ITUPublications

Union internationale des télécommunications
Secteur du développement

Rapport final sur la Question 3/2 de l'UIT-D

Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité

Période d'études 2022-2025

Rapport final sur la Question 3/2 de l'UIT-D

Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité

Période d'études 2022-2025

Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité: Rapport final sur la Question 3/2 de l'UIT-D pour la période d'études 2022-2025

ISBN 978-92-61-41102-2 (version électronique)
ISBN 978-92-61-41112-1 (version EPUB)

Crédits photo de couverture: Adobe Stock

Remerciements

Les commissions d'études du Secteur du développement des télécommunications de l'UIT (UIT-D) offrent un cadre neutre où des experts des pouvoirs publics, du secteur privé, des organisations de télécommunication et des établissements universitaires du monde entier se réunissent pour élaborer des outils et des ressources pratiques permettant de traiter les questions de développement. À cette fin, les deux commissions d'études de l'UIT-D sont chargées d'élaborer des rapports, des lignes directrices et des recommandations sur la base des contributions soumises par les membres. Les Questions à étudier sont définies tous les quatre ans à la Conférence mondiale de développement des télécommunications (CMDT). Les membres de l'UIT, réunis à la CMDT-22 qui s'est tenue à Kigali en juin 2022, sont convenus que pour la période 2022-2025, la Commission d'études 2 examinerait sept Questions relevant du domaine de compétence général "Transformation numérique".

Le présent rapport a été établi en réponse à la Question 3/2 intitulée "**Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité**", sous la houlette et la coordination générales de l'équipe de direction de la Commission d'études 2 de l'UIT-D, dirigée par M. Fadel Digham (République arabe d'Égypte), Président, et secondé par les Vice-Présidents suivants: M. Abdelaziz Alzarooni (Émirats arabes unis), Mme Zainab Ardo (République fédérale du Nigéria), M. Javokhir Aripov (République d'Ouzbékistan), Mme Carmen-Mădălina Clapon (Roumanie), M. Mushfig Guluyev (République d'Azerbaïdjan), M. Hideo Imanaka (Japon), Mme Mina Seonmin Jun (République de Corée), M. Mohamed Lamine Minthe (République de Guinée), M. Víctor Antonio Martínez Sánchez (République du Paraguay), Mme Alina Modan (Roumanie)[1], M. Diyor Rajabov (République d'Ouzbékistan)[1], M. Tongning Wu (République populaire de Chine) et M. Dominique Würges (France).

Le rapport a été élaboré sous la direction des Corapporteurs pour la Question 3/2, Mme Vanessa Copetti Cravo (République fédérative du Brésil), Mme Nicole Darabian (Royaume-Uni de Grande-Bretagne et d'Irlande du Nord) et Mme Jabin Vahora (États-Unis d'Amérique)[1], en collaboration avec les Vice-Rapporteurs suivants: M. Damnam K. Bagolibe (République togolaise), M. Daniel Batty (Access Partnership Limited)[1], Mme Maria Bolshakova (Fédération de Russie)[1], M. Tommaso De Zan (Access Partnership Limited), M. Idrissa Diallo (République de Guinée), M. Sidy Mouhamed Fall (République du Sénégal), M. Álvaro García (Axon Partners Group), M. Doğukan Ömer Gür (République de Türkiye), M. Prachish Khanna (République de l'Inde), M. Teng Ma (China International Telecommunication Construction Corporation), M. Rodgers Mumelo (République du Kenya), Mme Uliana Stoliarova (Fédération de Russie), M. Samuel Tew (Axon Partners Group)[1], Mme Xinxin Wan (République populaire de Chine), Mme Kacie Yearout (États-Unis d'Amérique), et M. Jaesuk Yun (République de Corée).

Des remerciements particuliers vont aux auteurs principaux des chapitres du présent rapport pour leur dévouement, leur appui et leur expertise.

Le présent rapport a été élaboré avec l'appui des coordonnateurs pour la Question 3/2 de l'UIT-D, des éditeurs, de l'équipe chargée de la production des publications et du secrétariat de la Commission d'études 2 de l'UIT-D.

[1] Ont quitté leurs fonctions au cours de la période d'études.

Table des matières

Liste des figures et encadrés

Figures

Encadrés

Résumé analytique

Le Rapport final sur la Question 3/2 de l'UIT-D pour la période d'études 2022-2025 est le fruit d'un effort concerté visant à tirer parti des expériences et des pratiques nationales en matière de cybersécurité dans le monde entier. Ce rapport constitue une ressource à même d'aider les pays à élaborer les stratégies nécessaires à la mise en place d'une culture de la cybersécurité efficace. Il tient compte des contributions des membres de l'UIT, ainsi que des discussions qui ont eu lieu lors des ateliers organisés pendant la période d'études, et reflète un large éventail de points de vue et d'expériences visant à sécuriser les réseaux d'information et de communication.

À l'heure où les technologies numériques font partie intégrante de notre vie quotidienne et constituent le pilier des économies du monde entier, le présent rapport met en évidence la vulnérabilité accrue des personnes, des organisations et des nations face à des cybermenaces de plus en plus sophistiquées. Autrefois une préoccupation mineure, la cybersécurité est désormais un élément fondamental de la transformation numérique comme de l'évolution des technologies, et doit figurer au premier rang des priorités de toutes les parties prenantes, y compris des gouvernements, du secteur privé, des particuliers et du monde universitaire. Selon le Rapport sur les risques mondiaux 2024 du Forum économique mondial[2], au niveau mondial, la cybersécurité est classée au quatrième rang des risques à court terme les plus graves.

Outre les initiatives et les ressources de l'UIT et de ses membres mentionnées dans le présent rapport, il est important de souligner qu'il existe également un certain nombre d'initiatives mondiales visant à partager des informations et des bonnes pratiques en matière de cybersécurité, conçues pour aider les pays et les différentes parties prenantes à poursuivre leurs efforts en matière de cybersécurité, car il peut être difficile pour les pays en développement, en particulier les pays les moins avancés (PMA), de trouver ces informations et d'y accéder. Dans ce contexte, il convient donc de citer deux ressources complètes, mentionnées au cours de la période d'études, et dont les membres de l'UIT pourraient tirer parti: le Portail des politiques de cybersécurité de l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR)[3], et le Portail de connaissances pour le renforcement en matière de cybersécurité du Forum mondial sur la cyberexpertise (GFCE)[4].

Le présent rapport fait mention à plusieurs reprises d'une autre ressource pertinente, à savoir l'Indice mondial de cybersécurité de l'UIT (GCI)[5], qui permet de mesurer l'engagement des pays en faveur de la cybersécurité selon cinq piliers fondamentaux: mesures juridiques, mesures techniques, mesures organisationnelles, mesures de renforcement des capacités et mesures de coopération. L'Indice GCI a été lancé par l'UIT en 2015 et a fait l'objet d'améliorations constantes pour pouvoir servir d'outil d'évaluation, de sensibilisation et de renforcement des capacités aidant les pays à renforcer et à mettre en œuvre leurs capacités en matière de cybersécurité.

Le présent rapport se veut une ressource qui fournit à la fois des réflexions et des pratiques innovantes tenant compte de la dynamique et de l'évolution constantes des menaces, et qui

[2] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
[3] https://cyberpolicyportal.org/fr
[4] https://cybilportal.org/
[5] https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

donne un aperçu de l'état actuel de la cybersécurité, tout en proposant une voie stratégique pour l'avenir.

Le rapport est structuré comme suit, de manière à ce que chaque chapitre soit consacré à un aspect distinct de la cybersécurité:

- Le Chapitre 1 concerne l'aspect humain, un élément essentiel de la cybersécurité, et met l'accent sur la nécessité urgente d'investir massivement dans la sensibilisation des utilisateurs, ainsi que dans l'éducation et la formation du personnel chargé de la cybersécurité. Ce chapitre souligne combien il est essentiel de disposer de professionnels de la cybersécurité qualifiés, capables de gérer la complexité des menaces numériques contemporaines, et invite instamment les pays à donner la priorité aux programmes éducatifs et aux plans de recrutement afin de former une main-d'œuvre compétente et résiliente dans le domaine de la cybersécurité, ainsi qu'à accorder une attention particulière à la sensibilisation en tant qu'élément clé de la promotion d'une culture de la cybersécurité.
- Le Chapitre 2 met l'accent sur les pratiques en matière d'assurance de la cybersécurité dont le rôle est essentiel pour protéger les réseaux, les systèmes et les données contre les activités malveillantes. Il évalue les diverses méthodologies, mesures de contrôle, lignes directrices et normes adoptées à travers le monde qui peuvent contribuer à prévenir et à atténuer le risque de cyberattaques.
- Le Chapitre 3 met en lumière le rôle crucial des équipes d'intervention en cas d'incident informatique (équipes CIRT) dans la protection des infrastructures vitales. Il présente des modèles efficaces d'intervention en cas d'incident et souligne l'importance de mettre en place et de renforcer les capacités de telles équipes, ainsi que de coordonner leurs activités.
- Le Chapitre 4 examine l'élaboration et la mise en œuvre de stratégies nationales en matière de cybersécurité. Il souligne l'importance de faire concorder les stratégies de cybersécurité avec les programmes généraux de transformation numérique, de sécurité nationale et d'économie afin de renforcer la résilience numérique.
- Le Chapitre 5 est consacré aux efforts déployés pour sécuriser les réseaux 5G. Face aux défis mondiaux que pose le déploiement des réseaux 5G, ce chapitre met en lumière les politiques, les cadres réglementaires et les mesures proactives prises par le secteur des télécommunications pour contribuer à atténuer les menaces pour la cybersécurité 5G.
- Le Chapitre 6 se penche sur l'utilisation croissante par les cybercriminels de tactiques sophistiquées d'hameçonnage par texto pour tromper les utilisateurs via le service de messages courts (SMS). Il démontre la nécessité d'une approche collective englobant les réglementations gouvernementales, les initiatives du secteur et une sensibilisation accrue du public pour protéger les consommateurs et maintenir la fiabilité des réseaux de communication.

Le présent rapport est complété par des annexes qui fournissent des ressources supplémentaires, notamment des contributions détaillées des membres de l'UIT présentées dans le cadre de ce cycle, ainsi qu'un résumé des projets et programmes en cours de l'UIT-D dans le domaine de la cybersécurité. Ces annexes apportent des informations précieuses et constituent des documents de base pour les parties prenantes qui souhaitent approfondir leur compréhension de la cybersécurité et de son rôle capital à l'ère numérique.

En résumé, le Rapport final sur la Question 3/2 de l'UIT-D pour la période d'études 2022-2025 constitue un plan stratégique visant à assurer un niveau élevé de cybersécurité parmi les membres de l'UIT. Il appelle à l'adoption d'une approche unifiée pour sécuriser notre avenir numérique, soulignant à ce titre l'importance de la sensibilisation, de l'éducation, de l'élaboration de stratégies, du renforcement des capacités des équipes CIRT, de la mise en place de politiques et de stratégies, et de la coopération internationale pour gérer la complexité des défis liés à la cybersécurité et en atténuer les effets dans le contexte de la transformation numérique.

Abréviations et acronymes

Abréviation	Terme
2G	technologie mobile de deuxième génération
3G	technologie mobile de troisième génération
3GPP	Projet de partenariat de troisième génération (3rd Generation Partnership Project)
4G	technologie mobile de quatrième génération
5G	technologie mobile de cinquième génération [6]
CE 17	Commission d'études 17 de l'UIT-T
CIRT	équipes d'intervention en cas d'incident informatique (cybersecurity incident response teams)
CISA	Agence pour la cybersécurité et la sécurité des infrastructures (Cybersecurity and Infrastructure Security Agency)
COP	protection en ligne des enfants (child online protection)
ENISA	Agence européenne pour la cybersécurité (European Union Agency for Cybersecurity)
ETSI	Institut européen des normes de télécommunication (European Telecommunications Standards Institute)
FIRST	Forum des équipes de sécurité et d'intervention en cas d'incidents (Forum of Incident Response and Security Teams)
GCI	indice mondial de cybersécurité (global cybersecurity index)
GFCE	Forum mondial sur la cyberexpertise (Global Forum on Cyber Expertise)
GSMA	Association GSM (GSM Association)
IoT	Internet des objets (Internet of Things)
NESAS	système d'assurance de sécurité des équipements de réseau (network equipment security assurance scheme)
NIST	Institut national des normes et de la technologie (National Institute for Standards and Technology)
OCDE	Organisation de coopération et de développement économiques

[6] Bien qu'il ait été pris soin dans le présent document d'utiliser la définition officielle des différentes générations d'IMT et d'y faire référence convenablement (voir la Résolution UIT-R 56, "*Appellations pour les Télécommunications mobiles internationales*"), on trouvera, dans certaines parties du présent document, du contenu fourni par les membres dans lequel les générations d'IMT sont désignées par les noms commerciaux "xG" couramment utilisés. Une correspondance ne peut pas forcément être établie entre ces noms et les différentes générations d'IMT, puisque l'on ignore les critères sous-jacents des membres, mais, en règle générale, les IMT-2000, les IMT évoluées, les IMT-2020 et les IMT-2030 sont connues respectivement sous les noms 3G, 4G, 5G et 6G.

(suite)

Abréviation	Terme
PMA	pays les moins avancés
RAN	réseau d'accès radioélectrique (radio access network)
SDN	réseau piloté par logiciel (software-defined network)
SMS	service de messages courts (short message service)
TIC	technologies de l'information et des communications
UE	Union européenne
UIT	Union internationale des télécommunications
UIT-D	Secteur du développement des télécommunications de l'UIT
UIT-R	Secteur des radiocommunications de l'UIT
UIT-T	Secteur de la normalisation des télécommunications de l'UIT
UNIDIR	Institut des Nations Unies pour la recherche sur le désarmement (United Nations Institute for Disarmament Research)

Chapitre 1 – Sensibilisation des utilisateurs et renforcement des capacités en matière de cybersécurité

Afin de pouvoir continuer à profiter en toute sécurité des avantages du numérique, il est essentiel de mettre en œuvre de solides programmes de sensibilisation et de renforcement des compétences en matière de cybersécurité. De tels programmes permettront non seulement d'atténuer les risques liés à l'hameçonnage et à d'autres cybermenaces, mais aussi de constituer une main-d'œuvre qualifiée, capable de relever les défis complexes de l'ère numérique. Le présent chapitre se penche sur les éléments clés de la cybersécurité et met en avant des exemples dignes d'intérêt, avant de proposer une voie à suivre pour les pays qui souhaitent renforcer leurs capacités en matière de cybersécurité.

1.1 Sensibilisation à la cybersécurité

L'erreur humaine demeure un facteur prépondérant dans les atteintes à la cybersécurité. En effet, des études indiquent que plus de 88% des incidents de cybersécurité impliquent de quelque manière que ce soit une erreur humaine[7]. Il apparaît donc nécessaire de mettre en place des programmes de sensibilisation complets qui vont au-delà des solutions techniques et prennent en compte la dimension humaine de la cybersécurité.

La sensibilisation à la cybersécurité désigne l'approche stratégique consistant à faire connaître aux personnes, aux organisations et aux communautés les cyberrisques ainsi que les bonnes pratiques pour protéger les actifs et les informations numériques. L'objectif principal des initiatives de sensibilisation à la cybersécurité consiste à promouvoir une culture de la sécurité et à donner aux personnes les moyens de reconnaître les risques de cybersécurité, de les prévenir et d'y répondre de manière efficace. Les programmes de sensibilisation peuvent faire appel à divers outils et méthodes (tels que les programmes de formation, les exercices de simulation d'hameçonnage, la ludification et les modules de micro-apprentissage). Ils couvrent généralement des sujets tels que l'ingénierie sociale, la sensibilisation à l'hameçonnage, la gestion des mots de passe, la protection des données et l'utilisation sécurisée des appareils mobiles et des médias sociaux.

Bien exécutés, les programmes de sensibilisation à la cybersécurité peuvent avoir un impact considérable[8]. Les organisations qui mettent l'accent sur la sensibilisation à la cybersécurité constatent souvent une réduction drastique des attaques d'hameçonnage réussies et une amélioration globale de leur dispositif de sécurité, certaines études faisant état d'une réduction des attaques réussies allant jusqu'à 70%[9]. Investir dans la sensibilisation à la cybersécurité génère également un retour sur investissement élevé, puisque des études ont montré que même les programmes de formation les plus modestes pouvaient générer un retour sur investissement

[7] https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error
[8] https://www.sciencedirect.com/science/article/pii/S0167404823004959
[9] https://keepnetlabs.com/blog/security-awareness-training-statistics; https://www.knowbe4.com/press/knowbe4-analysis-finds-security-awareness-training-and-simulated-phishing-effective-in-reducing-cybersecurity-risk

sept fois supérieur[10]. Ces programmes contribuent, en outre, à instaurer une culture de la cybersécurité qui s'étend au-delà du lieu de travail, en aidant les personnes à devenir également des "cybercitoyens" responsables même dans leur vie privée. Par ailleurs, la sensibilisation à la cybersécurité joue un rôle essentiel dans le respect des réglementations sectorielles et des lois sur la protection des données, telles que la Directive révisée de l'Union européenne (UE) concernant la cybersécurité des réseaux et des systèmes d'information (Directive SRI 2). De nombreux secteurs exigent des organisations qu'elles mettent en œuvre des programmes de formation à la sécurité afin de respecter les normes réglementaires et d'éviter d'éventuelles amendes ou conséquences juridiques[11].

Des données de l'Indice GCI indiquent que 152 pays ont mené des campagnes de sensibilisation à la cybersécurité ciblant le grand public entre 2021 et 2024[12]. Les États Membres de l'UIT ont déjà mis en œuvre plusieurs initiatives pour sensibiliser davantage leurs citoyens aux menaces relatives à la cybersécurité. Ces initiatives comprennent notamment des programmes complets ciblant divers groupes de population. Certains projets sont spécifiquement axés sur la prévention de la cybercriminalité et de la fraude, tandis que d'autres font appel à divers supports en ligne pour promouvoir les pratiques de cybersécurité auprès de la population.

Parmi les exemples de programmes complets adaptés à différents groupes de population, on peut citer le programme en matière de cybersécurité de la **Fédération de Russie**. Il s'agit d'une initiative globale d'une durée de trois ans, lancée en août 2022, qui vise à sensibiliser davantage les citoyens russes à la cybersécurité. Afin de pouvoir assurer une communication plus ciblée et efficace, le programme découpe la population en trois groupes d'âge: les enfants et les adolescents (12-18 ans), les adultes (18-45 ans) et les seniors (45 ans et plus). En ce qui concerne les 12-18 ans, qui font l'objet d'une attention particulière en raison de leur vulnérabilité aux cybermenaces, deux projets majeurs ont été mis en œuvre:

- Consacré au cyberharcèlement, le premier projet fournit des conseils aux victimes, aux agresseurs et aux témoins d'actes de cyberharcèlement, et insiste sur l'importance de répondre au cyberharcèlement avec humour et indifférence, de manière saine.
- Le projet "Améliore tes compétences en matière de protection" vise, pour sa part, à sensibiliser les enfants aux escroqueries dans les jeux en ligne.

S'agissant des adultes âgés de 18 à 45 ans, le programme englobe plusieurs projets tels que:

- "Adopter de bonnes habitudes en ligne";
- "Choisir un mot de passe complexe facilement"; et
- "Apprenez votre rôle".

Ces projets abordent des sujets tels que la protection des appareils mobiles, la prévention de l'hameçonnage, la sécurité des mots de passe et la sensibilisation à la fraude téléphonique. Le programme répond également aux besoins des adultes de plus de 45 ans, en mettant l'accent sur la protection contre la fraude téléphonique. De plus, le programme comporte encore un cours spécialisé visant à améliorer les connaissances des fonctionnaires en matière de sécurité de l'information. Une étude menée à l'échelle de la Fédération de Russie en 2022 a révélé un indice global de compétences en matière de cybersécurité de 48,2 sur 100, dans

[10] https://blog.usecure.io/does-security-awareness-training-work; https://ostermanresearch.com/wp-content/uploads/2021/01/ORWP_0313-The-ROI-of-Security-Awareness-Training-August-2019.pdf
[11] https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/
[12] https://www.itu.int/epublications/fr/publication/global-cybersecurity-index-2024

des domaines tels que la protection antivirus, l'utilisation sûre de l'Internet et la sécurité des données personnelles. Le programme national russe en matière de cybersécurité est conçu pour être mis à jour chaque année, afin de s'assurer qu'il reste adapté aux nouvelles menaces numériques ainsi qu'à l'évolution des besoins de la population[13].

En **République de Côte d'Ivoire**, un programme de sensibilisation à la cybersécurité, axé spécifiquement sur la cybercriminalité, faisait partie d'une série d'initiatives de formation et de sensibilisation à la cybersécurité mises en œuvre par les principales institutions de cybersécurité du pays. La Plate-forme de lutte contre la cybercriminalité met ainsi en œuvre des campagnes de sensibilisation dans les établissements d'enseignement, y compris les écoles et les universités, ainsi que dans les institutions financières et religieuses, et publie des contenus à visée pédagogique ainsi que des informations sur les arrestations de cybercriminels sur les réseaux sociaux. L'équipe d'intervention en cas d'urgence informatique de la Côte d'Ivoire (CI-CERT), point focal national de cybersécurité, propose un programme de formation spécialisé appelé "DIGISEC" à l'intention des entreprises et des institutions afin de renforcer la sensibilisation à la sécurité numérique au travail. Autre initiative récente notable, déployée à l'occasion de l'édition 2024 de la Coupe d'Afrique des Nations: le CyberCAN23. Ce système de cybersécurité, géré par le CI-CERT, visait à sensibiliser aux escroqueries sur les plates-formes numériques, en particulier les fraudes par hameçonnage, grâce à la diffusion d'informations sur la cybersécurité sur les plates-formes de médias sociaux, à la télévision et à la radio. La Côte d'Ivoire a également lancé une campagne de sensibilisation à l'échelle nationale intitulée "En ligne tous responsables" dans plusieurs villes et villages[14].

La **République du Rwanda** a mis en œuvre des initiatives visant à améliorer la sensibilisation, l'éducation et la formation à la cybersécurité, notamment le Programme national de sensibilisation et de formation à la cybersécurité, qui a vocation à sensibiliser les internautes du pays à la cybersécurité tout en formant une main-d'œuvre qualifiée dans le domaine de la cybersécurité afin d'aider les institutions publiques et privées à protéger les systèmes essentiels contre les cybermenaces[15].

En ce qui concerne la prévention de la fraude informatique, la **Chine** a travaillé à la création d'un "réseau de lutte contre la fraude" multi-dimensionnel appliqué à l'ensemble de la société. Cette initiative, qui cible un éventail de groupes démographiques, comme les étudiants, les personnes âgées ou encore les agriculteurs[16], vise à encourager ces groupes à installer l'application du Centre national de lutte contre la fraude et à les sensibiliser à l'adoption de mesures de cybersécurité.

Enfin, au **Brésil**, une initiative a été lancée pour améliorer les pratiques en matière de cybersécurité de la population, en s'appuyant sur des outils de communication en ligne tels que "YouTube". Le Brésil a mis en œuvre des initiatives relatives à la cybersécurité par l'intermédiaire de l'agence nationale de télécommunications, Anatel. Dans le cadre de sa planification stratégique pour la période 2023-2027, Anatel a créé un portail dédié à la prévention de la fraude numérique et à la cybersécurité, dans lequel elle fournit des informations sur les menaces numériques courantes et les stratégies de prévention. L'agence organise également régulièrement des événements de sensibilisation avec des partenaires et tient à jour une liste de lecture dédiée à

[13] Document 2/71 de la CE 2 de l'UIT-D (Fédération de Russie).
[14] Document SG2RGQ/160 de la CE 2 de l'UIT-D (Réseau international des femmes expertes du numérique (RIFEN)).
[15] Document 2/35 de la CE 2 de l'UIT-D (Rwanda).
[16] Document 2/370 de la CE 2 de l'UIT-D (Chine).

la cybersécurité sur sa chaîne YouTube. Parmi les autres initiatives notables, citons la campagne #OctoberCyberSafe menée en octobre 2023 et 2024 ainsi que les célébrations de la Journée pour un Internet plus sûr en février 2024 et 2025[17].

1.2 Renforcement des capacités en matière d'éducation et de formation à la cybersécurité

Le rapport Global Cybersecurity Outlook 2025, établi par le Forum économique mondial, a mis en évidence une pénurie croissante de compétences en cybersécurité. Plus particulièrement, il indique une augmentation de 8% du déficit de compétences en cybersécurité depuis l'édition de 2024 et souligne le fait que deux organisations sur trois font état de lacunes critiques en matière de compétences dans le domaine de la cybersécurité, avec pour conséquence qu'elles ne sont pas en mesure de répondre à leurs besoins en matière de sécurité. Le rapport souligne le besoin urgent d'initiatives pour remédier à ce déficit de compétences, notamment des mesures en faveur de la formation, de la reconversion, du recrutement et de la rétention des travailleurs dans le domaine de la cybersécurité[18].

L'éducation et la formation à la cybersécurité peuvent être considérées comme un processus complet visant à doter les utilisateurs des connaissances, des compétences et des aptitudes nécessaires pour protéger les actifs numériques, détecter et atténuer les cybermenaces et assurer la sécurité des systèmes d'information. Ce processus englobe un large éventail de sujets et d'approches dont l'objectif est de former une main-d'œuvre capable de relever les défis en constante évolution que pose le domaine de la cybersécurité. L'éducation et la formation à la cybersécurité peuvent prendre diverses formes, y compris des programmes universitaires officiels, des certifications professionnelles, des ateliers pratiques et des initiatives de formation continue.

Dans le contexte numérique actuel, les programmes d'éducation et de formation à la cybersécurité jouent un rôle essentiel, car ils contribuent à prévenir les atteintes à la sécurité des données et à atténuer les cyberrisques en dotant les utilisateurs – particuliers comme professionnels – des connaissances et des compétences nécessaires pour détecter les cybermenaces potentielles et y répondre[19]. De fait, l'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) des États-Unis considère que l'éducation et la formation à la cybersécurité sont "*essentielles à la protection des infrastructures essentielles de la nation*"[20], soulignant ainsi le rôle crucial que jouent des professionnels de la cybersécurité bien formés pour préserver la sécurité nationale et les intérêts économiques.

La portée et le niveau des politiques d'éducation et de formation à la cybersécurité varient considérablement d'un État Membre de l'UIT à l'autre; certains États Membres déploient des outils politiques complets pour augmenter le nombre de professionnels de la cybersécurité à tous les niveaux, tandis que d'autres se concentrent sur des programmes de formation spécifiques dans ce domaine. Plusieurs États Membres de l'UIT ont ainsi ciblé leurs efforts sur la formation des étudiants des cycles supérieurs en mettant en place des programmes de niveau tertiaire dans les universités, tandis que d'autres ont privilégié la formation des employés

---

17 Document SG2RGQ/165 de la CE 2 de l'UIT-D (Brésil); https://www.youtube.com/playlist?list=PLOmVJ5Ex3R10wEUM3edKTSErojXs_07xg (Liste de lecture sur la cybersécurité).

18 https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

19 https://www.forbes.com/councils/forbestechcouncil/2025/01/21/protecting-our-future-why-cybersecurity-training-is-essential-for-students/

20 https://niccs.cisa.gov/education-training.

déjà sur le marché du travail. Il convient également de noter la création d'un certain nombre de programmes internationaux gérés par des organisations internationales. On observe également des disparités au niveau régional, puisque des cours de cybersécurité sont dispensés à l'université dans 91% des pays européens, contre 60% pour les pays de la région Amériques et 61% pour les pays de la région Afrique[21].

Au **Royaume-Uni**, une approche avancée en matière d'éducation et de compétences en cybersécurité a permis de mettre en œuvre une série de politiques et de programmes à tous les niveaux afin de réduire le déficit de compétences en cybersécurité. La stratégie du pays est axée sur trois domaines principaux: les compétences en matière de cybersécurité pour les adultes, les compétences en matière de cybersécurité pour les jeunes et le recrutement de cyberprofessionnels. Le Royaume-Uni propose ainsi des stages intensifs de 12 à 16 semaines pour les adultes, notamment dans le cadre de l'initiative "Compétences avancées dans le domaine de la cybersécurité", afin de permettre la reconversion et le renforcement des compétences des participants en la matière. Il encourage également les apprentissages, tels que le CyberFirst Degree Apprenticeship, qui permet d'acquérir une expérience pratique en cours d'emploi. En ce qui concerne les jeunes, le Royaume-Uni a créé un large éventail d'offres dans le cadre de l'initiative "CyberFirst". Parmi ces offres figurent un concours national à l'intention des filles qui souhaitent faire carrière dans le domaine de la cybersécurité, des stages de formation initiale pendant les vacances scolaires et un programme de reconnaissance des écoles ayant d'excellents programmes de formation en cybersécurité. Tous les jeunes de 11 à 14 ans peuvent également accéder gratuitement à la plate-forme d'apprentissage phare pour les jeunes au Royaume-Uni, Cyber Explorers, qui affiche un taux d'utilisation quasiment paritaire. Par ailleurs, le pays s'efforce de promouvoir les métiers de la cybersécurité par l'intermédiaire du Conseil britannique de la cybersécurité. Cet organisme professionnel vise à créer des filières et des normes claires dans le domaine de la cybersécurité, afin de le rendre plus accessible aux citoyens quel que soit leur niveau de carrière[22].

