ITU Publications
Période d'études 2018-2021

Union internationale des télécommunications
Secteur du développement

Commission d'Études 2 Question 3

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

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

Période d'études 2018-2021

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

978-92-61-34102-2 (version électronique)
978-92-61-34112-1 (version EPUB)
978-92-61-34122-0 (version Mobi)

Libellé proposé: 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 2018-2021. Genève: Union internationale des télécommunications, 2021. Licence: CC BY-NC-SA 3.0 IGO.

Crédits photos couverture: Shutterstock

Remerciements

Les commissions d'études du Secteur du développement des télécommunications de l'UIT (UIT-D) offrent un cadre neutre permettant à des experts issus du secteur public, du secteur privé, d'organisations de télécommunication et d'établissements universitaires du monde entier de se réunir, afin d'élaborer des outils pratiques et des ressources pour examiner les questions touchant au 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. La Conférence mondiale de développement des télécommunications (CMDT) décide de mettre à l'étude des Questions tous les quatre ans. Les membres de l'UIT, réunis à la CMDT-17 tenue à Buenos Aires en octobre 2017, ont décidé que pendant la période 2018-2021, la Commission d'études 2 serait chargée de l'étude de sept Questions, qui s'inscrivent dans le cadre général des "services et applications reposant sur les technologies de l'information et de la communication pour promouvoir le développement durable".

Le présent rapport a été élaboré au titre de la Question 3/2, intitulée **"Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité"**, sous la supervision et la coordination générales de l'équipe de direction de la Commission d'études 2 de l'UIT-D, dirigée par M. Ahmad Reza Sharafat (République islamique d'Iran), Président, secondé par les Vice-Présidents suivants: M. Nasser Al Marzouqi (Émirats arabes unis) (qui a démissionné en 2018); M. Abdelaziz Alzarooni (Émirats arabes unis); M. Filipe Miguel Antunes Batista (Portugal) (qui a démissionné en 2019); Mme Nora Abdalla Hassan Basher (Soudan); Mme Maria Bolshakova (Fédération de Russie); Mme Celina Delgado Castellón (Nicaragua); M. Yakov Gass (Fédération de Russie) (qui a démissionné en 2020); M. Ananda Raj Khanal (République du Népal); M. Roland Yaw Kudozia (Ghana); M. Tolibjon Oltinovich Mirzakulov (Ouzbékistan); Mme Alina Modan (Roumanie); M. Henry Chukwudumeme Nkemadu (Nigéria); Mme Ke Wang (Chine); et M. Dominique Würges (France).

Ce rapport a été rédigé sous la direction des Corapporteurs pour la Question 3/2, à savoir M. Michael Beirne (États-Unis) (qui a démissionné en 2020); M. Kwadwo Burgee (États-Unis) (qui a démissionné en 2020); Mme Aimee K. Meacham (États-Unis); et M. Dominique Würges (France), en collaboration avec les Vice-Rapporteurs suivants: M. Damnam Kanlanfei Bagolibe (Togo); M. Amine Adoum Bakhit (Tchad); Mme Maria Bolshakova (Fédération de Russie); Mme Sonam Choki (Bhoutan); M. Yakov Gass (Fédération de Russie) (qui a démissionné en 2020); M. Karim Hasnaou (Algérie); M. Cissé Kane (Société civile africaine pour la société de l'information); Mme Miho Naganuma (Japon); M. Jean-David Rodney (Haïti); Mme Jabin Vahora (États-Unis); Mme Xinxin Wan (Chine); M. Jaesuk Yun (République de Corée); et M. Mohamadou Zarou (Mali).

Nous remercions tout particulièrement les coordonnateurs des chapitres pour leur appui, leur travail inlassable et leurs compétences techniques.

Le présent rapport a été élaboré avec le concours le concours des coordonnateurs du BDT, des éditeurs, ainsi que de l'équipe du Service de la production des publications et du secrétariat des Commissions d'études de l'UIT-D.

Table des matières

Liste des tableaux et figures

Tables

Figure

Résumé analytique

L'objectif de la Question 3/2 ("Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité") du Secteur du développement des télécommunications de l'UIT (UIT-D) est d'élaborer des rapports sur les bonnes pratiques concernant divers aspects de la cybersécurité.

Le présent document constitue le rapport final sur la Question 3/2 pour la période d'études quadriennale la plus récente (2018-2021), pour laquelle le programme de travail au titre de la Question 3/2 a été défini par la Conférence mondiale de développement des télécommunications qui s'est tenue à Buenos Aires en 2017 (CMDT-17).

Les activités menées lors des dernières périodes d'études étaient axées sur les différentes formations disponibles (2010-2014) et l'organisation d'ateliers visant à rassembler un large éventail d'acteurs et à mettre leurs contenus à la disposition des pays en développement (2014-2017).

Durant la période d'études 2018-2021, la Commission d'études 2 de l'UIT-D a traité la plupart des points du programme de travail. Un atelier a aussi été organisé au cours de cette même période d'études.

Le présent rapport sur la Question 3/2 s'appuie sur les éléments fournis dans les contributions des membres de l'UIT soumises pendant cette période d'études. Le rapport présente une vue d'ensemble de la question du spam et des logiciels malveillants et des moyens d'y remédier. Il expose un certain nombre d'enseignements pour la planification des interventions nationales en matière de cybersécurité et des campagnes de sensibilisation. Il met en avant les actions particulières à mener en faveur des populations vulnérables, notamment les personnes handicapées et les enfants. En outre, le rapport contient des idées sur les villes intelligentes, les technologies émergentes et la protection des données.

Dans le monde numérique actuel, où la vie quotidienne des citoyens et les économies dans leur ensemble sont devenues de plus en plus dépendantes des technologies numériques, il existe un risque accru de devenir plus vulnérable et plus exposé aux cyberattaques. La cybersécurité a été identifiée comme étant une priorité et une préoccupation majeure du secteur privé, des gouvernements et des internautes dans le monde entier, et elle est essentielle à un progrès sûr et sécurisé qui permet à la société de se développer.

Le présent rapport vise à fournir des réflexions et des pratiques actualisées fondées sur l'expérience des membres de l'UIT. Partant du constat que l'environnement général et le paysage des menaces sont en constante évolution, il se veut simplement un instantané de la situation actuelle dans ce domaine très sensible de la cybersécurité. Ce rapport est également publié dans un contexte très particulier et inédit: bien qu'il ne comprenne pas de références spécifiques à la pandémie actuelle, les répercussions du COVID-19 ont été dans l'esprit de nombreux contributeurs et ont influencé les débats au cours des activités menées au titre de la Question 3/2.

Les réponses et les propositions compilées dans le présent rapport visent à contribuer à atteindre un niveau élevé de cybersécurité parmi les membres de l'UIT et peuvent également

servir d'outil utile permettant de faire face à d'éventuelles crises futures, en plus des autres actions entreprises par l'UIT.

Le **Chapitre 1** fait le point sur la situation du spam, des logiciels malveillants et des mesures d'atténuation. Il est à noter que la Commission d'études n'a pas reçu de contributions directes sur cette question.

Le **Chapitre 2** porte sur l'amélioration des choix nationaux en matière de cybersécurité par le biais de la sensibilisation et du renforcement des capacités.

Le **Chapitre 3** fournit des informations sur les activités de protection en ligne des enfants.

Le **Chapitre 4** traite des problèmes en matière de cybersécurité pour les personnes handicapées.

Le **Chapitre 5** porte sur les problèmes de cybersécurité associés aux technologies émergentes comme l'Internet des objets (IoT) et l'informatique en nuage.

Le **Chapitre 6** présente des pistes de réflexion sur la manière dont la cybersécurité peut contribuer à la protection des données à caractère personnel.

Enfin, le **Chapitre 7** est consacré aux domaines futurs à examiner.

Outre le présent rapport, il convient également de noter que la Question 3/2 a permis de revoir le questionnaire servant de base à l'Indice mondial de cybersécurité (GCI) et de formuler des commentaires et des propositions, ce qui a permis au Bureau de développement des télécommunications (BDT) de mener son enquête annuelle auprès des États Membres de l'UIT. En particulier, et à l'initiative du Brésil, les responsables de la Question 3/2 ont contribué à l'élaboration de l'enquête, qui a été intégrée dans le GCI en tant qu'annexe. Les révisions proposées ont été incluses dans la quatrième édition du GCI 2020.

Le présent rapport ne traite pas du GCI de manière approfondie. Néanmoins, les responsables de la Question 3/2 mettent en avant les retombées positives de l'effort collectif et de la collaboration enrichissante avec le BDT, puisque les réponses à l'enquête fourniront des informations sur les politiques réglementaires que le BDT mettra à la disposition des membres, conformément au point "n" du mandat relatif à la Question 3/2.

Chapitre 1 – Spam, logiciels malveillants et mesures d'atténuation: le point sur la situation

La présente section traite de l'évolution du spam et des logiciels malveillants et présente un certain nombre de contre-mesures à mettre en œuvre aux niveaux national, régional et international, conformément à la Résolution 45 (Rév.Dubaï, 2014) de la Conférence mondiale de développement des télécommunications (CMDT)[1] sur les mécanismes visant à renforcer la coopération en matière de cybersécurité, y compris la lutte contre le spam. Elle répond ainsi aux points 2(b) et (m) du mandat relatif à la Question 3/2 figurant dans le rapport final de la CMDT-17:

b) examiner les méthodes et les bonnes pratiques permettant d'évaluer les incidences du spam et des logiciels malveillants sur un réseau, ainsi que les menaces émergentes et en évolution, et proposer les éléments d'information nécessaires pour les mesures et les lignes directrices, notamment les techniques de lutte contre le spam et les aspects législatifs et réglementaires auxquels les pays peuvent avoir recours, compte tenu des normes existantes et des outils disponibles;

m) fournir des orientations concernant les mesures pour lutter contre le spam et les logiciels malveillants aux niveaux national, régional et international[2].

1.1 État des lieux du spam et des logiciels malveillants

Bien qu'il n'existe aucune définition universellement acceptée du spam, il désigne généralement les communications électroniques non sollicitées en masse transmises par des ordinateurs ou des téléphones mobiles par courrier électronique et par messages texte[3]. Les consommateurs voient généralement le spam sous forme de publicité, y compris des courriers électroniques commerciaux poubelle ou inopportuns, des textes et des contacts dans les réseaux sociaux.

Bien que le spam soit généralement synonyme de prospection commerciale, il peut également utiliser des données similaires générées par les utilisateurs à des fins criminelles, y compris l'hameçonnage. En se faisant passer pour des tiers de confiance, les attaquants utilisent des courriers électroniques d'hameçonnage pour encourager les destinataires à révéler des données personnelles (comptes d'accès, mots de passe, etc.) et/ou des données bancaires.

Le spam crée des risques pour la sécurité des utilisateurs et des organisations connectés, non seulement parce qu'il est facilement diffusé via l'Internet et les services de communication électronique (courrier électronique, sites web, réseaux sociaux, SMS et MMS), mais aussi parce qu'il peut véhiculer des logiciels malveillants. Les pays mettent en œuvre divers mécanismes techniques et réglementaires pour lutter contre le spam, avec un certain succès.

---

1 UIT, Rapport final de la Conférence mondial de développement des télécommunications (Buenos Aires, 2017), p. 409.
2 Ibid., pp. 727-728.
3 Voir les Recommandations UIT-T X.1230 à X.1240 sur la lutte contre le spam.

Les logiciels malveillants, pour leur part, ont connu une forte croissance ces dernières années en raison du développement de l'Internet et, plus particulièrement, de l'Internet mobile. Les logiciels malveillants sont un terme général qui désigne les logiciels conçus spécifiquement pour nuire aux ordinateurs ou aux systèmes informatiques[4].

De plus, l'augmentation de la connectivité, les nouvelles technologies et l'accroissement du nombre d'utilisateurs ont ouvert de nouvelles possibilités de création et d'utilisation de logiciels malveillants. Cette situation engendre une plus grande complexité pour la cybersécurité en ouvrant des brèches et en élargissant les surfaces d'attaque disponibles pour les menaces de logiciels malveillants. Outre les logiciels malveillants traditionnels (virus, vers, chevaux de Troie, logiciels espions, logiciels publicitaires, spam, outils de dissimulation d'activité (rootkits), etc.), de nouveaux types de logiciels malveillants plus évolués sont apparus, comme les botnets, les rançongiciels et les logiciels malveillants mobiles.

En bref, la lutte contre le spam et les logiciels malveillants est essentielle pour la sécurité des utilisateurs et la croissance des entreprises.

1.2 Spam et logiciels malveillants: statistiques, tendances, évolution et incidences sur les réseaux de communication électronique

En mars 2020, la proportion de spam dans le trafic mondial de courrier électronique était de 53,95%[5]. Ces dernières années, ce pourcentage a considérablement diminué, passant de 69% en 2012 à 55% en 2018, peut-être en raison des progrès de la sensibilisation à la cybersécurité et des avancées technologiques. La plupart des spams reçus par les utilisateurs sont de nature promotionnelle et incluent des informations commerciales. Selon une estimation, le spam coûte chaque année aux entreprises près de 20,5 milliards USD en perte de productivité et en dépenses techniques. Il a été avancé que ce coût pourrait atteindre 257 milliards USD par an si le spam continuait à se développer au rythme actuel[6].

Selon une estimation, les escroqueries et les fraudes représentent environ 2,5% de l'ensemble du spam, dont une proportion importante (92%) peut être de nature malveillante, c'est-à-dire associée à des logiciels malveillants dans le but de nuire aux utilisateurs ou de compromettre leurs systèmes informatiques à diverses fins[7]. Selon une autre estimation, environ 812,67 millions d'infections de divers types liées à des logiciels malveillants ont été identifiées en 2018[8]. Les logiciels malveillants mobiles ont augmenté de 54% et les rançongiciels de 350%, tandis que les pertes financières liées aux infections par des rançongiciels sont estimées à 6 milliards USD par an (jusqu'en 2021).

Comme le spam et les logiciels malveillants peuvent générer un trafic important, ils peuvent avoir des répercussions négatives considérables sur l'infrastructure et les opérateurs de réseau et, par conséquent, sur l'expérience des consommateurs. Les problèmes liés au spam, y compris les problèmes de réseau qui en résultent, peuvent également nuire à la réputation des opérateurs.

---

4 Voir le Supplément 9 à la Recommandation UIT-T X.1205 (09/2011). Supplément sur les lignes directrices visant à réduire les maliciels dans les réseaux TIC.

5 Statista, Global spam volume as percentage of total e-mail traffic from January 2014 to September 2020, by month.

6 Spam Laws, Spam statistics and facts.

7 DataProt, What's on the other side of your inbox – 20 SPAM statistics for 2021.

8 PurpleSec, 2021 Cyber Security Statistics – The Ultimate List of stats, data & trends.

Pour faire face à ces préoccupations, y compris aux flux potentiellement massifs de trafic indésirable, et garantir la qualité du réseau, les opérateurs peuvent avoir besoin d'élaborer de nouveaux outils, notamment en investissant dans la sauvegarde et l'extension des infrastructures existantes. Par exemple, les fournisseurs de services pourraient investir dans des filtres antispam afin d'améliorer la qualité des services qu'ils offrent. Ces mesures pourraient entraîner des coûts supplémentaires nécessaires pour les opérateurs et les fournisseurs de services de communication électronique.

1.3 Approches adoptées pour combattre et atténuer les effets du spam et des logiciels malveillants

1.3.1 Approches techniques pour combattre et atténuer les effets du spam et des logiciels malveillants

Le courrier électronique non sollicité est l'un des principaux canaux de transmission des logiciels malveillants. Pour lutter efficacement contre le spam et les logiciels malveillants, la chaîne de transmission doit être rompue. Avec les progrès technologiques, des outils comme les filtres antispam et les logiciels antivirus restent des mécanismes efficaces pour lutter contre le spam et les logiciels malveillants. L'efficacité de ces outils peut être renforcée en les utilisant conjointement avec de nouvelles technologies comme l'intelligence artificielle (IA). La mise à jour régulière des filtres antispam et des logiciels antivirus est donc une bonne pratique pour les utilisateurs.

