs informations personnelles en ligne. Des discussions ont été entamées sur la protection des informations personnelles et sur l'équilibre entre sécurité et vie privée. Des actions concrètes ou des politiques de confidentialité sont en cours d'élaboration. policies are being developed.	Une proportion croissante d'utilisateurs dispose des compétences nécessaires pour gérer leur vie privée en ligne et se protéger contre les intrusions, les interférences ou l'accès indésirable à des informations par d'autres personnes. La protection des informations personnelles et l'équilibre entre sécurité et vie privée font l'objet d'un débat public considérable. Des politiques de protection de la vie privée ont été élaborées dans les secteurs public et privé.	Toutes les parties prenantes disposent des informations, de la confiance et de la capacité nécessaires pour prendre des mesures visant à protéger leurs informations personnelles en ligne et à garder le contrôle de la diffusion de ces informations. Les utilisateurs et les parties prenantes des secteurs public et privé reconnaissent largement l'importance de la protection des informations personnelles en ligne et sont conscients de leurs droits en matière de vie privée. Des mécanismes sont en place dans les secteurs privé et public pour façonner les pratiques de l'internet et des médias sociaux et veiller à ce que la vie privée et la sécurité ne soient pas en concurrence.	Les utilisateurs disposent des connaissances et des compétences nécessaires pour protéger leurs informations personnelles en ligne, en adaptant leurs capacités à l'évolution de l'environnement de risque. Les politiques des secteurs privé et public font l'objet d'un examen proactif afin de s'assurer que la vie privée et la sécurité ne sont pas en concurrence dans un environnement en mutation et sont alimentées par les réactions des utilisateurs et le débat public. De nouveaux mécanismes sont mis en place, tels que le respect de la vie privée par défaut, en tant qu'outils de transparence, et sont promus.

Facteur - D 2.4 : Mécanismes de rapport

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Mécanismes de rapport s	Il n'existe pas de mécanismes de rapport officiels, mais les discussions pourraient avoir commencé. Les utilisateurs n'utilisent pas les médias sociaux pour faire part de leurs préoccupations concernant les cybermenaces et les problèmes. Il n'existe aucune mesure des incidents signalés.	Les secteurs public et privé proposent des canaux de signalement des cybermenaces (fraude en ligne, cyberharcèlement, maltraitance des enfants en ligne, usurpation d'identité, atteintes à la vie privée et à la sécurité, et autres incidents), mais ces canaux ne sont pas coordonnés et ne sont pas utilisés de manière systématique. Les internautes utilisent les médias sociaux pour informer les autres utilisateurs au coup par coup. La mesure des incidents signalés est en cours d'élaboration.	Des mécanismes d'établissement de rapports ont été mis en place, promus et sont régulièrement utilisés. Les internautes utilisent largement les médias sociaux pour informer les autres utilisateurs. Il existe de bonnes mesures des incidents signalés.	Les mécanismes de rapport coordonnés sont largement utilisés et encouragés dans les secteurs public et privé. Les internautes utilisent couramment les médias sociaux pour informer les autres utilisateurs. Des mesures de cyberdommages ont été utilisées pour informer la révision et la promotion de nouvelles politiques et pratiques.	Des mécanismes ont été développés pour coordonner la réponse aux incidents signalés entre les forces de l'ordre et la capacité nationale de réponse aux incidents. Les internautes utilisent habituellement les médias sociaux pour informer les autres utilisateurs et partager les bonnes pratiques. Des mesures sont couramment utilisées pour informer les politiques et les décideurs.

Facteur - D 2.5 : Médias et plateformes en ligne

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Médias et médias sociaux	Les médias de masse ne couvrent que rarement, voire jamais, les informations relatives à la cybersécurité ou ne traitent pas de questions telles que les failles de sécurité ou la cybercriminalité. Il n'y a pas, ou rarement, de discussion sur les médias sociaux à propos de la cybersécurité. Toute représentation des dénonciateurs est négative, et fondée sur des stéréotypes criminels ou autres stéréotypes négatifs.	La couverture médiatique de la cybersécurité n'est pas perçue comme systématique, les informations fournies et les reportages sur les problèmes spécifiques auxquels les individus sont confrontés en ligne, tels que la protection des enfants en ligne ou la cyberintimidation, étant limités. On a l'impression qu'il y a peu de discussions sur la cybersécurité dans les médias sociaux. Il existe des exemples positifs de cas où les dénonciateurs ont eu un impact constructif.	La cybersécurité est perçue comme un sujet courant dans les médias grand public, et les informations et les rapports sur un large éventail de questions, y compris les failles de sécurité et la cybercriminalité, sont largement diffusés. La cybersécurité fait l'objet d'un large débat sur les médias sociaux. Il est admis que les dénonciateurs peuvent jouer un rôle positif.	On estime que la couverture médiatique va au-delà du signalement des menaces et peut informer le public sur les mesures de cybersécurité proactives et réalisables, ainsi que sur les impacts économiques et sociaux. La cybersécurité fait souvent l'objet de discussions sur les médias sociaux et les particuliers utilisent régulièrement les médias sociaux pour partager leurs expériences en ligne. La transparence est encouragée, de même que les dénonciateurs.	On estime que le large débat sur les expériences personnelles et les attitudes personnelles des individus dans les médias grand public et sociaux permet d'éclairer l'élaboration des politiques et de faciliter le changement sociétal. Les médias sociaux sont devenus une composante majeure du suivi et de la lutte contre les cybermenaces. La dénonciation a été encouragée et protégée en tant que moyen de responsabilisation sociale.

3e dimension : renforcement des connaissances et des capacités en matière de cybersécurité

Cette *dimension* passe en revue la disponibilité, la qualité et l'adoption de programmes destinés à divers groupes de parties prenantes, notamment le gouvernement, le secteur privé et la population dans son ensemble. Ces programmes concernent les programmes de sensibilisation à la cybersécurité, les programmes éducatifs formels en matière de cybersécurité et les programmes de formation professionnelle.

Facteur
D 3.1 : Sensibilisation à la cybersécurité

Ce *facteur* se concentre sur la disponibilité de programmes de sensibilisation à la cybersécurité dans tout le pays, en se concentrant sur les risques et les menaces liés à la cybersécurité et sur les moyens d'y faire face.
> Navigate to Factor

Aspects

- **Initiatives de sensibilisation du gouvernement :** cet *aspect* examine l'existence d'un programme national coordonné de sensibilisation à la cybersécurité mené par le gouvernement, couvrant un large éventail de données démographiques et de questions, élaboré en consultation avec les parties prenantes de divers secteurs ;
- **Initiatives de sensibilisation du secteur privé :** cet *aspect* examine l'existence de programmes de sensibilisation menés par le secteur privé et la mesure dans laquelle ils sont alignés sur les initiatives du gouvernement et de la société civile ;
- **Initiatives de sensibilisation de la société civile :** cet *aspect* examine l'existence de programmes de sensibilisation menés par la société civile et la mesure dans laquelle ils sont alignés sur les initiatives du gouvernement et du secteur privé ; et
- **Sensibilisation des cadres :** cet *aspect* examine les efforts déployés pour sensibiliser les cadres aux questions de cybersécurité dans les secteurs public, privé, universitaire et de la société civile, ainsi que la manière dont les risques de cybersécurité pourraient être traités.

Facteur
D 3.2 : Éducation à la cybersécurité

Ce *facteur* traite de la disponibilité et de l'offre de programmes d'éducation à la cybersécurité de haute qualité et d'un nombre suffisant d'enseignants et de conférenciers qualifiés. En outre, ce *facteur* examine la nécessité d'améliorer l'éducation à la cybersécurité aux niveaux national et institutionnel et la collaboration entre le gouvernement et l'industrie pour s'assurer que les investissements éducatifs répondent aux besoins de l'environnement éducatif en matière de cybersécurité dans tous les secteurs.
> Navigate to Factor

Aspects

- **Offre :** cet *aspect* examine s'il existe des offres éducatives en matière de cybersécurité et des programmes de qualification des éducateurs qui permettent de comprendre les risques actuels et les compétences requises ; et
- **Administration :** cet *aspect* explore la coordination et les ressources nécessaires au développement et à l'amélioration des cadres d'éducation à la cybersécurité, avec un budget et des dépenses alloués en fonction de la demande nationale.

Facteur

D 3.3 : Formation des professionnels de la cybersécurité

Ce *facteur* aborde et examine la disponibilité et l'offre de programmes de formation professionnelle abordables en matière de cybersécurité afin de constituer un cadre de professionnels de la cybersécurité. En outre, ce *facteur* examine l'adoption de la formation à la cybersécurité, le transfert horizontal et vertical des connaissances et des compétences en matière de cybersécurité au sein des organisations, et la manière dont ce transfert de compétences se traduit par une augmentation continue des cadres de professionnels de la cybersécurité.

> Navigate to Factor

Aspects

- **Mise à disposition :** cet *aspect* examine le développement, la disponibilité et la mise à disposition de programmes de formation à la cybersécurité pour améliorer les compétences et les capacités ; et
- **Adoption :** cet *aspect* examine l'adoption et le caractère abordable de ces programmes pour produire un cadre de professionnels certifiés de la cybersécurité. Les questions examinées comprennent les initiatives visant à s'inscrire à ces programmes, les initiatives visant à rester dans le pays après avoir terminé avec succès, le partage des connaissances après avoir terminé un programme, et l'existence d'un registre national des étudiants ayant réussi et certifié.

Facteur

D 3.4 : Recherche et innovation en matière de cybersécurité

Ce *facteur* tient compte de l'importance accordée à la recherche et à l'innovation en matière de cybersécurité pour relever les défis technologiques, sociétaux et commerciaux et pour faire progresser le développement des connaissances et des capacités en matière de cybersécurité dans le pays.

> Navigate to Factor

Aspects

- **Recherche et développement en matière de cybersécurité :** cet *aspect* examine l'existence d'une culture de la recherche et de l'innovation dans le pays, liée à une liste nationale de projets en cours et achevés, au soutien financier, aux incitations et aux résultats de recherche utilisables.

Facteur - D 3.1 : Sensibilisation à la cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Initiatives du gouvernement	Aucun programme national global de sensibilisation à la cybersécurité n'a été élaboré par le gouvernement. La nécessité de sensibiliser les pouvoirs publics aux menaces et aux vulnérabilités en matière de cybersécurité n'est pas reconnue ou n'en est qu'au stade initial de la discussion.	Un programme coordonné de sensibilisation à la cybersécurité avec la participation du gouvernement est en cours d'élaboration, avec la participation des parties prenantes concernées, notamment le secteur privé et la société civile. Des programmes de sensibilisation, des cours, des séminaires et des ressources en ligne lancés par le gouvernement sont disponibles, mais ne sont pas suffisamment pris en compte dans la stratégie nationale de cybersécurité ou sont en cours d'élaboration. Les actions menées dans le cadre des programmes sont dirigées par différents « responsables », mais elles ne sont pas encore coordonnées. La disponibilité de ressources adéquates n'a pas encore été confirmée. Le système initial de mécanismes et d'indicateurs pour examiner les processus est limité ou au coup par coup.	Un programme national coordonné de sensibilisation à la cybersécurité, assorti d'un plan de mise en œuvre détaillé, est publié. Le contenu comprend des liens explicites avec la stratégie nationale de cybersécurité. Un organisme de coordination a été désigné, doté de l'autorité et des ressources suffisantes pour mener à bien les actions du programme national. Un portail national de sensibilisation à la cybersécurité existe pour améliorer les compétences et les connaissances de la société et est diffusé via ce programme. Des processus de révision des programmes et des mesures axées sur les résultats sont en place, sont financés de manière adéquate et permettent de mesurer l'efficacité.	Le programme national de sensibilisation est pleinement intégré aux programmes de sensibilisation sectoriels et personnalisés, tels que ceux axés sur l'industrie, les universités, la société civile et/ou les femmes et les enfants. Les risques émergents en matière de cybersécurité sont régulièrement évalués et utilisés pour mettre à jour le programme national de sensibilisation à la cybersécurité. Il est prouvé que ces paramètres sont utilisés pour affiner les actions dans le cadre du programme national de sensibilisation et de la stratégie nationale de cybersécurité.	Le programme national de sensibilisation à la cybersécurité avec les acteurs du secteur privé et de la société civile est revu de manière proactive pour tenir compte des évolutions stratégiques plus larges du pays (politiques, économiques, sociales, techniques, juridiques et environnementales). Le pays participe activement à la création de nouveaux programmes régionaux/internationaux de sensibilisation à la cybersécurité qui contribuent à étendre et à renforcer les bonnes pratiques internationales en matière de sensibilisation. Le programme national de sensibilisation à la cybersécurité a un impact mesurable sur la réduction du paysage global des menaces.