Le **Brésil** a mis en place une politique de cybersécurité bien conçue, axée sur des objectifs et des résultats spécifiques visés. Le pays a en effet lancé le programme "Hackers do Bem" (Hackers éthiques) afin de former 30 000 professionnels de la cybersécurité pour occuper un poste parmi les 230 000 postes manquants recensés. Le programme est mis en œuvre par le Réseau national brésilien d'enseignement et de recherche, le SENAI-SP et Softex, avec le soutien du Ministère brésilien des sciences, de la technologie et de l'innovation. Il repose sur une approche structurée en cinq niveaux de l'éducation à la cybersécurité et comprend d'abord une phase de mise à niveau des connaissances informatiques de base, avant de poursuivre avec une éducation aux concepts de base et aux concepts fondamentaux de la cybersécurité, et enfin une formation spécialisée. La formation spécialisée se concentre sur cinq profils professionnels clés chargés respectivement de l'évaluation de la sécurité, de l'architecture de sécurité, de la sécurité des applications, de l'intervention en cas d'incident informatique et de la composante gouvernance, risque et conformité. Le dernier niveau comprend un programme de résidence de six mois dans le domaine de la cybersécurité assorti d'un mentorat professionnel dans différents États brésiliens. Pour garantir la pérennité du programme, un centre national de cybersécurité a été mis en place et permet de mettre en relation diverses parties prenantes, notamment des établissements d'enseignement, des organismes publics, des entreprises et

[21] https://www.itu.int/epublications/fr/publication/global-cybersecurity-index-2024
[22] Document 2/77 de la CE 2 de l'UIT-D (Royaume-Uni).

des étudiants. Ce centre vise à faire correspondre les besoins du secteur avec les résultats de l'enseignement et à élargir les possibilités de formation à la cybersécurité dans tout le Brésil[23].

Certains pays promeuvent l'éducation à la cybersécurité dans les établissements d'enseignement supérieur afin d'améliorer les compétences de leur population. À titre d'exemple, le Gouvernement du **Rwanda** a ajouté des cours sur la sécurité de l'information dans les programmes d'informatique et de génie informatique des établissements d'enseignement supérieur. L'Université Carnegie Mellon Africa de Kigali propose ainsi des programmes de formation axés sur la cybersécurité, le génie logiciel et d'autres sujets liés aux technologies de l'information et de la communication (TIC). Ces programmes mettent l'accent sur l'enseignement et la recherche dans les domaines de la cybersécurité et du respect de la vie privée, allant de la sécurisation des logiciels et des systèmes de réseau à l'amélioration de la sécurité et de la confidentialité[24].

D'autres pays, au lieu de privilégier les établissements d'enseignement, ciblent les professionnels déjà sur le marché du travail, en particulier dans les secteurs davantage exposés aux cybermenaces. La **République argentine**, par exemple, a conçu des programmes de formation spécialement destinés aux employés du secteur public et couvrant des sujets essentiels liés à la sécurité des données et aux bonnes pratiques en matière de gestion de l'information. Ces cours visent à doter les apprenants des connaissances et des compétences nécessaires à la protection de la vie privée, de la confidentialité, de l'intégrité et de la disponibilité de l'information. Des formations spécialisées sont également dispensées aux fonctionnaires désignés comme coordonnateurs en matière de cybersécurité. Ces formations abordent des sujets tels que les nouveaux défis en matière de cybersécurité, les preuves numériques, les tests d'intrusion et le renforcement des systèmes informatiques[25].

De même, la **République arabe syrienne** a organisé des activités de formation à l'intention des fonctionnaires du secteur public, des universités et du secteur bancaire. L'Autorité nationale des services de réseau a mis en place un centre d'excellence qui a dispensé des cours de formation à la sécurité de l'information, dont les activités ont été interrompues pendant la guerre, avant d'être relancées en 2021[26].

L'**Égypte**, pour sa part, a créé en 2021 le Centre égyptien de formation à la réglementation des télécommunications pour l'Afrique, qui illustre toute l'importance de la coopération régionale en proposant des formations universitaires et professionnelles visant à renforcer les compétences des citoyens africains dans le domaine de la sécurisation des informations et des réseaux[27].

Un autre exemple concerne le Centre de cybercompétences pour l'Amérique latine et les Caraïbes, une initiative menée par l'**Union européenne**, CyberNet et le Gouvernement de la République dominicaine. Ce centre renforce les cybercapacités régionales grâce à un vaste échange de connaissances, à des formations ainsi qu'à l'élaboration de bonnes pratiques en matière de cybersécurité et de transformation numérique. Situé à Saint-Domingue, en République dominicaine, il fait office de plate-forme d'échange d'expériences collectives et aide plus de 25 pays d'Amérique latine et des Caraïbes à renforcer leurs cadres de cybersécurité et à encourager la coopération régionale. Sa large gamme d'activités de formation et

[23] Document SG2RGQ/184 de la CE 2 de l'UIT-D (Brésil).
[24] Document 2/35 de la CE 2 de l'UIT-D (Rwanda).
[25] Document 2/150 de la CE 2 de l'UIT-D (Argentine).
[26] Document SG2RGQ/163 de la CE 2 de l'UIT-D (République arabe syrienne).
[27] Document 2/329 de la CE 2 de l'UIT-D (Égypte).

de cyberexercices porte notamment sur la sensibilisation, la gestion des cyberrisques, la protection des infrastructures essentielles et l'élaboration de politiques et de lois en matière de cybersécurité. Il propose également de nombreuses sessions de formation technique visant à améliorer les compétences et les connaissances des professionnels de la cybersécurité dans la région. Il est important de noter que le Centre de cybercompétences pour l'Amérique latine et les Caraïbes attache une grande importance à la diversité de genre dans le domaine de la cybersécurité et organise des ateliers de formation spécialisés visant à renforcer l'autonomie des femmes dans ce domaine. Ce sont là des efforts déterminants pour constituer une main-d'œuvre diversifiée et résiliente dans le domaine de la cybersécurité, capable de relever les défis en constante évolution du paysage numérique[28].

Les cyberexercices, qui consistent à simuler des cyberattaques, des incidents en matière de sécurité de l'information et d'autres types de dysfonctionnement, constituent un élément important des initiatives de renforcement des capacités en matière de cybersécurité et sont au cœur des actions menées par le Bureau de développement des télécommunications de l'**UIT** (BDT) pour améliorer l'état de préparation et renforcer la protection et les capacités d'intervention en cas d'incident des pays dans le domaine de la cybersécurité. L'UIT organise des cyberexercices régionaux et mondiaux, ainsi que des exercices nationaux, et élabore des supports d'information pour appuyer ces activités[29].

Alors que la cybersécurité progresse dans l'ordre des priorités politiques mondiales, les organisations internationales se sont également engagées dans ce domaine en mettant en place des programmes visant à améliorer les compétences des générations futures en matière de cybersécurité. Parmi les initiatives internationales notables, on peut citer les projets mis en œuvre par l'UIT. Le programme Her CyberTracks du BDT comporte trois volets comprenant des formations techniques en ligne et sur site sur la politique et la diplomatie en matière de cybersécurité, des cours de formation aux compétences non techniques, des cercles de mentorat mensuels encadrés, des conférences thématiques, ainsi que des événements de réseautage régionaux – tous mis à disposition sous la forme d'un programme d'études complet dans le cadre du projet Policy & Diplomacy Track. L'objectif du projet est de promouvoir la représentation et la participation des femmes, tout en améliorant leur contribution aux processus politiques nationaux et internationaux en matière de cybersécurité[30].

1.3 Protection en ligne des enfants

Selon le Global Child Safety Institute (Childlight), en 2024, un enfant sur huit dans le monde, soit environ 302 millions de jeunes, s'est retrouvé confronté à des images et à des vidéos à caractère sexuel de manière non consentie. Cela inclut des prises ou des partages d'images sans l'accord du jeune, ou encore son exposition à des contenus à caractère sexuel[31].

La protection et la sécurité en ligne des enfants désignent les mesures, les pratiques et les stratégies mises en œuvre pour protéger les enfants et les jeunes contre les risques et les menaces potentiels associés à l'environnement numérique. La protection en ligne des enfants englobe un large éventail d'actions visant à rendre l'expérience en ligne plus sûre pour les mineurs, notamment la protection contre toutes les formes de violence en ligne,

[28] Document SG2RGQ/117 de la CE 2 de l'UIT-D (République dominicaine).
[29] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx
[30] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Skills-Development/Her-CyberTracks.aspx
[31] https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-globa

dont l'exploitation sexuelle et la sollicitation d'enfants à des fins sexuelles[32], l'exposition à des contenus préjudiciables et inappropriés pour des enfants, le cyberharcèlement, la pornographie et l'utilisation de plates-formes en ligne pour des activités illégales[33].

Dans le monde numérique d'aujourd'hui, où les enfants sont de plus en plus exposés à l'Internet et à ses risques potentiels, la protection et la sécurité en ligne des enfants revêtent une importance cruciale, de sorte que l'éducation à la sécurité en ligne est indispensable pour apprendre aux enfants à utiliser Internet de manière responsable. En sensibilisant les enfants aux risques en ligne, en leur permettant de développer leur esprit critique et en leur apprenant à se comporter de manière responsable en ligne, nous pouvons les aider à acquérir les compétences nécessaires pour se protéger et prendre des décisions éclairées en ligne[34].

Il ressort des contributions des États Membres que les pays ont pris très au sérieux la protection en ligne des enfants au cours des dernières années, nombre d'entre eux s'étant dotés de divers instruments pour assurer la sécurité en ligne des enfants. Les données de l'indice GCI indiquent que, dans le monde, 69% des gouvernements ont mis en œuvre des campagnes ciblant spécifiquement les parents, les éducateurs et les enfants dans le cadre des activités de protection en ligne des enfants[35]. Un certain nombre de pays ont ainsi élaboré des cadres juridiques et politiques détaillés, ainsi que des programmes et des outils pratiques, afin de rendre l'environnement en ligne plus sûr pour les enfants. Des données empiriques sur le comportement en ligne des enfants ont été recueillies en vue de mieux comprendre certains des problèmes les plus épineux en matière de sécurité en ligne et de les résoudre. Les pays ont reconnu l'importance des solutions multipartites qui associent les parties prenantes compétentes pour s'attaquer à ce problème aux multiples facettes. Enfin, certains pays ont également mis en œuvre des programmes qui allient sensibilisation à la cybersécurité et sécurité en ligne, ce qui démontre l'importance d'une approche globale.

L'**Australie** a fait le choix de mettre en place un cadre juridique solide pour faciliter la protection en ligne des enfants. En 2021, le Gouvernement australien a en effet établi un cadre solide grâce à la Loi sur la sécurité en ligne (Online Safety Act), qui porte sur le cyberharcèlement, la cyberviolence chez les adultes et la violence liées à l'image. En 2022, l'Australie a également créé le Conseil de la jeunesse en matière de sécurité en ligne, composé de 24 membres âgés de 13 à 24 ans, qui contribue directement à l'élaboration des politiques et des programmes, tout en collaborant avec les grandes entreprises technologiques pour renforcer la responsabilisation des utilisateurs[36].

La **Chine** s'est, elle aussi, dotée d'une politique globale de protection en ligne des enfants et a mis en œuvre des programmes d'éducation à la sécurité sur Internet de grande envergure. L'éducation à la cybersécurité est dispensée en priorité dans les écoles, qui touchent 90,3% des mineurs, et en second lieu dans les familles, pour 61,7% des mineurs. Au total, 85,4% des

---

[32] La sollicitation d'enfants à des fins sexuelles peut être définie comme le fait pour un adulte de proposer intentionnellement, par le biais des technologies de l'information et des communications, une rencontre à un enfant n'ayant pas atteint l'âge légal pour avoir des relations sexuelles, dans le but de commettre à son encontre des atteintes sexuelles ou de produire du matériel montrant des atteintes sexuelles sur des enfants, conformément à l'article 23 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels. (https://www.coe.int/fr/web/conventions/full-list?module=treaty-detail&treatynum=201).

[33] https://www.nspcc.org.uk/keeping-children-safe/online-safety/

[34] https://www.cois.org/about-cis/child-protection/resources; https://learning.nspcc.org.uk/online-safety

[35] https://www.itu.int/epublications/fr/publication/global-cybersecurity-index-2024

[36] Document 2/167 de la CE 2 de l'UIT-D (Australie).

mineurs chinois ont bénéficié d'une manière ou d'une autre d'une éducation à la sécurité sur l'Internet. Le programme "Le large bande au service de la protection des mineurs" a été mis en place par l'intermédiaire des opérateurs nationaux de télécommunications et a permis d'aider à protéger 160 millions de familles composées d'enfants en âge de fréquenter l'école, et peut traiter plus de 1,02 milliard d'appels. De plus, le Gouvernement chinois a mené plusieurs campagnes visant à répondre aux préoccupations en matière de sécurité en ligne. La Chine a promulgué plusieurs politiques importantes, notamment une réglementation relative à la protection des données personnelles des enfants sur les réseaux et une réglementation relative à la protection des mineurs sur Internet. L'efficacité de ces programmes se vérifie dans les statistiques: plus de 70% des mineurs chinois savent désormais reconnaître la fraude en ligne, et plus de la moitié d'entre eux sont conscients de l'importance d'utiliser Internet de manière saine[37].

D'autres pays associent également sensibilisation à la cybersécurité et éducation à la sécurité en ligne. C'est le cas de la **Fédération de Russie**, qui a mis en œuvre une campagne de formation aux outils numériques dans le cadre de son programme national plus large consacré à l'économie numérique, lancé en 2018. La campagne fournit du contenu sous forme de vidéos animées interactives couvrant des sujets essentiels en matière de cybersécurité, tels que la détection de l'hameçonnage, la protection des données personnelles, la lutte contre le cyberharcèlement, les bonnes pratiques en matière de médias sociaux et la vérification de l'information. Elle s'étend à des domaines spécifiques, notamment la sensibilisation au droit d'auteur, la prévention de la fraude en ligne, la protection contre les virus informatiques, l'étiquette numérique et la sécurité de la monnaie électronique. Dans un souci d'efficacité, la campagne fournit aux enseignants des supports pédagogiques à intégrer aux leçons sur la cybersécurité dans les cours d'informatique et à l'occasion des réunions parents-professeurs[38].

Un certain nombre d'administrations gouvernementales ont créé des outils technologiques spécifiques visant à protéger les enfants en ligne. Dans le cadre d'une stratégie nationale plus large de protection et d'autonomisation des enfants et des jeunes en ligne, la **Côte d'Ivoire** a lancé le site web "jemeprotegeenligne.ci"[39], qui propose des outils interactifs, des moteurs de recherche et des sites de médias sociaux spécialement conçus pour les enfants. Le site comprend également un mécanisme de signalement permettant aux utilisateurs de signaler les mauvais comportements de manière anonyme et en toute discrétion. Cette initiative, qui repose sur la collaboration de différentes parties prenantes, a reçu le soutien de l'Internet Watch Foundation[40].

Par ailleurs, plusieurs pays et organisations ont également reconnu la nécessité d'associer différentes parties prenantes au processus de protection en ligne des enfants. Au **Nigéria**, l'Initiative pour la protection en ligne des enfants constitue un cadre de référence pour l'intégration des politiques dans les conditions générales des fournisseurs de services Internet. La Commission nigériane des communications, l'un des principaux acteurs politiques du pays, a mis en place des mécanismes permettant de signaler les contenus présentant des actes de maltraitance à l'égard des enfants et mis en œuvre des mesures de blocage de ces contenus[41]. En 2020, la **République de Zambie** a, pour sa part, lancé une Stratégie nationale de protection

[37] Document SG2RGQ/212 de la CE 2 de l'UIT-D (China Mobile Communications Co. Ltd).
[38] Document SG2RGQ/170 de la CE 2 de l'UIT-D (Fédération de Russie).
[39] https://www.jemeprotegeenligne.ci/
[40] Documents 2/34 et 2/137 de la CE 2 de l'UIT-D (Côte d'Ivoire).
[41] Document SG2RGQ/20 de la CE 2 de l'UIT-D (Nigéria).

en ligne des enfants, assortie d'un plan de mise en œuvre quinquennal (2020-2024) axé sur les structures organisationnelles, le renforcement des capacités, les mesures juridiques, la coopération internationale et les procédures techniques. Le pays en a tiré plusieurs enseignements, notamment en ce qui concerne la mise en place d'une coopération plus large avec les parties prenantes, l'importance d'un financement durable et pérenne et l'élaboration d'un cadre de suivi et d'évaluation solide[42]. Enfin, l'initiative de l'**UIT** pour la protection en ligne des enfants sert de cadre directeur rassemblant une communauté multipartite dotée de compétences spécialisées éprouvées et d'une expérience de plus de dix ans dans le domaine de la fourniture d'une assistance technique efficace pour les activités de protection en ligne des enfants dans le monde entier. Cette initiative, regroupant plus de 80 partenaires du savoir, vise à élaborer des supports destinés aux enfants[43], des lignes directrices à l'intention des parents et des éducateurs[44], du secteur[45] et des décideurs[46], ainsi que des formations en ligne dispensées par l'Académie de l'UIT. Elle propose également des formations en présentiel pour les éducateurs et les jeunes[47]. Les lignes directrices susmentionnées constituent un ensemble complet de recommandations à l'intention de toutes les parties prenantes sur la façon de contribuer à instaurer un environnement en ligne sécurisé favorisant l'autonomisation des enfants et des jeunes. Elles ont fait l'objet de traductions et d'adaptations locales avant d'être diffusées dans le cadre de campagnes de sensibilisation.

Plusieurs pays se sont également attachés à renforcer les capacités et à collecter des données empiriques afin de comprendre comment les enfants interagissent en ligne. Au **Kenya**, l'Autorité des communications a ainsi lancé les campagnes "Be the COP" et "Huwezi Tucheza, Tuko Cyber Smart", qui s'adressent à la fois aux parents, aux représentants légaux, aux enseignants et aux jeunes. En outre, le pays, en collaboration avec l'Institut régional africain de formation supérieure en télécommunications, a élaboré des ressources éducatives ainsi que des initiatives de renforcement des capacités, notamment un programme de formation sur les mesures de protection et de sécurité en ligne des enfants. Ce programme a permis de former 951 participants issus de divers secteurs à la protection et à la sécurité en ligne des enfants. Le Kenya réalise également une enquête nationale sur la protection et la sécurité en ligne des enfants afin de recueillir des données empiriques sur le comportement en ligne des enfants, dont la clôture était prévue en 2024[48].

42 Document SG2RGQ/114 de la CE 2 de l'UIT-D (Zambie).
43 https://www.itu-cop-guidelines.com/children
44 https://www.itu-cop-guidelines.com/parentsandeducators
45 https://www.itu-cop-guidelines.com/industry
46 https://www.itu-cop-guidelines.com/policymakers
47 https://www.itu-cop-guidelines.com/
48 Document 2/119 de la CE 2 de l'UIT-D (Kenya).

Chapitre 2 – Pratiques en matière d'assurance de la cybersécurité

Les pratiques en matière d'assurance de la cybersécurité sont apparues comme un élément essentiel de la protection des réseaux, des systèmes et des données contre les activités malveillantes[49]. Ces pratiques désignent de manière générale les procédures utilisées pour s'assurer que des contrôles appropriés sont en place pour protéger la confidentialité, l'intégrité et la disponibilité des appareils, systèmes, réseaux et données électroniques. Bien qu'elles n'empêchent pas directement les cyberattaques, leur objectif, s'il est correctement mis en œuvre, est de réduire au minimum le risque que de telles attaques se produisent. Les pratiques en matière d'assurance de la cybersécurité peuvent être évaluées sur la base de contrôles, de directives et de normes de sécurité spécifiques et peuvent être imposées par la réglementation ou adoptées volontairement par le secteur. Cependant, il n'existe pas d'approche universelle, les autorités nationales et les organismes de régulation sectorielle recourant souvent à des pratiques différentes, allant de l'auto-évaluation et des lignes directrices appliquées sur une base volontaire aux systèmes d'étiquetage et aux contrôles de conformité stricts.

Bien qu'il n'y ait pas d'approche unique à recommander, on observe, depuis ces dernières années, une tendance constante privilégiant l'adoption de pratiques en matière d'assurance de la cybersécurité partout dans le monde, caractérisée par des évolutions différentes selon les pays et les régions. Pour preuve de cette dynamique, en décembre 2022, l'**Organisation de coopération et de développement économiques (OCDE)** a publié la Recommandation du Conseil sur la sécurité numérique des produits et des services, qui préconise l'adoption de politiques visant à améliorer la sécurité numérique des produits et services qui soient proportionnées au risque, et qui commencent par une approche modérée, fondée sur des mesures volontaires, avant d'étudier la nécessité éventuelle de recourir à des mesures contraignantes[50]. Le présent chapitre rend compte des difficultés rencontrées lors de la définition et de la mise en œuvre des pratiques en matière d'assurance de la cybersécurité, et évalue les répercussions et présente les enseignements tirés à ce jour de ces pratiques.

2.1 Méthodes d'évaluation de la criticité, des risques et des coûts

Lorsque l'on envisage de mettre en œuvre des pratiques en matière d'assurance de la cybersécurité, il est essentiel de déterminer d'abord ce qu'une entité essaie de protéger et les risques auxquels sont exposés les actifs identifiés. En effet, les pays et les entreprises qui souhaitent se prémunir contre les cyberattaques doivent en priorité recenser les systèmes et les actifs qui ont besoin d'être protégés et évaluer leurs vulnérabilités. À cet égard, il est utile de disposer d'un outil tel qu'un cadre ou un plan directeur pour la réalisation d'évaluations des risques. L'un des cadres les plus connus en la matière est le cadre de cybersécurité de l'Institut

[49] La sécurité opérationnelle est étroitement liée aux pratiques en matière d'assurance de la cybersécurité, en ce sens que la sécurité opérationnelle peut fournir une base solide pour les pratiques en matière d'assurance. Broadcom a présenté le modèle de bonnes conditions en soulignant qu'il se compose de quatre éléments clés, à savoir les personnes et les processus, les connaissances, les produits de sécurité (sécurité exogène) et la sécurité des actifs (sécurité endogène). Voir "Reduce Risk and Protect Reputation", Document SG17-C214 de la CE 17 de l'UIT-T soumis par Broadcom Corporation.

[50] https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0481

national des normes et de la technologie des **États-Unis** (NIST)[51], qui a été récemment mis à jour[52] et contient une approche largement utilisée pour aider à déterminer et à atténuer les risques organisationnels. Il établit des lignes directrices non réglementaires permettant aux organisations du monde entier de dresser un état des lieux de leur propre environnement de risque et d'appliquer des contrôles de cybersécurité appropriés. Le cadre révisé, publié début 2024, s'appuie sur un engagement large et à long terme avec la communauté des parties prenantes qui utilisent ces lignes directrices, ainsi que sur un alignement continu sur d'autres normes internationales[53].

La position privilégiée du NIST en tant qu'organisme non réglementaire a permis un engagement plus profond avec les parties prenantes du secteur des télécommunications partout dans le monde, ce qui a donné lieu à une meilleure compréhension des défis du monde réel et à un retour d'information, dont les nouvelles lignes directrices tiennent compte[54]. Ces dernières sont conçues pour être adaptables et souples, et applicables à toutes les organisations et à tous les secteurs. **BitSight** a intégré le cadre de cybersécurité du NIST dans sa plate-forme, qui a été utilisée par divers organismes publics responsables de la cybersécurité (équipes d'intervention informatique d'urgence, agences nationales de cybersécurité, régulateurs des télécommunications, etc.)[55]. Grâce à la plate-forme, les pays peuvent évaluer les risques de leurs infrastructures et de leurs actifs considérés comme étant essentiels et mesurer leurs facteurs de risque.

Les évaluations des risques peuvent également aider à déterminer le niveau d'assurance approprié, compte tenu de la sensibilité des données et des actifs protégés, des conséquences d'une atteinte à la sécurité et de l'environnement des menaces (c'est-à-dire si une entité est susceptible de subir une cyberattaque). Dans certains cas, les niveaux d'assurance seront dictés par des exigences réglementaires. Plus le niveau d'assurance est élevé, plus les contrôles de sécurité sont stricts. Par exemple, dans le cas d'un faible niveau d'assurance, un mot de passe ou un pare feu peuvent suffire, alors que dans le cas d'un niveau d'assurance plus élevé, il peut être nécessaire de recourir à des contrôles plus sophistiqués tels que le chiffrement avancé et l'authentification à plusieurs facteurs.

Bien que les pratiques en matière d'assurance de cybersécurité alourdissent les budgets alloués aux technologies de l'information, ne pas mettre en place de contrôles de sécurité peut même s'avérer encore plus coûteux. Le coût d'une cyberattaque n'est pas seulement financier, car le coût supplémentaire en termes de réputation peut être bien plus dommageable. En effet, perdre la confiance des clients et des citoyens entraîne des effets à long terme qui vont au-delà du coût financier; les organisations doivent donc en être conscientes d'un point de vue stratégique. De même, pour le secteur public, les cyberattaques peuvent avoir une incidence sur la fourniture de services publics et sur des activités essentielles, dont la perturbation ne peut pas être évaluée uniquement en termes financiers, car elle affecte aussi la vie des citoyens.

Pour certaines organisations, planifier et budgétiser les investissements en matière de cybersécurité en vue de garantir la conformité avec les réglementations nationales peut s'avérer difficile. Afin d'aider les organisations à planifier les coûts des contrôles de cybersécurité prévus par la loi, l'Autorité nationale de cybersécurité du **Royaume d'Arabie saoudite** a mis au point

---

51 https://www.nist.gov/cyberframework
52 https://www.nist.gov/cyberframework/nists-journey-csf-20
53 https://www.nist.gov/cyberframework
54 Document Q3/2_2023_07 présenté lors d'un atelier de la CE 2 de l'UIT-D par les États-Unis.
55 Document Q3/2_2023_02 présenté lors d'un atelier de la CE 2 de l'UIT-D par BitSight.

un outil d'estimation des coûts pour la mise en œuvre des contrôles essentiels de cybersécurité en Arabie saoudite[56]. Après avoir procédé à des essais préliminaires, l'Autorité a conclu que l'outil se révélait efficace et qu'il fournissait une bonne estimation des coûts, en particulier pour les organisations qui en sont aux premiers stades de la mise en œuvre des contrôles liés à la cybersécurité et qui ne disposent généralement pas d'informations sur le budget, le temps ou les ressources nécessaires à la mise en œuvre de ces contrôles.

2.2 Approches multipartites

Lors de l'élaboration d'une initiative, il est important de comparer les initiatives déjà existantes entre elles afin de repérer les bonnes pratiques et d'apprendre des succès et des erreurs des autres. Il importe également de travailler avec plusieurs parties prenantes, notamment du secteur des télécommunications, en vue d'obtenir des informations pertinentes dans le cadre de l'élaboration de l'initiative en question.

Alors que les pratiques en matière d'assurance de la cybersécurité deviennent de plus en plus nécessaires, elles peuvent être encore difficiles à appliquer dans les pays les moins avancés (PMA). Au **Togo**, le cas de Cyber Defense Africa peut aider à rendre compte de certaines des difficultés rencontrées sur les marchés locaux pour fournir une assurance de cybersécurité aux opérateurs de services essentiels[57]. Le manque de financement, le manque de confiance dans le gouvernement en tant que fournisseur de services ainsi que le manque de capacités humaines et d'infrastructures locales ont ainsi été cités au nombre des difficultés rencontrées. Pour aider les opérateurs de services essentiels à se conformer aux contrôles de cybersécurité récemment adoptés, le Gouvernement du Togo a établi un partenariat public privé avec un grand fournisseur de cybersécurité réputé dans le but de fournir des services de cybersécurité au secteur public comme au secteur privé. Grâce à ce modèle de partenariat, le Togo a fait de Cyber Defense Africa un fournisseur local de cybersécurité autosuffisant et de haute qualité, capable de soutenir les opérateurs de services essentiels sur une base volontaire. Le modèle d'autosuffisance employé a permis au pays de relever les nombreux défis mentionnés ci-dessus et de favoriser l'émergence de talents locaux dans le domaine de la cybersécurité, tout en stimulant le développement du marché local. En tant qu'entité privée dans un marché concurrentiel, Cyber Defense Africa joue un rôle primordial pour garantir l'adaptabilité, la qualité des services et la compétitivité des prix.

Il importe également de promouvoir la coopération entre les décideurs, qui peuvent définir l'environnement réglementaire, et les organisations de la société civile, qui peuvent stimuler la demande de sécurité et éclairer l'élaboration de politiques et de réglementations sur la base des pratiques régionales et internationales existantes et recensées. C'est ce que fait par exemple la **DiploFoundation**, une organisation internationale qui met à disposition ses compétences spécialisées en proposant des programmes de formation et de renforcement des capacités aux gouvernements, aux régulateurs, aux entreprises et à la société civile sur des questions d'actualité liées à la cybersécurité, et qui participe également au Dialogue de Genève sur les comportements responsables dans le cyberespace[58]. En 2020, le Dialogue de Genève a publié un ensemble de bonnes pratiques[59] dans lequel sont proposées des définitions de la conception sécurisée et de la gestion des vulnérabilités, de la modélisation des menaces, de

[56] Document SG2RGQ/201 de la CE 2 de l'UIT-D (Arabie saoudite).
[57] Document Q3/2_2023_09 présenté lors d'un atelier de la CE 2 de l'UIT-D par Cyber Defense Africa.
[58] Document Q3/2_2023_11 présenté lors d'un atelier de la CE 2 de l'UIT-D par DiploFoundation.
[59] https://genevadialogue.ch/goodpractices/

la sécurité des tiers et de la chaîne d'approvisionnement, du développement sécurisé, de la gestion et de la divulgation des vulnérabilités, ainsi que de la culture institutionnelle.