Parmi les fournisseurs de services, des mesures comme le cadre des politiques de l'expéditeur (sender policy framework)[9], le courrier identifié par clés de domaine (domain keys identified mail)[10], l'authentification des messages fondée sur le domaine (domain-based message authentication), la notification et la conformité[11] et l'inscription sur des listes de blocage en temps réel peuvent être utilisées pour réduire ces chaînes de transmission.

Les opérateurs de réseaux de communications électroniques et les fournisseurs de services Internet peuvent également prendre certaines mesures pour répondre aux préoccupations liées au blocage des adresses IP. Un exemple est la sécurité du protocole de passerelle frontière à l'aide de l'infrastructure de clés publiques cryptographique (RPKI)[12]. D'autres initiatives incluent:

- des normes de sécurité de routage convenues d'un commun accord, qui visent à empêcher, par la collaboration, le détournement de voies d'acheminement par des techniques évoluées, l'usurpation d'adresse IP et d'autres activités malveillantes pouvant entraîner des attaques par déni de service réparti (DDoS), l'écoute clandestine, la perte de recettes, l'atteinte à la réputation, etc.[13];
- le Groupe de travail contre l'utilisation abusive des messagerie, des téléphones portables et contre les logiciels malveillants, qui publie régulièrement de bonnes pratiques pour lutter contre les messages illicites, tous les types de logiciels malveillants (y compris les botnets), le spam, les virus, les attaques par déni de service (DoS) et les abus en ligne de toute nature[14].

---

9 Mimecast, Everything you need to know about SPF.
10 DKIM.org, Domain Keys Identified Mail (DKIM).
11 DMARC, Domain-based Message Authentication, Reporting and Conformance.
12 RFC Editor, RFC 6480 – An Infrastructure to Support Secure Internet Routing, février 2012.
13 MANRS, Mutually Agreed Norms for Routing Security.
14 Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG), Why M³AAWG?

Parmi les autres initiatives dans la lutte contre le spam et les logiciels malveillants, citons l'Internet Society[15], la Global System for Mobile Communications Association[16], le Spamhaus Project[17], l'Anti-Phishing Working Group[18] et l'Anti-Spyware Coalition[19].

1.3.2 Exemples d'approches réglementaires pour combattre et atténuer les effets du spam et des logiciels malveillants

Compte tenu des préoccupations et des coûts liés à la lutte contre le spam et les logiciels malveillants, des régions et des pays ont adopté ou renforcé ces dernières années la législation existante afin de fournir des outils permettant d'intensifier la lutte contre ces attaques. Les pays ont élaboré des législations et des politiques fondées sur leurs propres besoins nationaux, comme le règlement général de l'Union européenne sur la protection des données (RGPD), qui exige le consentement de l'utilisateur pour la collecte de données.

Un autre exemple est la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo), qui fournit un ensemble de normes que les États parties de la région Afrique sont encouragés à intégrer dans leur législation nationale. À l'Article 4.3, la convention dispose que "Les États parties interdisent la commercialisation directe par n'importe quelle forme de communication indirecte utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen". Néanmoins, la convention autorise la commercialisation directe sous certaines conditions; par exemple, "la commercialisation directe par courrier électronique est autorisée si: a) les coordonnées du destinataire ont été recueillies directement auprès de lui; b) le destinataire a donné son consentement pour être contacté par ses partenaires; c) la commercialisation directe concerne les produits ou services analogues fournis par la même personne physique ou morale" (§ 4.4).

À mesure que le RGPD de l'Union européenne et la Convention de Malabo seront mis en œuvre, nous pourrons évaluer et comprendre leur plein effet sur la réduction du spam et des logiciels malveillants.

1.3.3 Contributions relatives aux travaux visant à combattre et à atténuer les effets du spam et des logiciels malveillants au titre de la Question 3/2

Au cours de la période d'études, certains pays et membres de Secteur de l'UIT ont fourni des exemples supplémentaires d'approches pour lutter contre le spam et les logiciels malveillants:

- certains contributeurs ont décrit comment ils collectent des informations en temps réel sur les menaces de cybersécurité afin d'inspirer et de mettre en place des stratégies de cybersécurité résilientes. Dans le monde complexe des technologies de l'information, les données en temps réel sont essentielles pour protéger l'information. La connaissance de la situation et les renseignements sur les cybermenaces, lorsqu'ils sont combinés, aident les pays et les organisations publiques et privées à identifier les menaces dès leur apparition afin de protéger leurs ressources plus efficacement. Ainsi, pour mieux protéger

15 Internet Society, The Internet Society's Anti-Spam Toolkit.
16 GSMA, GSMA Security.
17 Spamhaus, Spamhaus ZEN + DBL + RPZ.
18 APWG, Unifying the global response to cybercrime through data exchange research and public awareness.
19 Anti-Spyware Coalition, Internet, Marketing y Actualidad.

les organisations contre les attaques ciblées et les menaces persistantes, il est impératif d'élaborer des stratégies cyber-résilientes fondées sur des renseignements de sécurité[20];

- certains contributeurs cartographient les menaces de la cybercriminalité afin de comprendre les divers effets du spam et des logiciels malveillants sur les internautes (par exemple, l'hameçonnage et la fraude à la loterie) et les entreprises (par exemple, l'accès non autorisé au système et les attaques par refus de service (DoS)). Par exemple, en 2017, la Côte d'Ivoire a surveillé les menaces et les infractions liées à la cybercriminalité, qui ont été enregistrées par la Plate-forme de lutte contre la cybercriminalité (PLCC), fournissant ainsi des informations utiles et qualitatives pour guider les activités opérationnelles visant à améliorer l'éducation des consommateurs et des entreprises. Des modèles de fraude aux services financiers sur mobile ont été identifiés, avec 453 cas enregistrés, représentant une perte de près de 800 000 USD. La fraude aux services financiers sur mobile est une escroquerie bien conçue, dans laquelle, après avoir transféré des fonds vers ou depuis un compte sur mobile en utilisant une syntaxe de données de services supplémentaires non structurées (USSD), la victime reçoit un appel des fraudeurs affirmant qu'il y a eu un problème avec le transfert; si la victime se fait piéger, les fraudeurs peuvent retirer à distance de l'argent sur son compte en utilisant la même syntaxe USSD[21];
- certains contributeurs ont décrit comment ils créent des processus ouverts et transparents pour recenser et soutenir les mesures à prendre par les parties prenantes concernées en vue de réduire de manière significative les menaces que représentent les attaques automatisées et distribuées (par exemple les botnets). Avec l'arrivée de nouveaux botnets, qui peuvent créer une pression énorme sur les réseaux en utilisant plus d'un térabit de données par seconde, les techniques traditionnelles d'atténuation des DDoS fondées sur la réservation de ressources par les fournisseurs d'accès au réseau ne sont plus efficaces. L'atténuation des menaces liées aux cyberattaques automatisées et distribuées nécessite une collaboration permanente entre les secteurs public et privé[22];
- quelques mesures simples peuvent aider les entreprises à se protéger efficacement contre la menace d'attaques par des rançongiciels. Dans un récent document consacré aux attaques par des rançongiciels, le National Cyber Security Centre (NCSC) du Royaume-Uni recommande un certain nombre de techniques simples d'atténuation des risques, telles que:

  - maintenir les dispositifs et les réseaux à jour (par exemple, par des mises à jour et des correctifs rapides et des analyses régulières);
  - prévenir et détecter les mouvements latéraux dans les réseaux d'entreprise;
  - utiliser un scanner de virus;
  - sauvegarder tous les fichiers[23].

  Une liste complète et détaillée des recommandations peut être trouvée sur le site web du NCSC[24].
- Certains contributeurs ont décrit comment ils créent un cadre national de cybersécurité flexible et adapté à l'évolution des besoins. Par exemple, le Royaume-Uni a lancé le programme Active Cyber Defence, qui se concentre sur la prise de mesures techniques positives pour améliorer l'environnement en ligne pour tous. Ce programme a apporté des avantages considérables et mesurables aux réseaux gouvernementaux. Il a été mis en œuvre dans l'ensemble des réseaux du service public au Royaume-Uni afin de démontrer les avantages pratiques et les éventuelles mesures de suivi[25]. Dans le cadre de

---

20 Document 2/167 (Symantec Corporation (États-Unis)) de la CE 2 de l'UIT-D.
21 Document 2/174 (Côte d'Ivoire) de la CE 2 de l'UIT-D.
22 Document SG2RGQ/153 + Annexes (États-Unis) de la CE 2 de l'UIT-D.
23 Document SG2RGQ/155 (Royaume-Uni) de la CE 2 de l'UIT-D.
24 National Cyber Security Centre (NCSC), Guidance: Mitigating malware and ransomware attacks.
25 Document SG2RGQ/55 (Royaume-Uni) de la CE 2 de l'UIT-D.

la poursuite des efforts visant à surmonter ces difficultés, le Royaume-Uni a fait le point sur le programme un an après son lancement[26].

- Certains contributeurs prennent des mesures pour sensibiliser les communautés vulnérables (par exemple les personnes handicapées) à leur niveau de risque accru. Les spammeurs et les pirates informatiques utilisent des techniques de plus en plus évoluées pour déterminer si les cibles potentielles de détournement sont handicapées. Dans certains cas, les pirates utilisent le handicap d'une personne comme moyen de se faire passer pour cette personne à partir du compte de courrier électronique détourné[27].
- Certains contributeurs mettent en place des services de signalement pour les courriels hameçons. Procéder à une collecte participative des courriels malveillants et prendre des mesures contre les domaines et autres entités derrière ces courriels constituent un moyen efficace de lutter contre la cybercriminalité et la fraude. Par exemple, pendant les quatre premiers mois qui ont suivi la création du Service de signalement des courriels suspects, le NCSC du Royaume-Uni et la police de la ville de Londres ont éliminé plus de 16 000 menaces signalées par la population[28].

[26] Document SG2RGQ/175 (Royaume-Uni) de la CE 2 de l'UIT-D.
[27] Document 2/71 (Initiative mondiale pour des technologies de l'information et de la communication inclusives (G3ict)) de la CE 2 de l'UIT-D.
[28] Document SG2RGQ/234 (Royaume-Uni) de la CE 2 de l'UIT-D.

Chapitre 2 – Améliorer les choix nationaux en matière de cybersécurité: perspectives de sensibilisation et de renforcement des capacités

Ces dernières années, les TIC ont connu une croissance et une innovation rapides. Dans le monde entier, les TIC jouent un rôle important en permettant aux pays de développer leur économie numérique et de soutenir la prospérité sociale. En outre, la pandémie de COVID-19 a montré que les individus sont de plus en plus dépendants des TIC dans leur vie quotidienne. Compte tenu de cette réalité, il est primordial que les pays continuent à prendre des mesures décisives pour améliorer et renforcer leurs dispositifs nationaux de cybersécurité afin de se prémunir contre les risques et les défis liés à la cybersécurité.

Le présent chapitre traite des principaux domaines d'intervention pour l'amélioration des choix nationaux en matière de cybersécurité, notamment:

- mise en place des autorités nationales compétentes en matière de cybersécurité;
- équipes d'intervention en cas d'urgence informatique (CERT)/équipes d'intervention en cas d'incident de sécurité informatique (CSIRT)/équipes d'intervention en cas d'incident informatique (CIRT);
- campagnes de sensibilisation à la cybersécurité;
- cadres de gestion des risques en matière de cybersécurité;
- partenariats public-privé;
- autres initiatives de renforcement des capacités.

Au cours de la période d'études, un certain nombre d'entités ont apporté des contributions sur ces questions. Voir l'**Annexe 1** pour un recueil des activités pertinentes et en cours en matière de cybersécurité menées par les États Membres, les organisations, le secteur privé et la société civile aux niveaux national, régional et international. L'**Annexe 2** contient une liste des bonnes pratiques et des enseignements tirés de l'expérience présentés par certaines de ces entités.

2.1 Mise en place d'autorités nationales compétentes en matière de cybersécurité

Au fur et à mesure que de nouvelles avancées et innovations sont réalisées dans le domaine des TIC, les risques et les défis liés à la cybersécurité augmentent. Les gouvernements doivent évaluer et améliorer en permanence leurs choix et stratégies nationaux en matière de cybersécurité pour relever ces défis, notamment par la création d'autorités nationales compétentes en matière de cybersécurité. Au cours de la période d'études, les États Membres ont décrit leurs approches pour la mise en place de telles autorités. Les différents pays ont

adopté des méthodes différentes en fonction de leurs structures de gouvernance, règles, réglementations et politiques nationales.

Ces autorités de cybersécurité ont des compétences et des objectifs différents, mais elles remplissent généralement les mêmes fonctions essentielles, notamment l'élaboration et la coordination des politiques réglementaires; l'élaboration et la mise en œuvre de campagnes de sensibilisation à la cybersécurité; la fourniture aux utilisateurs (des grandes organisations aux particuliers et aux petites entreprises) d'informations actualisées; et la publication de déclarations et de conseils sur les incidents de cybersécurité. Compte tenu de l'étendue du paysage de la cybersécurité, il est essentiel que les gouvernements encouragent la coordination et la collaboration entre les différentes autorités et entités et entre les secteurs public et privé.

Au Royaume-Uni, par exemple, le National Cyber Security Centre (NSC) travaille avec d'autres entités gouvernementales concernées et dirige les efforts visant à réduire de manière mesurable les effets des attaques par rançongiciels[29]. En cas d'attaque, il est conseillé aux organisations de contacter la National Crime Agency, une entreprise certifiée pour les interventions en cas de cyberincident, ou le Cyber Security Information Sharing Partnership. Le NCSC a dirigé l'intervention du Royaume-Uni face à l'attaque du rançongiciel WannaCry, en collaboration avec la National Crime Agency. Au cours de chaque incident, le centre publie des déclarations et des conseils destinés aux grandes organisations ainsi qu'aux particuliers et aux petites entreprises. Les dernières informations sont également annoncées via le compte Twitter du centre (@NCSC).

Le Brésil a adopté sa stratégie nationale de cybersécurité (E-Ciber), qui a été ratifiée par le président brésilien et publiée en février 2020[30]. Pour cette stratégie prospective, qui représente la vision du gouvernement fédéral en matière de cybersécurité pour 2020-2023, le Brésil a adopté une approche exhaustive et globale, engageant la participation de nombreuses parties prenantes, y compris du gouvernement, du secteur privé et d'établissements universitaires. Avec la ratification d'E-Ciber, le Brésil a complété un cadre juridique qui faisait auparavant défaut. Dans le cadre d'E-Ciber, le Brésil a défini dix actions stratégiques pour chacune desquelles il a énoncé des mesures et des initiatives. Voici quelques exemples de ces actions stratégiques:

- Renforcer la gouvernance de la cybersécurité.
- Établir un modèle national centralisé de gouvernance de la cybersécurité.
- Améliorer le cadre juridique national pour la cybersécurité.
- Étendre la coopération internationale du Brésil en matière de cybersécurité.

Au Bénin, différentes entités gouvernementales participent à la gestion des TIC dans le pays[31]. L'Agence des Services et Systèmes d'Information (ASSI), ex-Agence Béninoise des Technologies de l'Information et de la Communication (ABETIC), est l'entité nationale chargée de la mise en œuvre opérationnelle de programmes et de l'élaboration de stratégies de développement de services et systèmes d'information numériques sécurisés dans le pays. Elle est responsable d'un certain nombre d'activités essentielles, notamment:

- l'exécution des projets phares relatifs à l'administration intelligente et au commerce électronique;
- l'élaboration, la mise à jour et l'exécution opérationnelle des schémas directeurs des systèmes d'information d'envergure nationale;

[29] Document SG2RGQ/155 (Royaume-Uni) de la CE 2 de l'UIT-D.
[30] Document SG2RGQ/216 (Brésil) de la CE 2 de l'UIT-D.
[31] Document 2/152 (Bénin) de la CE 2 de l'UIT-D.

- la garantie de la cohérence technique, applicative et financière des services et systèmes d'information nationaux;
- la garantie de l'hébergement, du contrôle et de l'accès sécurisé aux données et informations critiques de l'État et des opérateurs d'infrastructures essentielles.