Facteur - D 3.1 : Sensibilisation à la cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Initiatives du secteur privé	La nécessité de sensibiliser le secteur privé aux menaces et aux vulnérabilités en matière de cybersécurité n'est pas reconnue ou n'en est qu'au stade initial de la discussion.	Des programmes de sensibilisation, des cours, des séminaires et des ressources en ligne initiés par le secteur privé sont disponibles, mais aucun effort de coordination ou de mise à l'échelle n'a été réalisé. Le système initial de mécanismes et d'indicateurs pour examiner les processus est limité ou au coup par coup.	Des efforts de collaboration en matière de sensibilisation (par exemple : travail conjoint de politique et/ou de plaidoyer) avec les parties prenantes du gouvernement et de la société civile sont déployés afin de mettre en commun les ressources, les informations et d'identifier des solutions pour les pratiques de cybersécurité. Le rôle des « responsables » spécifiques affectés aux actions dans le cadre des initiatives du secteur privé est clair et des mécanismes sont en place pour permettre la coordination entre les niveaux de gouvernement, le secteur privé et la société civile. Des processus de révision des programmes et des mesures axées sur les résultats sont en place, bien financés et partagés avec les parties prenantes du gouvernement et de la société civile.	L'efficacité des efforts de sensibilisation conjoints avec les parties prenantes du gouvernement et de la société civile est régulièrement évaluée et utilisée pour améliorer les processus de collaboration. Les initiatives du secteur privé sont pleinement intégrées dans le programme national de sensibilisation. Les enseignements tirés sont pris en compte dans l'élaboration des futurs programmes.	Les efforts de sensibilisation conjoints avec les parties prenantes du gouvernement et de la société civile sont revus de manière proactive pour tenir compte des évolutions stratégiques plus larges dans le pays (politiques, économiques, sociales, techniques, juridiques et environnementales). Les efforts conjoints de sensibilisation avec les acteurs du gouvernement et de la société civile ont un impact mesurable sur la réduction du paysage global des menaces.

Facteur - D 3.1 : Sensibilisation à la cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Initiatives de la société civile	La nécessité de sensibiliser la société civile aux menaces et aux vulnérabilités en matière de cybersécurité n'est pas reconnue ou n'en est qu'au stade initial de la discussion.	Certains éléments indiquent que la société civile se rend compte qu'elle peut jouer un rôle dans les programmes de sensibilisation, les cours, les séminaires et les ressources en ligne, mais aucun résultat concret n'est encore évident. Un système initial de mesures peut exister.	Des efforts de collaboration en matière de sensibilisation (par exemple, une politique commune et/ou un travail de plaidoyer) avec les parties prenantes du gouvernement et du secteur privé ont lieu afin de mettre en commun les ressources et les informations et d'identifier des solutions pour les pratiques de cybersécurité. Le rôle des « responsables » spécifiques assignés aux actions au sein des initiatives de la société civile est clair et des mécanismes sont en place pour permettre la coordination entre les niveaux du gouvernement, du secteur privé et de la société civile. Des processus de révision des programmes et des mesures axées sur les résultats sont en place, bien financés et partagés avec les parties prenantes du gouvernement et du secteur privé.	L'efficacité des efforts de sensibilisation conjoints avec les parties prenantes du gouvernement et du secteur privé est régulièrement évaluée et utilisée pour améliorer les processus de collaboration. Les initiatives de la société civile sont pleinement intégrées dans le programme national de sensibilisation. Les enseignements tirés sont pris en compte dans l'élaboration des futurs programmes.	Les efforts de sensibilisation conjoints avec les parties prenantes du gouvernement et du secteur privé sont revus de manière proactive pour tenir compte des développements stratégiques plus larges dans le pays (politiques, économiques, sociaux, techniques, juridiques et environnementaux). Les efforts conjoints de sensibilisation du gouvernement et du secteur privé ont un impact mesurable sur la réduction du paysage global des menaces.
Sensibilisation des cadres	La sensibilisation des cadres aux questions de cybersécurité est limitée, voire inexistante. Les cadres ne sont pas encore conscients de leurs responsabilités envers les actionnaires, les clients et les employés en ce qui concerne la cybersécurité.	Les cadres sont sensibilisés aux problèmes généraux de cybersécurité, mais pas à la manière dont ces problèmes et menaces pourraient affecter leur organisation. Les dirigeants de secteurs particuliers, tels que la finance et les télécommunications, ont été sensibilisés aux risques de cybersécurité en général et à la manière dont l'organisation traite les questions de cybersécurité, mais pas aux implications stratégiques.	Sensibilisation des cadres des secteurs public, privé, universitaire et de la société civile aux risques de cybersécurité en général, à certaines des principales méthodes d'attaque et à la manière dont l'organisation traite les questions de cybercriminalité (généralement confiée au DSI*). Les membres sélectionnés de l'exécutif sont sensibilisés à la manière dont les risques de cybersécurité affectent la prise de décision stratégique de l'organisation, en particulier ceux des secteurs de la finance et des télécommunications. Les efforts de sensibilisation à la gestion des crises en matière de cybersécurité au niveau des dirigeants sont toujours axés sur la réactivité.	Les efforts de sensibilisation des cadres dans presque tous les secteurs comprennent l'identification des actifs stratégiques, des mesures spécifiques mises en place pour les protéger, et du mécanisme par lequel ils sont protégés. Les cadres sont en mesure de modifier la prise de décision stratégique et d'allouer des fonds et des personnes spécifiques aux différents éléments du cyberisque, en fonction de la situation de leur entreprise. Les cadres sont informés des plans d'urgence mis en place pour faire face à diverses cyberattaques et à leurs conséquences. Les cours de sensibilisation des cadres à la cybersécurité sont obligatoires dans presque tous les secteurs.	Les risques liés à la cybersécurité sont considérés comme un point à l'ordre du jour de chaque réunion de direction, et les fonds et l'attention sont réaffectés pour faire face à ces risques. Les cadres au niveau régional et international sont considérés comme une source de bonnes pratiques en matière de gouvernance responsable et redevable de la cybersécurité des entreprises.

* Directeur des Systèmes d'Information

Facteur - D 3.2 : Éducation à la cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Mise à disposition	Les éducateurs en cybersécurité sont peu nombreux, voire inexistants, et il n'existe aucun programme de qualification pour les éducateurs. Des cours d'informatique sont proposés qui peuvent avoir une composante de sécurité, mais aucun cours lié à la cybersécurité n'est proposé. Il n'existe pas d'accréditation pour l'enseignement de la cybersécurité.	Des programmes de qualification pour les éducateurs en cybersécurité sont à l'étude, avec un petit cadre d'éducateurs qualifiés existants. Certains cours éducatifs existent dans des domaines liés à la cybersécurité, tels que la sécurité de l'information, la sécurité des réseaux et la cryptographie, mais les cours spécifiques à la cybersécurité ne sont pas encore proposés. La demande d'éducation à la cybersécurité est attestée par les inscriptions aux cours et les retours d'information.	Les qualifications et l'offre d'éducateurs sont faciles à trouver dans le domaine de la cybersécurité. Des cours spécialisés en cybersécurité sont proposés et accrédités au niveau universitaire. Des modules de sensibilisation au risque de cybersécurité sont proposés dans le cadre de nombreux cours universitaires. Les diplômes dans les domaines liés à la cybersécurité sont proposés par des universités ou des établissements d'enseignement équivalents. Les universités et autres organismes organisent des séminaires/ conférences sur les questions de cybersécurité, destinés aux non-spécialistes. La recherche et le développement sont des considérations de premier plan dans l'éducation à la cybersécurité. L'éducation à la cybersécurité ne se limite pas aux universités ou aux établissements d'enseignement équivalents, mais s'étend des niveaux primaire, secondaire et tertiaire aux études supérieures, y compris l'enseignement professionnel. Des mesures auraient pu être prises pour intégrer un cadre éducatif STEM* ou équivalent mettant l'accent sur la cybersécurité dans les programmes d'enseignement primaire et secondaire.	Les éducateurs en cybersécurité ne sont pas seulement issus du milieu universitaire, mais des mesures incitatives sont en place pour que des experts de l'industrie et/ou du gouvernement occupent également ces postes. Des cours accrédités sur la cybersécurité sont intégrés dans tous les diplômes en informatique. Des diplômes sont proposés spécifiquement dans le domaine de la cybersécurité, et englobent des cours et des modèles dans divers autres domaines liés à la cybersécurité, y compris des éléments techniques et non techniques tels que les implications politiques et l'éducation multidisciplinaire. Les offres de formation en cybersécurité sont pondérées et axées sur la compréhension des risques actuels et des compétences requises. Le contenu des cours de cybersécurité couvre des sujets sur les menaces émergentes en matière de cybersécurité. Les cadres nationaux ou internationaux de cybersécurité et/ou les directives relatives aux programmes d'études sont pris en considération par les établissements universitaires lors de la conception des cours de cybersécurité. Des programmes d'apprentissage dans différents secteurs industriels sont proposés pour combiner connaissances et compétences pratiques.	Les cours, diplômes et recherches nationaux sont à la pointe de l'enseignement de la cybersécurité. Les programmes d'éducation à la cybersécurité maintiennent un équilibre entre la préservation des éléments fondamentaux du programme d'études et la promotion de processus adaptatifs qui répondent aux changements rapides de l'environnement de la cybersécurité. Les exigences actuelles en matière de cybersécurité sont prises en compte dans le réaménagement de tous les programmes d'études généraux.

* Science, Technology, Engineering, and Mathematics

Facteur - D 3.2 : Éducation à la cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Administration	La nécessité de renforcer l'éducation nationale en matière de cybersécurité n'est pas encore prise en compte. Un réseau de points de contact nationaux pour les organismes gouvernementaux et réglementaires, les industries critiques et les établissements d'enseignement n'est pas encore établi. La discussion sur la façon dont la gestion coordonnée de l'éducation et de la recherche en matière de cybersécurité améliore le développement des connaissances nationales n'a pas encore commencé ou vient seulement de commencer.	La nécessité de renforcer l'enseignement de la cybersécurité dans les écoles et les universités ou les établissements d'enseignement équivalents a été identifiée par les principaux acteurs gouvernementaux, industriels et universitaires. Les écoles, le gouvernement et l'industrie ne collaborent pas de manière systématique pour fournir les ressources nécessaires à l'enseignement de la cybersécurité. Un budget national axé sur l'éducation à la cybersécurité n'a pas encore été établi. Le système initial de mécanismes et de mesures permettant d'examiner l'offre et la demande de cours de cybersécurité est limité ou au coup par coup.	Une large consultation des parties prenantes du gouvernement, du secteur privé, du monde universitaire et de la société civile permet de définir les priorités en matière d'éducation à la cybersécurité et se reflète dans la stratégie nationale de cybersécurité. Un budget national est consacré à la recherche et aux laboratoires nationaux de cybersécurité dans les universités ou les établissements d'enseignement équivalents. Des concours, des initiatives et des programmes de financement pour les étudiants et les employés sont encouragés par le gouvernement et/ou l'industrie afin d'accroître l'attrait des carrières en cybersécurité. Des processus de contrôles des programmes et des mesures axées sur les résultats pour examiner l'offre et la demande de cours de cybersécurité sont en place et bien financés.	Des mesures sont utilisées pour affiner les actions dans le cadre de l'investissement éducatif afin de créer un cadre d'experts en cybersécurité dans le pays, tous secteurs confondus. La gestion du budget du gouvernement et les dépenses pour l'éducation à la cybersécurité sont basées sur la demande nationale. Les principales institutions universitaires nationales en matière de cybersécurité partagent les enseignements tirés avec leurs homologues nationaux et internationaux. Le gouvernement a créé des centres universitaires d'excellence en matière de cybersécurité.	Des centres d'excellence internationaux en matière de cybersécurité sont établis grâce à des programmes de jumelage dirigés par des institutions de classe mondiale. La coopération entre toutes les parties prenantes de l'éducation à la cybersécurité est courante et peut être prouvée. Le contenu des programmes d'enseignement de la cybersécurité est aligné sur les problèmes pratiques de cybersécurité et les défis des entreprises et fournit un mécanisme pour améliorer les programmes en fonction de l'évolution du paysage.