Le **Forum mondial sur la cyberexpertise (GFCE)**, pour sa part, est une plate-forme internationale chargée de coordonner les projets, de promouvoir le partage des connaissances et des compétences, de faire correspondre les demandes et les offres de soutien au renforcement des capacités et de mettre en place des projets de recherche[60]. Le Forum a créé quatre pôles régionaux – dans les îles du Pacifique, en Afrique, dans les Amériques et les Caraïbes et en Asie du Sud-Est. Fort de son ancrage mondial et de son soutien multiforme aux pays en développement, il est bien placé pour présenter des points de vue régionaux plus diversifiés sur les besoins et les exigences en matière de renforcement des cybercapacités. Le Forum dispose d'un portail en ligne qui répertorie les projets actuels et passés en matière de renforcement des cybercapacités au niveau mondial, ainsi que de ressources et d'outils. Ce portail en ligne contribue à éviter les doubles emplois et également à identifier certaines lacunes dans l'offre de renforcement des capacités[61].

2.3 Approches réglementaires évolutives

Dans de nombreux cas, les pratiques en matière d'assurance de la cybersécurité sont mises en place sur une base volontaire avant de devenir obligatoires. Le changement se produit généralement lorsque les gouvernements considèrent que le secteur des télécommunications n'en fait pas assez pour sécuriser les produits et que les consommateurs n'ont pas nécessairement les connaissances nécessaires pour évaluer si les produits sont sûrs ou non. Cela peut conduire les gouvernements et les autorités nationales à agir et à définir des pratiques en matière d'assurance que le secteur est censé respecter. Qu'elles soient prescrites par la loi ou non, il est conseillé de réviser et de mettre à jour les pratiques en matière d'assurance de la cybersécurité au fil du temps, compte tenu de l'évolution des menaces et des risques liés à la cybersécurité.

Au **Brésil**, le régulateur des télécommunications, Anatel, présente un exemple d'approche évolutive qui se traduit par la création d'un système d'organismes de certification et de laboratoires d'essai nationaux chargés de la certification des équipements des locaux d'abonné (également appelés "passerelles domestiques"). L'approche initiale d'Anatel consistait à fournir des lignes directrices sur la cybersécurité applicables au secteur des télécommunications sur une base volontaire. Toutefois, en procédant à des évaluations des risques, Anatel a constaté que les recommandations n'étaient pas suffisantes pour assurer la sécurité des équipements des locaux d'abonné, compte tenu des vulnérabilités et des menaces associées à ce type d'équipement, de sorte qu'il était nécessaire d'établir des exigences minimales de sécurité obligatoires pour ces produits. Les exigences obligatoires pour les fournisseurs de services de télécommunications au Brésil ont été publiées début 2023 et se concentrent sur des vulnérabilités telles que les mots de passe non sécurisés et les services inutilement activés[62]. Elles sont entrées en vigueur début 2024 dans le cadre des tests de laboratoire obligatoires pour l'approbation des produits[63]. Anatel a expliqué que le passage d'une approche non obligatoire à une exigence de certification obligatoire de cybersécurité pour un ensemble

---

60 Document Q3/2_2023_12 présenté lors d'un atelier de la CE 2 de l'UIT-D par le Forum mondial sur la cyberexpertise.

61 https://cybilportal.org/

62 Document SG2RGQ/58 de la CE 2 de l'UIT-D (Brésil).

63 Document Q3/2_2023_12 présenté lors d'un atelier de la CE 2 de l'UIT-D par le Brésil; https://informacoes.anatel.gov.br/legislacao/index.php/component/content/article?id=1505; et https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2023/1850-ato-2436.

spécifique d'équipements n'a été rendu possible qu'à l'issue d'un débat approfondi avec le secteur.

De même, en **Arabie saoudite**, l'Agence nationale de cybersécurité a mis en avant une initiative visant à créer un écosystème indépendant de vérification et de validation[64] destiné à tester et certifier les produits afin de garantir la cybersécurité à l'échelle du pays. Cette initiative vise en outre à recenser et à classer les matériels et les logiciels très sensibles aux cyberrisques et aux cybermenaces. Elle cherche également à contribuer au renforcement des capacités humaines dans le cadre de l'écosystème indépendant de vérification et de validation. La feuille de route de l'initiative envisage de commencer par un programme applicable sur une base volontaire avant de rendre obligatoire l'assurance en matière de cybersécurité. Pour l'Agence nationale de cybersécurité d'Arabie saoudite, il importe qu'un tel écosystème devienne à terme "autosuffisant", d'où l'adoption d'une approche consistant à encourager les acteurs du marché à mener des évaluations de vérification et de validation.

Dans le domaine de la sécurité de l'Internet des objets (IoT), le Royaume-Uni et l'Australie ont également présenté des études de cas sur le passage d'une approche volontaire à une approche obligatoire en ce qui concerne les assurances en matière de cybersécurité. Ces dernières années, les deux pays ont décidé d'imposer, par voie législative, une exigence minimale de sécurité pour les produits IoT grand public fondée sur la Norme EN 303 645 de l'Institut européen des normes de télécommunication (ETSI)[65], la première norme de cybersécurité applicable à l'échelle mondiale pour les produits IoT grand public.

Au **Royaume-Uni**, les fabricants, importateurs et distributeurs devront obligatoirement se conformer à trois des treize lignes directrices de l'ETSI en matière de sécurité, et la loi donne au gouvernement le pouvoir d'adopter des exigences supplémentaires si nécessaire, à la lumière d'évaluations régulières des menaces. La décision d'imposer des exigences minimales de sécurité a fait suite à une période durant laquelle l'application de ces exigences se faisait sur une base volontaire. En 2018, le pays avait en effet élaboré un recueil de pratiques volontaires[66] concernant la sécurité des produits IoT grand public, toutefois l'adoption de ces pratiques par le secteur des télécommunications s'est avérée plus limitée que prévu. Or, les données recueillies dans le cadre d'exercices de consultation ont montré que les consommateurs accordent une grande importance à la sécurité et qu'ils sont disposés à payer un prix plus élevé pour des produits sûrs. Les risques liés à la cybersécurité ne font pas l'objet d'une réglementation aussi stricte que la sécurité des produits, ce qui entraîne un manque de transparence de la part des fabricants et une adoption plus lente des politiques de sécurité. Il est également apparu que le marché des produits connectés décourage l'adoption de fonctionnalités de sécurité de base, estimant que les consommateurs sont déjà convaincus que les produits sont sûrs. Les nouvelles exigences visent à combler cette lacune en rendant obligatoires certaines pratiques figurant dans le régime PSTI (Product Security and Telecommunications Infrastructure) pour inciter les fabricants à tenir compte des vulnérabilités et à prendre les mesures nécessaires pour les atténuer. Ce régime est entré en vigueur en avril 2024 et s'applique à tout produit grand public pouvant se connecter à l'Internet[67].

---

64 https://nca.gov.sa/en/news/535/

65 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

66 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

67 Document Q3/2_2023_03 présenté lors d'un atelier de la CE 2 de l'UIT-D par le Royaume-Uni.

Parallèlement, en **Australie**, le gouvernement a constaté que son recueil de pratiques volontaires publié en 2020 et intitulé "Sécuriser l'Internet des objets pour les consommateurs" n'avait été que très peu appliqué. En 2024, il a donc proposé une loi rendant obligatoire l'application des pratiques contenues dans le recueil, une proposition qui a fait l'objet d'un consensus à l'issue d'une consultation publique. La loi reflète étroitement l'approche du Royaume-Uni, puisqu'elle prévoit de donner aux autorités le pouvoir d'imposer des normes de sécurité spécifiques pour les produits IoT en vertu de réglementations ultérieures. En intégrant les normes dans des réglementations plutôt que dans la loi, le Gouvernement australien compte mettre à jour ces normes rapidement afin de garantir la protection des consommateurs dans le pays, et ainsi se doter des bonnes pratiques internationales et sectorielles[68].

Au **Royaume-Uni**, l'un des défis rencontrés dans l'application du nouveau régime PSTI concerne les conséquences potentielles sur les petites et micro-entreprises qui pourraient éprouver des difficultés à s'y conformer. L'autorité britannique chargée de l'application du PSTI élabore donc des lignes directrices en vue d'atténuer toute incidence disproportionnée. Dans le cadre de la coopération avec le secteur des télécommunications, le Royaume-Uni a fait observer que les trois principales exigences à imposer dans le cadre du régime ont été identifiées et communiquées de manière transparente depuis plusieurs années. Au cours de ces années, le pays a procédé à un certain nombre d'exercices sur le processus de mise en œuvre du régime, et notamment sur les exigences en matière de mot de passe, l'architecture fondamentale des produits, l'exposition aux vulnérabilités et les exigences de transparence en matière de sécurité. L'étude d'impact a montré que, globalement, les avantages liés à la réduction du nombre de cyberattaques contre les consommateurs et les entreprises devraient dépasser les coûts associés à la mise en œuvre du régime PSTI. Le PSTI Act (2022) étant la première loi obligatoire sur les produits de cybersécurité au monde, le coût de son application est incertain, mais les premières estimations suggèrent que les fonds alloués seront suffisants.

Dans certains cas, le choix d'imposer une pratique en matière d'assurance de la cybersécurité ou de laisser son application se faire sur une base volontaire est dicté par le profil de l'utilisateur ou du client. Par exemple, la **République de Corée** a lancé son programme d'assurance de sécurité en nuage, une certification de sécurité pour les services d'informatique en nuage[69]. Officiellement, l'obtention de cette certification se fait sur une base volontaire. Toutefois, les clients du secteur public (les organismes publics) sont tenus d'utiliser un service en nuage ayant obtenu cette certification en vertu de la réglementation pertinente, de sorte que les fournisseurs de services en nuage doivent obtenir la certification lorsqu'ils fournissent de tels services à des organismes publics.

Parmi les bonnes pratiques à adopter, il convient de mentionner la réalisation régulière d'audits internes, qui permet de détecter les lacunes lors des contrôles et les risques d'exposition, ainsi que l'abonnement à des bases de données sur les menaces. Même si un produit est certifié, il peut, tout au long de son cycle de vie, présenter des failles de sécurité. En effet, un processus de certification nécessite la soumission d'informations à un moment précis, sans tenir compte de l'évolution dynamique des menaces futures. Récemment, une étude de **BitSight** a mis en évidence une forte corrélation entre la faible "cadence de correction" des vulnérabilités et la

[68] Document 2/320 de la CE 2 de l'UIT-D (Australie).
[69] https://isms.kisa.or.kr/main/csap/intro/index.jsp et Document SG2RGQ/34 de la CE 2 de l'UIT-D (République de Corée).

probabilité de subir une cyberattaque[70], soulignant l'importance cruciale de mettre à jour les systèmes dès que des correctifs de sécurité sont disponibles, compte tenu de la répartition inégale des correctifs dans le monde.

Les tests de pénétration, ou tests d'intrusion, sont des exercices d'assurance de sécurité qui permettent d'évaluer la sécurité d'un système informatique et de détecter les vulnérabilités qui pourraient autrement être utilisées pour exploiter les systèmes. L'Ofcom, le régulateur des communications du **Royaume-Uni**, applique volontairement, conjointement avec les fournisseurs de télécommunications, le programme TBEST qui est un test d'intrusion visant à simuler une cyberattaque pour déceler les failles de sécurité avant de les corriger par un processus de correction, et ce, dans l'objectif d'améliorer les dispositifs de sécurité du réseau des opérateurs[71],[72]. Plus généralement, ce programme constitue un exemple d'approche de régime de surveillance adoptée par l'Ofcom, qui souligne l'importance d'établir des relations de coopération entre le secteur réglementé et le régulateur. À ce jour, tous les fournisseurs de services de communication du Royaume-Uni ont appliqué volontairement le programme TBEST, ou sont en train de le faire, et ont modifié leurs pratiques en conséquence. Ce programme n'est ni une "norme" ni un processus de certification. L'objectif est de permettre aux fournisseurs de services de communication de mieux comprendre les cybermenaces et d'appliquer les corrections nécessaires en temps opportun afin d'améliorer leurs capacités de cyberdéfense. La prise en compte de ces vulnérabilités et de ces failles permet aux fournisseurs de mieux protéger leurs réseaux.

2.4 Sensibilisation des consommateurs et des fabricants

Des efforts ont été faits pour sensibiliser le public à l'importance de la cybersécurité et aux avantages qu'il y a à choisir des produits plus sûrs.

L'une des approches adoptées en ce sens consiste à mettre en place un système d'étiquetage pour la cybersécurité qui permet, comme c'est le cas en **République de Singapour**, d'apposer un label sur les produits certifiés. Les systèmes d'étiquetage servent avant tout d'outil d'information pour les consommateurs. Le système d'étiquetage pour la cybersécurité, mis en place dans le pays par l'Agence de la cybersécurité qui en a la charge, vise à aider les consommateurs à faire la distinction entre les produits IoT en fonction de leur niveau de sécurité[73]. Il est mis en œuvre sur une base volontaire (à l'exception des routeurs WiFi, pour lesquels il est obligatoire) et comporte quatre niveaux, le niveau 1 étant le niveau de sécurité le plus faible. Les niveaux 1 et 2 sont attribués à la suite d'une auto-évaluation par les fabricants, tandis que les niveaux 3 et 4 impliquent une évaluation réalisée par un laboratoire agréé. Les différents niveaux ont pour but d'inciter les fabricants à intégrer des mesures de sécurité supplémentaires allant au-delà des exigences minimales.

L'Agence de la cybersécurité de Singapour a examiné les avantages et les inconvénients liés à l'imposition de normes de cybersécurité, notamment le risque que les fabricants court circuitent le marché en raison de l'augmentation des coûts de mise en conformité. L'objectif est plutôt de faire évoluer la mentalité des fabricants pour qu'ils considèrent la cybersécurité

---

[70] https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity

[71] Ce programme fonctionne en étroite collaboration avec le Ministère britannique de la science, de l'innovation et de la technologie et le Centre national pour la cybersécurité du Royaume-Uni.

[72] Document SG2RGQ/74 de la CE 2 de l'UIT-D (Royaume-Uni).

[73] Document Q3/2_2023_05 présenté lors d'un atelier de la CE 2 de l'UIT-D par Singapour.

comme un catalyseur et un facteur de différenciation sur le marché et non pas comme un coût supplémentaire. S'agissant des effets du système d'étiquetage pour la cybersécurité à Singapour, le processus en est encore à ses débuts et les efforts se poursuivent pour encourager les fabricants à adhérer au système et à renforcer la cybersécurité de leurs produits. Une enquête publique sera menée à l'avenir afin d'évaluer la sensibilisation et le comportement des consommateurs. Il convient de noter que, concernant les niveaux 1 et 2, le coût de la mise en conformité est réduit au minimum pour les fabricants, si bien qu'il n'y a pas eu d'augmentation significative du coût des produits pour les consommateurs. Une fois le système volontaire mis en place, on s'attend à ce que les forces du marché poussent les fabricants à renforcer la cybersécurité.

Aux **États-Unis**, le programme U.S. Cyber Trust Mark, récemment mis en place, constitue un autre exemple de programme volontaire d'étiquetage pour la cybersécurité des produits IoT[74]. Lors de l'élaboration du programme, la Commission fédérale des communications a souligné qu'il était essentiel de solliciter la participation du public et de recueillir l'avis de toutes les parties prenantes concernées, notamment le secteur des télécommunications, les pouvoirs publics et la société civile, afin de concevoir et de mettre en œuvre un programme qui réponde aux besoins recensés. Dirigé par la Commission fédérale des communications, le programme U.S. Cyber Trust Mark sera mis en œuvre en collaboration avec divers partenaires interinstitutionnels, ce qui nécessitera une coopération étroite avec tous les organes gouvernementaux concernés.

Outre l'étiquetage, les investissements dans les contrôles techniques ainsi que la sensibilisation et l'éducation de la population aux risques de cybersécurité auxquels les organisations et les pays sont confrontés revêtent, eux aussi, une importance cruciale. Actuellement, les attaques par rançongiciel suscitent le plus d'inquiétude. Pour ce type d'attaques, le principal vecteur d'attaque – c'est-à-dire la manière dont un criminel s'introduit dans un réseau ou un système – est l'hameçonnage[75]. De fait, les cybercriminels peuvent souvent contourner les contrôles de sécurité par le simple clic d'un internaute dans un courriel d'hameçonnage. Il est donc primordial, pour garantir la cybersécurité, que les citoyens et les employés soient sensibilisés à ces questions. La promotion de la sensibilisation des utilisateurs à la cybersécurité est abordée au Chapitre 1 du présent rapport.

2.5 Accords internationaux de synergie, d'harmonisation et de réciprocité

La conclusion d'accords de réciprocité entre les différents modèles d'assurance de cybersécurité, à savoir les systèmes de certification et d'étiquetage, peut être un facteur déterminant pour la transposition à plus grande échelle de ces pratiques. Comme l'ont souligné les parties prenantes, les accords de réciprocité peuvent faciliter la mise en conformité des acteurs du secteur des télécommunications opérant sur plusieurs marchés. Toutefois, étant donné que les accords de réciprocité sont un mécanisme formel, qu'ils peuvent comporter de nombreuses conditions au niveau national et que leur approbation et leur signature prennent du temps, il est nécessaire que les pratiques en matière d'assurance de cybersécurité trouvent des synergies avec les approches internationales existantes qui sont conformes aux priorités et aux besoins

[74] Document 2/196 de la CE 2 de l'UIT-D (États-Unis).

[75] Tactique couramment utilisée par les cybercriminels pour inciter les internautes à révéler des informations confidentielles ou à télécharger des logiciels malveillants qui corrompent le système ou le réseau pris pour cible.

nationaux. Cela permettra de réduire la charge réglementaire pesant sur les fournisseurs de produits et de services, l'objectif étant d'éviter les exigences contradictoires.

À cet égard, l'Agence de la cybersécurité de Singapour a souligné l'importance de la coopération internationale dans l'élaboration et la mise en œuvre de son système d'étiquetage pour la cybersécurité. **Singapour** a en effet signé des accords de reconnaissance mutuelle avec la Finlande et la République fédérale d'Allemagne, et s'efforce d'élargir ses partenariats dans ce domaine. Le pays, qui a fait part de son expérience, a indiqué que les gouvernements devaient être proactifs dans la mise en place de tels accords, tout en précisant que les fabricants avaient également intérêt à soutenir ce processus, car les accords de reconnaissance mutuelle réduisent les contraintes liées à la répétition des tests et des certifications et contribuent à faciliter l'accès aux marchés dans différentes juridictions. Le processus consiste à réunir les parties intéressées afin d'harmoniser les exigences et d'établir des normes communes à la fois réalistes et peu contraignantes.

Au niveau européen, l'**Agence européenne pour la cybersécurité (ENISA)** a pour mandat d'élaborer trois systèmes de certification devant être reconnus dans l'ensemble du marché intérieur et bénéficiant donc d'une "reconnaissance mutuelle" automatique dans l'ensemble de l'UE. Il s'agit du système de critères communs de l'UE pour les produits TIC, dont le règlement d'application a été adopté début 2024; du système de services en nuage, qui fait actuellement l'objet de discussions; et enfin du système 5G, qui est en cours d'élaboration[76].

Outre les accords de réciprocité, et compte tenu du fait que le secteur des télécommunications opère sur des marchés internationaux, l'harmonisation des exigences minimales en matière de sécurité est également un élément important à prendre en considération. Les normes de l'ETSI sur les produits IoT grand public constituent un exemple de tentative d'harmonisation de ces exigences minimales. La principale question est de savoir dans quelle mesure les différents cadres réglementaires doivent être harmonisés et dans quelle mesure ils doivent être soumis aux mêmes normes internationales. À cet égard, il a été noté que le renforcement et même la recherche d'un cadre propice au dialogue constituaient un défi. Aux fins d'une harmonisation, les activités de l'ENISA dans le domaine de la normalisation de la cybersécurité et de la 5G nécessitent la collaboration du Comité européen de normalisation, du Comité européen de normalisation électrotechnique, de l'ETSI, de l'Organisation internationale de normalisation, de la Commission électrotechnique internationale, de la GSM Association (GSMA), du Projet de partenariat de troisième génération (3GPP) ainsi que de GlobalPlatform. À ce jour, l'un des principaux résultats de l'ENISA a été de centraliser les contrôles de sécurité 5G de différentes organisations de normalisation dans un référentiel unique[77].

[76] Document Q3/2_2023_10 présenté lors d'un atelier de la CE 2 de l'UIT-D par l'Agence européenne pour la cybersécurité.

[77] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

Chapitre 3 – Coordination nationale des équipes CIRT aux fins de la résilience des infrastructures essentielles et des interventions en cas d'incident de cybersécurité

Dans un environnement numérique en constante évolution, les organisations sont confrontées à une menace toujours croissante: les incidents de cybersécurité. En effet, ces derniers peuvent compromettre des données confidentielles, perturber les différentes activités des organisations et saper la confiance des parties prenantes. C'est pourquoi les initiatives de coordination nationale des équipes d'intervention en cas d'incident informatique (CIRT) contribuent à renforcer la résilience des infrastructures essentielles. Ces initiatives, qui favorisent la coopération l'échange d'informations et l'adoption de protocoles normalisés, visent à renforcer les capacités collectives à détecter les cyberincidents, à en atténuer les effets et à se relever efficacement. Pour atteindre cet objectif, les États Membres doivent redoubler d'efforts afin de créer et de mettre en place des équipes CIRT, cette mesure constituant généralement la première étape majeure vers l'instauration d'une culture de la cybersécurité. Il convient de noter que les équipes CIRT sont également connues sous le nom d'équipes d'intervention en cas d'incident de cybersécurité (CSIRT) ou d'équipes d'intervention en cas d'urgence informatique (CERT), considérées comme des synonymes dans le présent rapport[78].

Les équipes CIRT ont notamment pour mission de lutter contre les menaces qui pèsent sur les infrastructures essentielles. Le terme "infrastructures essentielles" désigne un ensemble de systèmes, de réseaux et d'actifs considérés comme essentiels à la sécurité publique. Il n'existe pas de définition unique de ce qui constitue une "infrastructure essentielle", puisque cette notion est définie au niveau national, en fonction des besoins et des priorités des pays, mais elle englobe généralement des secteurs tels que les transports, les systèmes énergétiques, les systèmes de communication, les systèmes d'approvisionnement en eau, les systèmes financiers et les services de santé. Les cyberactivités malveillantes ciblant les infrastructures essentielles nationales restent un défi majeur pour les gouvernements et peuvent présenter des risques pour les citoyens. Selon un rapport de 2024 de KnowBe4, les cyberactivités malveillantes ciblant les infrastructures essentielles ont augmenté de 30% depuis 2022, totalisant plus de 420 millions d'attaques entre janvier 2023 et janvier 2024. Cela équivaut à 13 attaques par seconde[79].

Les attaques contre les infrastructures essentielles représentent une menace particulièrement grave pour les citoyens. Les services de santé et d'urgence sont souvent pris pour cibles, ce qui a une incidence sur leurs capacités à fournir des soins médicaux, comme réaliser des opérations chirurgicales et prescrire des ordonnances. Les infrastructures énergétiques, comme les réseaux électriques, constituent également des cibles privilégiées. Face aux risques de pertes de vies

[78] Pour de plus amples informations sur la terminologie, voir la publication de l'ENISA: "How to Setup CSIRT and SOC" (https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc).

[79] https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf?hsLang=en-us

humaines, la coordination et l'intervention en cas d'incidents de ce type sont essentielles et constituent l'une des fonctions clés des équipes CIRT.

Dans le cadre de la création et du renforcement des équipes CIRT, les pays élaborent souvent des plans d'intervention en cas d'incident informatique solides permettant de détecter, d'endiguer et d'atténuer efficacement les atteintes à la sécurité et d'y remédier. De tels plans, conçus de manière proactive et bien définis, sont indispensables pour aider les organisations à atténuer efficacement les effets des atteintes à la sécurité. Les pays ont adopté différents modèles de plan pour gérer au mieux les risques et lutter contre les cyberactivités malveillantes. Ces modèles reposent généralement sur une approche globale, intégrant les bonnes pratiques, et favorisant une culture de l'amélioration continue afin d'accroître la résilience face aux cybermenaces et de protéger les actifs numériques. Alors que les menaces continuent d'évoluer, les stratégies d'intervention en cas d'incident doivent conserver une longueur d'avance sur les cyberadversaires et protéger l'intégrité et la confiance des organisations.

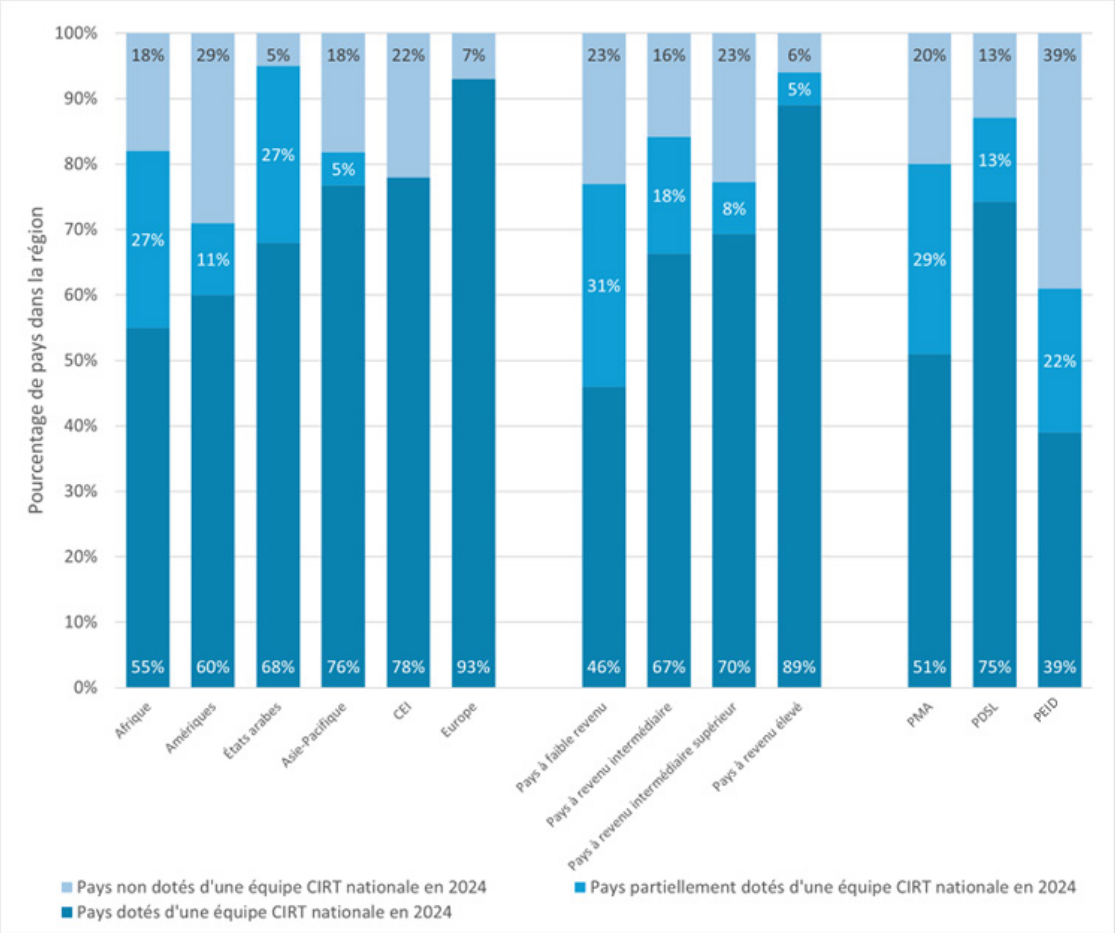
Plus récemment, on a vu émerger des centres nationaux de coordination informatique visant à améliorer la coordination de l'ensemble des pouvoirs publics en cas d'incident informatique. Un incident informatique grave touche souvent un certain nombre d'organismes gouvernementaux; coordonner une intervention rapide peut donc permettre d'éviter de graves conséquences. Le fait de disposer d'un centre ou d'une unité de coordination centralisé peut contribuer à assurer une intervention rapide et à gérer et à contrôler globalement l'incident. Il convient de mentionner que les infrastructures essentielles ne sont pas nécessairement détenues et gérées par le secteur public et que, par conséquent, assurer la coordination avec le secteur privé est également un élément extrêmement important pour faire face et réagir à un incident informatique.

3.1 Création d'équipes CIRT

Selon l'Indice mondial de cybersécurité (GCI) 2024[80], "139 pays disposent d'une équipe CIRT nationale, tandis que 55 n'ont aucune équipe CIRT".

[80] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Figure 1 – Répartition des pays disposant d'une équipe CIRT par région, par niveau de revenu et par niveau de développement



Source: UIT

Les équipes CIRT ont des rôles variés, mais l'une de leurs principales fonctions consiste à détecter et à analyser les menaces potentielles pour les réseaux et les systèmes et à intervenir pour atténuer les effets lorsque des incidents se produisent. La création d'une équipe CIRT constitue souvent une étape clé vers la promotion d'une culture de sensibilisation et de résilience en matière de cybersécurité. Cela passe notamment par le renforcement des capacités et des mécanismes nécessaires à la protection des infrastructures essentielles.

Le Gouvernement du **Kenya** a mis sur pied le Centre de coordination de l'équipe nationale d'intervention en cas d'incident informatique, un cadre de coopération multi-institutions responsable de la coordination de la cybersécurité à l'échelle nationale qui sert de point de contact national pour les questions de cybersécurité. Ce centre est composé d'une équipe multipartite dotée de compétences diversifiées pour faire face aux incidents relatifs à la sécurité informatique et les gérer de manière efficace. Consciente du rôle déterminant de la cybersécurité dans la promotion d'une économie numérique prospère, l'Autorité kenyane des communications a lancé une série de stages intensifs et d'hackathons sur la cybersécurité afin de renforcer les capacités locales en la matière[81].