Au Tchad, l'Agence nationale de sécurité informatique et de certification électronique (ANSICE), créée en février 2015, dépend directement de la Présidence de la République[32]. L'agence est opérationnelle depuis janvier 2018 et dispose d'une autorité et de compétences étendues, notamment en matière de sécurité des systèmes et réseaux informatiques dans tout le pays.

Le Royaume-Uni a aussi fait part d'une étude de cas mise à jour sur ses efforts visant à instaurer de bonnes pratiques de sécurité pour les dispositifs de l'Internet des objets (IoT) grand public, notamment en:

- publiant le code de bonne pratique pour la sécurité des consommateurs en matière d'IoT, qui énonce 13 principes de haut niveau (également disponible en allemand, espagnol, français, japonais, coréen, mandarin et portugais);
- organisant une consultation publique sur les propositions de réglementation et de législation;
- soutenant la norme ETSI EN 303 645[33], la première norme applicable au niveau mondial pour la sécurité de l'IoT, publiée par l'Institut européen des normes de télécommunication (ETSI). De nombreuses organisations ont déjà fondé leurs produits et leurs systèmes de certification sur cette norme et celle qui l'a précédée, ETSI TS 103 645;
- publiant un appel à commentaires sur les propositions réglementaires du Royaume-Uni afin de recueillir les réactions des parties prenantes sur le champ d'application, les obligations, les exigences de sécurité et l'approche d'exécution proposés;
- chargeant le ministère du numérique, de la culture, des médias et des sports et le NCSC d'élaborer conjointement des documents d'orientation et d'organiser des webinaires en ligne pour les fabricants d'IoT, qui ont été réalisés à plusieurs reprises pour tenir compte des différents fuseaux horaires;
- maintenant une carte du paysage qui décrit les normes existantes et en aidant les organisations à mettre en œuvre les bonnes pratiques dans le domaine de l'IoT[34].

2.2 Équipes d'intervention en cas d'urgence informatique (CERT)/ équipes d'intervention en cas d'incident de sécurité informatique (CSIRT)/équipes d'intervention en cas d'incident informatique (CIRT)

Les capacités nationales d'intervention en cas d'incident (sous la forme d'équipes CERT/CSIRT/CIRT) sont des outils essentiels pour surmonter les difficultés opérationnelles en matière de cybersécurité. Ces capacités facilitent la coordination des informations sur la cybersécurité et des interventions en cas d'incident de sécurité. Au cours de la période d'études, la commission d'études a reçu des contributions essentielles des États Membres et des Membres de Secteur de l'UIT sur le sujet, dont beaucoup partageaient l'avis que les équipes CERT/CSIRT/CIRT nationales devraient servir de point de contact principal pour les questions de cybersécurité et de coordonnateurs pour les interventions en cas d'incident.

[32] Document 2/136 (Tchad) de la CE 2 de l'UIT-D.
[33] ETSI, Norme ETSI EN 303 645. Cyber Security for Consumer Internet of Things: Baseline Requirements.
[34] Document SG2RGQ/241 (Royaume-Uni) de la CE 2 de l'UIT-D.

Par exemple, la Bhutan Computer Incident Response Team (BtCIRT) a été créée en avril 2016 pour renforcer la cybersécurité dans le pays en facilitant la coordination des informations relatives à la cybersécurité et en établissant des capacités nationales pour la gestion des incidents de sécurité informatique[35]. La BtCIRT est une unité qui dépend du département des technologies de l'information et des télécommunications du ministère de l'information et des communications. En vertu de son mandat, la BtCIRT fait office de point de contact national pour les questions de cybersécurité et représente le pays dans les enceintes internationales. Le fait qu'une seule organisation coordonne toutes les initiatives de cybersécurité garantit l'absence de chevauchement des efforts ou des activités de développement. Comme la plupart des forums et groupes internationaux axés sur la cybersécurité communiquent avec les CIRT qui ont un mandat national, il est important que les gouvernements désignent soit une CIRT, soit une organisation unique désignée pour mener les initiatives et les plans nationaux de cybersécurité.

Bien que la BtCIRT ait été établie comme point de contact pour les questions liées à la cybersécurité au Bhoutan, il a été difficile pour l'équipe de gagner la confiance des parties prenantes, principalement en raison de ses capacités techniques limitées et du fait qu'il s'agit d'une équipe relativement nouvelle. En outre, les grandes entreprises comme les opérateurs de télécommunication et les banques disposent déjà d'une infrastructure TIC solide dotée de capacités techniques, ce qui rend difficile la coopération entre les pouvoirs publics et ces grandes organisations. La collaboration et la coopération entre les parties prenantes, en particulier les fournisseurs de services Internet et les CIRT, sont essentielles pour fournir des solutions de sécurité concertées aux internautes. Le Bhoutan s'est tourné vers les organisations internationales pour l'aider à renforcer les capacités techniques essentielles de la BtCIRT.

Enfin, la société lituanienne NRD Cyber Security a proposé qu'en plus d'assurer les fonctions de point de contact principal et de coordonnateur des interventions en cas d'incident de cybersécurité, les CSIRT nationales et sectorielles jouent aussi un rôle de facilitateur ou de catalyseur pour développer une résilience indépendante et élargie face aux cybermenaces qui touchent le pays[36].

2.3 Campagnes de sensibilisation

Diverses parties prenantes dans le monde entier – des gouvernements et des entités commerciales aux organisations communautaires et aux citoyens individuels – font un usage intensif des TIC. Toutefois, de nombreux utilisateurs ne sont pas pleinement conscients des risques en matière de cybersécurité liés à leur utilisation. Pour certains pays en développement, le plus grand défi est le manque de sensibilisation des utilisateurs. Dans les contributions reçues au cours de la période d'études, une convergence de vues s'est dégagée sur le fait que les campagnes de sensibilisation à la cybersécurité jouent un rôle important pour relever ces défis. L'objectif premier de ces campagnes est d'encourager l'adoption d'un comportement sûr en ligne.

Les pays et les entreprises recherchent des moyens créatifs pour mettre au point des campagnes efficaces, notamment pour atteindre un large éventail d'utilisateurs.

[35] Document SG2RGQ/79 (Bhoutan) de la CE 2 de l'UIT-D.
[36] Document 2/172 (NRD Cyber Security (Lituanie)) de la CE 2 de l'UIT-D.

Par exemple, le Mexique a fait part de son expérience en matière d'élaboration et de réalisation d'une enquête auprès des internautes, qui peut être utilisée pour orienter les différentes approches des campagnes de sensibilisation à la cybersécurité[37].

Certains pays ont utilisé des enquêtes pour recenser les principales préoccupations des citoyens et élaborer des campagnes de sensibilisation sur mesure en fonction des résultats. Sur la base de son expérience, le Mexique a également tiré les enseignements suivants:

- Installer et mettre à jour la protection antivirus.
- Changer régulièrement les mots de passe et s'assurer que les mots de passe sont solides (c'est-à-dire utiliser une combinaison de chiffres, de lettres et de caractères spéciaux).
- Sauvegarder les données régulièrement.
- Se connecter uniquement à des réseaux publics sécurisés.

Dans un autre exemple, la BtCIRT du Bhoutan a créé des programmes de sensibilisation adaptés pour répondre aux besoins de cybersécurité découlant des engagements professionnels et personnels quotidiens des utilisateurs finals dans tout le pays[38]. Les participants ont pu voir comment les attaques sont exécutées par des escroqueries d'ingénierie sociale et par hameçonnage, comment communiquer en toute sécurité en utilisant le courrier électronique et les services des réseaux sociaux et quelles sont les menaces courantes et les mesures correctives. Les programmes de sensibilisation du Bhoutan ont remporté un vif succès en sensibilisant les utilisateurs aux risques de sécurité et ont reçu un écho positif. Bien qu'elle se concentre actuellement sur les fonctionnaires, l'équipe BtCIRT cherche à étendre ses efforts aux enfants et aux autres utilisateurs vulnérables.

Un autre exemple créatif fourni par le Bhoutan est le lancement d'un concours national annuel de sites web, organisé par le département des technologies de l'information et des télécommunications du ministère de l'information et des communications[39]. Tous les sites web gouvernementaux participent au concours, dans le cadre duquel les meilleurs sites web du pays sont sélectionnés sur la base des critères fondamentaux suivants:

- facilité d'utilisation et fiabilité;
- pertinence et actualité du contenu;
- sécurité et disponibilité;
- apparence;
- conception interactive.

De même, en novembre 2019, le Brésil a lancé la campagne de sensibilisation à la cybersécurité #ConexãoSegura ("Connexion sécurisée") par l'intermédiaire de l'Agence nationale brésilienne des télécommunications (Anatel)[40]. Les messages publiés ont donné des conseils sur la protection des données personnelles et la création de mots de passe sécurisés. La campagne a vu le jour à la suite de plaintes de consommateurs concernant des tentatives d'escroquerie et de questions sur la manière de protéger leurs données personnelles. Avec l'apparition de la pandémie de COVID-19 et le déferlement de nouvelles escroqueries, de nouveaux messages sur la fraude et les escroqueries liées au COVID-19 ont été créés pour aider les utilisateurs à se protéger. Les messages ont également été publiés sur les réseaux sociaux de l'Agence,

[37] Document 2/165 (Mexique) de la CE 2 de l'UIT-D.
[38] Document SG2RGQ/79 (Bhoutan) de la CE 2 de l'UIT-D.
[39] Document SG2RGQ/135 (Bhoutan) de la CE 2 de l'UIT-D.
[40] Document SG2RGQ/215 (Brésil) de la CE 2 de l'UIT-D.

notamment Facebook, Twitter, Instagram et LinkedIn. Certaines des principales bonnes pratiques recommandées par la campagne étaient les suivantes:

- Utiliser toutes les options de sécurité offertes par les applications mobiles, comme l'authentification à deux facteurs.
- Créer des mots de passe solides et sûrs en combinant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.
- Se méfier des courriers électroniques et des messages contenant des factures jointes et toujours contacter le service clientèle de l'entreprise pour vérifier si un document est authentique.
- Ne pas fournir d'informations personnelles ou de mots de passe lorsqu'on répond à des appels inconnus[41].

Le Royaume-Uni a présenté une étude de cas sur les bonnes pratiques en matière de résilience de la cybersécurité pour les petites et moyennes entreprises, dans laquelle il a décrit les efforts déployés pour améliorer la cyberrésilience des organisations dans tout le pays[42]. Un exemple de ces efforts est la campagne de communication Cyber Aware, qui, au-delà de la simple sensibilisation, cherche à encourager l'adoption généralisée de comportements de base en matière de cybersécurité. Cette campagne, qui s'adresse au public et aux petites entreprises, a été lancée en avril 2020, après avoir été rapidement remaniée pour répondre à l'évolution du paysage de la cybermenace entraînée par la pandémie de COVID-19. La campagne a encouragé des mesures d'atténuation réalisables, étayées par de nouvelles orientations sur la manière de travailler en toute sécurité depuis son domicile, de faire basculer en ligne les activités des entreprises et d'utiliser la vidéoconférence. Parmi les autres outils, citons:

- Guide des petites entreprises sur la cybersécurité.
- Guide des petites entreprises sur l'intervention et le rétablissement, qui fournit un plan de continuité pour aider les PME à se préparer aux cyberincidents et à en atténuer les répercussions potentielles.
- Exercise in a Box, un outil en ligne gratuit pour aider les PME à tester leur cyberrésilience et à suivre des micro-cours sans avoir besoin de connaissances techniques particulières.
- Guide COVID-19 pour aider les entreprises à rester en sécurité tout en s'adaptant à la pandémie, couvrant des sujets comme le travail à domicile et le basculement en ligne des activités commerciales.

Le Royaume-Uni a également fourni des détails sur son programme de certification soutenu par le gouvernement, Cyber Essentials, qui vise à protéger les entreprises contre les cyberattaques visant les produits de base sans leur imposer de se conformer à de multiples normes complexes. Cyber Essentials a été conçu pour être accessible à toutes les organisations, même à celles qui n'ont pas de connaissances préalables en matière de cybersécurité ou qui ne disposent pas d'une cyberéquipe spécialisée.

2.4 Cadres de gestion des risques en matière de cybersécurité

Les cadres de gestion des risques en matière de cybersécurité sont essentiels pour les organisations gouvernementales et non gouvernementales. Il s'agit généralement de cadres volontaires qui fournissent des lignes directrices et de bonnes pratiques pour la gestion des

[41] De plus amples informations sur la campagne "Connexion sécurisée" d'Anatel sont disponibles sur le site web suivant: https://www.anatel.gov.br/consumidor/component/content/article/109-manchetes/960-conexaoseguro-confira-dicas-para-proteger-dados-pessoais

[42] Document SG2RGQ/272 (Royaume-Uni) de la CE 2 de l'UIT-D.

risques numériques. Au cours de la période d'études, la commission d'études a reçu des contributions d'entités qui ont fourni différents exemples et approches de cadres de gestion des risques en matière de cybersécurité.

Par exemple, le National Institute of Standards and Technology (NIST) des États-Unis a récemment mis à jour son Cadre pour l'amélioration des infrastructures essentielles en matière de cybersécurité[43]. Il s'agit d'un cadre dynamique pour la gestion volontaire des cyberrisques, conçu pour les entreprises de toutes tailles actives dans divers secteurs de l'économie. Il offre un point de départ et une terminologie communs utilisables pour évaluer les cyberrisques. Ce cadre est facilement adaptable, ce qui permet aux organisations – indépendamment de leur taille, de l'ampleur des risques en matière de cybersécurité ou de la complexité de celle-ci – d'appliquer les principes et bonnes pratiques de la gestion des risques pour améliorer la sécurité et la résilience de leurs infrastructures essentielles.

L'élaboration de ce cadre représente un exemple de collaboration réussie entre secteur public et secteur privé en matière de gestion des risques de cybersécurité. Il est l'aboutissement d'un processus volontaire d'une année auquel ont contribué plus de 3 000 représentants du secteur privé, des milieux universitaires et du secteur public, y compris des partenaires internationaux.

Le cadre s'appuie sur des normes internationales et lignes directrices existantes, ainsi que sur les bonnes pratiques de l'industrie qui ont fait la preuve de leur efficacité, que ce soit pour protéger les systèmes informatiques des cybermenaces, assurer la confidentialité dans les entreprises ou protéger la vie privée et les libertés individuelles. Il vise à soutenir la protection des infrastructures essentielles par la gestion des risques. Il offre en outre une structure pour l'organisation des pratiques, ainsi que des outils pour l'adoption et l'utilisation de ces normes et pratiques. Dans la mesure où il fait référence à des normes internationalement reconnues, il est suffisamment souple pour servir aussi de modèle international pour la gestion des cyberrisques.

Sur la base des commentaires des parties prenantes, le NIST a effectué les mises à jour suivantes dans la version 1.1 du cadre:

- Déclarer que le cadre est applicable aux "technologies", qui comprennent au minimum les technologies de l'information, les technologies opérationnelles, les systèmes cyberphysiques et l'Internet des objets.
- Améliorer les orientations à suivre pour appliquer le cadre à la gestion des risques liés à la chaîne d'approvisionnement.
- Résumer la pertinence et l'utilité des mesures fournies dans le cadre pour l'auto-évaluation organisationnelle.
- Fournir davantage de renseignements sur l'auto-évaluation des risques en matière de cybersécurité.
- Mieux prendre en considération les prescriptions en matière d'autorisation, d'authentification et de confirmation de l'identité ainsi que de divulgation des vulnérabilités.
- Procéder à une mise à jour d'ordre administratif des références fournies pour information, afin de rendre compte de l'état d'avancement de l'élaboration de normes et de lignes directrices par des organisations du secteur privé et du secteur public.