Facteur - D 3.3 : Formation des professionnels de la cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Mise à disposition	Il existe peu ou pas de programmes de formation en matière de cybersécurité.	La nécessité de former des professionnels à la cybersécurité a été documentée au niveau national. Le personnel informatique général reçoit une formation sur les questions de cybersécurité afin de pouvoir réagir aux incidents lorsqu'ils se produisent, mais il n'existe aucune formation destinée aux professionnels de la sécurité. La certification professionnelle ICT* est proposée, avec certains modules ou composants de sécurité. Les formations et certifications relatives aux meilleures pratiques peuvent être accessibles via des sources internationales en ligne (par exemple : CISSP**). Des formations au coup par coups, des séminaires et des ressources en ligne sont disponibles pour les professionnels de la cybersécurité par le biais de sources publiques ou privées, mais les preuves de leur utilisation sont limitées.	Des programmes structurés de formation à la cybersécurité existent pour développer les compétences en vue de constituer un cadre de professionnels spécialisés dans la cybersécurité. Les cadres professionnels nationaux ou internationaux en matière de cybersécurité et les meilleures pratiques internationales sont pris en considération lors de la conception des cours de formation professionnelle. La certification professionnelle en matière de sécurité est proposée dans tous les secteurs du pays. Les besoins de la société sont bien compris, et une liste des exigences de formation est documentée. Les programmes de formation destinés aux non professionnels de la cybersécurité sont reconnus et proposés. Des initiatives gouvernementales permettant de rester dans le pays après avoir suivi avec succès des programmes de formation en cybersécurité pourraient être mises en place.	Une gamme de cours de formation à la cybersécurité est conçue pour répondre à la demande stratégique nationale et s'aligner sur les bonnes pratiques internationales. Les programmes de formation reprennent les priorités de la stratégie nationale de cybersécurité. Les programmes de formation sont proposés aux professionnels de la cybersécurité et se concentrent sur les compétences nécessaires pour communiquer des défis techniquement complexes à des publics non techniques, tels que la direction et les employés en général. Des paramètres axés sur les résultats, tirés de données complètes sur l'offre et la demande de professionnels de la cybersécurité, sont utilisés pour définir les modes, la durabilité et les procédures des futurs programmes de formation.	Les secteurs public et privé collaborent pour proposer des formations, s'adaptent en permanence et cherchent à développer des compétences issues des deux secteurs. Les offres de formation et les programmes d'enseignement sont coordonnés afin que les bases établies dans les écoles puissent permettre aux programmes de formation de constituer une main-d'œuvre hautement qualifiée. Des programmes et des structures d'incitation sont en place pour garantir le maintien de la main-d'œuvre formée dans le pays.

Technologies de l'information et des communications
** Professionnel certifié en sécurité des systèmes d'information

Facteur - D 3.3 : Formation des professionnels de la cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Adoption	L'adoption de la formation par le personnel informatique désigné pour répondre aux incidents de cybersécurité est limitée ou inexistante. Il n'y a pas de transfert de connaissances entre les employés formés à la cybersécurité et les employés non formés.	Les mesures qui évaluent l'utilisation des formations ponctuelles, des séminaires, des ressources en ligne et des offres de certification ont une portée limitée ou ne sont pas systématiques. Le transfert de connaissances des employés formés à la cybersécurité vers des employés non formés, dans le secteur public et privé, estau coup par coup.	Il existe un cadre établi d'employés certifiés formés aux questions de cybersécurité, aux processus, à la planification et à l'analyse. Il pourrait exister un registre national d'étudiants et de professionnels ayant réussi et certifiés. Le transfert de connaissances entre les employés formés à la cybersécurité et les employés non formés des secteurs public et privé est établi. Des initiatives de création d'emplois dans le domaine de la cybersécurité au sein des organisations sont en place et encouragent les employeurs à former leur personnel pour en faire des professionnels de la cybersécurité. Des processus de révision du programme et des paramètres sont en place pour permettre de mesurer les progrès et d'évaluer l'offre et la demande de travailleurs qualifiés en matière de cybersécurité dans les environnements publics et privés. Ces processus sont financés de manière adéquate.	La participation à la formation en matière de cybersécurité est utilisée pour informer les futurs programmes de formation. La coordination de la formation dans tous les secteurs permet de répondre à la demande nationale de professionnels.	Les professionnels de la cybersécurité ne se contentent pas de répondre aux exigences nationales, mais les professionnels nationaux à l'étranger sont consultés pour partager les leçons apprises et les meilleures pratiques.

Facteur - D 3.4 : Recherche et innovation en matière de cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Recherche et développement	Les activités de recherche et développement (R&D) en matière de cybersécurité sont limitées, voire inexistantes, dans le pays. Il n'y a pas d'accès aux activités de R&D en cybersécurité d'autres pays.	Une certaine intégration des activités de R&D en matière de cybersécurité a lieu au sein du pays, ou avec un pays partenaire qui comprend comment la R&D en matière de cyberactivité s'applique au contexte local du pays. Le pays peut participer à des réseaux régionaux ou internationaux de collaboration en matière de recherche sur la cybersécurité. Les mesures de la performance de la R&D en matière de cybersécurité ont une portée limitée ou ne sont pas systématiques.	Des activités de R&D en matière de cybersécurité ont été mises en place et sont indiquées dans la stratégie nationale de cybersécurité. La stratégie de R&D peut être en cours d'élaboration. Les ressources et les processus nécessaires pour mener à bien les actions de R&D en matière de cybersécurité ont été identifiés et sont en place. Le financement est suffisant pour mener à bien ces actions. Il existe une collaboration régionale/internationale active avec des pratiques et des développements de pointe. Le pays participe et contribue activement aux réseaux régionaux et internationaux de collaboration en matière de recherche sur la cybersécurité. Les paramètres de mesure des performances de la R&D sont en place et permettent de mesurer les progrès et d'améliorer les capacités de R&D en matière de cybersécurité du pays.	Le pays s'emploie activement à créer des communautés d'intérêts autour des priorités de R&D en matière de cybersécurité. La stratégie de R&D est en place et entièrement mise en œuvre. Le pays apporte une contribution majeure à la R&D en matière de cybersécurité et participe activement au renforcement des capacités d'innovation par le biais de consortiums internationaux de R&D et d'investissements. Les risques émergents en matière de cybersécurité sont régulièrement évalués et utilisés pour mettre à jour la stratégie nationale en matière de cybersécurité et le développement des futurs programmes de la stratégie de recherche et développement. La synergie entre les établissements universitaires et l'industrie soutient les activités de R&D et sert à concevoir des cyberprogrammes qui couvrent les besoins de l'industrie.	Le pays est un acteur de premier plan dans le domaine de la recherche et de l'innovation en matière de cybersécurité et oriente les débats internationaux sur l'élaboration de plans stratégiques de recherche et développement. Le pays est tourné vers l'avenir, il voit les problèmes émergents (autour des nouvelles technologies ou des nouveaux types de menaces) et utilise la R&D pour préparer un environnement de menaces futures. Le pays contribue aux meilleures pratiques internationales en matière de R&D sur la cybersécurité.

4e dimension : cadres juridiques et réglementaires

Cette *dimension* examine la capacité du gouvernement à concevoir et à promulguer une législation nationale directement ou indirectement liée à la cybersécurité, en mettant l'accent sur les exigences réglementaires en matière de cybersécurité, la législation relative à la cybercriminalité et la législation connexe. La capacité à faire appliquer ces lois est examinée par le biais des capacités des services répressifs, des poursuites judiciaires, des organismes de réglementation et des tribunaux. En outre, cette *dimension* observe des questions telles que les cadres de coopération formels et informels pour lutter contre la cybercriminalité.

Facteur
D 4.1 : Dispositions légales et

Ce *facteur* aborde diverses dispositions législatives et réglementaires relatives à la cybersécurité, notamment les exigences légales et réglementaires, la législation sur la cybercriminalité de fond et de procédure, et l'évaluation de l'impact sur les droits de l'homme.
> Navigate to Factor

Aspects

- **Législation de fond sur la cybercriminalité :** cet *aspect* examine si la législation existante criminalise une variété de cybercrimes dans une législation spécifique ou dans le droit pénal général ;
- **Exigences juridiques et réglementaires en matière de cybersécurité :** cet *aspect* examine l'existence de cadres juridiques et réglementaires en matière de cybersécurité ;
- **Législation procédurale en matière de cybercriminalité :** cet *aspect* examine si un droit procédural pénal complet — avec des pouvoirs procéduraux pour les enquêtes sur la cybercriminalité et des exigences en matière de preuve pour dissuader, répondre et poursuivre la cybercriminalité et les crimes impliquant des preuves électroniques — est mis en œuvre ; et
- **Évaluation de l'impact sur les droits de l'homme :** cet *aspect* examine si des évaluations de l'impact sur les droits de l'homme de la législation substantielle et procédurale sur la cybercriminalité et des réglementations sur la cybersécurité sont effectuées.

Facteur
D 4.2 : Cadres législatifs connexes

Ce *facteur* traite des cadres législatifs liés à la cybersécurité, notamment la protection des données, la protection des enfants, la protection des consommateurs et la propriété intellectuelle.
> Navigate to Factor

Aspects

- **Législation sur la protection des données :** cet *aspect* examine l'existence et la mise en œuvre d'une législation complète sur la protection des données ;
- **Protection des enfants en ligne :** cet *aspect* se concentre sur la protection législative des enfants en ligne, y compris la protection de leurs droits en ligne et la criminalisation de l'abus des enfants en ligne ;
- **Législation sur la protection des consommateurs :** cet *aspect* traite de l'existence et de la mise en œuvre de la législation protégeant les consommateurs en ligne contre la fraude et d'autres formes de mauvaises pratiques commerciales ; et
- **Législation sur la propriété intellectuelle :** cet *aspect* concerne l'existence et la mise en œuvre d'une législation sur la propriété intellectuelle en ligne.

Facteur

D 4.3. Capacités et moyens juridiques et réglementaires

Ce *facteur* étudie la capacité des forces de l'ordre à enquêter sur la cybercriminalité, la capacité du ministère public à présenter des affaires de cybercriminalité et de preuves électroniques, et la capacité des tribunaux à présider les affaires de cybercriminalité et celles impliquant des preuves électroniques. Enfin, ce *facteur* examine l'existence d'organismes de réglementation intersectoriels chargés de surveiller le respect des réglementations spécifiques en matière de cybersécurité.

> Navigate to Factor

Aspects

- **Application de la loi :** cet *aspect* examine si les agents et organismes chargés de l'application de la loi ont reçu une formation pour enquêter et gérer les affaires de cybercriminalité et les affaires impliquant des preuves électroniques, et si les ressources humaines, procédurales et technologiques sont suffisantes ;
- **Application de la loi :** cet *aspect* examine si les procureurs ont reçu une formation sur le traitement des affaires de cybercriminalité et des affaires impliquant des preuves électroniques, et si les ressources humaines, procédurales et technologiques sont suffisantes ;
- **Tribunaux :** cet *aspect* examine si les tribunaux disposent de ressources et d'une formation suffisantes pour garantir des poursuites efficaces et efficientes dans les affaires de cybercriminalité et les affaires impliquant des preuves électroniques ; et
- **Organismes de réglementation :** cet *aspect* examine l'existence d'organismes de réglementation intersectoriels chargés de surveiller le respect de réglementations spécifiques en matière de cybersécurité.

Facteur

D 4.3 : Cadres de coopération formelle et informelle pour lutter contre la cybercriminalité

Ce *facteur* traite de l'existence et de la fonction des mécanismes formels et informels qui permettent la coopération entre les acteurs nationaux et au-delà des frontières pour dissuader et combattre la cybercriminalité.

> Navigate to Factor

Aspects

- **Coopération des services répressifs avec le secteur privé :** cet *aspect* examine le mécanisme d'échange d'informations sur la cybercriminalité entre les secteurs public et privé nationaux, y compris la coopération avec les prestataires de services Internet et d'autres technologies ;
- **Coopération avec les homologues étrangers chargés de l'application des lois :** cet *aspect* examine l'existence de mécanismes formels de coopération internationale en matière d'application des lois ; et
- **Collaboration entre le gouvernement et le secteur de la justice pénale :** cet *aspect* passe en revue les canaux de communication officiels entre le gouvernement et les acteurs de la justice pénale.