[81] Document 2/112 de la CE 2 de l'UIT-D (Kenya).

Avec l'aide de l'UIT, la **République kirghize** a entrepris de créer une équipe CIRT nationale. Cette équipe a notamment pour mission de détecter, de gérer et de contrer les cybermenaces, ainsi que de mettre en place des capacités de surveillance, d'alerte et d'intervention en cas d'incident, de renforcer les capacités nationales et de transférer le savoir-faire nécessaire à la protection des infrastructures informatiques essentielles[82].

L'**UIT** travaille en coopération avec les États Membres et des organisations internationales en vue de renforcer la cybersécurité, moyennant la création et le renforcement d'équipes CIRT nationales et régionales. Pour ce faire, par l'intermédiaire du BDT, l'UIT évalue les capacités des équipes CIRT et aide à ce jour 84 pays à évaluer leur capacité d'intervention dans le domaine de la cybersécurité et à créer ou à renforcer des équipes CIRT nationales. L'UIT a mis en œuvre 21 projets ayant trait aux équipes CIRT et travaille actuellement sur trois autres projets. Des évaluations des capacités des équipes CIRT ont ainsi été réalisées pour l'Azerbaïdjan, la Sierra Leone et la République-Unie de Tanzanie, tandis que des évaluations sont en cours pour la République du Zimbabwe, le Royaume du Bhoutan et le Royaume du Lesotho[83]. Ces évaluations permettent aux équipes CIRT nationales d'élaborer des plans opérationnels axés sur l'amélioration. L'UIT collabore également avec le Forum pour les équipes d'intervention en cas d'incident en vue de consolider le cadre de services des équipes CIRT et de réviser des supports de formation pour le renforcement des capacités dans la gestion des interventions des équipes CIRT nationales[84].

3.2 Rôle et responsabilités des équipes CIRT et des infrastructures essentielles

Les équipes CIRT jouent un rôle essentiel dans la protection des infrastructures essentielles de divers secteurs dans la mesure où elles assurent une surveillance en temps réel, une gestion des incidents, une analyse des menaces et des évaluations de vulnérabilité. En règle générale, elles sont responsables de la résilience des systèmes TIC, de la détection et de la résolution rapides des menaces de cybersécurité et de la coordination des efforts visant à réduire au minimum les incidences sur la sécurité nationale, l'ordre public et l'économie. En fonction des besoins du pays, de son niveau de développement et de ses infrastructures essentielles, les équipes CIRT assument différents rôles et entretiennent différentes relations pour garantir la cybersécurité.

En **République de Lituanie**, l'équipe CIRT nationale relève du Centre national de cybersécurité et se consacre plus particulièrement à la coordination des interventions en cas de cyberincident et au renforcement de la résilience dans l'ensemble des infrastructures essentielles. Le Gouvernement lituanien a veillé à ce que l'équipe CIRT soit dotée des fonctions et des capacités techniques nécessaires pour protéger activement les infrastructures essentielles, si bien que son action sert de modèle aux autres pays qui cherchent à renforcer les capacités de leurs propres équipes. L'équipe CIRT lituanienne contribue à fournir des services de gestion des incidents aux parties prenantes des secteurs public et privé ainsi qu'à garantir que des interventions appropriées soient mises en œuvre aussi bien pendant qu'après les cyberattaques. L'un des aspects clés du rôle d'une équipe CIRT dans la gestion des incidents est sa capacité à se

[82] Document 2/170 de la CE 2 de l'UIT-D (BDT de l'UIT); Document SG2_2023_05 présenté lors d'une séance d'information de la CE 2 de l'UIT-D par le BDT de l'UIT.
[83] Document 2/201 de la CE 2 de l'UIT-D (BDT de l'UIT).
[84] Pour de plus amples informations sur les activités de l'UIT relatives aux équipes CIRT: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx.

coordonner avec l'administrateur du réseau ou du système touché, ce qui facilite la reprise rapide des opérations.

En cas d'incident majeur, les spécialistes de l'équipe CIRT lituanienne sont déployés sur place pour aider les opérateurs des infrastructures essentielles à retrouver un fonctionnement normal. Par exemple, lors d'une attaque par déni de service visant le secteur des télécommunications lituanien, l'équipe CIRT nationale a joué un rôle crucial en coordonnant les communications entre les opérateurs touchés et en fournissant des recommandations techniques qui ont permis de rétablir rapidement les services.

La protection des infrastructures essentielles ne consiste pas seulement à faire face aux cyberincidents malveillants, mais aussi à les prévenir au moyen d'une autre fonction, plus avancée, des équipes CIRT. La Lituanie a confié à son équipe CIRT la responsabilité de gérer les vulnérabilités. Celle-ci s'en acquitte en recueillant des informations auprès de sources publiques, de réseaux privés et de mécanismes de signalement des vulnérabilités. Elle analyse activement les actifs numériques lituaniens afin de recenser les vulnérabilités qui pourraient être exploitées par des acteurs malveillants. Par la suite, elle diffuse les informations obtenues sur les vulnérabilités et les menaces, contribuant ainsi à renforcer les systèmes des infrastructures essentielles contre d'éventuelles cyberattaques et assurant une protection proactive dans les secteurs clés[85].

Le **Brésil** a mis sur pied plusieurs organisations de premier plan pour veiller à ce que ses infrastructures essentielles puissent continuer à faire face aux menaces, soient protégées et appliquent les procédures de cybersécurité nécessaires. Le pays compte deux équipes CIRT assumant des responsabilités au niveau national: l'équipe nationale d'intervention informatique d'urgence (CERT.br) et le Centre de prévention, de traitement et d'intervention en cas d'incident informatique au niveau gouvernemental (CTIR Gov). Il dispose aussi de plusieurs équipes CIRT sectorielles ainsi que du Réseau fédéral de gestion des incidents informatiques (ReGIC), créé en 2021 et coordonné par le CTIR Gov[86].

Pour illustrer en quoi consiste une équipe CIRT sectorielle, on peut citer le Centre d'intervention en cas d'incident de sécurité (CAIS) du Réseau national pour l'enseignement et la recherche. Depuis sa création en 1997, le CAIS constitue la principale équipe CIRT du réseau universitaire brésilien. Agissant conformément aux lignes directrices de la Demande d'observations 2350, le CAIS a pour mission de détecter, de résoudre et de prévenir les incidents de sécurité au sein du réseau universitaire brésilien. Bien qu'il n'ait pas compétence directe sur les établissements universitaires, il joue un rôle de coordination essentiel dans le traitement des incidents. Les activités du CAIS traduisent le besoin croissant de coopération au sein de secteurs spécifiques pour gérer efficacement les risques de cybersécurité. Le CAIS constitue un exemple de ce à quoi peut ressembler une équipe CIRT sectorielle assurant la protection des infrastructures essentielles[87].

Dans le cadre d'autres efforts récents menés au Brésil visant à renforcer la cybersécurité nationale, le ReGIC, le Réseau fédéral de gestion des incidents informatiques a été créé afin de renforcer la coordination entre les entités gouvernementales fédérales aux fins de la protection des infrastructures essentielles.

---

[85] Document 2/322 de la CE 2 de l'UIT-D (NRD Cyber Security).
[86] Document SG2RGQ/182 de la CE 2 de l'UIT-D (Brésil).
[87] Document SG2RGQ/183 de la CE 2 de l'UIT-D (Brésil).

Le ReGIC définit des mandats et des objectifs que les organismes fédéraux doivent remplir. Les organismes fédéraux sont ainsi tenus de participer au réseau et notamment d'appliquer des mesures de partage de renseignements concernant les menaces et les alertes en cas de cyberattaque et de se coordonner lorsqu'un incident survient. Le ReGIC joue également un rôle spécifique en matière de coordination sectorielle, puisque les organismes de régulation, comme l'Agence nationale des télécommunications (Anatel), sont tenus de créer des équipes CSIRT sectorielles et de rendre des comptes au ReGIC.

La **Tanzanie**, en plus d'avoir créé une équipe CERT nationale, a également mis sur pied des équipes CERT sectorielles[88], comme l'équipe TZ-Fincert pour les institutions financières et bancaires, une équipe pour les établissements universitaires et une équipe pour les ministères, les départements, les agences et les autorités de l'État. Il en a résulté une amélioration de l'efficacité des mesures prises pour répondre aux menaces, qui s'est traduite par un renforcement de la protection, une amélioration globale des interventions en cas d'incident et une meilleure coordination des différentes questions liées à certains secteurs.

Les équipes CIRT jouent un rôle indispensable dans la protection des infrastructures essentielles de leur pays contre les cybermenaces. En coordonnant la gestion des incidents, en partageant des informations sur les menaces, en évaluant les vulnérabilités ou encore en offrant des conseils sur mesure, les équipes CIRT favorisent la cyberrésilience des infrastructures essentielles, garantissant ainsi un relèvement rapide et une atténuation des effets des cyberattaques. Les exemples mentionnés dans ce chapitre soulignent l'importance des interventions sectorielles, de la coopération entre entités publiques et privées, et de la nécessité de poursuivre les efforts de résilience pour protéger les infrastructures nationales contre les cybermenaces sophistiquées. Afin de veiller à ce que les équipes CIRT nationales appliquent de bonnes pratiques pour faire face aux incidents en matière de cybersécurité et pour promouvoir une coopération technique entre les équipes CIRT des différents pays, l'**UIT** organise des cyberexercices[89] aux niveaux régional et intrarégional. Les exercices de cybersécurité permettent aux États Membres de l'UIT de renforcer leurs capacités en matière de préparation en cas d'incident, de protection face aux incidents et d'intervention à la suite d'un incident.

3.3 Au-delà de l'essentiel: Se coordonner pour réussir au-delà des frontières

À mesure que les pays se dotent d'équipes CIRT et renforcent leur culture de la cybersécurité, plusieurs étapes et modèles doivent permettre de coordonner la protection des infrastructures essentielles au-delà des principes de base. Une fois qu'un pays s'est doté d'une équipe CIRT efficace et de programmes et politiques nationaux pour la gestion des incidents informatiques, il est essentiel de se projeter au-delà des frontières nationales et d'établir une coordination internationale afin de prévenir les cyberincidents, d'y faire face et d'en atténuer les effets. Aujourd'hui, dans le monde interconnecté qui est le nôtre, les cybermenaces ne connaissent souvent pas de frontières, ce qui nécessite des stratégies de coopération pour renforcer la résilience mondiale en matière de cybersécurité. À cet égard, les États-Unis comme l'Union européenne ont mis au point des modèles de coopération internationale efficaces qui démontrent l'importance de tels efforts, notamment en ce qui concerne l'établissement de relations tant au niveau national qu'international.

[88] Document 2/346 de la CE 2 de l'UIT-D (Tanzanie).
[89] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx

Aux **États-Unis**, l'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) a mis en œuvre le programme Pre-Ransomware Notification, une initiative tournée vers l'avenir, conçue pour détecter les menaces liées aux rançongiciels et y répondre avant qu'elles ne puissent causer des dommages. Ce programme permet une cybersécurité proactive grâce à des alertes précoces, qui visent à aider les organisations à éviter la perte de données critiques, la perturbation des activités ainsi que les répercussions financières causées par les attaques par rançongiciel. Le programme repose sur deux piliers clés: des partenariats solides et la collecte systématique de renseignements exploitables[90].

Le Joint Cyber Defense Collaborative (JCDC) de la CISA occupe un rôle central, puisqu'il recueille les informations émanant de la communauté des chercheurs en cybersécurité, des fournisseurs d'infrastructures et des organisations de renseignement sur les menaces. Grâce aux relations étroites qu'il entretient avec les entités du secteur privé et les chercheurs, le JCDC est en mesure de fournir des renseignements de qualité en temps opportun. Lorsqu'une information crédible est reçue, le JCDC s'appuie sur son personnel au niveau national et sur le terrain pour avertir les organisations touchées et fournir des conseils sur les mesures à prendre pour atténuer les effets de la menace.

De plus, le programme doit son succès à sa portée internationale assurée par une étroite coordination avec des équipes CIRT étrangères. Lorsqu'une communication informant d'une menace concerne une organisation située en dehors du territoire des États-Unis, le JCDC travaille avec ses homologues internationaux pour s'assurer que l'entité en question est alertée rapidement. Ces relations entre équipes CIRT sont indispensables, en particulier lorsqu'une action rapide est nécessaire pour empêcher le déploiement de rançongiciels. Dans les cas où un rançongiciel a déjà été déployé, le JCDC apporte son soutien aux organisations touchées en leur fournissant des informations sur les stratégies, les techniques et les procédures des auteurs de la menace, ainsi qu'en les aidant à mener des enquêtes et à prendre des mesures de correction. Cette aide comprend souvent l'identification des données dont la sécurité a été compromise et la fourniture de conseils pour atténuer les effets à long terme de l'attaque.

L'**Union européenne** (UE) a également donné la priorité à l'établissement d'une coordination internationale afin de renforcer sa cyberrésilience. Le projet de la Coopération structurée permanente (PESCO) concernant la création d'équipes d'intervention rapide aux cyberattaques et l'assistance mutuelle dans la cybersécurité[91] en est un excellent exemple. Ce projet prévoit le déploiement rapide d'experts en cybersécurité dans les États membres de l'UE en cas d'incidents de grande ampleur, en particulier lorsque des infrastructures essentielles sont visées. La mise en commun des compétences et des ressources permet à l'UE de renforcer ses capacités collectives à faire face aux cybercrises tant au niveau national que régional. Cette initiative témoigne également de l'engagement de l'UE en faveur d'une cybersécurité collaborative, puisqu'elle permet à ses États membres de se soutenir mutuellement en cas d'urgence.

En outre, ces initiatives, tant aux États-Unis que dans l'UE, soulignent combien il est important de partager les renseignements sur les menaces, d'instaurer des relations de confiance et d'établir des protocoles normalisés pour la coordination transfrontière.

Face à des cybermenaces de plus en plus sophistiquées et de plus en plus étendues, la coordination transfrontière devient un enjeu crucial. Les exemples mentionnés ci-dessus

[90] Document SG2RGQ/164 de la CE 2 de l'UIT-D (États-Unis).
[91] Document 2/322 de la CE 2 de l'UIT-D (NRD Cyber Security); https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.

montrent comment la coopération internationale peut renforcer les capacités d'intervention en cas d'incident et améliorer la cyberprotection mondiale. En donnant la priorité à la coopération et en tirant parti des compétences spécialisées des partenaires mondiaux, les pays seront plus à même de relever les défis inhérents à un monde numérique de plus en plus interconnecté.

3.4 Création de centres de coordination

L'Australie comme la Fédération de Russie ont toutes deux établi des centres de coordination nationaux et ont profité des avantages de leurs modèles respectifs. Pour ces deux pays, la création de centres de coordination nationaux s'inscrit dans le cadre d'une réponse plus large impliquant l'ensemble des pouvoirs publics aux cyberincidents. Ces centres de coordination ne sont pas des équipes CIRT, mais travaillent à leurs côtés.

Le gouvernement de l'**Australie** a ainsi créé l'Unité de coordination des interventions en matière de cybersécurité, qui relève du Ministère de l'intérieur, à la suite d'atteintes à la sécurité des données d'Optus et de Medibank en 2022. L'objectif était de créer une coordination centrale pour les cyberincidents de portée nationale[92]. Quant à la **Fédération de Russie**, elle a créé son Centre national de coordination et d'intervention en cas d'incident informatique, conformément à une loi nationale visant à renforcer les infrastructures informatiques essentielles. Ces centres accomplissent des tâches similaires: coordonner les interventions en cas d'incident et communiquer des informations essentielles. Le centre russe, néanmoins, est également responsable de la coordination des mesures d'intervention en cas d'incident informatique, de la communication avec les infrastructures essentielles concernant les moyens et les méthodes permettant de recueillir, de stocker et d'analyser les données relatives à ces incidents[93]. Les deux centres sont habilités à créer des groupes de travail, à réunir les organisations et les experts concernés et à diffuser des informations et des documents de référence.

[92] Document SG2RGQ/218 de la CE 2 de l'UIT-D (Australie).
[93] Document SG2RGQ/79 de la CE 2 de l'UIT-D (Fédération de Russie).

Chapitre 4 – Approches, bonnes pratiques, et partage d'expériences concernant la mise en œuvre de stratégies et de politiques nationales en matière de cybersécurité

Alors que la dépendance mondiale à l'égard des technologies numériques ne cesse de croître, on ne saurait trop insister sur l'importance d'élaborer des stratégies et des politiques nationales solides en matière de cybersécurité. En effet, les cybermenaces évoluent rapidement et visent aussi bien les pays développés que les pays en développement. C'est pourquoi, pour protéger les infrastructures essentielles, l'économie numérique et la vie privée des citoyens, les pays se doivent d'adopter des stratégies de cybersécurité complètes et adaptables. Le présent chapitre passe en revue les différentes approches et bonnes pratiques adoptées par différents pays pour mettre en place des cadres de cybersécurité résilients. Grâce à une analyse des expériences de différents pays, il vise à fournir une feuille de route pour l'élaboration et la mise en œuvre de politiques et de stratégies nationales dans le domaine de la cybersécurité.

Les politiques et stratégies nationales consacrées à la cybersécurité englobent un large éventail de pratiques, qui sont toutes adaptées aux contextes politiques, sociaux, économiques, juridiques et technologiques propres à chaque pays. La mise en œuvre de ces politiques et stratégies se caractérise par un ensemble unique de défis et de possibilités, profondément influencés par les conditions spécifiques auxquels chaque est confronté. Cette section s'intéresse aux expériences pratiques de différents pays, en mettant l'accent sur les difficultés rencontrées et les succès obtenus dans leurs efforts pour renforcer leur protection et leur résilience numériques face à l'évolution des menaces.

La réflexion menée s'étend à des questions fondamentales telles que l'alignement stratégique, la participation des parties prenantes, le renforcement des capacités et l'adaptation continue à l'évolution constante des cybermenaces. Cette analyse approfondie vise non seulement à élucider les complexités que soulève la protection efficace des intérêts nationaux dans un environnement numérique de plus en plus concurrentiel, mais aussi à offrir des informations stratégiques susceptibles d'aider les décideurs et les professionnels de la cybersécurité à améliorer leurs propres stratégies.

4.1 Alignement stratégique et cadre politique

Le succès de la mise en œuvre des stratégies nationales de cybersécurité dépend essentiellement de l'alignement de ces stratégies sur la transformation numérique, la sécurité nationale et les politiques économiques au sens large. Cet alignement permet de s'assurer que les initiatives en matière de cybersécurité non seulement soutiennent les objectifs généraux et les cadres de gouvernance du pays, mais qu'elles y sont aussi intégrées. À titre d'exemple, la **République d'Estonie**, largement reconnue comme étant la société numérique la plus avancée au monde, a su aligner sa stratégie de cybersécurité sur ses objectifs en matière de cybergouvernance

et d'économie numérique, créant ainsi une infrastructure numérique résiliente qui soutient les initiatives du secteur public comme celles du secteur privé[94]. L'alignement stratégique de l'Estonie repose sur des mises à jour régulières de sa stratégie de cybersécurité, réalisées en fonction de l'évolution des technologies et du contexte géopolitique mondial.

De plus, pour être efficaces, les politiques et stratégies de cybersécurité doivent être alignées sur les politiques et les objectifs économiques nationaux au sens large. Ainsi, les mesures de cybersécurité répondent aux menaces immédiates, mais soutiennent également les intérêts nationaux à long terme, en favorisant un environnement numérique sûr et résilient, propice à la croissance et à l'innovation. Un tel alignement stratégique est nécessaire pour garantir l'efficacité des mesures de cybersécurité et soutenir des objectifs nationaux plus larges, et par conséquent renforcer les capacités des pays à prévenir, traiter et répondre aux cyberincidents, tout en favorisant la croissance du secteur national de la cybersécurité.

Le cas de la **République démocratique du Timor-Leste**[95] illustre parfaitement l'importance de mettre l'accent sur la cybersécurité dans les politiques, les stratégies, les plans et les feuilles de route relatifs à la transformation numérique. En effet, le pays est conscient que la transformation numérique implique de gérer les risques liés à la cybersécurité de manière à prévenir les cyberattaques et les atteintes à la sécurité des données. À l'instar du Timor-Leste, les PMA doivent donner la priorité à la cybersécurité et en faire un pilier fondamental de leur développement, reflétant ainsi leur compréhension du rôle essentiel que joue la cybersécurité dans la transformation numérique et, in fine, dans le développement national.

Faire progresser la cybersécurité passe également par la mise en place d'un leadership fort et cohérent au sein des organisations chargées de la coordination nationale de la cybersécurité et faisant partie intégrante de la communauté élargie de la cybersécurité au niveau gouvernemental. La désignation d'un coordonnateur peut, en effet, favoriser et susciter une réponse impliquant l'ensemble des pouvoirs publics. À cet égard, l'**Australie** s'est justement dotée d'un coordonnateur national de la cybersécurité, dont la principale fonction est de diriger la gestion des cyberévénements nationaux. Créé en février 2023, ce poste de coordonnateur est placé sous l'autorité du Ministère en charge de la cybersécurité[96]. De même, la présidence de la **Fédération de Russie** a publié, en mai 2022, un décret définissant des critères stricts pour la nomination des personnes responsables de la sécurité de l'information, notamment en ce qui concerne les conditions d'éligibilité, y compris la formation et l'expérience dans ce domaine, ainsi que les exigences organisationnelles. Ce décret encourage également la reconversion professionnelle des personnes qui n'ont pas une formation spécialisée dans la sécurité de l'information[97].

4.2 Cadres juridiques et gouvernance

Les cas de la **République centrafricaine**[98] et de la **République démocratique du Congo**[99] illustrent la manière dont des mesures législatives et des cadres de gouvernance adaptés peuvent renforcer considérablement les capacités en matière de cybersécurité. En République

94 https://www.weforum.org/stories/2020/07/estonia-advanced-digital-society-here-s-how-that-helped-it-during-covid-19/
95 Document 2/120 de la CE 2 de l'UIT-D (Timor-Leste).
96 Document SG2RGQ/218 de la CE 2 de l'UIT-D (Australie).
97 Document SG2RGQ/79 de la CE 2 de l'UIT-D (Fédération de Russie).
98 Document 2/141 de la CE 2 de l'UIT-D (République centrafricaine).
99 Document 2/115 de la CE 2 de l'UIT-D (République démocratique du Congo).

centrafricaine, le Gouvernement a engagé des réformes juridiques et créé des agences spécialisées dans la cybersécurité afin de faire appliquer ses politiques, adoptant ainsi une approche proactive pour renforcer les défenses numériques. Dans le même ordre d'idées, la République démocratique du Congo a adopté une charte complète établie sur la base des bonnes pratiques internationales et qui englobe des mesures législatives, une coopération à plusieurs niveaux et de vastes campagnes de sensibilisation de l'opinion publique. Ces mesures sont essentielles pour permettre aux pays, en particulier dans les régions en développement, de protéger leur cyberespace contre les menaces croissantes.

Les réformes globales de la cybersécurité menées récemment par la **République d'Albanie**[100] enrichissent encore un peu plus la réflexion. En créant une équipe CSIRT nationale et en restructurant son autorité de cybersécurité, le pays s'est engagé à aligner son cadre de cybersécurité sur les normes et les bonnes pratiques internationales. Ces mesures stratégiques visent à renforcer l'infrastructure nationale de cybersécurité de l'Albanie en assurant une réponse coordonnée aux cyberincidents et en améliorant la gouvernance des efforts en matière de cybersécurité. En outre, les réformes juridiques de l'Albanie tendent à actualiser et à renforcer le cadre législatif existant, afin qu'il réponde aux défis et aux menaces actuels en matière de cybersécurité. Cet alignement des composantes juridiques, institutionnelles et opérationnelles au sein de la stratégie de cybersécurité albanaise est un modèle à suivre pour les pays qui cherchent à renforcer leurs défenses en matière de cybersécurité grâce à des réformes globales de la gouvernance.

La **Côte d'Ivoire** procède également à une série de mises à jour législatives dans le cadre de son objectif politique visant à instaurer la confiance numérique à l'horizon 2025[101]. Parmi les efforts notables figure le renforcement des structures juridiques pour soutenir une société de l'information fiable par l'alignement sur les normes régionales telles que celles de la Communauté économique des États de l'Afrique de l'Ouest et la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel. L'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire joue un rôle central en mettant particulièrement l'accent sur la confiance numérique et la sécurité des réseaux, la protection des données à caractère personnel ainsi que la gestion des transactions électroniques. La création de comités consultatifs tels que le Comité consultatif pour la confiance numérique et le Comité consultatif pour la protection des données à caractère personnel souligne le degré d'engagement en faveur d'un cyberenvironnement sécurisé. Ces initiatives structurées ont pour objectif de bâtir un espace numérique de confiance, de renforcer la sécurité des infrastructures numériques de la Côte d'Ivoire et d'encourager la confiance du public dans l'économie numérique.

Tous ces exemples montrent combien il est important d'aligner les stratégies de cybersécurité sur les cadres de gouvernance nationaux, ce qui non seulement renforce l'efficacité de ces stratégies, mais garantit également leur pérennité et leur adaptabilité face à l'évolution des cybermenaces.

4.3 Coopération et soutien au niveau international

Le rôle des organisations internationales dans la fourniture d'un appui aux efforts nationaux en matière de cybersécurité est crucial, comme l'illustrent des initiatives de la **Banque mondiale**[102].

[100] Document 2/309 de la CE 2 de l'UIT-D (Albanie).
[101] Document SG2RGQ/29 de la CE 2 de l'UIT-D (Côte d'Ivoire).
[102] Document 2/74 de la CE 2 de l'UIT-D (Banque mondiale).

La Banque mondiale aide ses pays clients, en particulier ceux qui entrent dans la catégorie des PMA, en leur apportant un soutien financier et technique qui leur permet de mettre en place des bases numériques solides et d'accélérer l'utilisation du numérique dans différents secteurs. Ce soutien est essentiel pour que ces pays puissent faire évoluer leurs politiques et stratégies de cybersécurité en fonction du contexte mondial, et rester ainsi à l'abri des cybermenaces actuelles et futures.

Les efforts de la Banque mondiale mettent en évidence l'impact significatif des partenariats mondiaux et du partage d'expertise dans le renforcement des cadres nationaux de cybersécurité. En facilitant l'intégration des technologies de pointe et des bonnes pratiques, la Banque mondiale aide les pays non seulement à se défendre contre les cybermenaces, mais aussi à tirer parti de la transformation numérique pour favoriser la croissance économique et sociale.

En **République d'Haïti**[103], les partenariats internationaux, notamment avec la Banque mondiale et la Banque interaméricaine de développement, procurent un soutien financier et technique essentiel. Ce soutien se révèle indispensable au développement d'infrastructures numériques solides et au renforcement des mesures de cybersécurité à travers le pays.

L'une des principales initiatives mises en œuvre dans le cadre de ces partenariats concerne la création d'un groupe de travail conjoint formé par le Conseil national des télécommunications d'Haïti et l'Institut haïtien de statistique et d'informatique. Ce groupe est chargé d'élaborer une stratégie nationale harmonisée en matière de cybersécurité, axée sur la protection des infrastructures essentielles et la lutte contre la cybercriminalité. En tant que régulateur, le Conseil national des télécommunications d'Haïti veille au respect des protocoles de sécurité, tandis que l'Institut haïtien de statistique et d'informatique gère les menaces et les risques liés à la cybersécurité, renforçant ainsi la sécurité globale des systèmes numériques haïtiens.

En outre, ces efforts sont soutenus par des projets internationaux comme le Projet d'accélération numérique en Haïti, qui vise à améliorer la connectivité large bande et à établir la résilience numérique. Grâce à cette approche globale, Haïti est non seulement protégé contre les cybermenaces émergentes, mais il favorise également sa croissance socio-économique à l'ère numérique. Pour renforcer encore ces efforts, Haïti a procédé à une évaluation détaillée des capacités en matière de cybersécurité en collaboration avec le Centre mondial des capacités en matière de cybersécurité et la Banque mondiale. Cette évaluation a mobilisé diverses parties prenantes et a utilisé le modèle de maturité des capacités en matière de cybersécurité du centre afin d'identifier les domaines critiques nécessitant des investissements stratégiques. Les résultats ont permis de cibler les améliorations à apporter pour renforcer l'infrastructure de cybersécurité d'Haïti.

4.4 Cadres de coopération et participation des parties prenantes

Le **Brésil**[104] a mis en œuvre une série de mesures stratégiques visant à renforcer son infrastructure nationale de cybersécurité grâce à une participation active et inclusive des parties prenantes. L'approche adoptée par le pays met l'accent sur l'importance de la coopération entre les organismes publics, les entités du secteur privé et les établissements universitaires. Cette coopération multipartite est facilitée par plusieurs initiatives et partenariats qui se fondent sur

[103] Document SG2RGQ/121 de la CE 2 de l'UIT-D (Haïti).
[104] Documents SG2RGQ/57 et SG2RGQ/181 de la CE 2 de l'UIT-D (Brésil).

les forces et les points de vue uniques de chaque secteur pour améliorer l'environnement global de la cybersécurité. Dans ce contexte, la création récente du Comité national de cybersécurité a permis de suivre la mise en œuvre et l'évolution de la politique nationale de cybersécurité. Ce comité compte 25 membres issus du secteur public, dont 15 sont des entités et des organismes de l'administration publique fédérale, parmi lesquels Anatel, et 10 sont des organisations telles que le Comité directeur brésilien pour Internet, tandis que trois membres sont issus de la société civile, trois membres représentent les établissements universitaires et trois autres membres sont issus du secteur privé lié à la cybersécurité.