De plus, au Bhoutan, l'Autorité monétaire royale (la banque centrale) a publié une directive encourageant la mise en œuvre d'un cadre de cybersécurité pour les institutions financières afin

[43] Document SG2RGQ/151 (États-Unis) de la CE 2 de l'UIT-D.

de renforcer la résilience du système bancaire face aux cyberrisques inconnus et avancés[44]. La directive couvre les domaines suivants:

- Toutes les banques membres doivent s'efforcer de se conformer à la norme de sécurité des données du secteur des cartes de paiement, qui vise à protéger les environnements de données des titulaires de cartes. En outre, les banques doivent mettre en œuvre la norme ISO/IEC 27001:2013 relative aux systèmes de gestion de la sécurité de l'information pour compléter leurs propres mesures de cybersécurité.
- La directive souligne la nécessité d'établir une équipe de cyberintervention des institutions financières pour promouvoir une collaboration active et un partage efficace des informations relatives à la cybersécurité entre les banques et l'Autorité monétaire royale. Cette équipe surveillerait activement les cybermenaces, planifierait et coordonnerait les mesures de lutte contre les menaces afin de prévenir les risques en matière de cybersécurité et signalerait tout incident à son supérieur hiérarchique ou aux autorités compétentes dans les plus brefs délais. Une cyberéquipe pour les banques a été récemment formée, l'Autorité monétaire royale jouant le rôle de chef de file.
- Les banques membres doivent également mettre en œuvre le cadre de contrôle de la cybersécurité approprié et des actions réactives en tant que mesure immédiate pour garantir la sécurité des informations de base.

Dans un autre exemple, la Chine a créé un indice d'évaluation pour mesurer la vision nationale en matière de planification, de développement et de mise en œuvre de la sécurité des réseaux, en utilisant trois niveaux d'indicateurs de plus en plus complexes[45]. Le premier niveau évalue cinq indicateurs:

- Politiques: stratégies nationales, législation, organismes gouvernementaux et coopération internationale.
- Industrie: développement du secteur de la sécurité des réseaux dans un environnement axé sur le marché, y compris l'environnement, l'échelle, les capacités et la viabilité du développement.
- Technologie: recherche et développement et niveau d'application de la sécurité nationale dans la technologie, y compris les projets de recherche scientifique, les investissements, les normes techniques et la formation de personnel.
- Capacités: niveau de protection des réseaux et de prévention des menaces, y compris la perception des risques, la protection de la sécurité, les interventions d'urgence et la défense active.
- Ressources: ressources nécessaires au renforcement des capacités, y compris les infrastructures de réseau, la sensibilisation à la sécurité et l'influence internationale.

L'indice comprend également 19 indicateurs de deuxième niveau et 53 de troisième niveau. Selon le système de notation de l'indice, chaque indicateur vaut entre 0 et 1 point, 53 étant le score le plus élevé possible. Les calculs pour chaque indicateur sont fondés sur les informations publiques officielles publiées sur des sites web nationaux et internationaux et par des institutions de recherche.

2.5 Partenariats public-privé

Les entités gouvernementales ne peuvent à elles seules améliorer les choix nationaux en matière de cybersécurité. La réussite des efforts et des projets de cybersécurité exige des partenariats solides entre les entités du secteur public et celles du secteur privé.

---

[44] Document SG2RGQ/135 (Bhoutan) de la CE 2 de l'UIT-D.
[45] Document 2/155 (Chine) de la CE 2 de l'UIT-D.

Aux États-Unis, le National Institute of Standards and Technology a élaboré son Cadre pour l'amélioration des infrastructures essentielles en matière de cybersécurité par le biais d'un processus de coopération à l'occasion d'un partenariat public-privé[46]. Comme indiqué plus en détail dans la section 2.4, l'institut a veillé à ce que toutes les parties prenantes participent à l'élaboration de la mise à jour afin d'encourager un respect maximal du cadre. En faisant participer les parties prenantes et en intégrant leurs commentaires dans la version 1.1 du cadre, les parties prenantes étaient plus susceptibles d'adhérer aux meilleures pratiques, lignes directrices et normes qu'il comprenait et de les mettre en œuvre.

En République de Corée, le ministère des sciences et des TIC a élaboré le Plan national de base de cybersécurité 2019 pour le secteur privé, en consultation avec les parties prenantes concernées, notamment les établissements universitaires, l'industrie et les organismes publics[47]. Le plan a fixé deux objectifs: garantir un cyberespace sûr et développer le secteur de la sécurité de l'information. Les principaux projets stratégiques à cette fin visaient à étendre le réseau de cybersécurité, à soutenir le secteur de la sécurité de l'information et à renforcer l'infrastructure de sécurité de l'information.

Compte tenu de l'évolution rapide de l'environnement des TIC, le ministère a l'intention de mettre à jour le plan chaque année. Par ailleurs, le Conseil de consultation public-privé de la République de Corée se réunit deux fois par an pour suivre l'évolution du plan et recenser les domaines à améliorer.

Comme décrit dans la section 2.1, la stratégie nationale de cybersécurité du Brésil, E-Ciber, est un autre exemple de l'importance des partenariats public-privé (PPP) dans l'élaboration de stratégies nationales globales de cybersécurité. Les PPP sont mis en évidence dans les actions stratégiques clés contenues dans E-Ciber, qui comprennent l'encouragement d'un environnement collaboratif, participatif, sûr et fiable entre les secteurs public et privé et la société civile et l'élargissement des partenariats de cybersécurité entre les secteurs public et privé, les établissements universitaires et la société civile.

Dans un autre exemple concluant de PPP, le Brésil a donné un aperçu de son expérience de l'organisation d'un cyberexercice national, connu sous le nom de Cyber Guardian Exercise, en 2018, qui plaçait l'accent sur les infrastructures essentielles nationales[48]. En 2019, le Brésil a mené un exercice de suivi, élargissant considérablement l'éventail des participants pour inclure des représentants des ministères de la défense, de la justice et des affaires étrangères, du Bureau de la sécurité institutionnelle, des forces armées, des agences gouvernementales fédérales comme Anatel, des équipes CSIRT nationales, de la Banque centrale du Brésil, des banques publiques et privées, des entreprises des secteurs du nucléaire, de l'électricité et des télécommunications, des chercheurs universitaires et des observateurs régionaux et internationaux invités.

Les équipes CERT/CSIRT/CIRT sont d'autres exemples de PPP. Grâce à ces équipes, les organismes publics et le secteur privé sont en mesure de travailler ensemble pour résoudre les problèmes de cybersécurité. La collaboration et la confiance sont toutefois nécessaires pour garantir que ces équipes restent efficaces.

---

46 Document SG2RGQ/151 (États-Unis) de la CE 2 de l'UIT-D.
47 Document 2/168 (République de Corée) de la CE 2 de l'UIT-D.
48 Document SG2RGQ/214 (Brésil) de la CE 2 de l'UIT-D.

2.6 Mesures/initiatives supplémentaires de renforcement des capacités

2.6.1 Création d'établissements d'enseignement de la cybersécurité

Après avoir compris qu'il était nécessaire d'investir dans la formation et l'éducation à la cybersécurité pour lutter contre les défis croissants dans ce domaine, de nombreux gouvernements ont créé des établissements d'enseignement pour former la prochaine génération d'experts en cybersécurité. Plusieurs contributions reçues des États Membres de l'UIT au cours de la période d'études ont fait état de la nécessité de déployer des efforts dans ce domaine, notamment en renforçant les relations entre les acteurs publics, les établissements universitaires et les centres de recherche.

Par exemple, en 2015, le Tchad a créé l'École nationale supérieure des technologies de l'information et de la communication (ENASTIC), démontrant ainsi clairement la volonté politique des plus hautes autorités du pays de fournir un cadre pour l'enseignement avancé des TIC (y compris la délivrance de diplômes en cybersécurité, réseaux, télécommunications, etc.)[49].

De même, le Sénégal a créé l'École nationale de cybersécurité (ENC), axée sur la région, pour renforcer les capacités et sensibiliser les décideurs, les hauts responsables de la défense et les autres acteurs de l'écosystème numérique de la région[50].

Les principales missions de l'école sont les suivantes:

- Former et sensibiliser les agents de l'État, les personnels, étudiants et personnes de nationalité sénégalaise et étrangère des secteurs public et privé actifs dans le domaine de la cybersécurité pour améliorer leur compréhension des risques et des menaces.
- Former régulièrement le personnel des CERT/CSIRT pour qu'il puisse faire face aux cyberattaques les plus évoluées.
- Former périodiquement le personnel des institutions de l'État et de la sous-région pour qu'il ait la capacité et les connaissances nécessaires pour préparer, protéger, intervenir et effectuer les retours d'incidents.

2.6.2 Autres initiatives de renforcement des capacités

Tout au long de la période d'études, le coordonnateur chargé de la cybersécurité du Bureau de développement des télécommunications (BDT) a fourni des mises à jour régulières sur le programme de travail du BDT, y compris ses diverses initiatives de renforcement des capacités. Le Bureau a travaillé conjointement avec différentes organisations et entités pour fournir une formation au renforcement des capacités pour les pays en développement, notamment en organisant des cyberexercices, en contribuant au développement des équipes CSIRT et en organisant des sessions de formation. Ces efforts ont également été soulignés dans les contributions des États Membres et des Membres de Secteur. Voir l'**Annexe 1** pour de plus amples informations.

[49] Document 2/136 (Tchad) de la CE 2 de l'UIT-D.
[50] Document SG2RGQ/146 (Sénégal) de la CE 2 de l'UIT-D.

Chapitre 3 – Protection en ligne des enfants

3.1 Aperçu

L'Internet moderne n'est plus seulement une banque de connaissances – une "immense bibliothèque désordonnée" – comme à l'époque du Web 1.0. Il est devenu une plate-forme de communication utilisée par tous, y compris les enfants. En fait, les enfants représentent un tiers de la population mondiale sur Internet, selon le Fonds des Nations Unies pour l'enfance (UNICEF)[51].

La nature des menaces en ligne auxquelles sont confrontés les enfants a évolué. Alors que les menaces antérieures étaient purement fondées sur l'information – par exemple, l'accès à des informations sur la drogue, la pornographie ou des mouvements extrémistes – les menaces actuelles sont également de nature comportementale, comme la désocialisation, la dépendance au jeu, les dépenses incontrôlées, le harcèlement virtuel, la divulgation de données personnelles et les connaissances dangereuses faites en ligne.

Au cours des dix dernières années, la communauté technologique n'a cessé d'inventer des moyens de protéger les enfants des sites qui contiennent des informations inappropriées, mais les concepteurs et les parents font maintenant face à un nouveau défi, à savoir comment initier correctement les jeunes utilisateurs à l'espace numérique et comment contrôler et corriger rapidement les comportements virtuels. Avec le développement rapide de la technologie Internet, la question de la protection des enfants, sur laquelle il existe un consensus mondial, s'est naturellement étendue au cyberespace. La sécurité dans le cyberespace est primordiale lorsqu'il s'agit d'initier les enfants aux appareils numériques et à l'Internet.

Aux termes de la Déclaration de Buenos Aires adoptée par la CMDT-17, "*il convient de tirer pleinement parti des possibilités qu'offrent les télécommunications/TIC, afin d'assurer un accès équitable aux télécommunications/TIC et aux innovations qui favorisent le développement socio-économique durable, la réduction de la pauvreté, la création d'emplois, l'égalité hommes-femmes, la protection en ligne des enfants, l'esprit d'entreprise et la promotion de l'inclusion numérique ainsi que l'autonomisation de tous*"[52].

La Résolution 179 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires de l'UIT et la Résolution 67 (Rév.Buenos Aires, 2017) de la CMDT définissent le rôle que doivent jouer l'UIT et l'UIT-D dans la protection en ligne des enfants.

Comme l'a montré la pandémie de COVID-19, les modèles de comportement des agresseurs et des réseaux criminels évoluent constamment, et les criminels profitent du fait que de nombreux enfants passent beaucoup plus de temps en ligne que d'habitude. Dans ces circonstances,

[51] UNICEF, La situation des enfants dans le monde 2017, décembre 2017.
[52] UIT, Conférence mondiale de développement des télécommunications (Buenos Aires, 2017), Déclaration de Buenos Aires, octobre 2017.

la publication des Lignes directrices de 2020 sur la protection en ligne des enfants de l'UIT, conçues pour préserver le bien-être, l'intégrité et la sécurité des enfants, tombe à point nommé[53].

Les Lignes directrices de 2020 sur la protection en ligne des enfants ont été corédigées par l'UIT et un groupe de travail d'auteurs collaborateurs d'institutions de premier rang actives dans le secteur des TIC, ainsi que dans les domaines qui concernent les droits et la protection (en ligne) des enfants. Elles 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. L'objectif de ces Lignes directrices est de sensibiliser à la portée de la protection en ligne des enfants et de fournir des ressources et des outils pour aider les enfants et leurs familles à acquérir des compétences numériques. Elles visent aussi à aider les parties prenantes de l'industrie et des gouvernements à élaborer des politiques et des stratégies de protection en ligne des enfants au niveau des entreprises et au niveau national. S'adressant aux enfants, aux parents, aux enseignants, au secteur privé et aux décideurs, les Lignes directrices sur la protection en ligne des enfants sont destinées à servir de guide pouvant être adapté et utilisé par les différents pays et acteurs en conformité avec les coutumes et les lois nationales et locales.

Dans le cadre du plan stratégique de l'UIT défini dans la Résolution 71 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires de l'UIT, l'un des objectifs de l'UIT-D est d'"*encourager le développement et l'utilisation des télécommunications/TIC et d'applications pour mobiliser les individus et les sociétés en faveur du développement durable*" (§ D.4). En particulier, l'UIT-D doit fournir des "*produits et services relatifs à l'inclusion numérique des jeunes filles et des femmes ainsi que des personnes ayant des besoins particuliers (personnes âgées, jeunes, enfants et populations autochtones, entre autres), par exemple activités de sensibilisation sur les stratégies, les politiques et les pratiques en matière d'inclusion numérique, perfectionnement des compétences numériques, kits pratiques et lignes directrices et forums de discussion pour échanger des pratiques et des stratégies*", dans le but, entre autres, de soutenir la protection en ligne des enfants (§ D.4-3).

Les activités de protection en ligne des enfants de l'UIT-D et de ses membres relèvent du point 2(d) du mandat de la Question 3/2:

d) continuer de recueillir auprès des États Membres des données d'expérience concernant la cybersécurité et la protection en ligne des enfants et de recenser et d'étudier les thèmes communs qui s'en dégagent et, à partir de ces informations, fournir des contributions pour l'établissement de [lignes directrices] qui aideront les États Membres à élaborer des mécanismes efficaces en matière de sécurité dans l'environnement numérique.

3.2 Bonnes pratiques et tendances communes aux États Membres de l'UIT

Au cours du cycle d'études, les principales activités de protection en ligne des enfants entreprises par les États Membres se sont concentrées sur la sensibilisation, l'élaboration de réglementations et la réalisation d'enquêtes thématiques.

[53] UIT, Lignes directrices sur la protection en ligne des enfants.

Sensibilisation

La protection des enfants dans le cyberespace comporte de nombreux aspects, ce qui nécessite non seulement des outils et des plates-formes, mais aussi des données appropriées. Les programmes culturels devraient être utilisés pour diffuser ces ressources dans toute la société.

Par exemple, l'Organisation iranienne des technologies de l'information a mis au point le projet "Kids and Internet" (KOVA) pour protéger les enfants dans le cyberespace, qui a été sélectionné comme projet champion lors du concours des prix du Sommet mondial sur la société de l'information en 2018.

Compte tenu du développement rapide de l'infrastructure Internet ces dernières années et du grand nombre de jeunes internautes, dont des enfants, le Gouvernement iranien a lancé en 2016 un programme national de protection des enfants sur Internet. Dans le cadre de ce programme, le ministère des TIC a lancé le projet KOVA pour sensibiliser les enfants et leurs parents aux risques de l'Internet et à la manière de protéger les enfants contre ces risques. Les principaux objectifs du projet sont les suivants:

- Recenser les menaces les plus importantes pour les enfants dans le cyberespace et fournir des solutions et des services de protection juridique.
- Sensibiliser les élèves du primaire, les lycéens, les enseignants et les parents aux diverses menaces qui pèsent sur les enfants à différents âges.
- Aider les enfants et les adolescents à utiliser les réseaux sociaux et l'Internet en toute sécurité.
- Répondre aux questions posées par les enfants, les adolescents, les éducateurs et les parents sur les problèmes de sécurité et de sûreté dans le cyberespace.