Facteur - D 4.1: Legal and Regulatory Provisions

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Législation de fond sur la cybercriminalité	Il n'existe pas de droit pénal matériel spécifique à la cybercriminalité . Un droit pénal général peut exister, mais son application à la cybercriminalité n'est pas claire.	Il existe une législation partielle qui aborde certains aspects de la cybercriminalité, ou des dispositions légales en matière de cybercriminalité sont en cours d'élaboration.	Les dispositions juridiques de fond en matière de cybercriminalité sont contenues dans une législation spécifique ou un droit pénal général. Le pays peut avoir ratifié des instruments régionaux ou internationaux sur la cybercriminalité. Le pays cherche systématiquement à mettre en œuvre ces mesures dans le droit national.	Des mesures sont en place pour dépasser les niveaux de référence minimaux spécifiés dans les traités internationaux, le cas échéant. Le pays cherche à adapter sa législation de fond sur la cybercriminalité pour tenir compte des technologies émergentes et de leur utilisation.	Le droit substantiel en matière de cybercriminalité est construit de manière à pouvoir s'adapter aux changements dynamiques de la technologie sous-jacente et de l'environnement des menaces, sans qu'il soit nécessaire de procéder à une révision substantielle et longue. Le pays contribue activement à la promotion internationale d'une législation efficace en matière de cybercriminalité.
Exigences légales et réglementaires en matière de cybersécurité	Les exigences en matière de cybersécurité définies par la réglementation ou la loi sont limitées. La nécessité de créer des cadres juridiques et réglementaires sur la cybersécurité peut avoir été reconnue et avoir donné lieu à une analyse des lacunes.	Les parties prenantes des secteurs concernés ont été consultées pour soutenir l'établissement de cadres juridiques et réglementaires. Des projets de législation et de réglementation peuvent être en place, mais ils doivent encore être adoptés et peuvent ne pas couvrir tous les secteurs concernés.	Des exigences complètes en matière de cybersécurité sont définies dans la réglementation et la législation pertinentes (y compris les exigences spécifiques au secteur, le cas échéant). Ces exigences peuvent inclure des normes obligatoires, ou des exigences de notification des violations et de divulgation des vulnérabilités. Les responsabilités civiles et pénales pertinentes sont clairement définies et comprises par les entités réglementées. Les organes juridiques et réglementaires compétents disposent des pouvoirs nécessaires pour faire respecter ces exigences.	L'efficacité de la législation et de la réglementation en matière d'amélioration des pratiques de cybersécurité est régulièrement évaluée et utilisée pour guider leur développement futur. Les réglementations sont mises à jour pour tenir compte des technologies émergentes.	Les cadres réglementaires sont suffisamment souples pour s'adapter aux changements rapides de l'environnement technologique ou des menaces sous-jacentes. Le pays promeut les meilleures pratiques en matière de législation et de réglementation au niveau international. Le pays participe activement à l'élaboration d'accords internationaux visant à promouvoir une harmonisation et une reconnaissance mutuelle des lois et réglementations en matière de cybersécurité.

Facteur - D 4.1: Legal and Regulatory Provisions

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Législation procédurale sur la cybercriminalité	Il n'existe pas de droit pénal procédural spécifique à la cybercriminalité. La manière dont le droit procédural pénal général s'applique aux enquêtes, aux poursuites et aux preuves électroniques en matière de cybercriminalité n'est pas claire.	L'élaboration d'une législation procédurale spécifique à la cybercriminalité, ou la modification du droit pénal procédural général pour l'adapter aux cas de cybercriminalité a commencé.	Une loi de procédure pénale complète contenant des dispositions relatives aux enquêtes sur la cybercriminalité et aux exigences en matière de preuves a été adoptée et est appliquée. Le pays peut avoir ratifié des instruments régionaux ou internationaux sur la cybercriminalité. Le pays cherche systématiquement à mettre en œuvre ces mesures dans le droit national. Les lois procédurales relatives à la cybercriminalité permettent l'échange d'informations (et d'autres actions requises) pour favoriser le succès des enquêtes transfrontalières sur la cybercriminalité.	Des mesures sont en place pour dépasser les niveaux de référence minimaux spécifiés dans les traités internationaux, le cas échéant. Le pays cherche à adapter les législations procédurales en matière de cybercriminalité pour tenir compte des technologies émergentes et de leur utilisation.	Le droit procédural en matière de cybercriminalité est construit de manière à pouvoir s'adapter aux changements dynamiques de la technologie sous-jacente et de l'environnement des menaces, sans qu'il soit nécessaire de procéder à une révision substantielle et longue. Le pays contribue activement à la promotion d'une législation procédurale efficace en matière de cybercriminalité et d'instruments visant à améliorer les enquêtes internationales sur la cybercriminalité.
Évaluation de l'impact sur les droits de l'homme	Une législation substantielle et procédurale sur la cybercriminalité et des réglementations sur la cybersécurité sont peut-être en cours d'élaboration, mais aucune évaluation d'impact sur les droits de l'homme n'a été réalisée.	Des évaluations de l'impact sur les droits de l'homme de la législation sur la cybercriminalité et de la réglementation sur la cybersécurité, tant sur le fond que sur la forme, ont pu être réalisées, y compris l'examen des conséquences sur la vie privée et la liberté d'expression. Certaines questions n'ont toutefois pas encore été résolues. Des experts en droits de l'homme ont été consultés lors de l'élaboration de la législation et de la réglementation.	Des évaluations complètes de l'impact sur les droits de l'homme de la législation sur la cybercriminalité et des réglementations sur la cybersécurité, tant sur le fond que sur la forme, ont été réalisées et les normes internationales sont respectées. La mise en œuvre de cette législation fait l'objet d'un contrôle régulier du respect des droits de l'homme, qui est vérifié de manière indépendante.	Les évaluations d'impact sur les droits de l'homme sont régulièrement révisées afin de garantir que les pratiques restent compatibles avec les exigences en matière de droits de l'homme et que l'effet des technologies émergentes est pris en compte. La manière dont la cybersécurité peut renforcer la protection des droits de l'homme dans le pays et au niveau international a également été examinée.	Le pays contribue activement au développement et à la promotion des évaluations d'impact sur les droits de l'homme en matière de cybersécurité.

Facteur - D 4.2: Cadres législatifs connexes

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Législation sur la protection des données	La législation sur la protection des données n'existe pas.	La législation sur la protection des données est en cours d'élaboration. Les parties prenantes des secteurs concernés ont été consultées pour soutenir l'élaboration de cette législation.	Une législation complète sur la protection des données, conforme aux normes internationales et aux meilleures pratiques, a été adoptée et est appliquée. Un organisme responsable de la protection des données a été désigné.	L'efficacité de la législation sur la protection des données est régulièrement évaluée et utilisée pour son développement. Le pays cherche à adapter les lois sur la protection des données pour tenir compte des technologies émergentes et de leur utilisation.	La législation sur la protection des données est conçue de manière à pouvoir s'adapter aux changements dynamiques de la technologie sous-jacente et de l'environnement des menaces, sans qu'il soit nécessaire de procéder à une révision substantielle et prolongée. Le pays développe et promeut des normes internationales en matière de législation sur la protection des données. Le pays participe activement à l'élaboration d'instruments juridiques permettant d'améliorer la collaboration internationale dans ce domaine.
Protection de l'enfance en ligne	La législation relative à la protection de l'enfance est limitée et son application dans l'environnement en ligne n'a pas encore été examinée.	La législation relative à la protection des enfants est en place et est adaptée pour refléter son application dans l'environnement en ligne. Les parties prenantes des secteurs concernés ont été consultées pour soutenir le développement et l'adaptation de cette législation.	L'application de la protection des enfants dans l'environnement en ligne est comprise et reflétée dans la législation pertinente. La législation est appliquée conformément aux normes internationales et aux meilleures pratiques.	L'efficacité de la législation sur la protection des enfants en ligne est régulièrement évaluée et utilisée pour son développement. Le pays cherche à adapter la loi sur la protection de l'enfance pour tenir compte des technologies émergentes et de leur utilisation.	La législation sur la protection des enfants en ligne est conçue de manière à pouvoir s'adapter aux changements dynamiques de la technologie sous-jacente et de l'environnement des menaces, sans qu'il soit nécessaire de procéder à une révision substantielle et longue. Le pays est en train d'élaborer et de promouvoir des normes internationales pour la loi sur la protection des enfants en ligne. Le pays participe activement à l'élaboration d'instruments juridiques permettant d'améliorer la collaboration internationale dans ce domaine.

Facteur - D 4.2: Cadres législatifs connexes

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Législation sur la protection des consommateurs	La législation relative à la protection des consommateurs est limitée et son application dans l'environnement en ligne doit encore être envisagée.	La législation relative à la protection des consommateurs est en place et est en cours d'adaptation pour refléter son application dans l'environnement en ligne. Les parties prenantes des secteurs concernés ont été consultées pour soutenir l'élaboration de cette législation.	L'application de la protection des consommateurs dans l'environnement en ligne est comprise et reflétée dans la législation pertinente. La législation est mise en œuvre conformément aux normes internationales et aux meilleures pratiques.	L'efficacité de la législation sur la protection des consommateurs en ligne est régulièrement évaluée et utilisée pour son développement. Le pays cherche à adapter la législation sur la protection des consommateurs pour tenir compte des technologies émergentes et de leur utilisation.	La législation sur la protection des consommateurs est conçue de manière à pouvoir s'adapter aux changements dynamiques de la technologie sous-jacente et de l'environnement des menaces, sans qu'il soit nécessaire de procéder à une révision substantielle et longue. Le pays élabore et promeut des normes internationales en matière de législation sur la protection des consommateurs en ligne. Le pays participe activement à l'élaboration d'instruments juridiques permettant d'améliorer la collaboration internationale dans ce domaine.
Législation sur la propriété intellectuelle	La législation relative à la protection de la propriété intellectuelle est limitée et son application dans l'environnement en ligne doit encore être envisagée.	La législation relative à la protection de la propriété intellectuelle est en place et est adaptée pour refléter son application dans l'environnement en ligne. Les parties prenantes des secteurs concernés ont été consultées pour soutenir l'élaboration de cette législation.	L'application de la protection de la propriété intellectuelle dans l'environnement en ligne est comprise et reflétée dans la législation pertinente. La législation est mise en œuvre conformément aux normes internationales et aux meilleures pratiques.	L'efficacité de la législation sur la protection de la propriété intellectuelle en ligne est régulièrement évaluée et utilisée pour son développement. Le pays cherche à adapter la législation sur la protection de la propriété intellectuelle pour tenir compte des technologies émergentes et de leur utilisation.	La législation sur la propriété intellectuelle est conçue de manière à pouvoir s'adapter aux changements dynamiques de la technologie sous-jacente et de l'environnement des menaces, sans qu'il soit nécessaire de procéder à une révision substantielle et longue. Le pays élabore et promeut des normes internationales pour la législation sur la protection intellectuelle en ligne. Le pays participe activement à l'élaboration d'instruments juridiques permettant d'améliorer la collaboration internationale dans ce domaine.