Outre la création d'une équipe CIRT, l'**Australie** a pris des mesures visant à assurer la protection et la résilience de ses infrastructures essentielles, franchissant ainsi une étape supplémentaire dans le renforcement de la cybersécurité. Au lieu de simplement assurer des mesures de protection et d'intervention en cas de menace, le programme Critical Infrastructure Uplift Program (CI-UP) a été conçu pour aider les organisations australiennes à améliorer leur résilience face à des cyberattaques sophistiquées. Géré par le Gouvernement australien, ce programme est mené en étroite coopération avec les infrastructures essentielles du secteur privé afin de protéger les actifs de ces infrastructures et les environnements technologiques opérationnels. Il s'agit d'un programme national, appliqué à titre volontaire et axé sur les menaces[105].

L'objectif principal du programme CI-UP est d'aider les infrastructures essentielles à améliorer leur niveau de cybersécurité dans plusieurs domaines clés:

- Renforcer la visibilité et la sensibilisation: le programme CI-UP aide les entités à obtenir une meilleure visibilité sur les cyberincidents et à prendre conscience des vulnérabilités potentielles de leurs systèmes.
- Contenir les incidents et y répondre: le programme renforce les capacités des infrastructures essentielles à contenir les cyberincidents et à y répondre efficacement.
- Promouvoir une culture de la cybersécurité: le programme CI-UP encourage l'instauration d'une culture de la cybersécurité dans les secteurs liés aux infrastructures essentielles de l'Australie.

Ce programme reflète l'importance d'une coopération multipartite entre le secteur public et le secteur privé en matière de sécurité. Il fournit ces services par le biais de diverses activités axées sur la participation, notamment des conférences, des ateliers, des échanges d'informations et la fourniture de conseils détaillés en matière d'atténuation. Le programme intervient également sur le terrain auprès du personnel des infrastructures essentielles les plus importantes d'Australie et leur offre des conseils personnalisés et complets, adaptés aux besoins spécifiques de chaque organisation.

La participation d'un large éventail de parties prenantes est essentielle à la mise en œuvre efficace des politiques et stratégies nationales de cybersécurité. Cette participation doit s'étendre aux organismes publics, aux entités du secteur privé, aux établissements universitaires et aux membres de la société civile, chacun y apportant son point de vue, ses besoins, ses priorités et son expertise. La coopération entre ces acteurs permet d'élaborer, d'examiner, d'améliorer et d'adapter les politiques nationales, mais aussi de veiller à ce que les stratégies mises en œuvre soient pragmatiques et qu'elles tiennent compte des besoins et des réalités de tous les secteurs.

[105] Document SG2RGQ/214 de la CE 2 de l'UIT-D (Australie).

4.5 Développement des infrastructures pour la cybersécurité

La **République démocratique du Congo**[106] a lancé un plan ambitieux de refonte et de modernisation de son infrastructure numérique. Ce plan part du constat que des systèmes numériques solides et sûrs forment la base d'une cybersécurité efficace et sont essentiels au développement du pays. Le Gouvernement de la République démocratique du Congo a donc donné la priorité à la mise à niveau des infrastructures de réseau essentielles de manière à ce que celles-ci puissent non seulement résister au spectre grandissant des cybermenaces, mais aussi répondre aux exigences numériques de son économie en pleine expansion. La stratégie du pays comprend le déploiement de technologies de cybersécurité avancées telles que des pare-feu de pointe, des systèmes de détection des intrusions et des méthodes complètes de chiffrement des données. En effet, ces technologies jouent un rôle primordial dans la protection contre les accès non autorisés et la sauvegarde des informations confidentielles. En outre, le pays s'emploie à élargir son accès au large bande, essentiel pour que les mesures de cybersécurité soient appliquées dans toutes les régions du pays, y compris dans les zones isolées et mal desservies.

La **République du Burundi**[107], pour sa part, renforce son infrastructure de cybersécurité pour en faire une composante centrale de sa future stratégie nationale de cybersécurité. Conscient de l'importance vitale des TIC pour le développement, le Gouvernement burundais s'est en effet engagé en faveur de la transformation numérique et de la dématérialisation des services. Face à la multiplication des cybermenaces, le pays, par l'intermédiaire de son Ministère des technologies de l'information et de la communication, a mis en place une commission chargée d'élaborer une stratégie nationale de cybersécurité axée sur le renforcement des cadres juridiques régissant la cybersécurité, sur la promotion de la culture de la cybersécurité, sur l'amélioration des connaissances techniques, sur la participation aux efforts régionaux et internationaux ainsi que sur la sensibilisation aux menaces de cybersécurité dans tous les secteurs. Le développement des infrastructures s'accompagne de mécanismes de sécurité ainsi que de protection des données pour assurer l'intégrité et maintenir un climat de confiance parmi les utilisateurs et les prestataires de services.

4.6 Renforcement des capacités

Le renforcement des capacités nécessaires à la mise en œuvre des stratégies nationales de cybersécurité passe par l'amélioration des compétences des professionnels de la cybersécurité, la mise en place d'infrastructures technologiques ainsi que l'élaboration de cadres juridiques et réglementaires. Des investissements continus dans la formation et le renforcement des capacités constituent en effet un élément essentiel du maintien de la cybersécurité nationale. Comme nous l'avons vu dans le Chapitre 1, en améliorant continuellement les compétences des professionnels de la cybersécurité et en éduquant le public, les pays peuvent mieux gérer les cyberincidents et y répondre tout en soutenant des objectifs plus larges de développement économique et social grâce à une meilleure maîtrise des TIC.

[106] Document SG2RGQ/104 de la CE 2 de l'UIT-D (République démocratique du Congo).
[107] Document SG2RGQ/134 de la CE 2 de l'UIT-D (Burundi).

4.7 Adaptation continue à l'évolution des cybermenaces

En raison de l'évolution constante des cybermenaces, les politiques et stratégies nationales de cybersécurité doivent faire preuve d'une capacité d'adaptation intrinsèque, au même titre que toute autre législation ou réglementation en matière de cybersécurité. Une surveillance continue de l'évolution des cybermenaces, et notamment des défis posés par les technologies nouvelles et émergentes, ainsi qu'une évaluation de l'efficacité des politiques et stratégies et une mise à jour régulière des pratiques en matière de cybersécurité sont autant d'éléments clés de cette capacité d'adaptation. La nécessité d'adopter une stratégie de cybersécurité adaptable a été examinée au Chapitre 2 lorsque nous avons abordé les pratiques en matière d'assurance de la cybersécurité.

Chapitre 5 – Défis et approches en matière de cybersécurité 5G

L'introduction de la technologie 5G représente une évolution importante dans les télécommunications, offrant des vitesses plus élevées et une meilleure connectivité qui ont le potentiel d'améliorer les industries, d'étendre les applications de l'IoT et de faire naître de nouvelles approches en matière de communication numérique. Cependant, l'architecture sophistiquée qui permet ces avancées s'accompagne de défis complexes en matière de cybersécurité qui nécessitent une compréhension globale et des mesures de protection robustes.

Alors que les réseaux 5G sont déployés à l'échelle mondiale, il est impératif de mettre en place un écosystème sécurisé pour garantir l'intégrité, la disponibilité et la confidentialité des informations, ainsi que pour protéger l'infrastructure devenue l'épine dorsale de l'économie numérique.

Le présent chapitre examine les complexités de la cybersécurité 5G et vise à échanger des informations relatives aux pratiques existantes et à réfléchir à des solutions innovantes pour faire face aux menaces émergentes, ainsi qu'à partager des réflexions et des bonnes pratiques en matière de cybersécurité 5G pour les réseaux électroniques publics que les États Membres de l'UIT pourront prendre en compte et appliquer dans leur contexte national.

5.1 Aperçu général de la cybersécurité 5G

La 5G se caractérise par ses systèmes logiciels avancés qui permettent une configuration plus souple et une connectivité massive des abonnés et des appareils. Cette technologie prend en charge des applications à faible temps de latence, telles que la réalité augmentée, la téléchirurgie et les services Internet intégrés qui s'appuient sur un réseau robuste et fiable. L'un des principaux cas d'utilisation de la 5G est l'Internet des objets (IoT), qui tire parti de la capacité de la 5G à connecter un grand nombre de points de terminaison. La technologie 5G est sur le point de révolutionner la connectivité, ce qui présente également des risques et des défis nouveaux et dynamiques en matière de cybersécurité.

Contrairement aux générations précédentes de technologies hertziennes, la 5G s'oriente considérablement vers une architecture basée sur le nuage, des réseaux pilotés par logiciel (SDN) et la virtualisation des fonctions de réseau (NFV). Ce changement crée un paysage de cybersécurité plus complexe et plus dynamique.

Avec la généralisation de la 5G, l'infrastructure des télécommunications devrait devenir une cible de plus en plus attrayante pour les cyberactivités malveillantes, nécessitant la mise en place de mesures de sécurité évoluées capables de s'adapter à l'évolution des menaces. La cybersécurité 5G doit donc viser à accroître la résilience de l'ensemble de l'écosystème, y compris l'infrastructure et les applications. Il s'agit notamment de protéger les appareils connectés, les données et les réseaux contre les cybermenaces.

Étant donné que la définition de la cybersécurité varie d'une organisation à l'autre[108], il convient de garder à l'esprit que le terme "cybersécurité 5G" dont il est fait mention dans le présent rapport renvoie à la cybersécurité dans le contexte de la 5G, avec ses nouveaux paramètres, normes et fonctionnalités technologiques qui doivent être gérés correctement pour protéger l'ensemble de l'écosystème numérique et assurer la cyberrésilience.

Encadré 1 – Définition de la cybersécurité

À l'UIT, la cybersécurité est définie dans la Recommandation UIT-T X.1205 comme suit: "*ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les appareils informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunications et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux de sécurité sont les suivants:*

- *Disponibilité.*
- *Intégrité, ce qui peut inclure l'authenticité et la non-répudiation.*
- *Confidentialité.*"

5.2 Déploiements de réseaux traditionnels

Dans un premier temps, les fournisseurs de services de télécommunications ont tendance à déployer les réseaux 5G sur une base non autonome (NSA) et tirent ainsi parti de l'infrastructure 4G existante avant de déployer un réseau 5G de bout en bout autonome (SA)[109]. Les réseaux NSA héritent donc des vulnérabilités existantes des réseaux 4G, voire des réseaux 2G ou 3G, qui doivent être gérées en conséquence. Pour certains opérateurs, cela correspond à une "dette technique": la gestion d'anciens systèmes signifie qu'un ensemble de contrôles de sécurité normalisés doit être mis en place pour évaluer le niveau de sécurité des composants de l'infrastructure à différents stades de maturité générationnelle[110].

Il est important de souligner que la 5G SA présente des possibilités d'amélioration de la cybersécurité par rapport aux générations précédentes de technologies mobiles, puisqu'elle est conçue pour être plus sécurisée que la 4G. Des améliorations ont été notées dans des

[108] https://www.enisa.europa.eu/publications/definition-of-cybersecurity

[109] Les appareils fonctionnant sur des réseaux 5G NSA se connectent aux fréquences 5G pour la transmission de données lorsqu'ils ont besoin d'une plus grande largeur de bande et d'une latence plus faible (par exemple, pour la communication entre voitures intelligentes) ou pour réduire la consommation d'énergie des appareils compatibles IoT, mais continuent de s'appuyer sur les réseaux 4G et même 2G ou 3G pour les appels vocaux et les messages SMS. Source: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf.

[110] https://www.itu.int/md/D22-SG02.RGQ-ADM-0019/fr et https://www.itu.int/md/D22-SG02.RGQ-ADM-0043/fr

domaines tels que la sécurité et la confidentialité des abonnés, le réseau d'accès radioélectrique (RAN), le réseau central et la sécurité de l'itinérance[111],[112].

5.3 Activités de normalisation relatives à la sécurité 5G

5.3.1 Organisations de normalisation actives dans la cybersécurité 5G

En raison de la complexité de la technologie 5G et des questions qu'elle soulève, il n'existe aucune organisation de normalisation ayant un mandat exclusif en matière de cybersécurité 5G. Pour éviter les doubles emplois, des mécanismes ont donc été mis au point afin d'échanger des informations entre les organisations de normalisation et de coordonner les propositions et les sujets d'étude.

Pour mieux cartographier les différentes activités et orienter les travaux de normalisation de la sécurité liés à la 5G à l'**UIT**-T, la Commission d'études 17 (CE 17) a élaboré un rapport technique établissant une correspondance entre les normes existantes et les normes en cours d'élaboration, les organisations de normalisation et leur application dans les réseaux 5G[113]. Le rapport recense les normes de l'UIT-T, du 3GPP, de l'ETSI et de l'IEEE Standards Association, ainsi que les ressources non normalisées pertinentes pour la cybersécurité 5G.

La commission d'études a publié 11 Recommandations sur la sécurité de la 5G, sur la base de contributions rédigées par des opérateurs, des vendeurs, des fabricants de smartphones et des fournisseurs de contenu, entre autres. Ces Recommandations s'articulent autour de la sécurité dans cinq domaines: la sécurité des réseaux pilotés par logiciel (SDN) et de la virtualisation des fonctions de réseau (SDN-NFV), la sécurité du découpage de réseau, la sécurité en périphérie mobile, la sécurité de la gestion de réseau 5G et la sécurité des services 5G. De plus, la CE 17 a noué des partenariats avec d'autres organisations de normalisation, tels que le 3GPP et le Groupe d'étude sur l'ingénierie Internet, ainsi qu'avec des organisations professionnelles travaillant sur des spécifications pertinentes pour la normalisation de la cybersécurité 5G.

L'une de ces organisations est la **GSMA**. Bien qu'elle ne soit pas elle-même une organisation de normalisation, la GSMA élabore des spécifications, convoque ses membres et coopère avec les organisations de normalisation pour que ces spécifications soient améliorées et/ou adoptées en tant que norme. La GSMA a publié une liste des contrôles de sécurité de base que les opérateurs mobiles peuvent envisager, à titre volontaire, lors du déploiement de réseaux 5G[114].

Compte tenu des nombreuses sources d'information pertinentes dans le domaine de sécurité 5G, l'**Agence européenne pour la cybersécurité** (ENISA), a publié un référentiel unifié des contrôles techniques de sécurité pour les réseaux 5G, le 5G Security Controls Matrix[115]. Le référentiel se présente actuellement sous forme de tableur, mais l'ENISA est également en train de mettre au point un outil Web afin d'en améliorer l'utilisation.

---

111 https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf
112 https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era
113 https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-2-PDF-E.pdf
114 https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/
115 https://www.enisa.europa.eu/publications/5g-security-controls-matrix

La complexité croissante des réseaux et la convergence des télécommunications avec les réseaux IP font qu'il devient de plus en plus difficile de confier des travaux de normalisation dans des domaines spécifiques à une seule organisation de normalisation. Par conséquent, le risque de chevauchement et de duplication des travaux augmente, ce qui rend la communication et le partage d'informations entre les organisations de normalisation encore plus importants.

5.3.2 Intégration des normes dans les exigences réglementaires

De manière générale, les normes contribuent à assurer l'interopérabilité entre les technologies et à réduire le temps nécessaire à une innovation pour atteindre son marché mondial. Les normes de cybersécurité peuvent définir une base commune de sécurité qui reflète les bonnes pratiques universelles. Ces normes sont le résultat d'un processus fondé sur le consensus. Elles peuvent être obligatoires, mais, dans la plupart des cas, elles sont facultatives, ce qui laisse aux fournisseurs et aux opérateurs une plus grande latitude pour prendre des décisions quant à leur application. Dans certains cas, les normes peuvent devenir obligatoires si des réglementations techniques nationales intègrent une norme spécifique dans leurs exigences de sécurité.

Les stratégies nationales de cybersécurité 5G doivent refléter un équilibre entre les bonnes pratiques mondiales et les réalités opérationnelles locales. En règle générale, les exigences réglementaires nationales doivent s'inspirer des normes internationales convenues, en les adaptant aux contextes et aux besoins locaux afin d'assurer le succès du déploiement de la 5G et la cybersécurité des réseaux 5G.

5.4 Mesures de cybersécurité proactives visant à compléter les normes et les spécifications

5.4.1 Considérations de sécurité au niveau du fournisseur

Les normes et les spécifications ne sont qu'un élément de la cybersécurité 5G. La manière dont les fournisseurs et les opérateurs mettent en œuvre ces normes et les configurent définit le niveau de sécurité des réseaux 5G. Pour sa part, Ericsson a adopté une approche complète de la sécurité 5G, qui s'articule autour de quatre niveaux: les normes, le développement des produits des fournisseurs, le déploiement des réseaux et l'exploitation des réseaux[116]. L'entreprise considère qu'une telle approche globale peut garantir que les mesures d'atténuation seront mises en œuvre d'une manière qui tient compte des interdépendances entre les niveaux ainsi que des besoins spécifiques à chaque niveau.

Un exemple concret de mesure de sécurité 5G est le Système d'assurance de sécurité des équipements de réseau (NESAS)[117], élaboré par la **GSMA** et le **3GPP**, qui vise à améliorer les niveaux de sécurité des équipements de réseau mobile en fournissant un système de garantie qui peut être appliqué à l'échelle mondiale. Le système d'assurance repose sur un audit d'experts internes et indépendants, combinant une évaluation entre les processus des fournisseurs et une évaluation des produits, qui débouche sur une accréditation. L'objectif de ce système est d'alléger la charge des tests de sécurité pour les fournisseurs d'équipements de réseau qui opèrent généralement à l'échelle mondiale. Les principaux fournisseurs ont déjà

[116] https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security
[117] https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/network-equipment-security-assurance-scheme-nesas/

obtenu l'accréditation NESAS. Le système NESAS est également candidat au programme de certification de cybersécurité de l'UE pour la 5G[118], une certification de niveau européen qui garantirait la conformité dans tous les États Membres de l'UE. Cette certification ne remplacerait pas le système NESAS actuel, mais existerait en parallèle de celui-ci. Compte tenu de l'évolution des menaces, l'élaboration de programmes et d'initiatives de certification qui restent flexibles et peuvent être rapidement mis à jour apparaît comme essentielle.

Au **Royaume-Uni**, le Centre national pour la cybersécurité recommande d'utiliser le cadre d'évaluation des fournisseurs[119], guide qui aide les opérateurs à évaluer les cyberrisques liés à l'utilisation des équipements des fournisseurs.

5.4.2 Considérations de sécurité au niveau de l'opérateur

Le système NESAS permet de garantir la sécurité d'un équipement de réseau avant son déploiement. À mesure que les opérateurs déploient et exploitent leurs réseaux, d'autres considérations de sécurité doivent être prises en compte, notamment la détection des attaques et la réponse automatisée. C'est là que les opérateurs devraient envisager de tirer parti de l'intelligence artificielle (IA), des renseignements sur les menaces et de l'analyse pour renforcer la cybersécurité. La cybersécurité 5G offre des avantages, tels que la sécurité en temps réel et des stratégies telles que le Zero Trust, qui améliorent la visibilité du système. Cependant, elle pose aussi des défis qui lui sont propres, à savoir le maintien de la connectivité entre différents réseaux avec différents niveaux de sécurité, le fonctionnement avec des composants traditionnels et divers types de réseaux, et la complexité de l'intégration de l'IA dans les mesures de sécurité. À cet égard, l'application de contrôles d'accès stricts conformément au principe des "moindres privilèges" garantit que les différents droits dans le réseau (par exemple les droits d'accès entre les fonctions du réseau, les droits des administrateurs de réseau ou encore la configuration de la virtualisation) sont réduits au minimum. Un grand nombre de publications sur les stratégies de cybersécurité spécifiques à la 5G sont à la disposition des opérateurs[120].

Les tests des réseaux de télécommunications en direct sont également essentiels pour déterminer les cyberrisques réels auxquels sont exposés les réseaux de télécommunications. Les opérateurs peuvent effectuer certaines formes de test de sécurité sur leurs propres réseaux et systèmes, soit en faisant appel à des ressources internes, soit en faisant appel à des sous-traitants extérieurs indépendants. Au **Royaume-Uni**, TBEST est un programme de tests d'intrusion basé sur les résultats qui simule les techniques et tactiques que des cyberattaquants disposant de ressources suffisantes peuvent utiliser. Il évalue les capacités d'un fournisseur de services de communication à détecter et contenir une telle attaque et à y répondre. L'objectif général est de repérer et de corriger les failles de sécurité ou d'autres faiblesses dans les fonctions, processus, politiques, systèmes ou réseaux d'un fournisseur qui pourraient être utilisées ensemble pour compromettre les systèmes critiques d'une entreprise avant la détection. En adhérant au programme TBEST sur une base volontaire, les fournisseurs de services de communication peuvent ainsi identifier des domaines spécifiques dans lesquels leur sécurité pourrait être améliorée, pour que l'Ofcom, le régulateur des communications du Royaume-Uni, puisse ensuite les aider à mettre en œuvre les changements appropriés dans les meilleurs délais[121].

---

118 https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

119 https://www.ncsc.gov.uk/report/vendor-security-assessment

120 Voir par exemple https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf et https://www.5gamericas.org/security-for-5g/.

121 Document SG2RGQ/74 de la CE 2 de l'UIT-D (Royaume-Uni).

Une solide analyse de rentabilité de la cybersécurité 5G est essentielle. Néanmoins, même si les opérateurs ont besoin que leurs investissements dans les services 5G soient rentabilisés, les mesures de sécurité de base doivent être reconnues comme indispensables et être inscrites au budget en conséquence.

Encadré 2 – Réseau RAN ouvert

Le réseau RAN ouvert désigne la désagrégation du réseau d'accès radioélectrique (RAN) et la normalisation des interfaces connectant ces éléments désagrégés, permettant ainsi de construire des réseaux à partir d'équipements provenant de différents fournisseurs.

D'une part, l'architecture d'un réseau RAN ouvert peut compliquer davantage la chaîne d'approvisionnement des réseaux de télécommunications. Elle donne en effet naissance à une diversité de fournisseurs dans le réseau RAN ainsi qu'à de nouveaux vecteurs d'attaque, et exige donc des efforts d'intégration supplémentaires tout au long de la chaîne d'approvisionnement. D'autre part, le réseau RAN ouvert apporte plus de transparence dans les chaînes d'approvisionnement, offre une plus grande visibilité aux opérateurs et leur permet de surveiller et de détecter les risques de sécurité. En résumé, il aide les opérateurs à mieux comprendre l'architecture et les équipements de réseau, rendant possible une analyse et une gestion des vulnérabilités plus approfondies. L'O-RAN Alliance, la principale source de spécifications des réseaux RAN ouverts, travaille à l'élaboration de spécifications de sécurité pour l'architecture RAN ouverte et vise à faire normaliser ces spécifications par l'ETSI.

Au Japon, NTT Docomo est l'un des opérateurs à avoir adopté l'architecture RAN ouverte en raison de la souplesse de choix des équipements. Cette décision a soulevé des questions du point de vue de la sécurité, car on considère généralement que l'ouverture signifie plus de possibilités d'attaque. Toutefois, après avoir comparé le réseau RAN traditionnel et le réseau RAN ouvert, l'opérateur a conclu qu'il y avait peu de différence en matière de sécurité entre les deux[1].

[1] Pour de plus amples informations sur la sécurité des réseaux RAN ouverts, voir par exemple https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/enhancing-the-security-of-communication-infrastructure_79b78b4d/bb608fe5-en.pdf.

5.5 Exemples de politiques et de réglementations nationales visant à sécuriser les réseaux 5G

Outre les normes et les pratiques des fournisseurs et des opérateurs, des politiques et des réglementations visant à sécuriser les réseaux 5G peuvent être proposées au niveau national. Celles-ci peuvent se présenter sous différentes formes et porter, entre autres, sur l'évaluation des fournisseurs, la réalisation de tests, l'octroi de certifications, et l'établissement de directives ou d'exigences. Bien que les approches diffèrent selon les contextes nationaux, ces initiatives visent toutes à atténuer les risques pour la sécurité que présente la 5G, y compris les cyberrisques. Les régimes de mise en œuvre et de conformité devraient également être pris en compte dans le cadre général.

Les exemples ci-dessous donnent un aperçu des mesures prises par différents pays et régions pour parvenir à sécuriser les réseaux 5G et de leur état d'avancement:

- L'approche globale adoptée par le **Brésil** en matière de cybersécurité 5G se concentre sur la gestion des risques avec les opérateurs. En vertu des conditions de mise aux enchères

du spectre 5G et du Règlement sur la cybersécurité du secteur des télécommunications[122], les opérateurs 5G sont tenus de respecter le cadre réglementaire, qui comprend des principes, des lignes directrices et des contrôles ex ante pour garantir la cybersécurité dans l'ensemble du secteur. Les contrôles concernent la gouvernance de la cybersécurité, la notification obligatoire des incidents, le partage d'informations, les cycles d'évaluation des vulnérabilités, la notification des infrastructures essentielles ainsi que d'autres dispositions. L'Agence nationale des télécommunications du Brésil (Anatel) s'est également associée à des établissements universitaires pour mener des études dans ce domaine[123].

- Le Gouvernement du **Royaume-Uni** a mis en place un cadre de sécurité à l'intention des fournisseurs de réseaux ou de services publics de communications électroniques en vertu de la loi de 2003 sur les communications, telle qu'amendée par la loi de 2021 sur la sécurité des télécommunications. Ce cadre s'applique à la 5G et à tous les autres réseaux. En effet, alors que le Royaume-Uni passe à la 5G et à des réseaux entièrement fibrés, de nombreux fournisseurs de réseaux intègrent des technologies plus anciennes dans leurs infrastructures. La loi de 2021 sur la sécurité des télécommunications définit donc de nouvelles obligations en matière de sécurité pour tous les fournisseurs publics de télécommunications[124] et dote le Secrétaire d'État de nouveaux pouvoirs pour élaborer des réglementations et publier des codes de pratique, qui ont depuis lors été établis et soumis à une consultation publique[125]. La loi comprend également des dispositions renforçant les pouvoirs de régulateur de l'Ofcom pour surveiller et faire appliquer le respect par les fournisseurs de leurs nouvelles obligations.
- Les réglementations et les politiques en matière de cybersécurité 5G de la **République de Corée** sont reconnues comme faisant partie des plus strictes au monde, ce qui reflète la position de leader du pays dans l'adoption de la technologie 5G. Le gouvernement national, par l'intermédiaire du Ministère des sciences et des TIC et de l'Agence coréenne chargée d'Internet et de la sécurité, a mis en place un cadre complet pour protéger les réseaux 5G. Ce cadre impose des exigences strictes aux opérateurs de télécommunications pour qu'ils sécurisent l'infrastructure de réseau, protègent les données des utilisateurs et atténuent les risques en matière de cybersécurité. Cette réglementation souligne la nécessité de sécuriser les chaînes d'approvisionnement, d'élaborer des normes de chiffrement évoluées et d'intégrer des principes de sécurité dès la conception dans l'architecture des réseaux. En outre, la République de Corée collabore avec des partenaires internationaux et des organisations de normalisation pour veiller à ce que ses mesures de sécurité pour la 5G soient conformes aux bonnes pratiques mondiales.
- Le cadre juridique et technique établi dans le but de renforcer la cybersécurité 5G en **Inde** comprend:
  - des directives de sécurité nationale relatives au secteur des télécommunications, qui garantissent la fiabilité des chaînes d'approvisionnement et des origines des télécommunications;
  - des tests et certifications obligatoires des équipements de télécommunications, afin de garantir le respect des exigences essentielles de sécurité de chaque fonction du réseau 5G;
  - des conditions d'octroi de licences aux fournisseurs de services de télécommunications, qui prévoient que le gouvernement procède à des audits publics réguliers de la sécurité de l'infrastructure de télécommunications.

---

122 https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740; https://informacoes.anatel.gov.br/legislacao/resolucoes/2024 (en portugais).

123 Certains des résultats sont disponibles à l'adresse suivante: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas (en portugais).

124 Sauf les micro-entités.

125 https://www.legislation.gov.uk/uksi/2022/933/contents/made; https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

À cette fin, divers mécanismes institutionnels ont été mis en place: un centre national pour la sécurité des communications, chargé d'élaborer des exigences et des normes de sécurité des télécommunications (l'Indian Telecom Security Assurance Requirements, ITSAR) ainsi que ses laboratoires d'essais et de certification de la sécurité associés; une équipe d'intervention en cas d'incident de sécurité informatique pour le secteur national des télécommunications; et plusieurs mesures de gestion de la fraude et de protection des consommateurs centrées sur les citoyens, etc. S'agissant des protocoles et des normes de sécurité comme le 3GPP, l'Inde a examiné les spécifications proposées par les normes du secteur pour le contrôle de la conformité et les autres conditions de licence de télécommunications comprenant des audits de sécurité réguliers sur les réseaux des fournisseurs de services.