Pour atteindre les objectifs du projet, une gamme variée d'outils et de méthodes (comme le théâtre, les films et les animations) ont été utilisés pour enseigner aux enfants la sécurité en ligne. Dans la première phase du projet, plus de 200 000 élèves de 900 écoles ont reçu une formation, et l'objectif pour la deuxième phase est d'atteindre 4 000 écoles[54].

Au Bhoutan, le nombre d'internautes a augmenté de plus de 28% depuis 2016, grâce à la facilité d'accès croissante, au caractère abordable de la connexion et à la disponibilité de téléphones intelligents moins coûteux. La plupart des écoliers ont accès à un smartphone, ce qui crée un risque plus élevé d'incidents de sécurité. Le Bhoutan n'a pas encore de programme scolaire sur la cybersécurité, car l'augmentation de l'utilisation de l'Internet et des appareils mobiles est une tendance récente. Il est toutefois de la plus haute importance que les gouvernements s'adaptent à l'évolution de la situation en incluant la cybersécurité dans les programmes scolaires. Les collèges privés du Bhoutan ont déjà commencé à étudier comment offrir des programmes d'études connexes, en particulier dans le domaine de la cybersécurité. Les écoliers doivent être conscients des cyberrisques, car ils sont plus vulnérables aux attaques sous forme d'hameçonnage et de jeux en ligne[55].

Dans ce contexte, après avoir examiné les habitudes et les comportements en ligne des enfants, le Bhoutan élabore des vidéos animées portant sur des thèmes tels que la traite des enfants, le cyberharcèlement, le respect de la vie privée et la sécurité des jeux en ligne, qui seront diffusées sur les chaînes de télévision nationale. Le pays élabore également des affiches et

[54] Document 2/82 (Université iranienne des sciences et des technologies (République islamique d'Iran)) de la CE 2 de l'UIT-D.
[55] Document SG2RGQ/79 (Bhoutan) de la CE 2 de l'UIT-D.

des brochures contenant des bonnes pratiques en matière de cybersécurité à l'intention des élèves, qui seront distribuées dans diverses écoles du pays. Enfin, le Bhoutan met sur pied une équipe spéciale au niveau national, composée de représentants de plusieurs organismes pertinents, afin de définir des lignes directrices pertinentes en matière de protection en ligne des enfants à l'échelle du pays[56].

La Chine organise chaque année une semaine nationale de promotion de la sécurité des réseaux afin de sensibiliser à la cybersécurité et d'améliorer les compétences de l'ensemble de la population en matière de protection en ligne par le biais d'expositions, de forums, de concours, de conférences, de journées thématiques de promotion et d'autres activités. Par exemple, des conférences sur la sécurité des réseaux sont données pour partager les connaissances et les compétences en fonction des besoins de différents groupes, comme les élèves des écoles primaires et secondaires, les personnes âgées et les groupes particuliers (comme les personnes handicapées), selon leur niveau de compétences informatiques[57].

Aux États-Unis, des informations sont données aux parents et aux enseignants sur les pratiques des enfants et des adolescents, pour pouvoir notamment leur expliquer que ce qu'ils publient peut rester toute une vie en ligne, qu'ils doivent faire attention à ce qu'ils partagent, qu'ils ne doivent pas communiquer trop d'informations personnelles, que le contenu de leurs publications concernant d'autres personnes doit correspondre à ce qu'ils aimeraient que les autres publient sur eux, qu'ils doivent maîtriser leur présence en ligne en limitant le nombre de personnes pouvant voir et partager leurs informations, et quelles données sont recueillies[58].

Réglementation

Compte tenu de la grande disponibilité des technologies de l'information, les gouvernements prennent des mesures réglementaires d'envergure pour garantir la sécurité de tous les citoyens qui ont accès à l'Internet, en particulier les mineurs. Bien que la législation en matière de cybersécurité varie légèrement dans le monde, les racines du problème restent les mêmes.

L'une des principales raisons de l'apparition de ces réglementations est la vulnérabilité particulière des enfants d'âge préscolaire et primaire sur l'Internet, qui sont facilement victimes de prédateurs (personnes qui harcèlent sexuellement des mineurs via l'Internet), d'humiliation et de manipulation en ligne (lorsqu'un étranger gagne la confiance d'un enfant pour ses propres besoins), et d'utilisation abusive de données personnelles.

Les enfants sont progressivement devenus le groupe le plus exposé au risque de divulgation de renseignements personnels et de vol d'identité. Il est donc extrêmement urgent de protéger les informations personnelles des enfants.

Par exemple, la Chine a publié une réglementation spéciale relative à la protection en ligne des données à caractère personnel des enfants qui régit l'ensemble du cycle de collecte, stockage, utilisation, transfert et divulgation des données à caractère personnel des enfants[59]. La réglementation comprend des mesures spéciales de protection, des principes clairs et une gouvernance coopérative, dans le but de créer un environnement en ligne bénéfique pour le développement sain des enfants. Les mesures spéciales de protection comprennent

[56] Document 2/385 (Bhoutan) de la CE 2 de l'UIT-D.
[57] Document 2/286 (Chine) de la CE 2 de l'UIT-D.
[58] Document 2/400 (États-Unis) de la CE 2 de l'UIT-D.
[59] Document SG2RGQ/179 (Chine) de la CE 2 de l'UIT-D.

notamment le droit d'effacement des données et la non-divulgation des informations à caractère personnel des enfants, tandis que les principes incluent la finalité légitime, le consentement éclairé, l'objectif déterminé, la sécurité et l'utilisation légale. La réglementation s'applique principalement à la protection des informations à caractère personnel des enfants de moins de 14 ans.

En décembre 2010, la Fédération de Russie a adopté une loi relative à la protection des enfants contre les informations préjudiciables à leur santé et à leur développement qui garantit la sécurité informatique des mineurs et instaure les conditions et les modalités de diffusion de contenus aux enfants[60].

De plus, la Loi relative aux médias de la Fédération de Russie interdit dans les médias, ainsi que sur les réseaux d'information et de communication (comme l'Internet), la diffusion d'informations sur un mineur victime d'actes (inaction) illégaux, notamment:

- le nom, le prénom;
- une photo ou vidéo du mineur, de ses parents ou d'autres représentants légaux;
- sa date de naissance;
- un enregistrement audio de sa voix;
- son adresse permanente ou provisoire;
- son lieu d'étude ou de travail;
- toute information permettant directement ou indirectement d'établir son identité[61].

Enquêtes thématiques

L'UIT a fourni une assistance technique lors du processus d'élaboration en cours de la stratégie nationale de cybersécurité du Bhoutan[62]. Au cours de ce processus, une enquête a été menée auprès de 126 élèves (dont l'âge moyen était de 16 ans), dans le cadre de laquelle des questions à choix multiples ont été utilisées pour évaluer l'utilisation d'Internet, les incidents de sécurité tels que la cyberintimidation et la prévalence des virus informatiques ou des infractions commises par les élèves.

L'enquête a révélé que les étudiants utilisaient l'Internet de manière intensive. Presque tous les étudiants qui ont participé à l'enquête ont utilisé l'Internet, et plus de 40% l'ont utilisé pendant plus de deux heures par jour. La cybersécurité était un sujet d'actualité pour les étudiants: alors que près de 40% d'entre eux avaient été victimes d'une infection par un logiciel malveillant, seuls 10% environ ont déclaré utiliser un logiciel antivirus.

En ce qui concerne l'éducation à la cybersécurité, l'école reste une source importante de connaissances pour les élèves. Près de 40% des élèves ont déclaré que la cybersécurité leur était enseignée à l'école.

Les élèves avaient également été exposés à la cybercriminalité et à d'autres activités préjudiciables. Outre les virus informatiques, plus de 10% des élèves interrogés avaient été victimes de cyberintimidation, tandis que 25% avaient été contactés par un étranger en ligne. Le questionnaire contenait également une section sur les actes illicites ou inappropriés, qui a

60 Document 2/264 (Fédération de Russie) de la CE 2 de l'UIT-D.
61 Voir Article 4 de la Loi fédérale N° 2124, https://digital.gov.ru/ru/documents/6406/ [en russe], Document 2/264 (Fédération de Russie) de la CE 2 de l'UIT-D.
62 Document SG2RGQ/135 (Bhoutan) de la CE 2 de l'UIT-D.

révélé qu'environ 35% des élèves avaient envoyé des messages hostiles ou néfastes pouvant être considérés comme de la cyberintimidation. Environ le même nombre d'élèves avait tenté de s'introduire, avec succès ou non, dans un réseau sans fil sécurisé.

Compte tenu du caractère limité de cette enquête, le Bhoutan en a mené une autre sur la sécurité et la protection en ligne des enfants au niveau national. L'enquête s'inscrivait dans le cadre du projet "Digital Kids Asia Pacific" (DKAP, Les enfants et le numérique en Asie-Pacifique) lancé par le Bureau de l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO) à Bangkok, avec l'appui du Fonds d'affectation spéciale de la République de Corée (KFIT). 2 381 élèves âgés de 12 à 17 ans issus de 45 écoles du pays ont été interrogés sur 112 questions pour évaluer leur niveau de sensibilisation à la cybersécurité, aux menaces et aux mesures préventives. Il est ressorti de l'étude que la majorité des élèves (81%) ont accès à des smartphones à leur domicile. La plupart des élèves ont tendance à passer en moyenne une à deux heures en ligne par jour. En outre, 54% des élèves n'ont pas les connaissances pour distinguer les informations fiables de celles qui ne le sont pas. 49% des élèves redoutent qu'un tiers utilise leurs informations personnelles de manière abusive.

Certains élèves (10%) contournent les restrictions d'âge fixées pour des applications, en donnant de fausses informations, harcèlent des tiers et se connectent aux comptes d'autres utilisateurs. De plus, 85% des élèves souhaitent se faire de nouveaux amis en ligne et 68% ne voient pas d'inconvénient à s'entretenir avec des personnes issues d'un lieu ou d'un milieu différent du leur. L'enquête suscite des craintes en matière de sécurité, dans la mesure où 51% des élèves ont rencontré des inconnus qu'ils avaient d'abord rencontrés en ligne, 22,8% des élèves sont ouverts à l'idée de rencontrer des inconnus, et les filles rencontrent davantage d'inconnus que les garçons[63].

La PLCC, organe opérationnel de lutte contre la cybercriminalité en Côte d'Ivoire, a réalisé une enquête auprès de 200 jeunes issus de 3 lycées de la ville d'Abidjan afin d'analyser le comportement en ligne des enfants, de recenser les risques et de suggérer des stratégies de sécurité efficaces pour combattre les abus en ligne[64].

Au total, 83% des personnes interrogées dans le cadre de cette enquête ont déclaré utiliser l'Internet. La principale raison pour laquelle le pourcentage restant de personnes interrogées n'a pas utilisé l'Internet est le coût des téléphones intelligents et des terminaux. Pour les enfants âgés de 15 à 18 ans, la télévision avait été reléguée à un niveau d'utilisation secondaire, tandis que 86,3% avaient un compte sur les réseaux sociaux. Cette tranche d'âge préférait accéder à l'Internet par le biais des smartphones. Les images et les films violents ont été signalés comme la principale source d'expériences négatives en ligne, suivis par le piratage et, enfin, les insultes et les menaces. Dans une moindre mesure, les répondants ont fait état d'expériences négatives à connotation sexuelle. Certaines personnes interrogées ont déclaré avoir été victimes de chantage pour des vidéos au contenu sexuellement explicite.

Les expériences potentiellement les plus préjudiciables pour les enfants, selon l'enquête, sont les suivantes:

- Virus, bugs, spam ou piratage (24%)
- Vidéos à caractère sexuel (7,5%)
- Images ou vidéos violentes (28,6%)

[63] Document 2/385 (Bhoutan) de la CE 2 de l'UIT-D.
[64] Document 2/201 (Côte d'Ivoire) de la CE 2 de l'UIT-D.

- Utilisation de photographies sans accord préalable (7,5%)
- Insultes, malveillance ou menaces (19,5%)
- Usurpation d'identité (6,7%)
- Contact avec un étranger (4,51%)
- Escroqueries (0,75%)
- Sextortion (0,75%).

Soutien de l'UIT aux États Membres en matière de protection en ligne des enfants

Du 4 au 6 avril 2018, en coopération avec l'Académie nationale des télécommunications A. S. Popov d'Odessa, l'UIT a organisé un atelier régional sur la cybersécurité et la protection en ligne des enfants pour l'Europe et la Communauté des États indépendants (CEI) à Odessa, en Ukraine[65]. Les versions finales de tous les documents (y compris l'ordre du jour, les rapports, les conclusions et recommandations, la liste des participants, les exposés et les photographies) ont été publiées sur le site web de l'académie[66] et sur le site web de l'UIT[67]. Les participants à l'atelier, représentant 14 États Membres, ont conclu que les régions d'Europe et de la CEI devaient accroître leur coopération afin d'optimiser l'utilisation des ressources disponibles et d'obtenir des résultats pratiques, notamment par la traduction de matériel de formation sur la cybersécurité et la protection en ligne des enfants. Les conclusions et recommandations élaborées par les participants à l'atelier sont présentées dans le document final[68].

La protection en ligne des enfants est l'un des principaux domaines d'intérêt de l'initiative régionale de l'UIT pour l'Europe, qui vise à renforcer la confiance et la sécurité dans l'utilisation des télécommunications/TIC. En réponse aux demandes des Membres concernant les feuilles de route pour les initiatives de protection en ligne des enfants, l'UIT a mené une enquête auprès des gouvernements nationaux visés par l'initiative régionale, abordant un large éventail de questions liées aux politiques et pratiques contemporaines sur toutes les plates-formes technologiques utilisées par les enfants et les jeunes dans l'espace numérique. L'enquête a été menée pour la première fois auprès de tous les États Membres en 2009 et une version révisée a été réalisée en 2016 auprès des États Membres d'Europe centrale et orientale, des pays baltes et des Balkans.

Sur la base des réponses à l'enquête, le BDT a publié en 2017 un examen régional des activités nationales en matière de protection en ligne des enfants en Europe, qui précisait quelle était la situation des pays participants concernant l'élaboration, l'adoption, la mise en œuvre et le suivi des politiques dans le domaine de la protection en ligne des enfants[69]. Il fournissait aussi des exemples de pratiques actuelles dans les pays suivants: Albanie, Bosnie-Herzégovine, Bulgarie, Chypre, Croatie, Estonie, Finlande, Grèce, Hongrie, Lettonie, Liechtenstein, Lituanie, Macédoine du Nord, Monaco, Monténégro, Pologne, Slovaquie, République tchèque, Roumanie, Serbie, Slovénie et Turquie.

---

65 Document 2/75 (Académie nationale des télécommunications A. S. Popov d'Odessa (Ukraine)) de la CE 2 de l'UIT-D.

66 Académie nationale des télécommunications A. S. Popov d'Odessa, Atelier régional de l'UIT pour l'Europe et la CEI – Cybersécurité et protection en ligne des enfants, 4-6 avril 2018, Odessa (Ukraine).

67 UIT, Atelier régional de l'UIT pour l'Europe et la CEI – Cybersécurité et protection en ligne des enfants, 4-6 avril 2018, Odessa (Ukraine).

68 UIT, Conclusions et recommandations, Atelier régional de l'UIT pour l'Europe et la CEI sur la cybersécurité et la protection en ligne des enfants, 4-6 avril 2018, Odessa (Ukraine).

69 UIT-D, Examen régional des activités nationales en matière de protection en ligne des enfants en Europe, 2017.

Le Groupe de travail du Conseil de l'UIT sur la protection en ligne des enfants (GTC-COP) mène ses travaux conformément à la Résolution 1306 adoptée par le Conseil de l'UIT (à sa session de 2009), en plus de la Résolution 179 (Rév. Dubaï 2018), dans laquelle la Conférence de plénipotentiaires a décidé que l'UIT devrait poursuivre l'initiative de protection en ligne des enfants en tant que plate-forme de sensibilisation aux questions de sécurité des enfants en ligne; continuer à fournir une assistance et un soutien aux États Membres, en particulier aux pays en développement, pour l'élaboration et la mise en œuvre de feuilles de route pour l'initiative; et continuer à coordonner l'initiative, en coopération avec les parties prenantes concernées[70].