Facteur - D 4.3: Capacités et moyens juridiques et réglementaires

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Application de la loi	Les agents/agences chargés de faire respecter la loi ne disposent pas de capacités suffisantes pour prévenir et combattre la cybercriminalité et ne reçoivent pas de formation spécialisée sur les enquêtes en matière de cybercriminalité.	Les mesures d'investigation traditionnelles sont appliquées aux enquêtes sur la cybercriminalité, mais les capacités d'investigation numérique sont limitées. Les agents des services répressifs peuvent recevoir une formation sur la cybercriminalité et les preuves numériques, mais cela n'est pas systématique.	Une capacité institutionnelle globale dotée de ressources humaines, procédurales et technologiques suffisantes pour enquêter sur les affaires de cybercriminalité a été mise en place. La chaîne de conservation numérique et l'intégrité des preuves sont établies, y compris les processus formels, les rôles et les responsabilités. Des normes pour la formation des agents des services répressifs en matière de cybercriminalité et de preuves numériques existent et sont mises en œuvre. Les rôles respectifs des forces de l'ordre nationales et étatiques/locales sont compris et les forces étatiques/locales sont équipées pour assumer leur rôle.	Les évaluations quantifiées des risques sont utilisées pour allouer des ressources aux unités opérationnelles chargées de la cybercriminalité (aux niveaux national et étatique/local). Les tendances et les statistiques sur la cybercriminalité, les interventions des services répressifs et leur impact sur la réduction des risques sont collectées, analysées et utilisées pour éclairer la stratégie et la décision d'affectation des ressources à long terme. Les stratégies de répression comprennent des mesures de prévention de la criminalité ainsi que des mesures de répression. Les renseignements sont utilisés pour soutenir les enquêtes proactives. Les services répressifs ont les moyens de maintenir l'intégrité des données afin de respecter les normes internationales en matière de preuve dans les enquêtes transfrontalières.	Le pays participe activement à la mise en place de plateformes de collaboration entre les services répressifs nationaux. Les services répressifs du pays sont à l'avant-garde du développement de nouvelles capacités et approches pour la prévention et la perturbation de la cybercriminalité et la promotion de leur utilisation au niveau international.
Ministère public	Les procureurs ne reçoivent pas la formation et les ressources adéquates pour examiner les preuves électroniques ou poursuivre la cybercriminalité. La consultation a peut-être commencé à envisager cette capacité dans la communauté des procureurs.	Un nombre limité de procureurs ont la capacité de mener des affaires de cybercriminalité et de traiter les preuves électroniques, mais cette capacité n'est pas systématique et n'est pas institutionnalisée. Si les procureurs reçoivent une formation sur la cybercriminalité et les preuves numériques, elle n'est pas systématique.	Une capacité institutionnelle complète, comprenant des ressources humaines et technologiques suffisantes, pour poursuivre les affaires de cybercriminalité et les affaires impliquant des preuves électroniques est établie. Un cadre spécialisé de procureurs spécialisés dans la cybercriminalité a peut-être été créé.	Des structures institutionnelles sont en place, avec une répartition claire des tâches et des obligations au sein des services du ministère public à tous les niveaux de l'État. Il existe un mécanisme qui permet l'échange d'informations et de bonnes pratiques entre les procureurs et les juges afin de garantir l'efficacité des poursuites dans les affaires de cybercriminalité.	Il existe une capacité nationale à poursuivre les affaires complexes de cybercriminalité nationale et transfrontalière.

Facteur - D 4.3: Capacités et moyens juridiques et réglementaires

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Tribunaux	Il n'existe aucun processus visant à équiper les juges afin qu'ils puissent présider des affaires de cybercriminalité ou des affaires impliquant des preuves électroniques. La consultation a peut-être commencé à prendre en compte cette capacité dans la communauté judiciaire.	Un nombre limité de juges ont la capacité de présider une affaire de cybercriminalité, mais cette capacité n'est pas systématique. Si les juges reçoivent une formation sur la cybercriminalité et les preuves numériques, elle n'est pas systématique.	Des ressources humaines et technologiques suffisantes sont disponibles pour assurer des procédures judiciaires efficaces et efficientes concernant les affaires de cybercriminalité et les affaires impliquant des preuves électroniques. Les juges reçoivent une formation spécialisée sur la cybercriminalité et les preuves électroniques. Les tribunaux nationaux/locaux sont équipés pour traiter les affaires de cybercriminalité, en fonction de leur niveau. Les tribunaux compétents sont équipés pour traiter les litiges civils relatifs à la responsabilité en matière de cybersécurité.	La capacité institutionnelle du système judiciaire à traiter les affaires de cybercriminalité est fréquemment examinée et révisée sur la base d'une évaluation de l'efficacité.	Le pays participe activement au développement et à la promotion des meilleures pratiques dans la conduite des affaires de cybercriminalité.
Organismes de réglementation	Les régulateurs sectoriels ont une compréhension limitée de l'impact potentiel de la cybernétique sur leurs entités réglementées. Il n'existe pas d'organisme de réglementation intersectoriel chargé de superviser les exigences spécifiques en matière de cybersécurité.	Les régulateurs sectoriels ont commencé à définir leur rôle en matière de cybersécurité. Une exigence de création d'organismes de réglementation intersectoriels chargés de surveiller le respect de réglementations spécifiques en matière de cybersécurité a pu être envisagée. Les parties prenantes concernées ont été consultées dans le cadre de ce processus.	Les régulateurs sectoriels (par exemple, dans les domaines de la finance, de l'énergie et des transports) disposent des capacités et des ressources nécessaires pour surveiller le respect des exigences de cybersécurité dans leur secteur. Lorsque des organismes de réglementation intersectoriels ont été créés pour superviser la cybersécurité, ils disposent des capacités et des ressources nécessaires pour assumer leur rôle.	L'impact des actions réglementaires sur les pratiques de cybersécurité des organisations est régulièrement évalué et utilisé pour informer l'activité de surveillance et l'élaboration de la réglementation. Les organismes de réglementation évaluent régulièrement les technologies émergentes et leur impact potentiel sur la cybersécurité des entités réglementées. Les interventions et les enquêtes réglementaires s'appuient sur les évaluations nationales du risque cybernétique et sont hiérarchisées en fonction de celles-ci.	Les organismes de réglementation participent activement au développement et à la promotion des meilleures pratiques réglementaires au niveau international.

Facteur - D 4.4 : Cadres de coopération formelle et informelle pour lutter contre la cybercriminalité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Coopération entre les services répressifs et le secteur privé	La coopération entre les secteurs public et privé nationaux en matière de cybercriminalité est limitée. Plus précisément, une coopération entre les prestataires de services Internet et d'autres technologies et les services répressifs n'a pas été établie.	L'échange d'informations sur la cybercriminalité entre les secteurs public et privé nationaux n'est pas systématique et non réglementé. Plus précisément, une coopération au coup par coup entre les prestataires de services Internet et d'autres technologies et les services répressifs existe, mais n'est pas toujours efficace.	Les informations sont régulièrement échangées entre les secteurs publics et privés nationaux et sont soutenues par une législation appropriée. Des mécanismes de coopération efficaces entre les prestataires de services Internet et d'autres technologies et les services répressifs ont été mis en place dans le cadre de ces accords de collaboration plus larges entre le secteur public et le secteur privé.	L'efficacité de la coopération publique et privée est régulièrement évaluée et utilisée pour améliorer les processus de collaboration. Les cadres de collaboration sont régulièrement adaptés pour tenir compte des nouvelles technologies et des formes émergentes de cybercriminalité.	Le pays contribue activement à la promotion du partenariat public-privé et au développement de plateformes internationales de partenariat public-privé.
Coopération avec les services répressifs étrangers	Il n'existe que peu ou pas de formes de coopération internationale pour prévenir et combattre la cybercriminalité.	Des mécanismes formels de coopération internationale en matière d'application de la loi peuvent exister, mais leur application à la cybercriminalité n'est pas systématique ou seulement possible dans certains cas. Les services répressifs ne sont pas formellement intégrés dans les réseaux régionaux et internationaux de lutte contre la cybercriminalité.	Des mécanismes formels de coopération internationale entre les services répressifs ont été mis en place pour faciliter la détection, les enquêtes et les poursuites en matière de cybercriminalité. Des accords et mécanismes d'entraide judiciaire et d'extradition ont été établis et sont appliqués aux affaires de cybercriminalité. Les services répressifs nationaux sont intégrés aux réseaux régionaux et internationaux, tels qu'Interpol ou les réseaux 24/7.	Les services répressifs travaillent conjointement avec leurs homologues étrangers, éventuellement par le biais de groupes de travail conjoints, ce qui permet de mener à bien des enquêtes et des poursuites transfrontalières en matière de cybercriminalité.	Le pays contribue activement à la promotion et au développement des mécanismes de coopération internationale.
Collaboration entre le gouvernement et le secteur de la justice pénale	L'interaction entre le gouvernement et les acteurs de la justice pénale est minime.	L'échange d'informations entre le gouvernement et les acteurs de la justice pénale est limité et n'est pas systématique.	Des relations formelles ont été établies entre le gouvernement et les acteurs de la justice pénale, ce qui se traduit par un échange régulier d'informations sur les questions de cybercriminalité.	Les relations entre les acteurs gouvernementaux, les procureurs, les juges et les organismes chargés de l'application de la loi sont régulièrement évaluées et utilisées pour améliorer leur efficacité.	Le pays contribue activement à la promotion internationale d'un échange efficace et rapide d'informations entre les pouvoirs publics et les acteurs de la justice pénale.

5e dimension : normes et technologies

Cette *dimension* concerne l'utilisation efficace et généralisée des technologies de cybersécurité pour protéger les personnes, les organisations et les infrastructures nationales. La *dimension* examine spécifiquement la mise en œuvre de normes et de bonnes pratiques en matière de cybersécurité, le déploiement de processus et de contrôles, et le développement de technologies et de produits afin de réduire les risques liés à la cybersécurité.

Facteur
D 5.1 : Adhésion aux normes

Ce *facteur* examine la capacité du gouvernement à promouvoir, évaluer la mise en œuvre et contrôler la conformité aux normes et bonnes pratiques internationales en matière de cybersécurité.
> Navigate to Factor

Aspects

- **Normes de sécurité des TIC :** cet *aspect* examine si les normes et les bonnes pratiques en matière de cybersécurité sont respectées et mises en œuvre à grande échelle dans le secteur public et les organisations de CI ;
- **Normes en matière de passation de marchés :** cet *aspect* concerne la mise en œuvre de normes et de bonnes pratiques dans tous les secteurs pour guider les processus de passation de marchés, y compris la gestion des risques, la gestion du cycle de vie, l'assurance des logiciels et du matériel, l'externalisation et l'utilisation des services infonuagiques ; et
- **Normes pour la fourniture de produits et la prestation de services :** cet *aspect* concerne l'utilisation de normes et de bonnes pratiques par les fournisseurs locaux de biens et de services, y compris les logiciels, le matériel, les services gérés et les services infonuagiques.

Facteur
D 5.2 : Contrôles de sécurité

Ce *facteur* examine les preuves concernant le déploiement des contrôles de sécurité par les utilisateurs et les secteurs public et privé, et vérifie si l'ensemble des contrôles technologiques de cybersécurité est basé sur des cadres de cybersécurité établis.
> Navigate to Factor

Aspects

- **Contrôles de sécurité technologique :** cet *aspect* examine dans quelle mesure les contrôles de sécurité technologique à jour, y compris les correctifs et les sauvegardes, sont déployés dans tous les secteurs ; et
- **Contrôles cryptographiques :** cet *aspect* examine le déploiement de techniques cryptographiques dans tous les secteurs et chez tous les utilisateurs pour la protection des données au repos ou en transit, et la mesure dans laquelle ces contrôles cryptographiques répondent aux normes et directives internationales et sont tenus à jour.

Facteur
D 5.3 : Qualité du logiciel

Ce *facteur* examine la qualité du déploiement des logiciels et les exigences fonctionnelles dans les secteurs public et privé. En outre, ce *facteur* examine l'existence et l'amélioration des politiques et des processus de mise à jour et de maintenance des logiciels en fonction des évaluations des risques et de la nature critique des services.
> Navigate to Factor

Aspects

- **Qualité et assurance des logiciels :** (comme ci-dessus)

Facteur

D 5.4 : Résilience des infrastructures de communication et d'Internet

Ce *facteur* traite de l'existence de services et d'infrastructures Internet fiables dans le pays, ainsi que de processus de sécurité rigoureux dans les secteurs privé et public. Ce *facteur* examine également le contrôle que le gouvernement peut avoir sur son infrastructure Internet et la mesure dans laquelle les réseaux et les systèmes sont externalisés.
> Navigate to Factor

Aspects

- **Fiabilité de l'infrastructure Internet :** cet *aspect* examine la fiabilité et la protection des services et de l'infrastructure Internet dans les secteurs public et privé ; et
- **Surveillance et réponse :** cet *aspect* examine si des mécanismes sont en place pour effectuer des évaluations des risques et surveiller la résilience des réseaux dans les secteurs public et privé.

Facteur

D 5.5 : Marché de la cybersécurité

Ce *facteur* concerne la disponibilité et le développement de technologies de cybersécurité compétitives, de produits de cyberassurance, de services et d'expertise en matière de cybersécurité, ainsi que les implications de l'externalisation en matière de sécurité.
> Navigate to Factor

Aspects

- **Technologies de cybersécurité :** cet *aspect* examine si un marché national des technologies de cybersécurité est présent et soutenu, et s'il répond à un besoin national ;
- **Services et expertise en matière de cybersécurité :** cet *aspect* explore la disponibilité des services de conseil en cybersécurité pour les organisations privées et publiques ;
- **Implications de l'externalisation en matière de sécurité :** cet *aspect* examine si des évaluations des risques sont effectuées pour déterminer comment atténuer les risques liés à l'externalisation de l'informatique vers un tiers ou des services infonuagiques ; et
- **cyberassurance :** cet *aspect* explore l'existence d'un marché de la cyberassurance, sa couverture et les produits adaptés aux différentes organisations.