- Aux **Émirats arabes unis**, la sécurisation des réseaux 5G s'appuie sur une stratégie sur plusieurs fronts qui comprend des cyberexercices rigoureux et une formation à l'échelle nationale, la création d'un Centre national d'opérations de sécurité chargé de détecter et de réagir en temps réel face aux menaces, et l'initiative Cyber Pulse, qui vise à sensibiliser et à former le personnel aux principales stratégies de défense. L'accent est mis sur la coopération et le partage d'informations avec les partenaires internationaux, les fournisseurs, les établissements universitaires et d'autres parties prenantes afin de renforcer les mesures de cybersécurité. En outre, un cadre de cybersécurité résilient conforme aux normes internationales, notamment de l'Organisation internationale de normalisation et du NIST, a été mis en place pour garantir la conformité dans l'ensemble du secteur des télécommunications. Pour renforcer la confiance des consommateurs et des entreprises dans la sécurité de la 5G, les Émirats arabes unis ont instauré des politiques, des procédures et des lois de gouvernance qui promeuvent des principes de sécurité dès la conception ainsi que des pratiques de sécurité responsables parmi les fournisseurs. Enfin, les Émirats arabes unis ont adopté une approche de la cybersécurité centrée sur les personnes, en mettant l'accent sur la formation, la sensibilisation et l'assistance pour donner aux personnes et aux organisations les moyens de lutter contre les cybermenaces, consolidant ainsi une défense solide contre les menaces potentielles auxquelles est confronté le réseau 5G.
- Le **Zimbabwe** s'attaque à la cybersécurité 5G, en mettant l'accent sur l'importance croissante de l'informatique en périphérie et en explorant l'adoption de la technologie de réseau RAN ouvert pour la flexibilité des fournisseurs. Bien qu'il n'existe pas de loi spécifique sur la sécurité de la 5G, la législation existante en matière de protection des données et un document en cours sur la gouvernance de l'IA sous-tendent l'approche du pays. Le Zimbabwe alignera ses pratiques de sécurité sur les normes internationales telles qu'ISO/CEI 27001 et les normes du NIST, en veillant à ce que les nouvelles interfaces radioélectriques 5G soient conformes aux protocoles de sécurité établis. Enfin, l'Autorité de régulation des postes et des télécommunications du Zimbabwe veille à l'application des directives en matière de sécurité et sensibilise le secteur à la préservation de l'intégrité de l'infrastructure nationale des télécommunications.
- Le **Kenya** a adopté sa feuille de route et sa stratégie pour la 5G dans les communications mobiles en avril 2022. La stratégie reconnaît que la sécurité est un aspect important de l'architecture des réseaux 5G. La nature évolutive des services connectés et l'augmentation considérable attendue du nombre et des types d'appareils connectés donnent encore plus d'importance à la confidentialité des données, à la protection des données et à la cybersécurité au Kenya, notamment à la détection des menaces, à l'authentification des utilisateurs et aux bonnes pratiques de fonctionnement. Or, la 5G offre une meilleure sécurité dès la conception en intégrant des exigences de sécurité renforcées sur la base de l'évolution des réseaux et de l'adaptation des enseignements tirés des technologies antérieures. Par conséquent, l'Autorité des communications du Kenya a adopté une norme internationale approuvée, élaborée par l'UIT et par le 3GPP pour assurer l'interopérabilité et la sécurité des systèmes mobiles. L'Autorité prévoit de tirer parti de l'expertise de diverses parties prenantes et des bonnes pratiques internationales en matière de cybersécurité pour élaborer des codes techniques et appliquer une liste de contrôle d'évaluation de la sécurité minimale normalisée afin de garantir que les réseaux

5G répondent aux normes techniques les plus récentes et sont conformes aux normes mondiales en matière de sécurité de la 5G.

- À la suite d'un examen approfondi des risques de cybersécurité pour les réseaux 5G, l'**UE** a élaboré une boîte à outils de mesures d'atténuation des risques[126] dans le but d'identifier un ensemble commun de mesures visant à atténuer les principaux risques pour la cybersécurité 5G et à aider à hiérarchiser les mesures d'atténuation dans les plans aux niveaux européen et national. En outre, la Stratégie de cybersécurité pour la décennie numérique adoptée par l'UE souligne l'importance de la sauvegarde des réseaux mobiles large bande de prochaine génération, et contient un appendice spécifique sur les prochaines étapes de la cybersécurité des réseaux 5G[127]. Quant au cadre de certification de l'UE, il comprend l'élaboration en cours d'un programme de certification de cybersécurité pour la 5G[128].

5.6 Défis liés à la mise en œuvre et au contrôle du respect des dispositions

L'élaboration de politiques est essentielle, mais ne doit toutefois pas faire oublier l'importance d'une mise en œuvre efficace. La création de mécanismes de signalement, le respect des normes internationales et la mise en œuvre de mesures d'application pratiques sont nécessaires pour garantir la robustesse de la cybersécurité des réseaux 5G. De nouveaux cadres introduisant des changements importants pour la sécurité des réseaux de télécommunications exigeront que les fournisseurs s'acquittent en permanence d'un processus de conformité et, par conséquent, d'un engagement étroit avec le secteur. Au **Royaume-Uni**, l'Ofcom utilise un modèle de surveillance dans le cadre de sa politique de sécurité des télécommunications et collabore avec les équipes réglementaires et techniques des fournisseurs de télécommunications. Le régulateur considère en effet que la mise en œuvre n'est pas uniquement une question de mesures techniques. Elle nécessite aussi un changement culturel dans la façon dont les fournisseurs de télécommunications conçoivent la sécurité, à savoir les obliger à identifier et à assumer la responsabilité des parties de leurs réseaux et services qu'ils ont sous-traitées. Pour réussir, il est indispensable de faire participer les plus hauts responsables et d'obtenir l'engagement et le soutien des pouvoirs publics, des autorités de régulation et du secteur[129].

En **Malaisie**, le gouvernement a approuvé un nouveau projet de loi sur la cybersécurité, qui prévoit la création d'une agence unique pour la gestion de toutes les infrastructures essentielles. Les réseaux de télécommunication, y compris les réseaux 5G, entrent dans le champ d'application de ce nouveau projet de loi. Le régulateur[130] élabore actuellement un ensemble d'exigences à l'intention des opérateurs pour rendre compte de leur conformité en matière de sécurité. Dans le produit intérimaire sur la Question 3/2 concernant la cybersécurité 5G[131], l'un des opérateurs du pays a toutefois souligné que la mise en œuvre de la nouvelle politique peut s'avérer difficile, car elle implique de communiquer sur les risques et de définir des exigences minimales en matière de sécurité, ce qui demande du temps, de l'argent et beaucoup de travail en concertation, et influe souvent sur les considérations pour les actionnaires. De fait, pour les opérateurs actionnaires, les structures, politiques et réglementations en matière de sécurité ne sont pas toujours cohérentes, de sorte que les équipes chargées de la sécurité

126 https://digital-strategy.ec.europa.eu/fr/node/1215
127 https://digital-strategy.ec.europa.eu/fr/node/435
128 https://certification.enisa.europa.eu/index_en?prefLang=fr&etrans=fr
129 Document SG2RGQ/191 de la CE 2 de l'UIT-D (Royaume-Uni).
130 https://www.nacsa.gov.my/act854.php
131 https://www.itu.int/hub/publication/d-stg-sg02.03.2-2024/#/fr

peuvent être confrontées à des difficultés. Il est donc nécessaire d'impliquer toutes les parties prenantes, y compris les responsables de haut niveau dans la réflexion autour de nouveaux cadres de sécurité.

5.7 Nécessité d'investir en priorité dans l'éducation et la formation de la main-d'œuvre

Selon Allied Market Research[132], le marché mondial de la sécurité 5G devrait atteindre 37,8 milliards USD d'ici à 2031, et s'accompagner d'une demande croissante de professionnels de la cybersécurité, en particulier ceux qui ont des compétences spécialisées pour protéger les réseaux 5G. Les pays, les organisations et les institutions doivent donc accorder la priorité à la formation et au recrutement de la main-d'œuvre pour assurer la progression de la cybersécurité 5G. Les compétences spécialisées nécessaires sont actuellement difficiles à trouver au sein de la main-d'œuvre; en outre, il est difficile d'atteindre une représentation équilibrée des genres à l'embauche. Or, si la main-d'œuvre n'est pas prête, la transition vers la 5G s'en trouvera ralentie et compliquée. Alors que les pays devraient accorder la priorité à la formation et à l'éducation par le biais de programmes nationaux, le secteur privé peut quant à lui envisager des programmes de formation et de perfectionnement des compétences, la participation de l'ensemble du secteur étant nécessaire pour garantir que les besoins sont satisfaits.

Un exemple de pays qui trouve des solutions aux défis de la main-d'œuvre est la **Türkiye**, qui a augmenté ses investissements dans l'éducation et la formation d'une main-d'œuvre capable de gérer les complexités de la sécurité de la 5G. Dans le cadre de cet engagement, un site d'essai ouvert, la 5G Valley, a été créé par des institutions clés, notamment l'Autorité des technologies de l'information et des communications, l'Université technique du Moyen-Orient, l'Université İhsan Doğramacı Bilkent, l'Université Hacettepe, ainsi que les opérateurs de télécommunications Türk Telekomünikasyon A.Ş., Turkcell İletişim Hizmetleri A.Ş. et Vodafone Telekomünikasyon A.Ş. Ce site est une plate-forme essentielle pour la recherche, le développement et les tests des technologies 5G et au-delà, offrant des possibilités de coopération entre le monde universitaire et le secteur. Le Conseil d'administration de la 5G Valley, composé de représentants des institutions précitées, assure la mise en œuvre effective de cette initiative. En fournissant une plate-forme où les universitaires, les chercheurs, les doctorants et les start-ups peuvent s'engager dans des travaux liés aux technologies 5G et postérieures, le site d'essai ouvert de la 5G Valley favorise non seulement l'innovation, mais contribue également au développement d'une main-d'œuvre hautement qualifiée. Cette initiative s'inscrit dans la stratégie de la Türkiye visant à donner la priorité à la sécurité des réseaux 5G et à renforcer leur sécurité grâce à des investissements continus dans l'éducation, la formation et la recherche[133].

5.8 Au-delà de la 5G: Définir l'orientation de la cybersécurité 6G

Bien que la 5G en soit encore à l'étape de planification et de déploiement dans de nombreux pays et régions, dans les activités de recherche-développement et de normalisation, l'attention se porte déjà au-delà des réseaux 5G. Ainsi, à la fin de l'année 2023, le Secteur des radiocommunications de l'**UIT** (UIT-R) a approuvé le cadre et les objectifs généraux du

[132] https://www.alliedmarketresearch.com/5g-security-market-A12820
[133] https://5gtrforum.org.tr/en

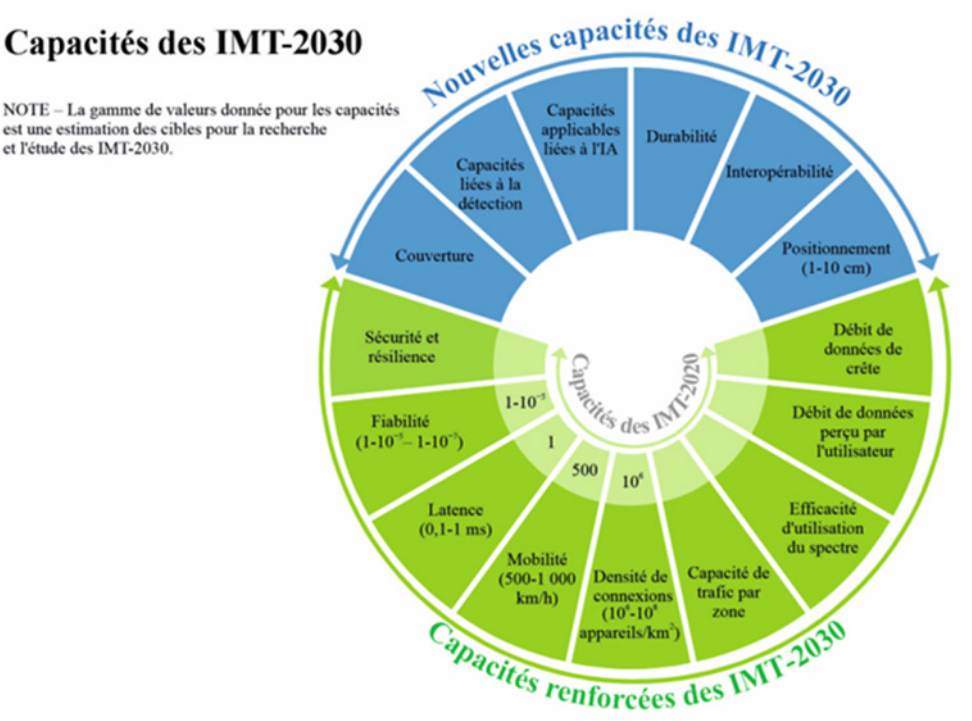
développement futur des télécommunications mobiles internationales (IMT) à l'horizon 2030 et au-delà[134], que l'on appelle commercialement la 6G.

Encadré 3 – IMT-2030

Ce cadre souligne que les IMT-2030 devraient contribuer de manière importante à l'amélioration de la sécurité et de la résilience. Il est censé être sécurisé de par sa conception et avoir la capacité de continuer de fonctionner pendant un événement perturbateur, qu'il soit naturel ou causé par l'homme, et de s'en remettre rapidement. Le document réaffirme également que la sécurité et la résilience des systèmes IMT-2030 sont fondamentales pour atteindre les objectifs sociétaux et économiques plus larges.

Dans le contexte des IMT-2030, la sécurité est définie par le cadre comme étant la *"préservation de la confidentialité, de l'intégrité et de la disponibilité des informations, telles que les données d'utilisateur et la signalisation, et la protection des réseaux, appareils et systèmes contre les cyberattaques telles que le piratage, les attaques par déni de service, les attaques par interposition, etc.". La résilience est définie comme étant la "capacité des réseaux et des systèmes à continuer de fonctionner correctement pendant et après une perturbation naturelle ou causée par l'homme, telle qu'une perte de la source principale d'alimentation, etc.".*

Figure 2 – Capacités des IMT-2030



Source: UIT

[134] Recommandation UIT-R M.2160, disponible à l'adresse https://www.itu.int/rec/R-REC-M.2160-0-202311-I/fr.

À l'évidence, la 6G sera bientôt une réalité et le début de ses processus de normalisation devrait être conçu en tenant compte de la sécurité et de la résilience, à la différence des premières étapes de conception de la technologie 5G, notamment du point de vue de la normalisation. Une comparaison avec les IMT-2020 (commercialement connue sous le nom de 5G) approuvée en 2015[135] illustre de manière saisissante le changement d'approche et la prise en compte de la nécessité d'aborder comme il se doit la cybersécurité et la cyberrésilience en tant que piliers de la transformation numérique et de l'économie numérique.

[135] Recommandation UIT-R M.2083, disponible à l'adresse: https://www.itu.int/rec/R-REC-M.2083-0-201509-I/fr.

Chapitre 6 – Défis et approches de la lutte contre l'hameçonnage par texto

Les services de messages courts (SMS) sont utilisés par des acteurs malveillants comme vecteurs d'attaque. À l'échelle mondiale, l'utilisation des SMS à des fins de spam[136] et d'escroquerie a considérablement augmenté. Les auteurs de ces escroqueries ont recours à des tactiques visant à tromper les utilisateurs pour les inciter à fournir des données à caractère personnel, notamment des données financières, et à télécharger des logiciels malveillants sur leurs appareils. De ce fait, non seulement les escroqueries par SMS ébranlent la confiance des utilisateurs dans les services de messagerie des télécommunications et se traduisent par une baisse de leur satisfaction, mais elles constituent aussi un gaspillage des ressources du réseau.

Selon les données de la Commission fédérale du commerce des États-Unis, les escroqueries par SMS ont entraîné des pertes de 330 millions de dollars des États-Unis (USD) en 2022, soit plus de deux fois le montant des pertes estimé en 2021[137]. Au cours de la même période, en Australie, le programme Scamwatch du Centre australien de lutte contre les escroqueries a reçu près de 80 000 signalements d'escroqueries par SMS représentant des pertes équivalant à plus de 28 millions de dollars australiens (AUD)[138].

Bien que l'utilisation des services SMS varie d'un pays à l'autre et que l'innovation dans le secteur des télécommunications et des TIC ait donné naissance à de nouveaux modes de communication, notamment par le biais d'applications de messagerie mobile répandues dans le monde entier, ces services restent précieux pour les utilisateurs compte tenu de leur simplicité et de leur disponibilité sur tous les téléphones mobiles.

Dans ce contexte, le présent chapitre se penche sur "l'hameçonnage par texto", l'un des types d'incidents liés aux SMS les plus répandus, fournit des recommandations sur les mesures à prendre pour lutter contre ce fléau et décrit quelques exemples d'expériences et d'approches nationales permettant de relever ces défis[139].

6.1 Hameçonnage par texto

Le terme "hameçonnage" désigne l'utilisation de courriels, de messages, d'appels vocaux ou de messages sur les réseaux sociaux qui semblent légitimes, mais dont le but est de tromper le destinataire, généralement en usurpant l'identité d'une personne ou d'une entité digne de confiance comme une banque, un organisme public, un employeur ou un membre de la famille. L'utilisateur est souvent dirigé vers un site web où il est invité à saisir des données à caractère personnel, avec parfois pour conséquence de se faire voler son identité, à fournir des

---

136 La Recommandation UIT-T X.1242 définit le terme spam comme une "*information électronique transmise d'un expéditeur à un destinataire au moyen de terminaux, tels que des ordinateurs, des téléphones mobiles, des téléphones fixes, etc., et qui est généralement non sollicitée, non désirée et nuisible pour le destinataire*" (https://www.itu.int/rec/T-REC-X.1242-200902-I/fr).

137 https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

138 https://www.scamwatch.gov.au/research-and-resources/scam-statistics

139 Les questions traitées ici sont en lien avec les services de télécommunications au sens large et les activités de lutte contre la fraude en ligne. Le rapport final sur la Question 6/1 (Information, protection et droits du consommateur) consacre un chapitre à la fraude en ligne.

informations confidentielles, telles que des informations bancaires ou de carte de crédit, ou à effectuer un paiement vers un faux compte.

Dans le domaine de la cybersécurité, l'une des formes d'escroquerie les plus courantes est l'hameçonnage par texto, un terme qui fait référence à l'envoi de messages d'hameçonnage à des téléphones mobiles par SMS, d'où le terme "smishing" en anglais, construit à partir des mots "phishing" (hameçonnage) et "SMS". Selon le Supplément 29 à la Recommandation UIT-T X.1242[140], l'hameçonnage par texto est "*une attaque contre la sécurité où l'utilisateur est amené, par la ruse, à télécharger un cheval de Troie, un virus ou un autre logiciel malveillant sur son téléphone mobile ou un autre appareil mobile*", tandis que l'hameçonnage désigne une "*tentative frauduleuse visant à acquérir des informations confidentielles telles que des noms d'utilisateur, des mots de passe et des détails de carte de crédit à des fins malveillantes, en se faisant passer pour une entité digne de confiance dans une communication électronique*".

Au cours des dernières années, les attaques d'hameçonnage par texto sont devenues une menace de plus en plus grave, dont la prévalence s'est intensifiée sous l'effet de l'utilisation d'outils d'IA, ce qui met en évidence l'ampleur et le caractère de plus en plus sophistiqué de cette nouvelle forme de cyberattaque. En 2022, plus de la moitié des appareils mobiles personnels et un quart des appareils mobiles d'entreprise ont été la cible d'au moins une attaque d'hameçonnage chaque trimestre, l'hameçonnage par texto, qui compte parmi les attaques d'hameçonnage non basées sur des courriels, ayant été multiplié par plus de sept au deuxième trimestre de 2022[141].

Les utilisateurs des services de communication ont parfois du mal à reconnaître ce type d'attaque. Et pour cause, les acteurs malveillants exploitent des techniques d'ingénierie sociale pour envoyer de faux messages à des appareils mobiles et inciter les destinataires à cliquer sur des liens URL contenus dans ces messages. En règle générale, ils utilisent des services de raccourcissement d'URL pour dissimuler les faux liens de connexion, ce qui empêche de déterminer si le message provient d'un escroc ou non. Il existe tout de même quelques signes révélateurs qui indiquent qu'un message est frauduleux, à savoir: le message n'est pas pertinent pour le destinataire; le message est souvent empreint d'un sentiment d'urgence; le message est envoyé à partir d'un numéro de téléphone inconnu; le message contient des fautes d'orthographe et de grammaire; le message contient un lien suspect.

Les utilisateurs doivent être conscients des risques et des mesures qu'ils peuvent prendre pour éviter d'être victimes d'une attaque d'hameçonnage par texto. Néanmoins, les fournisseurs de services ont également un rôle important à jouer, de même que le secteur public qui peut non seulement coopérer avec le secteur des télécommunications pour faire en sorte que les normes et les bonnes pratiques soient respectées, mais aussi sensibiliser la population à ce fléau.

6.2 Approches adoptées pour lutter contre l'hameçonnage par texto

6.2.1 Approches des pays pour lutter contre l'hameçonnage par texto

Au cours de la période d'études, les États Membres de l'UIT se sont efforcés d'élaborer des réglementations, de sensibiliser l'opinion publique, de travailler avec le secteur privé et de mettre en place une coopération internationale pour lutter contre l'hameçonnage par texto.

[140] https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13409
[141] https://www.lookout.com/documents/reports/Global-State-of-Mobile-Phishing-Report.pdf

Bien que de nombreux efforts continuent d'être déployés pour relever les défis que pose ce type d'attaque, il est clair qu'il n'existe aucune solution unique pour mettre fin à l'hameçonnage par texto et qu'il faut adopter une approche multidimensionnelle, consistant notamment à considérer ces attaques comme des infractions pénales.

C'est cette dernière approche qui a été adoptée par la **Fédération de Russie**[142], où les tentatives d'escroquerie par téléphone, y compris l'hameçonnage par texto, sont qualifiées d'infraction pénale en vertu de l'Article 159 du Code pénal. En outre, l'administration russe a adopté des mesures visant à interdire la location de numéros mobiles virtuels, qui sont entrées en vigueur en septembre 2024. De fait, il a été reconnu que la location de ces numéros constituait une menace pour la sécurité, étant donné que les acteurs malveillants utilisent des numéros temporaires pour créer des comptes sur les réseaux sociaux et les applications de messagerie et se livrer à des activités frauduleuses. Autre mesure adoptée par l'administration russe: le lancement d'une plate-forme de lutte contre la fraude permettant de vérifier les appels téléphoniques. Grâce à cette plate-forme, les fournisseurs de services de télécommunications connectés vérifient les numéros et contrôlent leur authenticité, bloquant les appels et les SMS douteux, avant qu'ils n'atteignent le destinataire. L'utilisation du système, qui est obligatoire pour tous les services de télécommunications homologués fournissant des services de communication vocale, est gratuite, mais la non-utilisation entraîne une amende de 600 000 à 1 million de roubles. Ces initiatives ont également été complétées par des campagnes de sensibilisation visant à responsabiliser les utilisateurs.

Le Gouvernement de l'**Australie** a également adopté une approche globale, comprenant des initiatives menées à la fois par le secteur des télécommunications et par le gouvernement ainsi que des activités de sensibilisation. Ces dernières années, l'Autorité australienne des communications et des médias a fait de la lutte contre les escroqueries par SMS une priorité en matière de conformité et a ainsi publié une série de nouvelles réglementations. Ces dernières imposent notamment aux fournisseurs de télécommunications d'identifier, de suivre et de bloquer les appels et les SMS frauduleux; de renforcer les procédures de vérification de l'identité avant que les numéros mobiles puissent être transférés d'un fournisseur à l'autre; et de renforcer les procédures de vérification de l'identité pour les transactions à haut risque, notamment les demandes d'échange de carte SIM et de modification de compte, etc. L'autorité contrôle également les fournisseurs de services de télécommunications qui envoient des SMS en masse. Toutes ces mesures ont révélé que des acteurs malveillants utilisaient les vulnérabilités créées par le non-respect pour envoyer des SMS frauduleux aux Australiens[143].

Parmi les autres mesures prises par l'Autorité australienne des communications et des médias pour lutter contre les escroqueries dans le domaine des télécommunications figurent l'envoi d'alertes aux consommateurs sur l'usurpation de l'identité d'organismes publics et les escroqueries à l'accès à distance; le travail en coulisse avec les fournisseurs de services de télécommunications, les organismes publics et les marques connues pour déjouer les escroqueries téléphoniques; et la coopération internationale avec d'autres pays et régulateurs internationaux afin de renforcer l'engagement stratégique dans la lutte mondiale contre l'escroquerie, le télémarketing non sollicité et les spams.

En outre, en 2023, le Gouvernement de l'Australie a lancé le déploiement en plusieurs étapes de mesures de lutte contre la fraude spécifiques, notamment la création d'un Centre national de

[142] Document 2/158 de la CE 2 de l'UIT-D (Fédération de Russie).
[143] Document 2/154 de la CE 2 de l'UIT-D (Australie).

lutte contre la fraude, l'élaboration d'une page web dotée d'une fonction de retrait permettant de supprimer les pages créées pour les escroqueries à l'investissement, et l'introduction d'un registre d'identifiants des expéditeurs de SMS.

La coopération et le partenariat entre les acteurs concernés sont une constante dans un certain nombre de pays, dont la **République de Corée** qui en a fait les piliers de ses initiatives de lutte contre l'hameçonnage par texto. De fait, le pays a facilité l'échange de renseignements sur les tactiques d'hameçonnage par texto en vue d'accélérer la détection et le traitement plus rapides des nouveaux vecteurs d'attaque, et créé des systèmes de signalement automatisés utilisés par les utilisateurs et partagés avec les fournisseurs de services de télécommunications à des fins de blocage.

Les outils d'IA peuvent également aider à lutter contre l'hameçonnage par texto, comme en République de Corée, où le Ministère des sciences et des TIC et l'Agence coréenne chargée d'Internet et de la sécurité mettent en œuvre une série de mesures visant spécifiquement à lutter contre l'hameçonnage par texto, englobant:

- la surveillance et le blocage en temps réel des messages d'hameçonnage grâce à un système de détection et de filtrage basé sur l'IA qui analyse les profils des SMS;
- le signalement des messages suspects pour les bloquer et la détection des URL suspicieuses dans le contenu des SMS;
- la création d'une base de données des numéros malveillants tenue à jour et partagée avec les fournisseurs de services de télécommunications;
- la mise en œuvre de systèmes de filtrage basés sur l'IA; et
- la création d'une ligne téléphonique nationale de signalement (118) ainsi que des portails en ligne gérés par l'Agence coréenne chargée d'Internet et de la sécurité[144].

Ces activités montrent combien il est important de s'attaquer à ce phénomène sous plusieurs angles, et notamment faire participer les fournisseurs de services de télécommunications, adopter des technologies nouvelles et émergentes pour faciliter l'analyse, le filtrage et le blocage, mettre en œuvre les procédures et les processus nécessaires, élaborer et tenir à jour un système de signalement, utiliser les données collectées, et enfin, travailler intensément à la sensibilisation de la population. L'importance de la sensibilisation des utilisateurs ne peut être sous-estimée. Comme les acteurs malveillants modifient, affinent et réinventent fréquemment leurs méthodes, un utilisateur bien informé, responsabilisé et conscient a bien plus de chances de ne pas devenir victime.

6.2.2 Approches du secteur des télécommunications pour lutter contre l'hameçonnage par texto

Le secteur des télécommunications a pris des mesures concrètes pour contrer et atténuer les conséquences de l'hameçonnage par texto en particulier, et des escroqueries en général. En ce qui concerne les méthodes techniques, les fournisseurs ont adopté diverses mesures, telles que des mécanismes de signalement, des pare-feu SMS, le blocage des URL de sites d'hameçonnage connus et des registres d'identification des expéditeurs de SMS. Les pare-feu SMS peuvent empêcher de grandes quantités de messages indésirables d'atteindre les utilisateurs, tandis que les registres d'identification des expéditeurs de SMS permettent aux entreprises d'enregistrer et de protéger les en-têtes de message utilisés lors de l'envoi de

[144] Document 2/312 de la CE 2 de l'UIT-D (République de Corée).

SMS à leurs clients, limitant ainsi les impacts de l'hameçonnage par texto et de l'usurpation d'identité. Le signalement des escroqueries, lorsqu'il est bien coordonné entre de multiples opérateurs mobiles, constitue une solution efficace pour identifier et éliminer les escroqueries. La ligne téléphonique de signalement 7726 créée au **Royaume-Uni** et au **Canada** permet de signaler les messages suspects aux fins d'enquête[145]. En 2014, les quatre principaux opérateurs mobiles du Royaume-Uni, en collaboration avec le Bureau du Commissaire à l'information du Royaume-Uni, ont créé cette ligne sur une base volontaire pour permettre à la population de faire suivre gratuitement les messages suspects, ainsi que les messages indésirables. En mars 2025, 26 000 numéros frauduleux avaient été supprimés[146].

La fraude par paiement push autorisé est un autre problème qui entraîne des pertes financières considérables pour les consommateurs. Elle consiste pour les criminels à contacter les victimes par SMS ou par appel téléphonique en se faisant passer pour une organisation légitime, comme une banque, en vue d'obtenir un transfert d'argent. La **GSMA** et **UK Finance** ont réuni les opérateurs de téléphonie mobile et les banques britanniques pour mettre au point "Scam Signal", une solution qui utilise une interface de programmation d'applications (API) pour permettre aux banques de mieux reconnaître les transferts frauduleux et de les bloquer[147].

Dans de nombreux pays d'Afrique subsaharienne, où les services d'argent mobile sont très populaires, le renforcement de la sécurité des plates-formes d'argent mobile est un enjeu majeur. Au **Kenya**, "M-Pesa" et d'autres services similaires ont intégré des fonctions d'authentification biométrique, de chiffrement et de détection des fraudes afin de protéger les utilisateurs contre les attaques par usurpation d'identité et par hameçonnage[148]. À l'échelle mondiale, les opérateurs de toutes les régions du monde déploient diverses API telles que "Number Verify", qui suppriment la nécessité d'utiliser une autre méthode d'authentification (un code PIN à usage unique ou un mot de passe, par exemple) et vérifient à la place que l'utilisateur interagit avec un service à partir d'un appareil dont le numéro de téléphone mobile a été préenregistré et vérifié. Les processus de connaissance de l'identité des clients (KYC) sont également de plus en plus utilisés pour fournir un processus d'intégration plus sûr, y compris pour les services d'argent mobile, par la validation des informations de contact des utilisateurs et la lutte contre le vol d'identité.