Des renseignements sur les 15ème, 16ème et 17ème réunions du GTC-COP, tenues respectivement le 26 septembre 2019, le 4 février 2020 et le 26 janvier 2021 à Genève et à distance, ont été fournis pour l'examen de la Question 3/2[71],[72].

Durant ces réunions, les documents suivants ont été présentés:

- Point sur les Lignes directrices relatives à la protection en ligne des enfants[73]
- Présentation des résultats de la consultation en ligne menée auprès des jeunes[74]
- Présentation des travaux et activités de l'UIT dans le domaine de la protection en ligne des enfants[75]
- Exposé sur le processus d'examen des Lignes directrices relatives à la protection en ligne des enfants pour 2019-2020[76]
- Exposé sur l'initiative de l'UIT pour la protection en ligne des enfants et la mise en œuvre des Lignes directrices de 2020 sur la protection en ligne des enfants[77].

L'un des principaux résultats de ces réunions a été la reconnaissance de la nécessité de fournir des orientations sur la manière d'améliorer le nombre de réponses des jeunes et d'accroître la participation des parties prenantes au sein du GTC-COP, étant donné l'importance de l'évaluation de l'efficacité du programme.

En 2020, l'UIT a organisé une série de forums thématiques[78] pour mettre en commun les résultats d'expérience dans le domaine de la protection en ligne des enfants entre les différentes parties prenantes et pour faire connaître les Lignes directrices sur la protection en ligne des enfants et faciliter leur promotion, leur adaptation et leur mise en contexte aux niveaux national et régional:

- Afrique: 30 octobre 2020[79]
- Amériques: 19 octobre 2020[80]

---

70 Conférence de plénipotentiaires de l'UIT, Résolution 179 (Rév. Dubaï, 2018), "Rôle de l'UIT dans la protection en ligne des enfants".

71 Document SG2RGQ/242 (Groupe de travail du Conseil sur la protection en ligne des enfants (GTC-COP)) de la CE 2 de l'UIT-D.

72 Les contributions des membres et des experts externes peuvent être consultées aux liens suivants: 15ème réunion, 16ème réunion, 17ème réunion.

73 UIT, GTC-COP, Document CWG-COP-14/2, "Le point sur l'Initiative relative à la protection en ligne des enfants (COP) de l'UIT".

74 UIT, GTC-COP, Document CWG-COP-15/INF/3, "Consultation en ligne auprès des jeunes".

75 UIT, GTC-COP. Document CWG-COP-16/5, "Travaux et activités de l'UIT dans le domaine de la protection en ligne des enfants".

76 UIT, GTC-COP. Document CWG-COP-16/4, "Processus d'examen des Lignes directrices relatives à la protection en ligne des enfants de l'UIT pour 2019-2020".

77 UIT, GTC-COP. Document CWG-COP-17/2(Rév.1), "UIT COP 2020, Protection en ligne des enfants et autonomisation".

78 UIT, Lancements régionaux: Lignes directrices de 2020 sur la protection en ligne des enfants.

79 UIT-D, Lancement au niveau de la région Afrique des Lignes directrices révisées sur la protection en ligne des enfants, 30 octobre 2020.

80 UIT-D, Lignes directrices sur la protection en ligne des enfants pour la région Amériques, 19 octobre 2020.

- États arabes: 23 novembre 2020[81]
- Asie et Pacifique: 3 novembre 2020[82]
- Communauté des États indépendants: 27 octobre 2020[83]
- Europe: 26-27 novembre 2020[84]

3.3 Enseignements tirés, étapes futures, mesures et conclusions

Le besoin de protection en ligne des enfants est devenu particulièrement aigu pendant la pandémie de COVID-19.

Un certain nombre d'enseignements peuvent être tirés des activités des États Membres sur des questions liées à la protection en ligne des enfants, notamment:

- chaque pays devrait reconnaître qu'il se doit de veiller à ce que l'Internet et ses technologies associées soient sûrs pour les enfants et les jeunes;
- les pays intègrent de plus en plus la sensibilisation aux risques en ligne dans un programme plus large de protection des enfants et d'éducation parentale;
- alors que l'idée se répand qu'Internet peut également être un facteur positif de renforcement de la citoyenneté et de l'apprentissage, dans de nombreux cas, le manque de ressources et de compétences disponibles au niveau local semble être un frein au développement;
- si les cadres législatifs de nombreux pays sont globalement conformes aux instruments juridiques internationaux et régionaux, il est extrêmement important pour chaque pays de veiller à ce que ses mesures juridiques et son cadre législatif restent en phase avec les évolutions technologiques et les changements de comportement;
- les coordonnateurs nationaux sont un élément clé d'une protection en ligne efficace, et tous les pays devraient disposer d'un coordonnateur national doté de ressources suffisantes et participant aux initiatives régionales et internationales[85].

Il existe également plusieurs domaines dans lesquels les États Membres pourraient faciliter davantage les activités de protection en ligne des enfants, par exemple:

- sensibiliser et former à la culture numérique tant les spécialistes professionnels de la cybersécurité que les enfants, les parents et les enseignants;
- élaborer des lois et des règlements pour protéger les enfants en ligne;
- réaliser des enquêtes représentatives afin de mieux adapter les politiques, initiatives et mesures existantes en matière de protection en ligne des enfants.

Il serait souhaitable que les associations à but non-lucratif et les organisations communautaires prennent des mesures visant à favoriser la prise de conscience et le développement des compétences des enfants pour les aider à mieux utiliser l'Internet dans un environnement sûr. Par exemple:

- dédramatiser la prévention, faute de quoi elle risquerait de renforcer la culture de la peur chez les parents concernant l'utilisation de l'Internet par leurs enfants, et éviter ainsi une approche susceptible d'augmenter l'angoisse de parents déjà inquiets devant une

81 UIT-D, Dialogue régional en ligne sur les lignes directrices et opportunités de mise en œuvre de la COP de l'UIT pour 2020 dans la région des États arabes, 23 novembre 2020.
82 UIT-D, Forum régional sur le développement pour l'Asie-Pacifique (RDF-ASP), Session post-forum sur la cybersécurité – Lancement des Lignes directrices de 2020 sur la protection en ligne des enfants dans la région Asie-Pacifique, 3 novembre 2020.
83 UIT-D, Forum UIT-UNESCO-IITE sur la protection en ligne des enfants pour la CEI, 27 octobre 2020.
84 UIT-D, Forum de l'UIT pour l'Europe sur la protection en ligne des enfants, 26-27 novembre 2020.
85 Document SG2RGQ/47 (Coordonnateur du BDT pour la Question 3/2) de la CE 2 de l'UIT-D.

technologie qu'ils comprennent mal, sabotant ainsi l'extraordinaire outil d'apprentissage qu'est l'Internet;

- encourager les programmes éducatifs visant à développer les bonnes pratiques dans la gestion de contenus et sensibiliser les enfants aux usages responsables de l'Internet;
- créer un portail Internet afin d'offrir aux enfants, aux adolescents, aux parents et aux enseignants une base éducative;
- engager tous les intervenants dans des activités de prise de conscience communautaire: agences gouvernementales, secteur Internet privé, organisations non gouvernementales, groupes communautaires et le grand public[86].

Dans l'ensemble, on peut conclure que:

- le rôle joué par la coopération internationale et le soutien des États pour assurer la cybersécurité et la protection en ligne des enfants sont essentiels;
- des instruments politiques nationaux devraient être utilisés pour élaborer des stratégies de cybersécurité dans les pays en développement;
- les partenariats public-privé sont importants pour accroître l'efficacité des outils techniques et d'organisation de la cybersécurité;
- l'élaboration de nouveaux mécanismes stratégiques et réglementaires pour la protection en ligne des enfants et l'évaluation des mécanismes existants ont atteint un point culminant;
- les établissements d'enseignement et les entreprises privées devraient participer à la mise en œuvre de projets visant à créer des outils techniques et d'organisation pour la protection en ligne des enfants, notamment dans le cadre des initiatives régionales de l'UIT;
- il convient d'élaborer des programmes et des outils éducatifs pour la protection en ligne des enfants qui tiennent compte des besoins des enfants handicapés;
- les États Membres devraient revoir leurs engagements au regard de l'Indice mondial de cybersécurité (GCI) et prendre de nouvelles mesures;
- les établissements d'enseignement, les entités du secteur privé et les organisations non gouvernementales devraient participer aux activités de l'UIT-D, y compris aux travaux des commissions d'études de l'UIT et des centres d'excellence qui dispensent des cours de formation à la cybersécurité.

Si l'on veut élaborer des solutions plus efficaces, il est essentiel que toutes les parties prenantes partagent des informations sur les outils disponibles dans le domaine de la cybersécurité et de la protection en ligne des enfants, étant donné l'importance croissante de cette protection dans le monde entier et la nécessité d'efforts de collaboration dans ce domaine, notamment dans le cadre des activités de l'UIT-D[87].

[86] Document 2/201 (Côte d'Ivoire) de la CE 2 de l'UIT-D.
[87] Document 2/75 (Académie nationale des télécommunications A. S. Popov d'Odessa (Ukraine)) de la CE 2 de l'UIT-D.

Chapitre 4 – Problèmes en matière de cybersécurité pour les personnes handicapées

4.1 Introduction

Les cyberattaquants ne s'interdisent de viser aucun individu. Les personnes handicapées ne devraient pas devoir faire face à des cyberrisques plus élevés simplement par manque d'information ou de sensibilisation.

Au cours de la période d'études 2014-2017, la Commission d'études 2 de l'UIT-D a mené une enquête sur la sensibilisation à la cybersécurité, dont les résultats ont été publiés dans le rapport final[88]. Les résultats ont montré que les personnes âgées et les personnes handicapées étaient les deux groupes les moins ciblés par les campagnes de sensibilisation à la cybersécurité. De plus, 69 pour cent des États Membres ayant pris part à l'enquête n'ont pas inclus les personnes handicapées dans les groupes cibles.

Ces résultats montrent clairement que les travaux doivent se poursuivre dans ce domaine. Afin de sensibiliser les personnes handicapées et les autres parties prenantes, y compris les pouvoirs publics et les organisations privées, aux besoins concrets en matière de cybersécurité, la Question 3/2 a continué d'examiner les considérations de sécurité particulières et les cybervulnérabilités sur la base de cas d'utilisation. Les cas d'utilisation, les enseignements tirés et d'autres informations utiles sont exposés dans le présent chapitre.

4.2 Cas d'utilisation

4.2.1 Auteurs de spams et usurpateurs d'identité qui ciblent les personnes handicapées

Aperçu

Les auteurs de spams et les pirates de messagerie électronique sont de plus en plus astucieux. En effet, ils ont acquis la capacité de déterminer si une cible potentielle a un handicap et d'utiliser ce handicap pour se faire passer eux-mêmes pour la cible. Les personnes handicapées ont également des difficultés à obtenir de l'aide de la part des services chargés de la sécurité et de la protection contre la fraude de leurs fournisseurs de courrier électronique.

Les personnes handicapées sont ciblées par les auteurs de spams et les pirates, qui se font passer pour la cible en utilisant le handicap de la personne comme identifiant. Dans un cas, le compte de courrier électronique d'une personne sourde qui utilisait la langue des signes

[88] UIT, Rapport final de la Commission d'études 2 de l'UIT-D sur la Question 3/2 pour la période d'études 2014-2017, Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité. UIT, 2017.

a été détourné. Dans ce cas, la victime possédait un compte Gmail, mais ce compte aurait pu appartenir à n'importe quel fournisseur de comptes de courrier électronique. Malheureusement, le service d'assistance Gmail n'a pas apporté beaucoup de soutien. Une fois que la victime a cliqué sur le lien d'hameçonnage et que son compte a été détourné, l'auteur de spams a pu accéder au carnet d'adresses de la victime et, éventuellement, à d'autres fichiers sur l'ordinateur de la victime.

Le service d'assistance a indiqué à la victime que la seule solution était de changer de fournisseur de messagerie électronique et d'adresse électronique. Si le handicap dans cet exemple était la surdité, il n'est pas inconcevable que n'importe quel handicap puisse être utilisé dans cette forme d'usurpation d'identité.

Il est important que les utilisateurs de courrier électronique, y compris les utilisateurs handicapés, comprennent l'importance de vérifier tous les liens qui leur sont envoyés, même par des amis, avant de cliquer sur un lien. Les services d'assistance des fournisseurs de messagerie électronique doivent également s'intéresser activement à cette forme d'abus, en particulier lorsque des communautés vulnérables sont visées. Dans ce cas, la victime a contacté le numéro de téléphone du service d'assistance par l'intermédiaire d'un ami ou d'un service de relais téléphonique pour sourds; les fournisseurs de services devraient traiter ces appels plus sérieusement ou fournir un numéro de téléphone spécial avec des interlocuteurs qui sont des êtres humains que les utilisateurs sourds peuvent contacter directement à l'aide d'un téléimprimeur. Mieux encore, les prestataires de services devraient engager du personnel d'assistance pratiquant couramment la langue des signes. Aux États-Unis, Amazon a pris des mesures pour fournir un tel service, par exemple.

Exemples de courriels

Vous trouverez ci-dessous deux exemples du type de courriel que l'auteur de spams du cas décrit ci-dessus a envoyé à la liste de contacts de la victime. En réponse, la victime a changé de fournisseur de messagerie électronique après avoir informé ses contacts que sa messagerie avait été piratée.

Exemple 1: L'auteur de spams se fait passer pour la personne handicapée.

De: Personne handicapée personnehandicapée@gmail.com

Date: 23 mars 2018 13:00

Objet: GÉNIAL!! Le pays X AUGMENTE L'ALLOCATION MENSUELLE POUR LES PERSONNES SOURDES DE 70%

Génial! Le Pays X a pensé à toutes les personnes Sourdes et Malentendantes et le dirigeant du Pays X a décidé d'augmenter les allocations SSA, SSI et SSDI de 70% et c'est une Bonne Nouvelle pour toutes les personnes Sourdes et Malentendantes du Pays X

Pour en savoir plus et savoir de combien votre allocation SSA, SSI ou SSDI ont augmenté,

Cliquez ici http://noisecancel.net/js/gggg/G/G/us/index.php

[Note: le lien d'hameçonnage d'origine a été modifié.]

Et Identifiez-vous avec votre e-mail et vérifiez que tout est correct

NouvellesSourds

Exemple 2: De la victime avertissant ses contacts que sa messagerie a été piratée.

Bonjour à tous!

Comme je l'ai dit plus tôt, après avoir été incité à visionner une vidéo en ASL il y a trois semaines, mon ancien gmail a été piraté!

[Note: ASL signifie langue des signes américaine.]

Le pirate continue d'envoyer de FAUX courriels en utilisant mon compte gmail. Ce qui est effrayant, c'est que le contenu semble réaliste et lié à mes activités liées à la surdité.

Après avoir passé des heures à parcourir le réseau robotique de Google, j'ai trouvé un numéro de téléphone, le (855) 836-3987, pour joindre un humain.

Devinez quoi? Au lieu d'essayer de m'aider, ils ont dit "dommage".

Est-ce que votre Gmail est sécurisé?

Dans l'intervalle, effacez TOUS les courriels.

<de personnehandicapée@gmail.com>

Avec toutes mes excuses.

Personne handicapée

Enseignements tirés et bonnes pratiques suggérées

- Les personnes handicapées devraient être sensibilisées aux problèmes connus de spam et de logiciels malveillants.
- Les prestataires de services devraient mettre à disposition du personnel qualifié pour traiter les demandes des clients handicapés.
- Les utilisateurs de courrier électronique ne devraient cliquer sur aucune adresse web à moins que la source n'ait été vérifiée.
- Les victimes de piratage de messagerie électronique devraient:
    - informer leur fournisseur de messagerie électronique;
    - transmettre le courriel suspect au service des fraudes du fournisseur de messagerie électronique;
    - demander que l'adresse électronique piratée soit bloquée;
    - changer d'adresse électronique;
    - informer tous leurs contacts que l'adresse électronique a été piratée et leur fournir la nouvelle adresse.