• Facteur

D 5.6 : Divulgation responsable

Ce *facteur* explore la mise en place d'un cadre de divulgation responsable pour la réception et la diffusion d'informations sur la vulnérabilité dans tous les secteurs, et examine s'il existe une capacité suffisante pour revoir et mettre à jour ce cadre en permanence.
> Navigate to Factor

Aspects

- **Partage des informations sur les vulnérabilités :** cet *aspect* explore les mécanismes ou canaux de partage d'informations existants sur les détails techniques des vulnérabilités entre les parties prenantes ; et
- **Politiques, processus et législation pour la divulgation responsable des failles de sécurité :** cet *aspect* explore l'existence d'une politique ou d'un cadre de divulgation responsable dans les organisations des secteurs public et privé et le droit à des protections juridiques pour ceux qui divulguent des failles de sécurité.

Facteur - D 5.1 : Adhésion aux normes

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Normes de sécurité des TIC	Aucune norme ou bonne pratique n'a été identifiée pour la sécurisation des données, des technologies ou des infrastructures, par les secteurs public et privé. Les secteurs public et privé ont procédé à une première identification de certaines normes et bonnes pratiques appropriées, et éventuellement à une mise en œuvre au coup par coup, mais aucun effort concerté pour mettre en œuvre ou modifier les pratiques existantes de manière mesurable.	Des normes de gestion des risques liés à l'information ont été identifiées en vue d'être utilisées et des premiers signes de promotion et d'adoption ont été observés dans les secteurs public et privé. Il existe quelques preuves de la mise en œuvre et de l'utilisation mesurables des normes et bonnes pratiques internationales.	Une base de référence convenue au niveau national de normes et de bonnes pratiques en matière de cybersécurité a été identifiée et largement mise en œuvre dans les secteurs public et privé. Une entité au sein du gouvernement existe pour évaluer l'utilisation des normes dans les secteurs public et privé. Des programmes gouvernementaux existent pour promouvoir des améliorations continues, et des mesures sont appliquées pour contrôler la conformité. Le gouvernement et les IC réfléchissent à la manière dont les normes et les meilleures pratiques peuvent être utilisées pour gérer les risques au sein des chaînes d'approvisionnement des IC.	Le gouvernement et les organisations encouragent l'utilisation des normes et des meilleures pratiques en fonction de l'évaluation des risques nationaux et des choix budgétaires. Le choix des normes et des meilleures pratiques ainsi que leur mise en œuvre sont continuellement révisés. Les risques émergents en matière de cybersécurité sont régulièrement évalués et utilisés pour réévaluer la nécessité de normes de sécurité TIC supplémentaires. Il existe des preuves d'un débat entre le gouvernement et d'autres parties prenantes sur la manière dont les décisions relatives aux ressources nationales et organisationnelles devraient s'aligner et conduire à la mise en œuvre des normes. Il existe des preuves de la contribution aux organismes internationaux de normalisation, ce qui contribue à la direction de la réflexion et au partage d'expérience par les organisations.	Le pays participe activement à l'élaboration et à la promotion de normes définies au niveau international. La mise en œuvre des normes et les décisions de non-conformité sont prises en réponse à l'évolution des environnements de menace et des facteurs de ressources dans les secteurs et les IC, par le biais d'une gestion collaborative des risques. Il existe des preuves d'un débat au sein de tous les secteurs sur la conformité aux normes et aux meilleures pratiques, sur la base d'évaluations continues des besoins.

Facteur - D 5.1 : Adhésion aux normes

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Normes en matière de passation de marchés	Aucune norme ou meilleure pratique n'a été identifiée pour guider les processus de passation de marchés des secteurs public et privé. Si elles sont reconnues, leur mise en œuvre est au coup par coup et non coordonnée.	Les normes de cybersécurité et les meilleures pratiques guidant les processus de passation de marchés (y compris la gestion des risques, la gestion du cycle de vie, l'assurance des logiciels et du matériel, l'externalisation et l'utilisation des services infonuagiques) ont été identifiées pour être utilisées. Il existe des preuves de la promotion et de la mise en œuvre des normes et des meilleures pratiques en matière de cybersécurité dans la définition des pratiques d'achat au sein des secteurs public et privé.	Les normes de cybersécurité et les meilleures pratiques en matière d'orientation des processus de passation de marchés (notamment la gestion des risques, la gestion du cycle de vie, l'assurance des logiciels et du matériel, l'externalisation et l'utilisation des services infonuagiques) sont largement respectées dans les secteurs public et privé. La mise en œuvre et le respect des normes dans les pratiques de passation de marchés dans les secteurs public et privé sont attestés par la mesure et l'évaluation de l'efficacité des processus.	Les organisations ont la possibilité de surveiller et de modifier l'utilisation des normes et des meilleures pratiques dans les processus d'achat, de soutenir les déviations et les décisions de non-conformité lorsque le besoin s'en fait sentir grâce à une prise de décision basée sur les risques. Les risques émergents en matière de cybersécurité sont régulièrement évalués et utilisés pour réévaluer la nécessité de normes supplémentaires dans les marchés publics. Les aspects essentiels des achats et de l'approvisionnement, tels que le coût total du cycle de vie, la qualité, l'interopérabilité, la maintenance, le soutien et les autres activités à valeur ajoutée, sont améliorés en permanence, et les améliorations du processus d'achat sont réalisées dans le cadre d'une planification plus large des ressources. Les organisations sont en mesure d'évaluer les compétences de leurs professionnels de la passation de marchés par rapport aux compétences décrites dans les normes de passation de marchés et d'identifier toute lacune en matière de compétences et de capacités.	Le pays participe activement à l'élaboration et à la promotion de ces normes au niveau international. La mise en œuvre des normes dans les processus d'approvisionnement et les décisions de non-conformité sont prises en fonction de l'évolution des menaces.

Facteur - D 5.1 : Adhésion aux normes

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Normes pour la fourniture de produits et la prestation de services	Soit aucune norme ou meilleure pratique n'a été identifiée pour être utilisée dans la sécurisation des produits et services (en particulier, les logiciels, le matériel, les services gérés et les services infonuagiques) développés ou offerts par les fournisseurs dans le pays. Ou bien il y a une certaine identification, mais seulement des preuves limitées d'utilisation.	Les activités et méthodologies de base pour le développement sécurisé et la gestion du cycle de vie des logiciels, du matériel et de la prestation de services gérés et de services infonuagiques sont identifiées et discutées au sein des communautés professionnelles. Le gouvernement promeut des normes pertinentes en matière de développement de logiciels, d'assurance qualité du matériel, de prestation de services gérés et de sécurité infonuagique, mais rien ne prouve que ces normes soient encore largement adoptées.	Il existe des preuves de la mise en œuvre généralisée de normes dans les processus de développement de logiciels, l'assurance qualité du matériel, la prestation de services gérés et de services infonuagiques par des organisations des secteurs public et privé. Le gouvernement dispose d'un programme établi pour promouvoir et surveiller l'adoption de normes dans le domaine du développement de logiciels, de l'assurance qualité du matériel et de la sécurité infonuagique, pour les systèmes publics et commerciaux. Il existe des preuves que les systèmes à haute intégrité et les techniques de développement de logiciels sont présents dans les offres d'enseignement et de formation du pays.	Les considérations de sécurité sont intégrées à tous les stades du développement des logiciels, du matériel et de la prestation de services gérés et de services infonuagiques. Les activités de développement de base, notamment la gestion de la configuration et de la documentation, le développement de la sécurité et la planification du cycle de vie, ont été adoptées dans les pratiques des fournisseurs de produits et prestataires de services. Les projets relatifs au développement de logiciels, à l'assurance qualité du matériel, aux services gérés et à la sécurité infonuagique évaluent en permanence la valeur des normes et réduisent ou renforcent les niveaux de conformité en fonction de décisions fondées sur le risque.	Le pays participe activement à l'élaboration et à la promotion de ces normes au niveau international. La mise en œuvre de ces normes et les décisions de non-conformité sont prises en fonction de l'évolution des menaces.

Facteur - D 5.2 : Contrôles de sécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Technologie Contrôles de sécurité	La compréhension et le déploiement des contrôles de sécurité technologiques disponibles sur le marché, par les utilisateurs et les secteurs public et privé, sont minimes, voire inexistants. Les prestataires de services Internet et d'autres technologies peuvent ne pas offrir de contrôles en amont à leurs clients.	Les contrôles de sécurité technologiques sont déployés par les utilisateurs et les secteurs public et privé, mais peut-être pas de manière uniforme dans tous les secteurs. Le déploiement de contrôles de sécurité technologiques modernes est encouragé de manière non-systématique et tous les secteurs sont incités à les utiliser. Les prestataires de services Internet et d'autres technologies peuvent offrir des services de sécurité dans le cadre de leurs services, mais au coup par coup Les prestataires de services Internet et d'autres technologies reconnaissent la nécessité d'établir des politiques internes pour le déploiement de contrôles de sécurité techniques, pour gérer les risques identifiés dans les produits et services qu'ils offrent.	Des contrôles de sécurité technologiques à jour, y compris des correctifs et des sauvegardes, sont déployés dans tous les secteurs. Des contrôles de sécurité physique sont utilisés pour empêcher le personnel non autorisé de pénétrer dans les installations informatiques dans tous les secteurs. Les prestataires de services Internet et d'autres technologies établissent des politiques internes pour le déploiement de contrôles de sécurité techniques, afin de gérer les risques identifiés dans les produits et services qu'ils offrent. L'ensemble des contrôles technologiques de cybersécurité reflète les cadres, normes et bonnes pratiques de cybersécurité établis au niveau international.	L'adoption généralisée de contrôles technologiques de sécurité conduit à une protection efficace en amont des utilisateurs et des secteurs publics et privés. Tous les secteurs sont en mesure d'évaluer en permanence l'efficacité et l'adéquation des contrôles de sécurité déployés, en fonction de l'évolution de leurs besoins. La compréhension des contrôles de sécurité technologiques déployés s'étend à leur impact sur les opérations organisationnelles et l'allocation budgétaire. Les secteurs public et privé ont la capacité d'évaluer de manière critique et de mettre à niveau les contrôles de cybersécurité en fonction de leur pertinence et de leur adéquation à l'usage, et compte tenu des risques émergents. L'authentification multifactorielle est largement adoptée pour les services en ligne et les comptes privilégiés. Les autorités de certification sont disponibles et les certificats numériques sont largement utilisés. Les prestataires de services Internet et d'autres technologies ont la possibilité d'empêcher l'accès à des sites ou à des adresses internet non fiables, conformément aux exigences de l'organisme de réglementation compétent.	L'application de contrôles technologiques avancés dans le pays exerce une influence de premier plan au niveau international. La mise en œuvre de contrôles de sécurité technologiques avancés est effectuée en réponse à l'évolution des menaces.

Facteur - D 5.2 : Contrôles de sécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Contrôles cryptographiques	Les techniques cryptographiques (par exemple, le cryptage et les signatures numériques) pour la protection des données au repos et des données en transit peuvent être une préoccupation, mais ne sont pas encore déployées au sein du gouvernement ou du secteur privé, ou par le grand public.	Les contrôles cryptographiques pour la protection des données au repos et en transit sont reconnus et déployés au coup par coup par de multiples parties prenantes et dans divers secteurs. Des outils, tels que TLS*, sont déployés au coup par coup par les prestataires de services pour sécuriser toutes les communications entre les serveurs et les utilisateurs.	Les techniques cryptographiques sont disponibles pour tous les secteurs et utilisateurs pour la protection des données au repos ou en transit. Les services de communication sécurisés, tels que le courrier électronique crypté ou signé, sont largement compris. Les contrôles cryptographiques déployés répondent aux normes et directives internationales pour chaque secteur et sont tenus à jour. Des outils, tels que TLS, sont couramment déployés par les prestataires de services pour sécuriser toutes les communications entre les serveurs et les utilisateurs.	Les secteurs public et privé évaluent de manière critique le déploiement des contrôles cryptographiques, en fonction de leurs objectifs et priorités. Les secteurs public et privé adaptent les politiques de chiffrement et de contrôle cryptographique en fonction de l'évolution des progrès technologiques et de l'évolution de l'environnement des menaces. Les secteurs public et privé ont élaboré des politiques de cryptage et de contrôle cryptographique sur la base de l'évaluation précédente, et revoient régulièrement l'efficacité de ces politiques. Le pays a envisagé de mettre en œuvre la gestion des identités numériques. Le pays a examiné s'il avait besoin d'une ICP nationale**.	Le pays contribue au débat international sur les meilleures pratiques en matière de contrôles cryptographiques. La mise en œuvre des contrôles cryptographiques se fait en réponse à l'évolution des menaces.