Telstra, le plus grand opérateur de télécommunications d'Australie, utilise un filtre pour lutter contre les escroqueries par SMS. Celui-ci analyse le contenu des messages, à la recherche d'éléments suspects, dans le but d'identifier et de bloquer les messages malveillants contenant des liens ou des numéros de téléphone suspects[149]. Les fournisseurs de télécommunications s'associent également au secteur bancaire pour lutter contre les escroqueries téléphoniques. Par exemple, le deuxième plus grand fournisseur de télécommunications d'Australie, **Optus**, a lancé l'initiative "Call Stop" conjointement avec l'Australian Financial Crimes Exchange et des membres du secteur bancaire, dont des grandes banques[150]. Cette initiative, qui cible

---

145 https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/7726-reporting-scam-texts-and-calls; https://www.pensezcybersecurite.gc.ca/fr/blogues/signaler-messages-textes-indesirables-numero-7726

146 Document 2/393 de la CE 2 de l'UIT-D (Royaume-Uni).

147 https://www.gsma.com/newsroom/press-release/mobile-and-banking-industries-join-forces-to-fight-fraud/

148 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/social-engineering-and-impersonation-fraud/; https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/05/Mobile-Money-Fraud-Typologies-and-Mitigation-Strategies-20.05.24.pdf

149 Document 2/154 de la CE 2 de l'UIT-D (Australie).

150 *Ibid*.

les escroqueries par rappel téléphonique, vise à empêcher les clients d'Optus de composer le numéro frauduleux identifié, puis transfère l'appel vers une messagerie automatisée pour les mettre en garde contre les risques d'escroquerie. Les banques et les opérateurs de télécommunications diffusent également des informations auprès de leurs clients concernant les méthodes préventives de lutte contre les escroqueries, afin de renforcer les efforts déployés pour combattre l'hameçonnage par texto et la fraude dans le secteur des télécommunications.

La **GSMA** facilite la coopération et l'échange de renseignements par l'intermédiaire du Groupe de travail sur la fraude et la sécurité[151] et du Centre d'analyse et de partage des informations sur les télécommunications[152]. Ces deux plates-formes sécurisées contribuent au partage d'informations en temps réel à l'échelle mondiale.

La lutte contre l'hameçonnage par texto et les escroqueries dans le domaine des télécommunications nécessitent des partenariats solides entre toutes les parties prenantes. À eux seuls, les pouvoirs publics n'ont pas les moyens de mettre fin aux activités frauduleuses. Après l'élaboration et l'application par l'Autorité australienne des communications et des médias des réglementations visant à identifier et à bloquer les appels frauduleux en décembre 2020 et les SMS frauduleux en juillet 2022, les fournisseurs de télécommunications ont déclaré avoir bloqué plus de 1,4 milliard d'appels frauduleux et plus de 257 millions de messages frauduleux au terme du mois de juin 2023[153].

Par ailleurs, il y a lieu d'envisager que les campagnes d'information publiques sur le signalement des escroqueries devraient faire augmenter le nombre de signalements. Au **Royaume-Uni**, certaines organisations, comme le Centre national pour la cybersécurité et des forces de police locales, ont porté à la connaissance du public l'existence de la ligne de signalement 7726, et l'Ofcom, le régulateur des télécommunications, a publié une vidéo présentant de façon simple les différentes étapes à suivre pour signaler des messages et des appels au 7726 sur la plupart des principaux modèles de smartphones. Par ailleurs, l'ajout récent d'un bouton de signalement des spams sur la grande majorité des smartphones dans le pays a donné lieu à une forte augmentation du taux de signalement des escroqueries par message. Ce bouton fonctionne de la même façon que la ligne 7726, l'information étant partagée avec les opérateurs mobiles via la base de données de tiers utilisée en partage. Cette évolution a eu pour conséquence une hausse des signalements d'environ 800% en un an[154].

Les mesures prises à ce jour ayant donné des résultats positifs, il convient d'envisager une approche globale qui englobe les différentes parties prenantes, à savoir les autorités gouvernementales, les banques et les opérateurs de télécommunications ainsi que les utilisateurs.

151 https://www.gsma.com/get-involved/working-groups/fraud-security-group/
152 https://www.gsma.com/solutions-and-impact/technologies/security/t-isac/
153 Document 2/154 de la CE 2 de l'UIT-D (Australie).
154 Document 2/393 de la CE 2 de l'UIT-D (Royaume-Uni).

Conclusions

L'utilisation des télécommunications et des TIC joue un rôle inestimable dans le développement et la croissance socio-économique partout dans le monde. C'est pourquoi il est devenu essentiel aujourd'hui de sécuriser les réseaux d'information et de communication et de créer une culture de la cybersécurité, et ce d'autant plus que l'adoption et l'utilisation des télécommunications et des TIC ne cessent de croître. Pendant la période d'études considérée, nous avons abordé au titre de la Question 3/2 de nombreux aspects de la cybersécurité, examiné les contributions des membres de l'UIT et organisé deux ateliers qui ont servi de base au présent rapport et à ses conclusions.

Dans le Chapitre 1, il a été constaté que les initiatives de sensibilisation à la cybersécurité comprenaient aussi bien des programmes de grande envergure ciblant divers groupes de population que des interventions spécifiques axées sur des thèmes tels que la cybersécurité et la sensibilisation aux escroqueries. De même, les politiques des États Membres en matière d'éducation et de formation à la cybersécurité ne sont pas toutes dotées des mêmes capacités. Si certains pays ont mis en œuvre des stratégies complètes visant à pallier la pénurie de professionnels de la cybersécurité, d'autres ont opté pour des solutions de formation plus spécifiques ciblant des composantes de la main-d'œuvre. Les États Membres ont, à juste titre, mis l'accent sur les initiatives de protection en ligne des enfants en instaurant des cadres juridiques solides et en élaborant des outils et des programmes concrets afin de rendre Internet plus sûr pour les enfants.

Le Chapitre 2 a examiné un large éventail de pratiques en matière d'assurance de la cybersécurité, considérées comme un élément essentiel de la protection des réseaux, des systèmes et des données contre les activités malveillantes. Bien qu'elles n'empêchent pas directement les cyberattaques, leur objectif, s'il est correctement mis en œuvre, est de réduire au minimum le risque que de telles attaques se produisent. Bien qu'il n'y ait pas d'approche unique à recommander, les initiatives citées en exemple ont montré une tendance durable vers l'adoption de ces pratiques partout dans le monde, les autorités nationales utilisant souvent des approches différentes, voire une combinaison d'approches, allant de l'auto-évaluation et des lignes directrices appliquées sur une base volontaire aux systèmes d'étiquetage et aux contrôles de conformité stricts.

Le Chapitre 3 a mis en lumière le rôle essentiel des équipes CIRT pour accroître la cyberrésilience d'un pays. Pour les pays en développement, la création et la gestion de telles équipes devraient être élevées au rang de priorité. L'UIT se tient à la disposition des pays qui souhaitent évaluer leurs équipes CIRT et les renforcer à des fins d'amélioration de la résilience des infrastructures essentielles.

Le Chapitre 4 s'est penché sur les approches et les expériences en matière de feuilles de route nationales qui peuvent guider l'amélioration des cadres nationaux de cybersécurité. On a pu y constater que si les cybermenaces évoluent en permanence, les principes fondamentaux que sont la planification globale, la participation de toutes les parties prenantes et l'adaptabilité proactive restent essentiels à la réussite de la mise en œuvre d'une stratégie de cybersécurité. À l'avenir, ce sont ces principes qui continueront de façonner les défenses de cybersécurité résilientes nécessaires à la sauvegarde des intérêts nationaux dans un monde interconnecté.

Consacré aux mesures de cybersécurité visant à sécuriser les réseaux 5G, le Chapitre 5 a décrit les normes et les spécifications élaborées par les organisations de normalisation et le secteur des télécommunications, dont la mise en œuvre doit être complétée par des mesures de cybersécurité proactives proposées par les fournisseurs et les opérateurs, ainsi que par des politiques et réglementations nationales. Celles-ci peuvent se présenter sous différentes formes en fonction des contextes nationaux et porter, entre autres, sur l'évaluation des fournisseurs, la réalisation de tests, l'octroi de certifications, et l'établissement de directives ou d'exigences.

Enfin, le Chapitre 6 a porté sur les efforts déployés pour lutter contre les escroqueries dans le secteur des télécommunications, en particulier l'hameçonnage par texto, et a souligné le besoin de partenariats solides entre le secteur public et le secteur privé. Ce chapitre a présenté des exemples d'initiatives fructueuses menées par les pouvoirs publics comme par le secteur des télécommunications dans le but de mettre un terme à l'hameçonnage par texto. La sensibilisation et l'éducation des utilisateurs sont également essentielles, d'autant plus que ces attaques deviennent de plus en plus sophistiquées et difficiles à détecter.

Pour ce qui est de l'avenir de la Question 3/2, tant que le paysage mondial de la cybersécurité continuera d'évoluer, le partage d'informations et de méthodes concernant la cybersécurité restera vital. Il y a tout lieu de maintenir la Question dans la prochaine période d'études, à condition toutefois d'en modifier le libellé de manière à ce qu'il soit davantage axé sur des questions spécifiques de cybersécurité, conformément au mandat et au public de la commission d'études de l'UIT-D.

Annexes

Annex 1: List of contributions and liaison statements received on Question 3/2

Contributions for Question 3/2

Web	Received	Source	Title
2/408	2025-04-29	RIFEN	Securing contractualization and deed production during the real estate sales process via blockchain technology and machine learning: practices and use cases
Describes the integration of blockchain technology and machine learning solutions for securing real estate transactions. Together, these technologies strengthen stakeholder confidence, while improving the efficiency of real estate transactions. This contribution takes into account existing work and provides an overview of the system we have implemented in Cameroon for the sale of real estate.			
2/405	2025-04-28	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
This contribution provides an update on the activities currently being undertaken by BDT to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated.			
2/393	2025-04-23	United Kingdom	Scam reporting within the UK
Summarises how the largest mobile operators in the United Kingdom voluntarily provide the 7726 reporting service, as a way of identifying, removing, and preventing scams calls and messages.			
2/392	2025-04-2025	RIFEN	Developing countries: strengthening cyber-security
Describes how developing countries face multiple and complex cybersecurity challenges, but with limited means to address the question of how they can ensure that disparities in technical capabilities and funding do not hamper their efforts to enhance cybersecurity.			
2/370	2025-04-14	China	Jointly building cybersecurity: typical practices of safeguarding cyberspace security
Provides an overview of the laws and regulations enacted by China to safeguard cyberspace security, the national campaigns launched to raise people's awareness of cybersecurity, as well as the international initiatives proposed by China on cybersecurity, with the aim of providing reference practices and paths for the world to build secure cyberspaces together.			
2/350	2025-02-27	RIFEN	Artificial intelligence for the detection and reporting of online cyberbullying
Presents the challenge to combat online harassment and the opportunity to integrating artificial intelligence, particularly deep learning techniques, as a promising avenue for improving the protection of sensitive data. The contribution highlights the advantages of designing an intelligent system capable of proactively and automatically identifying threats by combining advanced analysis techniques with proactive cybersecurity strategies.			

(suite)

Web	Received	Source	Title
2/346	2025-02-04	Tanzania	Best practices for coordinating efforts and developing cybersecurity culture
Highlights good practices for coordinating efforts to promote a culture of cybersecurity in Tanzania. It outlines how various legal, technical, organizational, and capacity development measures, along with cooperation, have been vital in enabling Tanzania to achieve a "Tier 1" ranking and be recognized as a "role model" in the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU). It also identifies areas for continuous improvement, especially in technical and capacity development measures.			
2/TD/10 +Ann.1	2024-11-12	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Reports on the recently conducted CIRT Maturity Assessments in Azerbaijan, Bhutan, Sierra Leone, and Tanzania, the cyberdrills carried out in 2024 to enhance incident response readiness across different regions, the launch of the 5th edition of the Global Cybersecurity Index, BDT assistance in countries and territories in the assessment of their cybersecurity strategies, the Women in Cyber Mentorship Programme and the Her CyberTracks programme, the launch of new online safety tools for children and ongoing capacity building efforts, and other initiatives.			
2/339	2024-11-07	Republic of the Congo	Online communication and transactions via new and emerging telecommunications/ICTs, such as the Internet of Things (IoT)
Outlines challenges in consumer protection with the rise of IoT technology. It highlights issues with data protection, privacy, fair business practices, and device security. Various international responses include legislation, certification, monitoring, and technical standards to safeguard consumer rights and ensure device security.			
2/329	2024-10-29	Egypt	Egypt capacity building centre for African countries (EG-ATRC)
Details Egypt's dedication to enhancing African nations' communication and information technology skills via the Egyptian African Telecom Regulatory Training Centre (EG-ATRC), providing ITU-accredited training and hosting 381 participants from 30+ countries.			
2/322	2024-10-29	NRD Cyber Security	Strengthening cyber resilience: the role of Lithuania's national CIRT in critical infrastructure protection
Presents a case study on Lithuania's National Computer Incident Response Team within the National Cyber Security Centre, highlighting its functions in critical infrastructure protection through monitoring, incident handling, threat analysis, and collaboration efforts, including European Union initiatives.			
2/320	2024-10-29	Australia	Mandating a minimum standard for consumer-grade smart devices
Describes Australia's transition to mandatory smart device security standards from voluntary security standards, prompted by poor guideline adoption. A Bill proposes enforceable Internet of Things standards, requiring compliance statements from manufacturers and suppliers, and introduces a regulatory model with update flexibility.			
2/312	2024-10-28	Republic of Korea	Challenges and approaches to addressing smishing and SMS incidents in South Korea

(suite)

Web	Received	Source	Title
Examines smishing threats in the Republic of Korea, detailing the Ministry of Science and ICT and Korea Internet & Security Agency countermeasures, challenges, and government strategies such as AI detection, awareness campaigns, and international cooperation, with recommendations for improvement.			
2/309	2024-10-25	Albania	Creation of a safer cyber ecosystem in a country: the case of Albania
Summarizes Albania's post-cyberattack cybersecurity reforms, including legal and strategic updates, new operations centres, human capital investment, and enhanced international cooperation with entities like the UN and NATO, leading to stronger legal frameworks and preparedness.			
2/301	2024-10-22	China	Mobile anonymous subscription service based on data security protection
Proposes a service for user privacy protection by using temporary numbers and anonymous IDs, with a focus on balancing privacy and digital economy growth, detailing a system architecture that ensures availability, scalability, reliability, usability, observability, and audit logs.			
2/300	2024-10-22	China	Based on anonymous data exchange network, release the value of telecommunications data
Examines the importance of telecommunications data in the digital economy and the challenges of using it, such as privacy issues and integration with Internet data. It details the China Academy of Information and Communications Technology creation of an anonymous data network, enhancing financial risk management and advertising, and supporting sustainable growth and employment in line with the United Nations Sustainable Development Goals.			
2/299	2024-10-22	China Telecommunications Corporation	Building security capabilities to alert phishing websites
Outlines the difficulties the elderly encounter with digital threats such as phishing, and details the China Telecom security tool, which shields them through gateway plug-ins, cloud engines, and a security database, serving over 10 million users in 31 provinces.			
2/276	2024-09-30	Côte d'Ivoire	Cybersecurity in action: strategies and challenges in a connected world - experience of Cote d'Ivoire
Presents the "O'KOHI" web series by a Platform for the Fight against Cybersecurity (PLCC), designed to educate on cybersecurity via videos. Funded by ARTCI and the *Ministère de l'Economie Numérique, des Télécommunications et de l'Innovation*, it addresses hacking, data protection, and cyberattacks, ensuring content accuracy through expert collaboration.			
2/273	2024-09-29	RIFEN	Machine learning-based CVE and CWE analysis
Highlights the need for machine learning to automate Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) analysis, improve identification and prioritization of software vulnerabilities, and overcome challenges such as data quality and model complexity through solutions including data validation and continuous learning. It advocates for collaboration to enhance cybersecurity.			
2/271	2024-09-29	RIFEN	Cybersecurity and cyberspace protection in developing countries

(suite)

Web	Received	Source	Title
Examines the Internet and information and communication technology impact on Africa's socio-economic progress, addressing cyberattack risks and the necessity for collaborative security efforts. It discusses Africa-specific challenges, infrastructure vulnerabilities, and advocates for a multi-stakeholder strategy to safeguard essential Internet resources.			
2/268	2024-09-24	RIFEN	Cybersecurity awareness for rural youth through online training organized by RIFEN-SADA
Outlines the RIFEN-SADA (Smart Africa Digital Academy) cybersecurity training, which enhanced awareness and skills in cybersecurity among young Africans through fourteen modules. It fostered a security-conscious culture, practical protection knowledge, and guided talent development, leading to certifications and improved job prospects.			
2/254	2024-09-19	Co-Rapporteur for Question 6/1; Co-Rapporteur for Question 3/2	Report of the workshop on Increasing Consumer Awareness Mechanisms to Promote Informed Consumer Decision: A joint workshop for Question 6/1 and Question 3/2 held in Brasilia from 18-20 June 2024
Presents the workshop on consumer protection in the digital age, discussing infrastructure in underserved regions, security, digital literacy, and data privacy. It stressed digital inclusion, consumer behaviour, and skill gaps, concluding with good practices for ITU deliverables.			
2/246	2024-09-16	RIFEN	Securing the contracting procedure and the production of deeds of purchase in the real estate sale process using blockchain technology and machine learning
Discusses how blockchain technology and machine learning are revolutionizing the real estate industry by enhancing security, efficiency, and decision-making in the sales process. It highlights the benefits of smart contracts and improved market analysis, while acknowledging the challenges of adoption and regulation.			
2/242	2024-09-12	Central African Republic	Operationalization of CSIRT/SOC/PKI platforms and training
Outlines the Central African Republic's cybersecurity measures post-broadband expansion, including the deployment of a Security Operations Centre - Computer Security Incident Response Team (SOC-CSIRT) and public key infrastructure (PKI) systems, and requests Union support for network security.			
RGQ2/218	2024-04-29	Australia	National Office of Cyber Security and the Cyber Security Response Coordination Unit
Presents the Cyber Security Response Coordination Unit, the National Office of Cyber Security and the National Cyber Security Coordinator, entities established by the Government of Australia within the Department of Home Affairs for central coordination, following the Optus and Medibank data breaches of 2022.			
RGQ2/214	2024-04-19	Australia	Critical Infrastructure Uplift Program (CI-UP)
Outlines the Critical Infrastructure Uplift Programme (CI-UP) in Australia, designed to enhance cyber security and resilience of critical infrastructure against cyber-attacks. It details CI-UP activities and emphasizes the voluntary and collaborative nature with industry partners.			

(suite)

Web	Received	Source	Title
RGQ2/212	2024-04-18	China Mobile Communications Co. Ltd.	China's initiatives to protect the cyber-security rights and interests of minors
Presents the critical nature of cybersecurity for Chinese minors, addressing their high online presence, urban-rural digital divide, and exposure to risks such as addiction and privacy violations. It underscores China's advancements in safeguarding minors' Internet use and the collective role of government, industry, and society in bolstering cyber-security education and safety.			
RGQ2/201	2024-04-16	Saudi Arabia	Cost estimation tool for cybersecurity controls
Outlines the National Cybersecurity Authority (NCA) development of the "ECC Cost Estimation Tool" to aid Saudi organizations in budgeting for cybersecurity compliance. It details the creation process, including research, implementation and testing phases.			
RGQ2/191	2024-04-16	United Kingdom	Considerations in implementing a new and significant regulatory security framework for the telecoms sector: an example from the UK's Telecoms Security Act (TSA)
Outlines the United Kingdom new telecoms security framework under the Telecommunications Security Act 2021, detailing enhanced security duties for providers, a tiered approach based on turnover, and the Ofcom role in ensuring compliance and fostering a collaborative security culture.			
RGQ2/184	2024-04-15	Brazil	Creating cybersecurity capabilities: Hackers do Bem
Describes Brazil's "Hackers do Bem" ("White Hat Hackers") initiative, aiming to train 30 000 students in cybersecurity through a five-level curriculum, with government support, to build a national hub, boost employability, and strengthen the cybersecurity ecosystem.			
RGQ2/183	2024-04-15	Brazil	Cybersecurity in Brazilian National Research and Education Network: CAIS
Outlines the work of the Brazilian National Research and Education Network (RNP), which created the first network security centre in Brazil in 1995 (CAIS). CAIS serves as CSIRT for the Brazilian academic network, being the focal point for security incident notifications and providing coordination and support for the incident handling.			
RGQ2/182	2024-04-15	Brazil	Brazilian Federal Cyber Incident Management Network
Presents the Brazilian Federal Cyber Incident Management Network (ReGIC), presenting the two CSIRTs with national responsibilities, such as the Brazilian National Computer Emergency Response Team (CERT.br) and the Centre for Prevention, Treatment and Response to Government Cyber Incidents (CTIR Gov), as well the CSIRT ecosystem in Brazil.			
RGQ2/181	2024-04-15	Brazil	Brazilian National Cybersecurity Policy
Summarizes Brazil's National Cybersecurity Policy and the formation of the National Cybersecurity Committee, detailing its principles, goals, and tasks like promoting cybersecurity, resilience, education, and global collaboration, with diverse members overseeing policy execution.			
RGQ2/170	2024-04-04	Russian Federation	Implementation of the educational project "Digital Literacy Campaign" in the Russian Federation

(suite)

Web	Received	Source	Title
Outlines the Russian Federation's "Digital Economy" programme for human capital and economic growth by 2024, including "Digital Literacy Campaign" with partners like Kaspersky Lab to educate children on digital safety through animated videos.			
RGQ2/165	2024-04-02	Brazil	Meaningful connectivity
Summarizes the Anatel 2023 Strategic Planning, highlighting digital transformation and meaningful connectivity, which encompasses a cyber safety perspective. It details cyber hygiene initiatives, including the launch of a dedicated page to combat digital scams and frauds.			
RGQ2/164	2024-03-29	United States	U.S. Pre-Ransomware Notification capability
Details the CISA Pre-Ransomware Notification programme to pre-empt ransomware attacks. It emphasizes early warnings, international cooperation, and the success of the #StopRansomware campaign in averting threats in 2023.			
RGQ2/163	2024-03-26	Syrian Arab Republic	A paper on digital development in Syria and the current reality
Summarizes the Syrian Arab Republic digital transformation strategy for government services, detailing a phased approach from 2021 to 2030, encompassing e-government services, citizen centres, and cybersecurity. It includes strategic axes, programmes, and annexes on Internet capacity and security.			
RGQ2/160	2024-03-26	RIFEN	Initiatives to strengthen digital trust in Côte d'Ivoire
Highlights Côte d'Ivoire's National Digital Development Strategy 2021-2025, aiming to transform the nation into West Africa's digital hub by improving digital skills, cybersecurity, and women's tech inclusion, and by creating a national data centre.			
RGQ2/155	2024-03-26	RIFEN	Building a resilient security culture: a comprehensive approach to cybersecurity enhancement
Highlights the need for a robust cybersecurity culture in organizations, advocating for comprehensive strategies such as employee training, simulations, incident response teams, access control, encryption, and continuous monitoring to combat cyber threats.			
RGQ2/149	2024-03-15	Democratic Republic of the Congo	Development of cybersecurity in the Democratic Republic of Congo: issues and strategies for the protection of ICT infrastructures and digital actors
Outlines the Democratic Republic of the Congo's cybersecurity challenges, including its vulnerability to cyberattacks and the lack of a national strategy, legal framework, and incident reporting. It mentions a workshop for creating a national CIRT and ITU strategy support.			
RGQ2/140	2024-03-11	RIFEN	Internet and ICT: development levers and cybersecurity challenges in developing countries
Highlights the importance of Internet and ICTs for development, stressing security against cyberthreats. It combines research with expert opinions, identifies vulnerabilities, and addresses Africa's connectivity issues, advocating for information sharing, legislation, and collaboration to protect digital infrastructure.			

(suite)

Web	Received	Source	Title
RGQ2/134	2024-03-05	Burundi	Implementation of a national cybersecurity strategy
Outlines the significance of information management and ICTs for a country's progress, emphasizing the necessity of cybersecurity measures in light of rising cybercrime. It details Burundi's efforts, supported by ITU, to create a national cybersecurity strategy by 2040, concentrating on legal structures, infrastructure security, and skill development.			
RGQ2/130	2024-02-29	RIFEN	Côte d'Ivoire's cybersecurity initiatives
Outlines Côte d'Ivoire's cybersecurity strategies, including the Platform for Combating Cybercrime and CI-CERT, stressing public awareness and education to foster a cybersecurity culture and safeguard the online space, particularly during events like the African Cup of Nations.			
RGQ2/128 +Ann.1	2024-02-29	Syrian Arab Republic	Cybersecurity strategy in Syria
Summarizes the Syrian Arab Republic cybersecurity strategy, focusing on creating a strong infrastructure, handling threats, legal development, capability enhancement, research, governance, and international collaboration via six programs, while stressing the importance of multi-layered protection.			
RGQ2/121	2024-02-29	Haiti	Taking control of cybersecurity in Haiti
Outlines Haiti's Haitian Institute for Statistics and Information and the CONATEL partnership to create a national cybersecurity strategy, aided by the World Bank and Inter-American Development Bank, including forming a working group, evaluating cybersecurity maturity, and establishing a CERT to enhance digital security.			
RGQ2/117 +Ann.1	2024-02-28	Dominican Republic	Cyberskills Center for Latin America and the Caribbean LAC4: Knowledge exchange, training and training in best practices at LAC4
Describes how the Latin America and Caribbean Cyber Competence Centre has enhanced cybersecurity in over 25 Latin American and Caribbean countries through workshops, legal framework support, and promoting regional cooperation, including empowering women and raising cyber awareness.			
RGQ2/114 +Ann.1	2024-02-27	Zambia	The role of the Authority in Child Online Protection in Zambia: A Zambia case study on the implementation of the National COP Strategy - Lessons learnt
Summarizes Zambia's dedication to child online safety by adopting ITU Resolution 179 and executing a national child online protection strategy, focusing on legal frameworks, education, combating exploitation, stakeholder cooperation, and ensuring effective oversight.			
RGQ2/104	2024-01-24	Democratic Republic of the Congo	Making Congolese cybersecurity a lever for integration and socio-economic growth
Describes the Democratic Republic of the Congo's strategy for using cybersecurity to enhance integration, governance, and growth, focusing on infrastructure, cybercrime, and digital services. It advocates for expert capacity building and ITU partnership for a secure digital transformation.			
2/212	2023-10-31	Republic of Korea	Misuse of Personally Identifiable Information

(suite)

Web	Received	Source	Title
Presents the Republic of Korea's data protection mechanism that has been updated to address concerns related to the misuse and abuse of personal identifiable information (PII). The Personal Information Protection Act (PIPA) amended the existing PII Anonymization Guidelines on 28 April 2022, which aim to offer six step-by-step guidelines for the treatment (de-identification) of personal information. The Republic of Korea highlighted the challenge of crafting guidelines that guard against the abuse and misuse of PII without jeopardizing the benefits of new technologies.			
2/201	2023-10-17	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Discusses ongoing efforts to improve cybersecurity in ITU Member States, including future plans and new initiatives as well as how the Global Cybersecurity Agenda, launched in 2007, promotes international cooperation, and how BDT works with Member States and global organizations to establish national and regional CIRTs, measures cybersecurity commitments, supports strategy development, encourages diversity, and works to protect children online through the child online protection initiative.			
2/199	2023-10-17	United Kingdom	Building local capacity to adopt secure connected place technology: the UK's Secure Connected Places Playbook
Recognizes the benefits that connected places ("smart cities") technology can bring societies and local areas. However, it also recognizes that this interconnectivity creates cyber vulnerabilities and the potential for cyberattacks. Through its National Cyber Strategy 2022, the United Kingdom has been developing a 'Secure Connected Places Playbook'. This product, currently in alpha phase, has been developed in partnership with a diverse set of local government authorities and an industry consortium. The Playbook provides guidance on: i) governance; ii) procurement and supply chain management; and iii) risk and threat analysis. The United Kingdom has identified several good practices, including: i) working hand-in-hand with intended beneficiaries; ii) using a "test and iterate" approach; and iii) co-developing and testing with local government authorities. The United Kingdom has now begun beta testing, working with 13 local authorities.			
2/196	2023-10-17	United States	U.S. proposed Cyber Trust Mark Program: certifying that IoT products meet U.S. cyber standards
Presents the proposed Cyber Trust Mark program, by the United States Federal Communications Commission (FCC), a voluntary cybersecurity labelling initiative for IoT products. The programme aims to help consumers make informed decisions, differentiate trustworthy products, and encourage manufacturers to meet higher cybersecurity standards. The FCC seeks input on various aspects of the programme, including eligible devices, oversight, security standards, and consumer education. Certified products could be available for purchase by the end of 2024.			
2/187	2023-10-16	Republic of Korea	Privacy by Design certification in South Korea
Shares its contribution on Privacy by Design (PbD), a proactive approach to embedding privacy into the design and operation of information technologies and systems. The Personal Information Protection Committee (PIPC) of the Republic of Korea is piloting a PbD certification system to strengthen the safety of personal information collection devices. The certification helps organizations demonstrate their commitment to user privacy, increasing consumer trust and reducing the risk of privacy breaches.			
2/167	2023-10-11	Australia	eSafety Youth Council

(suite)