4.2.2 Cyberrisques associés aux technologies d'assistance fondées sur l'IoT

Contexte

Selon l'Organisation mondiale de la santé (OMS), plus de 2 milliards de personnes sont handicapées, ce qui représente 37,5% de la population mondiale[89]. Comme le relève le Département des affaires économiques et sociales des Nations Unies, les pays ne partagent pas une définition uniforme des "personnes handicapées" et ont donc adopté des classifications et des seuils différents[90]. Selon la définition internationalement reconnue de l'OMS, une personne handicapée est toute personne qui a un problème de fonctionnement ou de structure corporelle, une limitation d'activité ou une difficulté à exécuter une tâche ou une action[91].

Comme il ressort de cette définition, il existe de nombreux types de handicaps. Chaque handicap représente un obstacle qui affecte la vie des gens. Cependant, la technologie joue un rôle important pour faire tomber ces barrières et aider les personnes handicapées à bénéficier de meilleures conditions de vie.

De nos jours, la technologie est très répandue et influence la vie quotidienne des individus et la société dans son ensemble. Au cours de la dernière décennie, l'IoT a démontré qu'il était possible d'améliorer la vie des personnes handicapées[92]. Les technologies d'assistance fondées sur l'IoT sont donc de plus en plus utilisées pour surmonter les limites découlant des handicaps[93].

La Convention relative aux droits des personnes handicapées cite les TIC comme un élément essentiel de l'assistance aux personnes handicapées. En particulier, l'article 9, sur l'accessibilité, souligne le rôle des TIC dans la promotion de l'indépendance et de la pleine participation des personnes handicapées dans différents domaines, et charge les États parties de faire des efforts conjoints délibérés pour faire progresser l'accès aux TIC[94].

Les TIC et l'IoT augmentent la sécurité, la mobilité et l'indépendance; des prothèses connectées à l'Internet aux chaussures intelligentes qui vibrent pour guider le porteur, de nombreux dispositifs et services de l'IoT sont conçus pour améliorer les conditions de vie et réduire la dépendance des personnes handicapées vis-à-vis d'autrui[95]. Par exemple, les personnes aveugles ou ayant une déficience visuelle peuvent utiliser la technologie pour les aider à s'orienter dans leur environnement et à accéder à des informations écrites. En outre, les technologies de la maison intelligente permettent aux individus de contrôler les appareils et autres éléments de leur domicile qui peuvent être difficiles à atteindre, tels que les lumières, les serrures de porte et les systèmes de sécurité.

---

89 OMS, Rapport mondial sur le handicap 2011. OMS, 2011.
90 Département des affaires économiques et sociales de l'ONU (DAES-ONU), Disability and Development Report: Realizing the Sustainable Development Goals by, for and with persons with disabilities, Nations Unies, New York, 2018.
91 OMS, op. cit., Chapitre 1.
92 Future of Privacy Forum, The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions, janvier 2019.
93 OMS, Thèmes de santé, Technologies d'assistance.
94 DAES-ONU, Convention relative aux droits des personnes handicapées (CPRD), Article 9 – Accessibilité.
95 Future of Privacy Forum, op. cit.

La technologie: une arme à double tranchant

Tout en offrant de nombreux avantages, les technologies d'assistance fondées sur l'IoT augmentent également de manière exponentielle l'exposition des utilisateurs aux cyberrisques. Étant donné la dépendance croissante à l'égard des technologies d'assistance, toute perturbation ou modification de ces technologies pourrait entraîner une vulnérabilité accrue.

Les dispositifs et services IoT sont souvent caractérisés par des niveaux de sécurité médiocres. Par exemple, ils peuvent ne pas utiliser un chiffrement approprié pour la transmission des données, ce qui peut entraîner une divulgation inappropriée des données et des fuites de données. Pour les personnes handicapées en particulier, les données personnelles peuvent être de nature sensible, car elles peuvent révéler des détails sur l'état de santé de l'individu.

Étant donné l'importance des technologies d'assistance pour les personnes handicapées, les incidences préjudiciables des cyberrisques peuvent être catastrophiques. Par exemple, certaines personnes handicapées physiques ont besoin de prothèses biomécaniques pour retrouver un mouvement complet ou partiel. Ces prothèses utilisent des capteurs spécifiques pour lire et analyser les paramètres de contraction musculaire afin de reproduire les mouvements au moyen des dispositifs (par exemple, le déplacement des doigts du bras prothétique). Les prothèses envoient régulièrement des données dans le nuage pour alimenter leur analyse informatique et améliorer leur efficacité. Cette connectivité rend ces dispositifs vulnérables aux attaques visant à accéder, manipuler ou supprimer les données contenues dans le nuage ou à accéder aux données personnelles des utilisateurs. De plus, les agresseurs pourraient prendre le contrôle des prothèses à distance. Si la prothèse est connectée à un implant cérébral, les conséquences pourraient être encore plus graves[96].

Autre exemple, certaines personnes malentendantes ont recours à des implants cochléaires, qui sont plus invasifs qu'une aide auditive classique. Cette technologie repose sur trois composants de base, à savoir un microphone, un processeur vocal et un récepteur-stimulateur implanté. Certains implants cochléaires modernes sont accompagnés de dispositifs de contrôle à distance qui permettent aux utilisateurs de contrôler les réglages de l'implant via une application mobile. À un niveau de base, les agresseurs pourraient chercher à désactiver l'implant, ce qui rendrait la victime sourde. Des attaques plus perfectionnées pourraient empêcher le processeur vocal de recevoir les signaux du microphone ou modifier le récepteur pour transmettre les sons générés par l'agresseur. Ces attaques plus avancées pourraient être plus difficiles à détecter, en particulier lorsque les utilisateurs d'implants cochléaires n'ont aucun autre moyen de vérifier ce qu'ils entendent.

En plus des attaques adaptées aux technologies d'assistance, les agresseurs peuvent également cibler les technologies couramment utilisées par les personnes handicapées. Par exemple, les malvoyants perdraient tout moyen de navigation fiable si les outils GPS qu'ils utilisent étaient défectueux ou étaient délibérément compromis par les agresseurs. Dans les attaques de piratage GPS, un émetteur radio situé près de la cible est utilisé pour brouiller un signal GPS légitime[97]. L'agresseur peut alors transmettre des coordonnées inexactes ou interrompre la transmission de données, ce qui peut entraîner des dommages physiques et d'autres conséquences importantes.

---

[96] Vladimir Dashchenko, "How to Attack and Defend a Prosthetic Arm", Securelist (Kaspersky), 26 février 2019.
[97] Maria Korolov, What is GPS spoofing? And how you can defend against it, *site web CSO*, International Data Group (IDG), 7 mai 2019.

Ce ne sont là que quelques exemples de cyberattaques possibles visant les technologies d'assistance numériques, mais ils mettent en évidence l'importance de la cybersécurité pour garantir la sécurité des personnes handicapées qui dépendent de ces technologies.

Prochaines étapes à examiner

L'internet et l'IoT peuvent faciliter la participation des personnes handicapées à la vie sociale, économique et civile. Si le potentiel de ces technologies est évident, des efforts constants sont nécessaires pour aligner les facteurs sociétaux, législatifs, personnels et infrastructurels au sein de l'écosystème IoT de manière à donner la priorité à la sécurité des dispositifs IoT. Il existe des mesures concrètes que les gouvernements pourraient prendre pour améliorer la sécurité et, par conséquent, la fiabilité des technologies d'assistance.

Les pouvoirs publics pourraient prendre des mesures pour améliorer la législation et les politiques en matière d'accessibilité et de sécurité de l'IoT et élaborer des mécanismes pour encourager et faire appliquer leur mise en œuvre. Ces cadres doivent commencer par une évaluation des besoins des personnes handicapées et doivent définir clairement les rôles et les responsabilités. Étant donné que le sujet est susceptible d'intéresser des représentants de divers domaines gouvernementaux (par exemple, la technologie et les télécommunications, le bien-être et la médecine), la collaboration est essentielle et doit être encouragée dans chaque initiative.

Des initiatives particulières pourraient être prises. Par exemple, les pouvoirs publics pourraient élaborer des systèmes de certification en matière de cybersécurité pour les technologies d'assistance, qui pourraient inclure des contrôles et des tests de sécurité périodiques et l'obligation de procéder à des mises à jour régulières du système pour l'adapter aux évolutions technologiques. Ils pourraient également soutenir les fabricants en offrant des incitations, en encourageant les partenariats public-privé et en proposant des financements de démarrage et des subventions de recherche et développement.

De même, il est nécessaire de promouvoir une culture de la sécurité qui réponde aux risques que ces technologies comportent. Les gouvernements devraient collaborer avec le secteur privé pour mener des campagnes de sensibilisation de la population à la cybersécurité.

En conclusion, si les technologies d'assistance fondées sur l'IoT sont un élément clé de l'aide aux personnes handicapées, elles peuvent également présenter un certain nombre de risques qui, s'ils ne sont pas correctement pris en compte, pourraient avoir de graves conséquences. Les technologies d'assistance doivent donc répondre aux normes de sécurité les plus élevées et doivent s'adapter aux évolutions technologiques.

Enseignements tirés et bonnes pratiques suggérées

Comme décrit ci-dessus, des mesures de cybersécurité devraient être mises en œuvre pour les personnes handicapées, en particulier celles ayant des difficultés auditives, comme les services de relais de télécommunication et le sous-titrage à distance, pour améliorer l'accessibilité des services d'information et de communication.

4.2.3 Prise en compte des questions de sécurité pour les services d'accessibilité aux TIC

Introduction

Les services d'accessibilité aux TIC comme les services de relais de télécommunication et le sous-titrage à distance permettent aux personnes handicapées de communiquer et d'accéder à l'information. Ces services exigent naturellement que des mesures de sécurité soient prises pour protéger la sécurité et la vie privée des personnes handicapées et pour atténuer la cybervulnérabilité de ces personnes et d'autres groupes ayant des besoins spécifiques, tels que les enfants et les personnes âgées.

Aspects relatifs à la sécurité du sous-titrage à distance

Le sous-titrage à distance est un service dans lequel les mots prononcés lors d'une réunion ou d'une conférence sont transcrits à un endroit différent de celui où la réunion a lieu[98]. Des dispositifs TIC comme des téléphones, des téléphones portables ou des microphones d'ordinateur sont utilisés pour envoyer la voix de l'orateur au sous-titreur, qui la transcrit en texte. Le texte transcrit est ensuite transmis en temps réel au lieu de la réunion, où le texte peut être lu. Le texte sous-titré à distance est souvent affiché sur un écran public dans la salle de réunion ou sur un écran personnel. Non seulement les services de sous-titrage à distance sont essentiels pour permettre aux personnes sourdes ou malentendantes de participer aux réunions, mais ils sont également utiles pour les personnes dont la langue maternelle est différente de celle utilisée dans la réunion ou pour les situations où des intervenants ayant des voix et des accents différents participent à des groupes variés (par exemple au travail, dans une salle de classe ou dans des salles de réunion). La personne qui fournit des transcriptions pour un service de sous-titrage à distance, appelée "sous-titreur", doit être un rédacteur de procès-verbaux qualifié.

Les services de sous-titrage à distance sont exigés par divers codes de conduite nationaux ou locaux. Le fournisseur doit prendre toutes les mesures de précaution raisonnables pour garantir la confidentialité de la réunion, car il se peut que des informations confidentielles y soient échangées.

Types d'informations confidentielles

Voici une liste non exhaustive d'informations potentiellement confidentielles:

- Renseignements sensibles examinés lors de réunions et/ou de conférences
- Informations médicales de patients
- Renseignements juridiques concernant des individus
- Consultations
- Informations sur le respect de la réglementation en matière de protection des données.

[98] Secteur de la normalisation des télécommunications de l'UIT (UIT-T), Document technique FSTP-ACC-RCS – Vue d'ensemble des services de sous-titrage à distance, 17 octobre 2019.

Les fournisseurs de services de sous-titrage à distance doivent respecter les lois et règlements applicables en matière de protection de la vie privée et des données, tels que ceux établis par l'Union européenne[99].

Chiffrement du texte sous-titré

Le texte diffusé sur un écran ou un terminal personnel doit être protégé par un mot de passe. Le fournisseur de services de sous-titrage à distance est responsable de la sécurité du script et est tenu de respecter les exigences en matière de protection des données. Il est recommandé que le texte et, le cas échéant, l'URL de la source de texte soient chiffrés à l'aide du protocole couche de connexion sécurisée (secure sockets layer) ou d'une autre technologie pertinente.

Chiffrement du signal audio

Les données audio originales de l'événement doivent être protégées de manière sûre.

Considération en matière de sécurité pour les services de relais de télécommunication

Équivalence fonctionnelle

L'équivalence fonctionnelle est définie comme *"la possibilité pour des personnes ayant une plage de capacités différentes (en particulier les personnes handicapées et les personnes ayant des besoins particuliers) d'utiliser un service ou un système de communication avec un niveau de fonctions offertes et une commodité d'utilisation similaires à ceux offerts au groupe plus large d'utilisateurs dans une population [...] Cela inclut des considérations à la fois techniques et économiques et qu'aucune discrimination financière ne soit imposée aux utilisateurs du service de relais"*[100].

L'équivalence fonctionnelle comprend les obligations de sécurité applicables aux fournisseurs de services de communication dans un pays donné. L'équivalence fonctionnelle suppose que les utilisateurs des services de relais doivent être sur un pied d'égalité avec les autres utilisateurs au sein d'une communauté donnée, notamment en ce qui concerne les types d'appels autorisés par les services de relais, ce qui peut avoir des conséquences pour la sécurité.

Prescriptions de sécurité pour l'équivalence fonctionnelle

Pour parvenir à une équivalence fonctionnelle, il est essentiel de garantir la confidentialité, la vie privée et la sécurité des services de relais téléphoniques, des technologies utilisées par ces services et des assistants de communication humaine qui travaillent pour eux.

Les prescriptions applicables aux services de relais téléphoniques en matière de confidentialité et de sécurité des appels, y compris le chiffrement, doivent être en harmonie avec celles applicables aux services généraux de télécommunications dans le pays ou la région en question.

---

99 Union européenne, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

100 UIT-T. Recommandation UIT-T F.930, "Services relais de télécommunications multimédias".

Considérations en matière de cybervulnérabilité pour les personnes ayant des besoins particuliers

Il est très important de garantir une utilisation sûre de l'Internet pour les personnes handicapées et les groupes ayant des besoins particuliers comme les personnes âgées et les enfants. La réduction de la cybervulnérabilité de ces groupes est une question urgente et essentielle qui nécessite l'élaboration et le respect de lignes directrices.

4.3 Renseignements utiles

La Question 7/1 ("Accès des personnes handicapées et des autres personnes ayant des besoins particuliers aux services de télécommunication/TIC"), dont l'étude a été confiée à la Commission d'études 1 de l'UIT-D, aborde plusieurs thèmes dans ce domaine[101].

Le Future of Privacy Forum a publié un rapport intitulé "The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions" ("L'Internet des objets (IoT) et les personnes handicapées: Explorer les avantages, les défis et les tensions en matière de protection de la vie privée")[102].

De plus amples informations sont disponibles dans ces sources.

[101] Commission d'études 1 de l'UIT-D, Question 7/1.
[102] Future of Privacy Forum, op. cit.

Chapitre 5 – État des lieux des problèmes de cybersécurité, dont ceux associés aux technologies émergentes comme l'Internet des objets et l'informatique en nuage

5.1 Introduction

La croissance exponentielle des capacités technologiques a conduit à un monde de plus en plus numérisé, connecté et interconnecté. Selon le Forum économique mondial, une période connue sous le nom de "mondialisation 4.0" a déjà commencé, dans laquelle les biens et services numériques constituent le fondement de l'économie et des exportations[103].

L'innovation transforme le paysage technologique pour répondre aux nouveaux besoins commerciaux et pratiques. Les dispositifs IoT, ainsi que la technologie 5G, sont de plus en plus omniprésents, avec un nombre estimé de 41,6 milliards de dispositifs connectés dans le monde d'ici à 2025[104]. Les solutions d'informatique en nuage sont devenues essentielles pour les activités, 94% des entreprises du monde entier y ayant recours[105]. Compte tenu de la disponibilité et de la précision croissantes des données, l'intelligence artificielle continue également à trouver des applications plus larges.