Sécurité de la couche de transport
** Infrastructure à clé publique

Facteur - D 5.3 : Qualité du logiciel

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Qualité et assurance des logiciels	La qualité et les performances des logiciels utilisés dans le pays sont préoccupantes, mais les exigences fonctionnelles ne sont pas encore totalement contrôlées. Il n'existe pas de catalogue des plateformes et applications logicielles assurées dans les secteurs public et privé. Les politiques et processus concernant les mises à jour et la maintenance (y compris la gestion des correctifs) des applications logicielles n'ont pas encore été formulés.	La qualité des logiciels et les exigences fonctionnelles dans les secteurs public et privé sont reconnues et identifiées, mais pas nécessairement de manière stratégique. Un catalogue de plateformes et d'applications logicielles assurées dans les secteurs public et privé est en cours d'élaboration. Les politiques et processus relatifs aux mises à jour et à la maintenance des logiciels (y compris la gestion des correctifs) sont en cours d'élaboration. Les preuves des déficiences de la qualité des logiciels sont recueillies et évaluées quant à leur impact sur la convivialité et les performances.	La qualité des logiciels et les exigences fonctionnelles dans les secteurs public et privé sont reconnues et établies. Les applications logicielles fiables qui respectent les normes internationales et les bonnes pratiques sont largement utilisées dans les secteurs public et privé. Des politiques et des processus relatifs aux mises à jour et à la maintenance des logiciels (y compris la gestion des correctifs) sont établis dans tous les secteurs. Les applications logicielles sont caractérisées par leur fiabilité, leur facilité d'utilisation et leurs performances, conformément aux normes internationales et aux bonnes pratiques.	La qualité des logiciels utilisés dans les secteurs public et privé est contrôlée et évaluée. Les politiques et processus relatifs aux mises à jour et à la maintenance des logiciels (y compris la gestion des correctifs) sont en cours d'amélioration, sur la base d'évaluations des risques et de la nature critique des services dans tous les secteurs. Les avantages pour les entreprises d'un investissement supplémentaire pour assurer la qualité et la maintenance des logiciels sont mesurés et évalués. Les défauts logiciels sont gérables en temps voulu et la continuité du service est assurée.	Des applications logicielles de haut niveau de performance, de fiabilité et de convivialité sont disponibles, avec des processus de continuité de service entièrement automatisés. Les exigences en matière de qualité des logiciels sont systématiquement revues, mises à jour et adaptées à l'évolution de l'environnement de la cybersécurité.

Facteur - D 5.4 : Résilience des infrastructures de communication et d'Internet

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Fiabilité de l'infrastructure Internet	Des services et des infrastructures Internet abordables et fiables n'ont peut-être pas été mis en place dans le pays ; s'ils l'ont été, les taux d'adoption de ces services sont préoccupants. Il n'y a que peu ou pas de surveillance nationale des infrastructures de réseau. Si les réseaux et les systèmes sont externalisés, la fiabilité des fournisseurs tiers peut ne pas avoir été prise en compte. Des mesures de redondance du réseau peuvent être envisagées, mais pas de manière systématique et complète (voir D 1.6).	Des services et des infrastructures Internet limités sont disponibles, mais avec un faible taux d'adoption et des problèmes de manque de fiabilité. La capacité de l'infrastructure Internet des secteurs public et privé à résister à des incidents avec un minimum de perturbations a été discutée par de nombreuses parties prenantes, mais n'a peut-être pas été entièrement prise en compte. Le soutien à la sécurisation de l'infrastructure Internet peut s'appuyer sur une assistance régionale.	Des services internet fiables sont largement disponibles et utilisés. Les services Internet font l'objet d'une large confiance pour la conduite du commerce électronique et des transactions commerciales électroniques ; des processus d'authentification appropriés sont mis en place. La technologie déployée et les processus utilisés pour gérer l'infrastructure de l'internet répondent aux normes internationales et suivent les bonnes pratiques. L'infrastructure nationale est gérée de manière formelle, avec des processus documentés, des rôles et des responsabilités, et une redondance limitée.	Les technologies, les processus de conformité aux normes internationales et les directives qui répondent aux besoins nationaux face aux risques émergents font l'objet d'évaluations régulières, et des modifications sont apportées si nécessaire. L'acquisition des technologies essentielles est efficace et contrôlée, et des processus de planification stratégique et de continuité des services sont en place.	L'acquisition de technologies d'infrastructure est contrôlée de manière efficace, avec une certaine souplesse en fonction de l'évolution de la dynamique du marché. Les coûts des technologies d'infrastructure sont évalués et optimisés en permanence. Les capacités scientifiques, techniques, industrielles et humaines sont systématiquement maintenues, améliorées et perpétuées afin de préserver la résilience indépendante du pays. Une efficacité optimisée est en place pour gérer les pannes prolongées des systèmes (voir D 1.6).
Suivi et réponse	Aucune évaluation des risques n'est réalisée par les propriétaires d'infrastructures Internet pour identifier les actifs vulnérables et hiérarchiser les actions de protection. Il n'y a pas de contrôle en place pour détecter que des incidents se sont produits. Aucun plan de réponse aux incidents n'est en place.	Les processus d'élaboration d'évaluations des risques pour les propriétaires d'infrastructures Internet ont été lancés. Il existe une surveillance au coup par coup de certaines parties de l'infrastructure Internet, mais elle n'est pas forcément exhaustive. Des plans de réponse aux incidents sont en cours d'élaboration dans certains secteurs.	Des mécanismes sont en place dans les secteurs public et privé pour effectuer des évaluations des risques, surveiller et tester la résilience des réseaux, et réagir aux incidents. Des plans de réponse aux incidents sont en place dans les secteurs public et privé et sont régulièrement testés et revus. Des ressources appropriées sont affectées à l'intégration du matériel, aux tests de résistance de la technologie, à la formation du personnel, à la surveillance, à l'intervention et aux exercices pour tester les plans d'intervention.	Les risques liés aux technologies émergentes et convergentes sont régulièrement évalués par les propriétaires d'infrastructures Internet. Les risques liés aux technologies émergentes et convergentes sont régulièrement évalués par les organismes de réglementation responsables des réseaux de communications électroniques, ce qui permet d'éclairer les décisions en matière de financement et de priorités.	Les ressources au niveau national peuvent agir pour travailler avec la communauté internationale en cas de crise ou incident transjuridictionnel. Les enseignements tirés des collaborations internationales sont utilisés pour faire évoluer les capacités de surveillance et de réaction. Il existe des preuves que des capacités de surveillance et de réponse souveraines et nouvelles sont développées en prévision des menaces émergentes.

Facteur - D 5.5 : Marché de la cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Technologies de cybersécurité	Si la production nationale de technologies de cybersécurité existe, elle ne suit pas des processus sécurisés. Le pays n'a pas pris en compte les conséquences sur la sécurité de l'utilisation de technologies étrangères en matière de cybersécurité.	S'il y a une production nationale, le besoin de processus sécurisés est reconnu. En cas de recours à des technologies étrangères, les implications en matière de sécurité sont prises en compte.	S'il y a une production nationale, des processus sécurisés sont en place. En cas de recours à des technologies étrangères, les implications en matière de sécurité sont identifiées et atténuées dans le contexte d'une chaîne d'approvisionnement internationale.	Si une technologie de cybersécurité est développée localement, elle respecte les directives de codage sécurisé, les bonnes pratiques et adhère aux normes internationalement reconnues. Les évaluations des risques et les incitations du marché permettent de définir les priorités en matière de développement de produits et d'atténuer les risques identifiés. Les implications en matière de sécurité de l'utilisation de technologies étrangères sont régulièrement analysées et révisées sur la base de l'évaluation des risques émergents en matière de cybersécurité.	Les fonctions de sécurité dans les configurations des logiciels et des systèmes informatiques sont automatisées lors du développement et du déploiement des technologies. Les produits nationaux de cybersécurité sont exportés vers d'autres pays et sont considérés comme des produits supérieurs. Le pays a créé un organisme chargé d'assurer la sécurité des technologies étrangères (dispositifs et logiciels) et des chaînes d'approvisionnement, ou de certifier les entités qui peuvent le faire.
Services et expertise en matière de cybersécurité	L'offre de services de conseil en cybersécurité n'est pas très répandue dans le pays. Peu de prestataires de services, voire aucun, ne disposent d'une certification professionnelle.	Il existe un nombre croissant de services de conseil en cybersécurité destinés aux organisations privées et publiques. Un nombre croissant de prestataires de services fournissent le détail des certifications professionnelles qu'ils possèdent. Il se peut qu'il n'y ait que peu ou pas de conseils pour aider les organisations à sélectionner les prestataires de services.	De nombreux services de conseil en cybersécurité sont disponibles pour les organisations privées et publiques. Tous les prestataires de services fournissent des détails sur les certifications professionnelles qu'ils possèdent. Un organisme national accrédite les prestataires de services, afin d'aider les organisations à sélectionner ces derniers.	Les organisations privées et publiques demandent régulièrement conseil aux services de conseil en cybersécurité, y compris sur les risques émergents. Le pays dispose d'une offre suffisante de professionnels de la cybersécurité.	Le secteur des services de cybersécurité dans le pays contribue à façonner le marché international.

Facteur - D 5.5 : Marché de la cybersécurité

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Implications de l'externalisation en matière de sécurité	Aucune évaluation des risques n'est effectuée pour déterminer comment atténuer les risques liés à l'externalisation de l'informatique vers un tiers ou des services infonuagiques. Il y a un manque de compréhension des mesures de sécurité que le prestataire de services informatiques externalisés applique.	Certaines organisations et certains secteurs procèdent à des évaluations des risques afin de déterminer comment atténuer les risques liés à l'externalisation de l'informatique vers un tiers ou des services infonuagiques. Au moins certaines organisations et certains secteurs comprennent les mesures de sécurité appliquées par le prestataire de services informatiques externalisés. Certaines organisations au moins ont mis au point des processus de continuité des activités et de reprise après sinistre.	La plupart des grandes organisations des secteurs public et privé procèdent à des évaluations des risques afin de déterminer comment atténuer les risques liés à l'externalisation de l'informatique vers un tiers ou des services infonuagiques. Les garanties de sécurité fournies par les prestataires de services informatiques externalisés sont largement comprises. La plupart des organisations ont développé et testé des processus pour soutenir la continuité des activités et la reprise après sinistre.	Les résultats des évaluations des risques sont régulièrement analysés afin d'établir et de promouvoir les meilleures pratiques en matière de cybersécurité pour atténuer le risque d'externalisation de l'informatique. Différents scénarios de risques avec le prestataire de services informatiques sont explorés et testés, y compris les risques émergents.	Le pays contribue aux meilleures pratiques internationales sur la manière d'atténuer les risques liés à l'externalisation des TI.
Cyberassurance	Le besoin d'un marché de la cyberassurance a peut-être été identifié, mais aucun produit ou service n'est largement disponible, que ce soit au niveau national ou auprès de fournisseurs externes.	La nécessité d'un marché de la cyberassurance a été identifiée par l'évaluation des risques financiers pour les secteurs public et privé, et l'adéquation des offres disponibles fait actuellement l'objet de discussions.	Un marché de la cyberassurance est créé et encourage le partage d'informations sur les menaces entre les participants au marché. Des produits adaptés aux petites et moyennes entreprises (PME) sont également proposés.	Le marché de la cyberassurance offre une variété de couvertures pour atténuer les pertes consécutives. La couverture est choisie par les organisations en fonction des besoins de planification stratégique et des risques identifiés. Le marché de la cyberassurance est innovant et s'adapte aux risques, normes et pratiques émergents, tout en couvrant l'ensemble des cyberdommages. Des réductions de primes d'assurance sont proposées pour un comportement cohérent en matière de cybersécurité.	Les pratiques en matière de cyberassurance dans le pays contribuent à façonner le marché international.