Web	Received	Source	Title
Presents the eSafety Youth Council, established in April 2022, that consists of 24 members aged 13-24 from diverse backgrounds in Australia. It aims to involve young people in decision-making processes for policies and programmes impacting them. The Council is informed by the Western Sydney University Youth Engagement Report and follows six good practice principles. Members engage in various activities, including conferences, resource launches, and discussions with technology companies. The Council priorities include collaboration, improved reporting processes, age-appropriate content access, and increased engagement on online safety.			
2/158	2023-10-09	Russian Federation	Challenges and approaches to addressing smishing and SMS incidents. Combating illegal use of virtual mobile numbers
Contextualize smishing as a type of phishing attack that uses SMS messages to trick users into downloading malware or revealing personal information. The rise of mobile services and the pandemic have increased its popularity. To combat smishing, users should be cautious of unexpected messages, use anti-spam settings, and report suspicious messages. Governments, banks, and telecommunication operators are also working together to fight smishing through regulations, public awareness campaigns, and technological solutions.			
2/154	2023-10-05	Australia	Combating telecommunications scams
Presents the Australian Communications and Media Authority (ACMA) work to combats scams through regulatory powers, new rules, and international cooperation. Initiatives include varying the telecommunications numbering plan, registering the Reducing Scam Calls and Scam SMS Code, and mandating stronger identity verification processes. ACMA also collaborates with other nations and industries to fight scams. Despite progress, SMS scams remain a significant issue. A holistic approach involving industry, government, and consumer awareness is needed.			
2/150 +Ann.1	2023-09-29	Argentina	Promoting cybersecurity in Argentina: challenges, strategies and advances in the digital era
Presents the growing reliance on ICT for essential services highlighting the need for governments to prioritize cybersecurity. Challenges include fostering a cybersecurity culture and promoting safe cyberspace usage. Efforts include a National Cybersecurity Awareness Campaign, a joint publication on cybersecurity issues, training programmes for civil servants, strengthening legal frameworks, and addressing the gender gap in ICT access and use through national and international initiatives.			
2/141	2023-09-28	Central African Republic	Criminal aspects of physical protection of information and communication network infrastructures
Central African Republic shares the implementation of legislative reforms and creation of agencies to control and secure information systems. However, the country faces vandalism and theft on its new fibre optic network. Proposed solutions include adopting laws against theft, fraud, and vandalism in public information networks and establishing a national CIRT team to coordinate incident management.			
2/137	2023-09-14	Côte d'Ivoire	Cybercrime: Continuing campaign on child online protection

(suite)

Web	Received	Source	Title
Discusses the digital knowledge challenge facing Côte d'Ivoire, that is hindering its development in the digital world. To address this, public and private sectors, along with international organizations, have launched an awareness campaign for middle and high school students. The campaign aims to educate and raise awareness about online risks, promote responsible digital behaviour, and provide support for reporting abuse. Over 1 000 students participated in the campaign, which emphasizes the importance of a safer digital environment for all citizens.			
2/120	2023-09-07	Timor-Leste	Advancing cybersecurity for Timor-Leste's digital transformation
Presents Timor-Leste digital transformation journey, focusing on improving government services, inclusivity, and crucial sectors such as healthcare, education, and agriculture. However, as a least developed country (LDC), it faces significant cybersecurity challenges, including weak frameworks, limited awareness, and inadequate resources. To enhance digital resilience, Timor-Leste must invest in infrastructure, capacity building, legal frameworks, public-private partnerships, awareness, incident response, and international cooperation. Addressing these challenges is crucial for sustainable development and economic growth in the digital era.			
2/119	2023-09-06	Kenya	The Authority's Child Online Protection and Safety Programme in Kenya: A case study on the implementation of the ITU's Guidelines on Child Online Protection
Shares the implementation of child online protection initiatives since 2011, by the Communications Authority of Kenya (CA), focusing on raising awareness and promoting responsible Internet usage. The CA has launched two campaigns, "Be The COP" and "*Huwezi Tucheza, Tuko Cyber Smart*," targeting parents, guardians, teachers, and children. The authority collaborates with various stakeholders, including government agencies, industry players, and NGOs, to implement the ITU Guidelines on Child Online Protection. Initiatives include legal and regulatory frameworks, reporting mechanisms, research and surveys, national strategies, industry initiatives, educational resources, capacity building, and national awareness campaigns.			
2/115	2023-09-04	Democratic Republic of the Congo	Digitalization of public services in the Democratic Republic of the Congo: key challenges and requirements for information security and cyberdefence
Presents the implementation of cybersecurity measures, including the enactment of Law No. 20/017 in 2020, and the adoption of a digital code in 2023. The country is working on creating a computer incident response team (CIRT) and improving its broadband infrastructure with a planned 50 000 km of optical fibre network. Cooperation and public awareness-raising are also essential components of their cybersecurity strategy.			
2/112	2023-08-21	Kenya	CSIRT/CIRT approaches and experiences towards the resilience of critical infrastructure in Kenya
Introduces the establishment of the National Computer Incidents Response Team (KE-CIRT) by the Communications Authority of Kenya to mitigate cyber threats and ensure a safer cyberspace. The country has a legal framework defining critical infrastructure and has adopted a cybersecurity framework supported by policy and operational frameworks. Challenges faced include a rapidly evolving threat landscape, lack of international cooperation, insufficient expertise, limited resources, balancing privacy and security, coordination and information sharing, technological advancements, insider threats, public-private collaboration, and public awareness and education.			
2/98	2023-07-25	Australia	Australia's national online safety awareness campaign

(suite)

Web	Received	Source	Title
Introduces the Online Safety Act 2021, to keep pace with new technology and emerging online threats. The Online Safety campaign aimed to raise public awareness of the Online Safety Act and the strengthened laws for online safety. The campaign targeted various audience groups and successfully drove traffic to the eSafety Commissioner website.			
RGQ2/85	2023-05-18	Beihang University	Development of policies and legislation to protect consumer rights and interests in China in the digital era
China attaches great importance to the protection of consumer rights and interests. Firstly, in terms of policy guidance, the goal is to improve the consumer environment, strengthen consumer rights protection, and achieve social fairness and justice, adhering to the equal emphasis on development and regulation; Secondly, in terms of the legal system, China has steadily promoted the formulation and implementation of laws, regulations, and standards related to consumer rights protection. It has continuously strengthened the protection of consumers' digital rights and focused on the special protection of vulnerable consumers, gradually forming a comprehensive and three-dimensional legal system for consumer rights protection to adapt to the new development and needs of consumer rights protection. The content of this paper is based on the policy and legislative protection of consumer rights in China's new development pattern, so as to provide assistance for the international consumer rights protection cause.			
RGQ2/80	2023-05-10	Russian Federation	Information sharing practices to protect children from disruptive online content - Award "For a Safe Digital Childhood"
Presents its contribution which contained information on some practices on the exchange of information between two Russian Federation federal executive bodies to protect children from destructive online content, as well as information about the award "For a Safe Digital Childhood" by Alliance for the Protection of Children in the Digital Environment, aimed at supporting projects to develop a safe digital environment throughout the Russian Federation.			
RGQ2/79	2023-05-10	Russian Federation	National computer incident response and coordination centre - information security leaders
Presents a contribution on the operation of its National Computer Incident Response & Coordination Centre (NCIRCC) to ensure a stable critical infrastructure, as well as approaches regarding the appointment of leaders in the field of information security. In response to questions received during the meeting, the Russian Federation clarified that NCIRCC is not the only such centre, and the main criteria for leaders in the field of information security is not only their professional degree, but also wide-ranging experience and relevant professional skills.			
RGQ2/74	2023-05-09	United Kingdom	TBEST: an example of outcome-based pen-testing for communications providers to help improve their network security posture

(suite)

Web	Received	Source	Title
Contribution on the TBEST scheme, an example of cybersecurity assurance practice that Ofcom, the United Kingdom regulator, runs voluntarily with communications providers. TBEST is a penetration testing that aims to stimulate a cyber-attack in telecommunications networks in order to identify security vulnerabilities which can then be, through a process of remediation, addressed to improve the operators' network security posture. The contribution provides an overview of the process, and the various stakeholders involved. More broadly, this scheme is an example of supervisory policy approach that Ofcom is taking, which stresses the importance of building collaborative relationships with the industry that Ofcom regulates. To date, all communications providers in the United Kingdom have already or are undergoing the TBEST scheme voluntarily and have implemented changes as a result. TBEST is not a "standard" nor a certification process. The goal is to enable communications providers to gain awareness of cyber threats and implement appropriate changes in a timely manner to improve their cyber defence capabilities. By being aware of, and addressing such vulnerabilities and weaknesses, the operator is in a much stronger position to protect their networks.			
RGQ2/66	2023-05-10	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated. The presentation addressed the ITU cybersecurity mandate, and through BDT, work on the national CIRT programme, regional and national cyberDrills, the Global Cybersecurity Index (GCI), national cybersecurity strategy (NCS) assistance, Women in Cyber, Her CyberTracks, child online protection, partnerships and collaboration, and Cyber for Good. The document emphasizes the importance of collaboration, partnerships, and resource mobilization to allow ITU to fulfil its mandate, considering the extensive list of tasks that membership have requested BDT to undertake. BDT also presented information about the 5th edition of the Global Cybersecurity Index.			
RGQ2/58	2023-04-27	Brazil	Cybersecurity assurance practices - Brazil experience
Introduces the contribution referring to the efforts of the Brazilian National Telecommunications Agency (ANATEL) regarding the establishment of cybersecurity minimum requirements for telecommunication equipment. ANATEL initially adopted a non-mandatory approach (Act 77/2021), which evolved into a cybersecurity compulsory certification requirement for a specific set of equipment (Act 2436/2023). This evolution was only possible with a comprehensive debate within the sector.			
RGQ2/57	2023-07-27	Brazil	Brazilian cybersecurity-related policies and regulations
Presents an overview on the cybersecurity-related policies and regulations that have been developed in Brazil in recent years, including the National Information Security Policy, the National Cybersecurity Strategy, the Cybersecurity Regulation for the Telecommunication Sector, the Federal Cyber Incident Management Network, and the 5G Spectrum Auction Notice. There were questions about the modular approach adopted by the National Information Security Policy, and the Brazilian delegation explained that in Brazil cybersecurity is one of the elements of Information Security.			
RGQ2/53	2023-04-25	Mexico	Privacy reports on user information in the use of digital platforms

(suite)

Web	Received	Source	Title
Presents the Privacy Reports, which purpose is to make available in a clear, simple and transparent manner the privacy policies of operating systems, terminal equipment, social networks, and digital platforms that enable the provision of services such as: online commerce, transport and entertainment. These reports published by the Federal Telecommunications Institute help users to learn about the information that is collected by the platforms, and how this information is treated, and helps users make responsible use of such platforms. The Reports also empower users by providing transparent information about privacy policies.			
RGQ2/51	2023-04-25	Mexico	Internet of Things Devices Catalog
The *Internet of Things Devices Catalogue* is an electronic tool that allows users of telecommunication services to know the main characteristics of IoT devices, as well as the privacy policies defined by the manufacturers. The IoT devices published are those that are marketed in Mexico and have been certified by the Federal Telecommunications Institute. The tool allows users to be empowered with transparent information about privacy policies and the characteristics of terminal equipment that comply with technical regulations, for informed decision-making and for the proper use of IoT equipment.			
RGQ2/48	2023-04-25	Access Partnership Limited	Cybersecurity assurance practices - international standards and satellite communications
Contains information related to developing cybersecurity assurance practices for commercial satellite operators, as well as highlighting some of the existing general cybersecurity assurance practices which may be adopted by any commercial satellite operator, including ISO 27001. The contribution noted some of the unique cybersecurity threats which need to be overcome in satellite operations, including the cross-jurisdictional nature of satellite operations, and the vulnerabilities of ground stations. The contribution explained specific technical standards including the ETSI technical standard 103 732 and its measures to protect consumer mobile devices, as an example of standards towards specific technology which could inform the further development of standards for commercial satellite operators.			
RGQ2/44	2023-04-24	South Africa	The domain name cybersecurity culture
Provides a contribution concerning the security of the country code top-level domain name (.za). The South African Domain Name Authority (ZADNA) manages the .za domain namespace under the mandate of the Electronic Communications and Transactions Act (ECTA). Its policy framework was designed to ensure a secure, resilient, and efficiently managed domain namespace, promoting stakeholder engagement, growth of the namespace, policy compliance, and entrance of new Internet service providers. ZADNA also addresses cybersecurity threats through education and awareness programmes, alternative dispute resolution (ADR) workshops and regulations, and DNS training courses. Additionally, it adheres to international standards for dispute resolution, working in line with the World Intellectual Property Organization (WIPO) and organizations such as the South African Institute of Intellectual Property Law (SAIIPL) and the Arbitration Foundation of Southern Africa.			
RGQ2/38	2023-04-13	Australia	Sharing advice from Australia on securing smart places

(suite)

Web	Received	Source	Title
Shares information on the lessons learned by the Australian Cyber Security Centre in response to risks identified for smart places. The contribution defined smart places as those designed to provide enhanced services through the use of smart information and ICT enabled systems and devices. The contribution noted that the highly connected nature of smart places makes them vulnerable to intrusions. This is exacerbated when the system scales. The contribution gave examples of Australian policies used to protect the various aspects of smart cities including IoT, supply chains, operational technology and cloud computing. The contribution also raised several examples of strategies which may be employed to mitigate security risks as well as ensuring operational redundancy.			
RGQ2/34	2023-04-06	Republic of Korea	Cloud Security Assurance Program (CSAP) in South Korea
Introduces the Cloud Security Assurance Programme (CSAP), a security certification for cloud computing services that meet security certification standards to improve and guarantee information protection levels. The purpose of the CSAP is to provide private cloud services with proven safety and reliability to national and public institutions. Also, it aims to implement an objective and fair security certification system for cloud services to address user security concerns and secure competitiveness of cloud services. The CSAP provides a number of benefits. By certifying the security level of a cloud system, CSAP helps to improve the cyber resilience of national and public institutions. This can also help to ensure that sensitive information is protected and that cloud services are reliable.			
RGQ2/29	2023-03-30	Côte d'Ivoire	Policy and strategy of Côte d'Ivoire for building a trusted digital space
Shares the initiatives taken by Côte d'Ivoire in its efforts to build digital trust, which concerns all economic sectors that use ICTs, such as media and communication, transport, health, industry, telecommunications and computing, distribution of goods and consumption, construction, finance and insurance, tourism, agriculture and e-commerce. To consolidate the freedom of online public communication and ensure interactions are secure, Côte d'Ivoire has enhanced the means for combating cybercrime and protecting personal data in order to build trust in cyberspace. Cybersecurity has become an issue of privacy, competitiveness and national sovereignty. A capacity to anticipate, build trust and protect personal data is essential. In this sense, the country has updated its legal and institutional framework, setting a visionary policy to enhance digital trust by 2025. The country has established a Consultative Committee for Digital Trust (CCCN) and a Consultative Committee for the Protection of Personal Data (CCDCP).			
RGQ2/20	2023-03-22	Nigeria	Child Online Protection practices in Nigeria
Presents its efforts in regard to child online protection through the Nigerian Communications Commission (NCC), the independent national regulatory authority for the telecommunication industry, in collaboration with the Office of the National Security Adviser in Nigeria who works with other stakeholders to ensure child protection in Nigeria's cyber space. It was decided by the meeting to liaise with the Council Working Group on Child Online Protection (CWG-COP) to share the relevant experiences shared by Nigeria.			
2/80	2022-11-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken by BDT and new initiatives to enhance cybersecurity in ITU Member States: CIRT programme, regional and national cyberdrills, national cybersecurity strategy (NCS) , work related to Bridge the Cybersecurity Divide: Cyber for Good project, work on promoting a diverse and inclusive cybersecurity community through the Women in Cyber Mentorship Programme and Youth4Cyber initiative, child online protection, and partnerships and collaboration initiatives.			

(suite)

Web	Received	Source	Title
2/77	2022-11-22	United Kingdom	Sharing experience from the UK on promoting and developing cybersecurity skills
Outlines the country's policy approach to address the cyber skills gap which, in addition to the final report of the study cycle, can also be included in a future repository of good practices as agreed through Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference. The United Kingdom's initiatives are focused in three areas: (1) cyber skills for young people, (2) cyber skills for adults, and (3) developing the cyber profession.			
2/74	2022-11-18	World Bank	World Bank Study Group 2 Submission: Digital transformation
Highlights their readiness to support the least developed client countries with a special emphasis on fragility, conflict and violence (FCV) and small island developing states (SIDS). Through the analytical work programme and strategic partnerships, the World Bank is working closely with client countries on issues related to the SG2 Questions' scopes. Relevant examples from the World Bank around using ICT services and applications for the promotion of transformative and sustainable development are provided in the contribution. For instance, one relating to cybersecurity is the Cybersecurity Multi-Donor Trust Fund, being a part of the broader Digital Development Partnership umbrella programme, aims at systematically incorporating cybersecurity in the development agenda as well as in World Bank operational programmes. Work includes building global knowledge to better define the cybersecurity development agenda, and country-specific technical assistance.			
2/71 (Rev.1)	2022-11-18	Russian Federation	New practices of the Russian Federation in the field of creating a culture of cybersecurity
Presents the Russian Federation Cyber Hygiene Program, launched in August 2022. The programme is planned for a three year period and includes various activities aimed at attracting the attention of citizens of the Russian Federation to the issues of cybersecurity and the training in skills on safe behaviour on the Internet. Large-scale information campaigns are one part of the programme. Citizens were segmented into age groups, and their online behaviour and the type of digital content consumed were taken into account. Based on this segmenting approach, more specifically targeted means of information dissemination could be applied for the 3 segmented groups of population (12-18 / 18-45 / 45+ years old). The contribution also covers the means of improving the information security literacy of civil servants, as well as the results of an all-Russian Federation study of the citizens' information security literacy.			
2/35	2022-10-12	Rwanda	National cybersecurity initiatives: current status
Highlights the programmes and initiatives put in place to guarantee the security and resilience of Rwanda's cyberspace. To support national economic growth and social mobility, the Government of Rwanda (GoR) is actively deploying various information technologies and has made major investments in ICT infrastructure and applications. GoR established the National Cybersecurity Authority (NCSA) as the authority to spearhead the implementation of National Cyber Security policies and strategies. Additionally, GoR established a law relating to protecting personal data and privacy and passed the prevention and punishment of cybercrimes law. NCSA roles include: coordinating national cybersecurity functions across the private and public sectors; promoting national education programmes and fostering awareness of cybersecurity good practices amongst the Rwandan population; operating the Rwanda Computer Security Incident Response Team (Rw-CSIRT); and overseeing the implementation of the Protection of Personal Data and Privacy Law. Furthermore, the Rwanda Utilities Regulatory Authority (RURA), Regulation No. 010/R/CR-CSI/RURA/020 OF 29/05/2020), Rwanda Information Society Authority (RISA), and capacity building collaborations and initiatives have been put in place to ensure preparation in preventing and responding to evolving cyber threats.			

(suite)

Web	Received	Source	Title
2/34	2022-10-12	Côte d'Ivoire	Initiatives to support children and young people, national strategy for the protection and empowerment of children and young people online: the experience of Côte d'Ivoire
Presents an initiative undertaken by Côte d'Ivoire to protect children against the dangers and threats of using ICTs. The initiative, www.jemeprotegeenligne.ci is a website targeted at children between 5 and 19 years old as well as teachers and parents with the goal of educating children and young people and raising awareness.			
2/30	2022-10-11	Côte d'Ivoire	Proposal for State actions and initiatives to foster a culture of cybersecurity and ensure that information and communication networks are secure: the case of Côte d'Ivoire
Contextualizes cyberattacks and threats as a major concern for governments in this increasingly connected world, particularly in developing countries. Cybersecurity is now the priority issue for many States. This contribution gives an overview of the cybersecurity situation in developing countries, notably Côte d'Ivoire, and highlights strategies for raising user awareness and experience-sharing among Member States.			

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
2/410 +Ann.1	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 LS on update on the work of the Correspondence Group on Child online protection (CG-COP)
2/409	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development
2/241	2024-09-11	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Groups 1 and 2 on SG17 update on the work of the Correspondence Group on Child online protection (CG-COP)
RGQ2/151	2024-03-18	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 1 Question 6/1 and ITU-D Study Group 2 Question 3/2 on Establishment of the Correspondence Group on Child online protection (CG-COP)
RGQ2/107	2024-02-12	Chairman, ITU Council Working Group on COP	Liaison statement from ITU Council Working Group on COP to ITU-D Study Group 2 Question 3/2 on child online protection
RGQ2/83	2023-03-08	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on status of security studies in ITU-T SG17
2/20	2022-06-16	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development

Annex 2: List and summary of BDT on-going cybersecurity activities

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Data	Global Cybersecurity Index v5	ITU Member States	GCI Expert Group	Global Cybersecurity Index report and country reports. Link
Governance	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau	Guinea-Bissau	Government of Guinea-Bissau	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau with the aim to empower Guinea-Bissau's cybersecurity ecosystem by guiding key national stakeholders in developing strategic approaches to CIRT implementation and enhancing cybersecurity in Guinea-Bissau
Governance	Mauritania's Cybersecurity Governance Development	Mauritania	Government of Mauritania	Sessions to enhance of a national cybersecurity governance framework to enable Mauritania to strengthen the protection of the critical information systems of official institutions and vital operators, the fight against cybercrime, awareness raising, training, confidence-building in digital, more effective regional and international integration through cooperation.
Governance	National cyber risk assessment	Lesotho	Ministry of Communications Science and Technology	Workshop to enhance strategic thinking on cybersecurity governance among key national stakeholders, thereby advancing the objectives of Lesotho's National Cybersecurity Strategy.
Governance	Strengthening Critical Information Infrastructure Resilience	Cambodia	Ministry of Post and Telecommunications Cambodia (MPTC, Japan International Cooperation Agency (JICA)	Workshops on technical incident response, national cybersecurity strategy, and crisis management for critical information infrastructure stakeholders
Governance	Tabletop Exercise and a Cybersecurity Incident Simulation Exercise	ITU Arab States region Member States	CSC UAE	Tabletop exercise centred around cyber-attack directed at a financial institution.
Incident Response	13th Event of Cyber Capacity Building in America - Andino	ITU Americas region Member States	Ministry of Popular Power for Science and Technology of Venezuela, National Commission of Information Technologies (CONATI), Superintendency of Electronic Certification Services (SUSCERTE)	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	Americas Regional CyberDrill	ITU Americas region Member States	INICTEL-UNI, Peruvian Ministry of Transportation and Communications, General Secretariat of the Andean Community	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CIRT Establishment in Bahamas	Bahamas	Government of Bahamas	Building and deploying the technical capabilities and related training necessary to develop Bahamas national cybersecurity strategy and to establish its National Cybersecurity Incident Response Team (CIRT). Link

(suite)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Incident Response	CIRT Maturity Assessment	Timor-Leste	ANC	Conducted Maturity Assessment of country CIRT through series of workshops, discussions, and inventories, providing recommendations for the Timor-Leste computer security incident response team (TLCSIRT) in collaboration with the Autoridade Nacional de Comunicações (ANC) to ensure TLCSIRT can enhance its cybersecurity maturity level. Link
Incident Response	Cyber 100x Global Cyber-Drill 2024	ITU Member States	Cyber Security Council United Arab Emirates	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CyberQ	ITU Member States	United Arab Emirates Cybersecurity Council	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Included specific trainings for women. Link
Incident Response	Cybersecurity Forum and CyberDrill for Europe and the Mediterranean	ITU Europe region and Arab States region Member States	Ministry of Transport and Communications of Bulgaria, Ministry of Electronic Governance of Bulgaria	Cybersecurity forum featuring trends and challenges, CSIRTs capacity-building training, and two days of cyberdrill exercises with emerging attack scenarios and collaborative learning sessions. Link
Incident Response	ITU National CyberDrill for Armenia	Armenia	Ministry of High-Tech Industry of Armenia	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Asia-Pacific CyberDrill	ITU Asia and the Pacific region Members States	Cyber Security Brunei (CSB)	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Cybersecurity Readiness Exercise	ITU Arab States region Member States	Directorate General for Information Systems Security (DGSSI) Morocco	Incident response trainings, discussions, and information sharing. Link
Incident Response	National CIRT Establishment in Gambia	Gambia	Ministry of Information and Communication Infrastructure (MOICI)	Assist MOICI in building and deploying the technical capabilities and related trainings necessary to establish its national CIRT. Link
Incident Response	National Computer Incident Response Team (CIRT) Implementation – Suriname	Suriname	e-Government Directorate, Cabinet of the President of Suriname	Support for operationalization of Computer Incident Response Team. Link
Incident Response	Regional Cybersecurity Week	ITU Arab States region Member States	ARCC Oman	Regional Cybersecurity Conference focusing on "Cybersecurity as an enabler for the Digital Economy", the FIRST Organization Seminar, and the Regional and OIC-CERT Cyber Drill. Link
Incident Response	Rwanda National CyberDrill	Rwanda	Rwanda National Cyber Security Authority, Ministry of Foreign Affairs of the Czech Republic	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link

(suite)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Incident Response	Twelfth Edition of the Regional Cyberdrill for Africa Region (ITU-INTERPOL CyberDrill)	ITU Africa region Member States	Ghana's Cyber Security Authority (CSA), INTERPOL	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Partnerships	Cyber for Good	Least developed countries (LDCs)	Axon Consulting, BitSight Technologies, CTM360, DreamLab Technologies, ImmuniWeb, WelchmanKeen	Tools, trainings, and services offered for free to Least Developed Countries. Link
Skills Development	Child Online Protection National Assessment - Andorra	Andorra	SWGfL/UK Safer Internet Centre	Child Online Protection National Assessment with the national stakeholder consultation event
Skills Development	Child Online Protection Train the Trainers and Cybersecurity briefings - Maldives	Maldives	National Centre for Information Technology (NCIT)	Trainings on Child Online Protection as well as briefings on key topics. Link
Skills Development	Creating a Safe and Prosperous Cyberspace for Children	ITU Member States	CTO, CNIL, Council of Europe, European Commission, EC-Council, EBU, Europol, ILO, Interpol, MICITT, NCA KSA, OECD, United Nations Human Rights Special Procedures, UNICRI, UNESCO, UNICEF, UNODC, WIPO, World Bank, UC Berkley, LSE, Middlesex University London, Western Sydney University, Youth and Media, BBC, Disney, Ericsson, worldwide Group, Facebook, IBM, IEEE, Microsoft, Sony, TIM, Privately, Tencent, TrendMicro, Twitter, ASCSA, ACOPEA, 5Rights Foundation, ASDRA, Child Helpline International, Child Rights Connect, Family Online Safety Institute, Childhood, ChildOnline Africa, DeafKidz International, DISC Foundation, Families Europe, Halley Movement, End Violence Against Children, DOInstitute, ecpat, Fard Digital, HABLATAM, Cuber Coluntarios.org, Global Kids Online, GSMA, iKeepSafe, Inclusion international, InHope, Ins@fe, International Centre for Missing & Exploited Children, International Disability Alliance, Internet Matters, Internet Watch Foundation (IWF), Human Trafficking Front, ParentZone, Plan International, RNW media, Save the Children, Paniamor, Stiftung digitale chancen, SWGfL, Tech Coalition, terre des hommes suisse, United Kingdom Safer Internet Centre, WeProtect Global Alliance, Wise Kids, World Economic Forum, YouthIGF, Together Against Cybercrime	Advocacy, research, and in-country programmes related to Child Online Protection. Link

(suite)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Skills Development	Her CyberTracks 2024	Algeria, Angola, Bahrain, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cabo Verde, Central African Republic, Comoros, Chad, Côte d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Iraq, Jordan, Kenya, Kuwait, Lebanon, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Oman, Qatar, Republic of the Congo, Rwanda, São Tomé and Príncipe, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, State of Palestine*, Sudan, Syrian Arab Republic, Tanzania, Togo, Tunisia, Uganda, United Arab Emirates, Yemen, Zambia, Zimbabwe	GIZ, Microsoft	Her CyberTracks provides specialized, targeted training, maintaining the essential mentorship and role modelling aspects. The programme is poised to propel the next generation of women in cybersecurity into roles of leadership, ensuring that their voices and expertise shape the future of this critical field through training, mentorship, and inspiration across three tracks: Policy & Diplomacy, Incident Response, and Criminal Justice (implemented by UNODC). Link
Skills Development	Translation of Child online protection guidelines and capacity building activities - Albania	Albania	National Authority on Electronic Certification and Cyber Security	Child online protection guidelines translated into Albanian and the roll out of capacity-building activities
Skills Development	Translation of Child online protection guidelines and capacity building activities - Malta	Malta	SWGfL/UK Safer Internet Centre	Child online protection guidelines translated into Maltese and the roll out of capacity-building activities

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

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

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

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

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

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

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

Afrique

Ethiopie

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

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

Cameroun

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

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

Sénégal

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

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

Zimbabwe

International Telecommunication Union (ITU) Bureau de zone
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Courriel: itu-harare@itu.int
Tél.: +263 242 369015
Tél.: +263 242 369016

Amériques

Brésil

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

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

La Barbade

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

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

Chili

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

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

Honduras

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

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

Etats arabes

Egypte

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

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

Asie-Pacifique

Thaïlande

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

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

Indonésie

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

Courriel: bdt-ao-jakarta@itu.int
Tél.: +62 21 380 2322

Inde

International Telecommunication Union (ITU) Area Office and Innovation Centre
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
Inde

Courriel:
Bureau régional: itu-ao-southasia@itu.int
Centre d'innovation: itu-ic-southasia@itu.int
Site web: ITU Innovation Centre in New Delhi, India

Pays de la CEI

Fédération de Russie

International Telecommunication Union (ITU) Bureau régional
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Fédération de Russie
Courriel: itu-ro-cis@itu.int
Tél.: +7 495 926 6070

Europe

Suisse

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

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

ISBN 978-92-61-41102-2

Publié en Suisse
Genève, 2025

Photo credits: Adobe Stock