Facteur - D 5.6 : Divulgation responsable

Aspect	Stade de démarrage	Stade de formation	Stade établi	Stade stratégique	Stade dynamique
Partage des informations sur les vulnérabilités	Il n'existe aucun moyen informel de partager des informations entre les parties prenantes sur les détails techniques des vulnérabilités. Les fournisseurs de logiciels et de services n'ont généralement pas la capacité de traiter les rapports de bogues et de vulnérabilités.	Les détails techniques des vulnérabilités sont partagés de manière informelle avec d'autres parties prenantes qui peuvent diffuser l'information à plus grande échelle. Les fournisseurs de logiciels et de services sont en mesure de traiter les rapports de bogues et de vulnérabilités, mais il se peut qu'il n'y ait pas de protocoles formels pour le faire.	Il existe des mécanismes ou des canaux formels d'échange d'informations pour partager les détails techniques des vulnérabilités avec d'autres parties prenantes, qui peuvent diffuser l'information à plus grande échelle. Une proportion importante des vulnérabilités des produits et services est corrigée dans des délais définis après leur découverte.	Les mécanismes de partage des informations sur la vulnérabilité sont continuellement révisés et mis à jour en fonction des besoins de toutes les parties prenantes concernées et à la lumière des risques émergents. Tous les produits et services concernés sont régulièrement mis à jour dans les délais prévus. Des processus sont en place pour examiner et réduire les délais lorsque cela est possible.	Le pays contribue au débat et aux meilleures pratiques internationales en matière de partage des informations sur la vulnérabilité.
Politiques, processus et législation relatifs à la divulgation responsable des failles de sécurité	La nécessité d'une politique de divulgation responsable dans les organisations des secteurs public et privé, et le droit à des protections juridiques pour ceux qui divulguent des failles de sécurité ne sont pas encore reconnus.	La nécessité d'une politique de divulgation responsable dans les organisations des secteurs public et privé est reconnue, mais les politiques ou les processus peuvent ne pas être en place, ou seulement en cours d'élaboration. Le droit à des protections juridiques pour ceux qui divulguent des failles de sécurité est reconnu, mais la législation peut ne pas être en place ou être seulement en cours d'élaboration. Les fournisseurs de logiciels et de services s'engagent à s'abstenir d'intenter une action en justice contre une partie qui divulgue des informations de manière responsable.	Une politique ou un cadre de divulgation responsable est en place dans les organisations du secteur public et privé, et comprend un délai de divulgation, une résolution programmée et la nécessité d'une reconnaissance formelle. Les organisations ont établi des processus pour recevoir et diffuser des informations sur la vulnérabilité de manière responsable. Le droit à des protections juridiques pour ceux qui divulguent des failles de sécurité de manière responsable est en place.	Les politiques et processus de divulgation responsable sont continuellement révisés et mis à jour en fonction des besoins de toutes les parties prenantes concernées et à la lumière des risques émergents. Une analyse des détails techniques des vulnérabilités est publiée et des informations consultatives sont diffusées en fonction des rôles et responsabilités de chacun.	Le pays contribue au débat sur les cadres de divulgation responsable et les protections juridiques pour ceux qui divulguent des failles de sécurité de manière responsable.

Évolution du CMM

Cette *édition 2021 du CMM* s'appuie sur le succès du CMM au cours des six dernières années en tenant compte de l'évolution de la cybermenace pour les utilisateurs, des enseignements tirés de plus de 120 révisions du CMM effectuées dans le monde entier et des commentaires des experts en cybersécurité.

La décision de réviser le CMM a été prise par deux acteurs clés :

- La nécessité de répondre à tous les *aspects* pertinents de la menace, des vulnérabilités des systèmes et des dommages consécutifs en raison de l'évolution des environnements opérationnels et des risques.
- Réévaluation de l'évolution du paysage du contrôle de la cybersécurité et des pratiques de gestion des risques à la disposition de la communauté.

Pour déterminer s'il faut ou non proposer un changement au CMM, ou aux preuves requises pour justifier l'atteinte de la maturité de la capacité, le processus de décision suivant a été suivi.

Tous les changements potentiels à inclure dans *l'édition 2021 du CMM* devaient répondre aux critères suivants :

- Le changement doit avoir été proposé par des partenaires stratégiques, des utilisateurs ou des conseillers experts. Elles doivent être basées sur l'expérience du déploiement du modèle, sur le retour d'information d'un pays qui a utilisé le modèle, ou sur un membre de la communauté internationale des parties prenantes ayant une connaissance particulière des environnements changeants qui doivent être pris en compte ;
- Le changement doit avoir été discuté avec le groupe consultatif d'experts de GCSCC, les partenaires stratégiques et de mise en œuvre et d'autres experts au cours des conférences téléphoniques en ligne et/ou des réunions en ligne individuelles. Un consensus clair doit avoir été atteint parmi les participants ;
- Le changement doit avoir été discuté lors de l'atelier de révision du CMM en février 2020. Un consensus clair doit avoir été atteint parmi les participants ;
- Les membres du Bureau technique de GCSCC doivent convenir que les changements ont un sens ; et
- Les partenaires de la constellation mondiale et les partenaires stratégiques et de mise en œuvre doivent accepter les changements.

Les critères qui ne répondaient pas aux exigences ont été documentés comme nécessitant des recherches et des consultations supplémentaires.

Remerciements

Cette *édition 2021 du CMM* a été élaborée par le GCSCC avec des contributions importantes de ses partenaires et collaborateurs :

Conseil technique du GCSCC

Équipe de recherche du GCSCC

Groupe consultatif d'experts du GCSCC

Partenaires de la Constellation mondiale

- Cybersecurity Capacity Centre for Southern Africa (C3SA, Centre de Capacité en Cybersécurité pour l'Afrique Australe), Le Cap, Afrique du Sud
- Oceania Cyber Security Centre (OCSC, Centre de cybersécurité d'Océanie), Melbourne, Australie

Partenaires stratégiques et de mise en œuvre

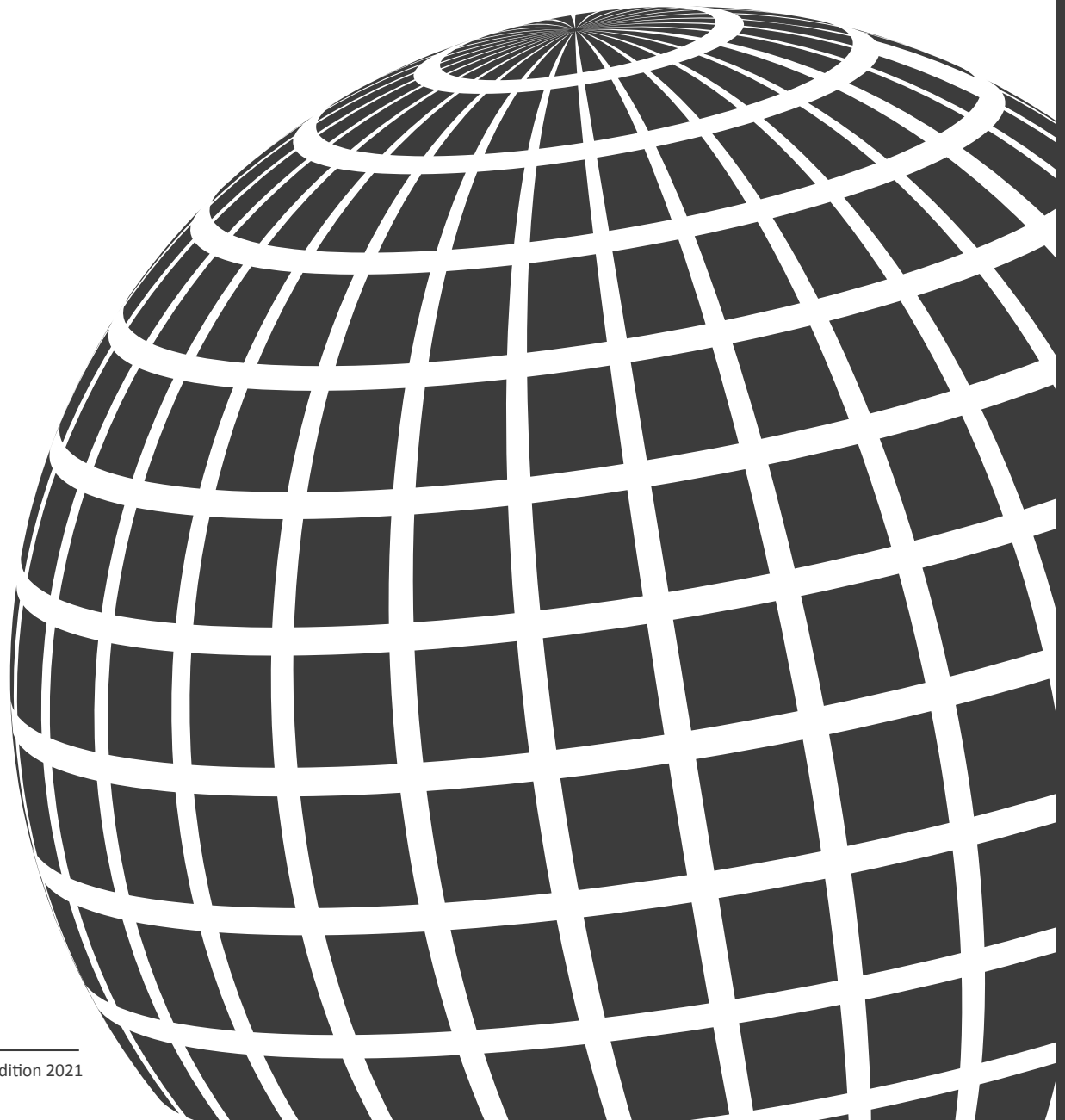
- Organisation des télécommunications du Commonwealth (CTO)
- Global Forum on Cyber Expertise (GFCE, Forum mondial sur la cyberexpertise)
- Union internationale des télécommunications (UIT)
- NRD Cyber Security
- Organisation des États Américains (OEA)
- Banque mondiale

Plus de 150 personnes ont contribué aux différentes stades du processus de révision, trop nombreuses pour les énumérer toutes. Nous tenons à les remercier toutes.

Nous tenons également à remercier nos bailleurs de fonds et partenaires de recherche qui ont fourni un soutien en nature : le Bureau des le gouvernement de l'État de Victoria (Australie), l'Organisation des États américains (OEA), la Banque interaméricaine de développement (BID), la Banque mondiale, l'Union internationale des télécommunications (UIT), l'Organisation des télécommunications du Commonwealth (CTO), le Forum mondial sur la cyberexpertise (GFCE), le ministère norvégien des Affaires étrangères, le ministère néerlandais des Affaires étrangères, la GIZ (l'agence allemande de coopération internationale) et le NRD Cyber Security.

À propos du GCSCC

Le Global Cyber Security Capacity Centre (GCSCC, le Centre de capacité mondiale de cybersécurité), un programme de l'Oxford Martin School et basé au département d'informatique de l'université d'Oxford, est un centre international de premier plan pour la recherche sur le renforcement efficient et efficace des capacités en matière de cybersécurité. Il encourage l'augmentation de l'échelle, du rythme, de la qualité et de l'impact des initiatives de renforcement des capacités en matière de cybersécurité dans le monde et vise à améliorer l'échelle et l'efficacité du renforcement des capacités en matière de cybersécurité en acquérant une compréhension plus complète et plus nuancée du paysage des capacités en matière de cybersécurité. L'objectif du GCSCC est de faire en sorte que les connaissances et les recherches recueillies et produites par le centre puissent aider les nations à améliorer leurs capacités en matière de cybersécurité de manière systématique et substantielle. En contribuant à la compréhension des capacités nationales en matière de cybersécurité, le GCSCC espère aider à promouvoir un cyberespace innovant au service du bien-être, des droits de l'homme et de la prospérité de tous.



Global
Cyber Security
Capacity Centre

Global Cyber Security Capacity Centre
Department of Computer Science, University of Oxford
Wolfson Building
Parks Road
Oxford
OX1 3QD
United Kingdom

Tél : +44 (0)1865 287430
Courriel : cybercapacity@cs.ox.ac.uk
Internet : https://gcscc.ox.ac.uk/ et https://www.oxfordmartin.ox.ac.uk/cyber-security/

Mars 2021