L'apparition de nouvelles technologies entraîne toutefois un besoin accru de cybersécurité. L'innovation numérique a donné naissance à davantage de produits et à une complexité considérable, augmentant ainsi la probabilité de vulnérabilités et de faiblesses qui pourraient être exploitées.

Les cybermenaces sont en constante augmentation. En 2018, il y a eu 80 000 cyberattaques par jour, ce qui représente plus de 30 millions d'attaques par an[106]. En 2019, plus de 90 milliards de tentatives de compromission d'informations sensibles ont été enregistrées chaque jour[107]. Les cybermenaces sont également de plus en plus perfectionnées, menaçant l'ensemble du monde et de l'économie numérique, y compris les systèmes cyberphysiques dans les foyers, les villes intelligentes, les véhicules, les systèmes de production et les infrastructures critiques.

---

103 Klaus Schwab, Globalization 4.0 – What Does It Mean?, *Forum économique mondial*, 5 novembre 2018.
104 Business Wire, The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast, 18 juin 2019.
105 Kim Weins, Cloud Computing Trends: 2019 State of the Cloud Report, *Flexera Blog*, 21 mai 2020.
106 PurpleSec, 2019 Cyber Security Statistics Trends & Data: The Ultimate List of Cyber Security Stats, *PurpleSec* (blog), consulté le 27 avril 2020.
107 Check Point, Prepare for a New Cyber Cold War in 2020, Warns Check Point, communiqué de presse, 24 octobre 2019.

Les experts ont démontré qu'il est même possible de pirater des dispositifs médicaux implantés dans le corps humain, tels que les stimulateurs cardiaques et les pompes à insuline[108].

Une telle augmentation des attaques est également due à la prolifération, via le "dark web", du piratage informatique en tant que service, souvent à un prix abordable. La cybercriminalité est de plus en plus commercialisée et est devenue un vaste secteur, dans lequel les pirates vendent une grande variété d'outils et de services malveillants, allant du vol de mots de passe de faible niveau à des kits d'exploitation et des technologies d'attaque très perfectionnées comme les attaques par déni de service réparti (DDoS), les logiciels malveillants, les rançongiciels et les logiciels espions[109]. De plus, les technologies émergentes, qui sont souvent utilisées pour améliorer les solutions de cyberdéfense, peuvent être utilisées de manière malveillante pour accroître l'efficacité et la portée des outils de piratage[110]. L'intelligence artificielle, les botnets automatisés, l'IoT et les solutions d'informatique en nuage sont de plus en plus utilisés dans les cyberattaques à grande échelle, et la combinaison de nouvelles techniques de piratage – comme les outils d'hameçonnage automatisés – avec les technologies émergentes a élargi le paysage du cyberrisque.

L'un des principaux défis de la cybersécurité est le manque général de compétences professionnelles et le manque de sensibilisation des employés. Alors que les cybermenaces deviennent de plus en plus évoluées, les organisations ont du mal à recruter des experts en cybersécurité capables de protéger leurs systèmes[111]. En 2017, 82% des employeurs ont déclaré que leur personnel n'avait pas de compétences suffisantes en matière de cybersécurité. D'ici à 2021, 4 millions de postes de professionnels de la cybersécurité seront vacants[112]. En outre, le personnel non spécialisé est peu sensibilisé aux cybermenaces. Le facteur humain joue un rôle clé dans la cybersécurité et s'est révélé être un handicap important. En 2018, une étude a révélé que 99% des incidents numériques étaient involontairement provoqués par des employés victimes d'ingénierie sociale, tandis que 1% seulement résultaient exclusivement de défaillances ou de l'exploitation de failles technologiques[113].

La cybersécurité est un domaine dynamique et les organisations doivent constamment revoir leurs choix de cybersécurité pour se défendre contre les nouvelles menaces. Afin de créer un environnement plus sûr, il importe d'entamer un dialogue avec les parties prenantes au sujet de la gestion des risques liés à la cybersécurité et à la vie privée, de vérifier, compléter et affiner les processus de gestion des risques liés à la cybersécurité et à la vie privée existants et d'identifier les principales considérations en matière de cybersécurité et de vie privée qui peuvent être propres à certaines solutions et environnements technologiques. Le présent chapitre traite de nombreuses menaces de cybersécurité liées aux technologies émergentes, notamment l'IoT, le nuage, la 5G, l'IA et la quatrième révolution industrielle (connue sous le nom d'"Industrie 4.0"). Il présente également les tendances actuelles, les défis et les solutions possibles pour faire face aux menaces qui pourraient neutraliser les gains réalisés grâce à l'innovation numérique.

---

108 Lily Hay Newman, These Hackers Made an App That Kills to Prove a Point, *Wired*, 16 juillet 2019; *Dan Goodin*, Insulin Pump hack delivers fatal dosage over the air, *The Register*, 27 octobre 2011.
109 Armor, The Dark Market Report: The New Economy, 28 septembre 2020.
110 Deloitte, Protecting against the changing cybersecurity risk landscape. Future of risk in the digital era, Deloitte & Touche LLC, 2019.
111 William Crumpler et James A. Lewis, The Cybersecurity Workforce Gap, Center for Strategic and International Studies, 29 janvier 2019.
112 Rob Saunders, 134 Cybersecurity Statistics and Trends for 2021, Varonis, mis à jour le 16 mars 2021.
113 Proofpoint, Proofpoint's Annual Human Factor Report Details Top Cybercriminal Trends: More than 99 Percent of Cyberattacks Need Humans to Click, 9 septembre 2019.

5.2 Menaces, acteurs et motivations dans le domaine de la cybersécurité

Le but des cybermenaces est de saper les trois objectifs traditionnels de la cybersécurité, à savoir la confidentialité, l'intégrité et la disponibilité. La confidentialité protège les informations contre tous, sauf ceux qui sont autorisés à y accéder. L'intégrité garantit l'exactitude et la fiabilité des informations et empêche toute altération non autorisée des données. La disponibilité fait référence à la capacité d'accéder aux données et aux informations en cas de besoin.

Le paysage de la cybermenace est un environnement hétérogène, peuplé de divers acteurs qui poursuivent des objectifs différents et qui ont des capacités différentes. De manière générale, les acteurs malveillants peuvent être classés comme suit:

- ***Utilisateurs internes***: selon des rapports récents, environ 40% des incidents sont perpétrés par le personnel interne, souvent des employés mécontents qui cherchent à se venger de leurs employeurs[114]. Les utilisateurs internes peuvent être particulièrement dangereux car ils ont un accès direct aux données, aux informations et aux actifs numériques.
- ***Activistes informatiques***: il s'agit d'individus motivés par des causes politiques et sociales. Ils volent et diffusent généralement des informations sensibles dans le but de mettre dans l'embarras des dirigeants politiques ou des célébrités et ils divulguent des données exclusives et confidentielles au nom de la liberté d'expression. Il est fréquent qu'ils défigurent aussi des sites web et mènent des attaques DDoS contre des services ou des sites web particuliers[115].
- ***Cybercriminels***: il s'agit de criminels motivés par le gain financier. Ils ciblent les informations relatives aux individus, aux entreprises et aux organisations dans le but de les monétiser. Ils font généralement du chantage aux cibles, exfiltrent et vendent des données et de la propriété intellectuelle sur le marché noir et exécutent des attaques par rançongiciel. Comme nous l'avons vu plus haut, la cybercriminalité a évolué pour devenir un service dans lequel divers groupes vendent des biens et des services offensifs, allant de l'exploitation de systèmes au cycle de vie complet des attaques.
- ***Menaces persistantes avancées***: selon la définition du United States National Institute of Standards and Technology (NIST), il s'agit d'adversaires très astucieux et ingénieux capables de s'implanter dans le réseau de la cible à des fins comme l'exfiltration d'informations, l'affaiblissement ou l'entrave d'aspects critiques de la mission de la cible ou la dégradation de ses biens numériques[116]. Les menaces persistantes avancées s'adaptent aux systèmes de défense des victimes en utilisant de multiples vecteurs d'attaque et elles sont capables de poursuivre furtivement leur objectif pendant de longues périodes. Ces adversaires sont les plus évolués en matière de compétences techniques, de financement et de ressources organisationnelles et ils sont souvent parrainés par des États qui cherchent à défendre leurs intérêts géopolitiques.

Alors que tous les acteurs malveillants visent la confidentialité, l'intégrité et la disponibilité des informations et des biens, l'intrusion sur les réseaux peut avoir de nombreuses conséquences. L'expression fourre-tout "cyberattaque" couvre une variété d'actions, allant des nuisances comme la dégradation de sites web ou les attaques par déni de service(DoS) à la destruction critique de données et de systèmes par des attaques armées.

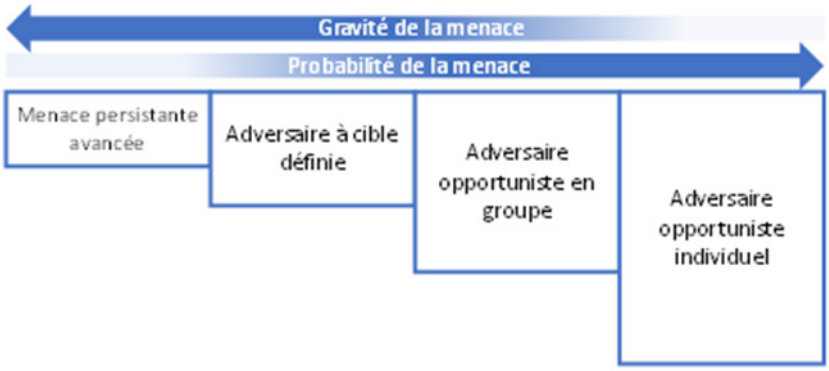
Les acteurs malveillants et leurs attaques diffèrent en matière de complexité, de durée et de nocivité. Bien qu'il soit impossible de se défendre contre tous les dangers, les organisations peuvent appliquer des modèles de menace pour identifier les menaces pertinentes en fonction

---

114 Verizon, 2019 Data Breach Investigations Report, Verizon, 2019.
115 Lillian Ablon, Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data, RAND Corporation, 2018.
116 NIST, Joint Task Force Transformation Initiative, NIST Special Publication 800-39: Managing Information Security Risk – Organization, Mission, and Information System View, mars 2011.

de leur profil, du risque et du contexte. La **Figure 1** illustre un modèle général de cybermenace qui montre que la plupart des organisations sont généralement confrontées à des menaces opportunistes et modérément complexes, nécessitant ainsi des dispositifs de défense moins élaborés.

Figure 1 – Modèle de menace



Au contraire, les grandes entreprises et les organisations actives dans des secteurs critiques et stratégiques ainsi que les entités qui gèrent des informations et des biens précieux sont plus susceptibles d'être attaquées par des menaces ciblées ou des menaces persistantes avancées.

La présente section a fourni un aperçu général des menaces qui pèsent sur le cyberespace. Le reste du chapitre fournit des informations sur la manière dont ces menaces s'appliquent aux technologies émergentes et sur les stratégies, cadres et solutions pratiques disponibles pour s'en défendre.

5.2.1 Menaces vues sous l'angle technologique

Les nouvelles technologies permettent de recueillir, de partager, de stocker et d'analyser d'énormes quantités de données, souvent à une vitesse sans précédent. Cependant, des caractéristiques particulières comme la connectivité et la complexité croissantes des environnements dans lesquels ces outils interagissent peuvent soulever un certain nombre de défis technologiques et d'organisation pour la sécurité.

Virtualisation

La virtualisation constitue un pilier essentiel des environnements technologiques contemporains car elle permet aux concepteurs de personnaliser les infrastructures afin de répondre aux besoins des applications de réseau et de prendre en charge le développement de nouvelles architectures et de nouveaux protocoles dans un environnement idéal[117]. Toutefois, le partage des canaux de communication et des dispositifs de routage dans les environnements multilocataires présente un certain nombre de risques pour la sécurité[118]:

- Le risque de divulgation non autorisée de données, qu'elle soit intentionnelle ou non, est exacerbé dans les environnements virtuels où les ressources physiques sont partagées

[117] Leonardo Richter Bays et al, Virtual network security: threats, countermeasures, and challenges, *Journal of Internet Services and Applications* 6, article N° 1 (2015).
[118] Agence de l'Union européenne pour la cybsersécurité (ENISA), Security aspects of virtualization, 10 février 2017.

entre plusieurs clients ou utilisateurs. Les activités malveillantes comme l'interception et le balayage (recherche de résidus de données dans un réseau afin d'acquérir des informations) peuvent être menées plus facilement si le système permet une inspection croisée des différents utilisateurs.

- L'environnement multilocataires peut accroître les risques qui découlent de la chaîne d'approvisionnement et rendre plus difficile la défense contre les intrusions. Les adversaires peuvent obtenir des privilèges et s'introduire dans le réseau de la cible en utilisant des ressources ayant un niveau de protection inférieur et partageant la même couche physique qu'un vecteur.
- Dans les environnements virtualisés, les résultats du traitement de l'identité sont particulièrement complexes en raison des systèmes très hiérarchisés d'administration des privilèges. Ce contexte offre aux acteurs malveillants la possibilité de commettre des fraudes à l'identité et de s'arroger des privilèges.
- Le partage des ressources peut également amplifier le risque de perturbations malveillantes ou involontaires du système qui peuvent avoir un effet négatif sur la fourniture de services. Par exemple, la surcharge des ressources physiques peut dégrader les performances des réseaux virtuels, avec pour conséquence une perturbation de la communication.

Sécurité de l'informatique en nuage

Dans les solutions d'informatique en nuage, la fourniture de services et de ressources informatiques, y compris les fonctions et responsabilités de sécurité associées, est sous-traitée au fournisseur d'informatique en nuage. D'une part, cela peut permettre aux nouvelles technologies de s'étendre rapidement et de renforcer la sécurité, puisque le fournisseur, en s'appuyant sur les économies d'échelle, peut potentiellement offrir des mesures de protection et des contrôles avancés. D'autre part, les vulnérabilités du nuage peuvent être tentantes pour les cyberattaquants, étant donné qu'un seul piratage réussi pourrait compromettre de nombreux clients. Les solutions en nuage comprennent plusieurs couches d'abstraction (à savoir l'application, le système d'exploitation, l'architecture et le réseau), ce qui signifie que les adversaires peuvent les cibler par le biais de multiples vecteurs:

- Les vulnérabilités logicielles peuvent être exploitées par des injections d'éléments en langage de requête structuré et d'autres modèles d'attaque. Dans ce scénario, il est important que les clients du nuage sachent qui est responsable des activités de correction (à savoir le fournisseur de solutions en nuage pour les solutions de logiciel en tant que service et le client pour les solutions d'infrastructure en tant que service et de plate-forme en tant que service).
- Les fournisseurs de solutions d'informatique en nuage offrent une large gamme de services et d'interfaces de programmation d'applications connectées à l'Internet pour permettre aux clients d'administrer et de surveiller leurs actifs. Cette connectivité fait des solutions en nuage une cible potentielle pour les attaques de réseau comme le reniflage/l'écoute du trafic réseau, les attaques par déni de service et les attaques par hôte interposé.
- Si un attaquant est capable d'acquérir illégitimement les identifiants des utilisateurs, il peut accéder à l'interface de gestion utilisée par les administrateurs pour gérer un grand nombre d'actifs. Il faut donc mettre en place des mécanismes d'authentification et d'autorisation forts, notamment pour les employés à haut niveau de privilèges.
- L'environnement multilocataires augmente le risque de brèches ou de fuites de données si les contrôles de séparation échouent ou sont piratés (échec de l'isolement).
- Lors du passage à des solutions d'informatique en nuage, les clients ont généralement moins de visibilité et de contrôle sur leurs données et leurs actifs. Cela augmente les risques liés à la suppression sécurisée des données stockées sur un certain nombre de dispositifs dans l'infrastructure du fournisseur de solutions en nuage. Il est important de

vérifier que les données ont été supprimées de manière sûre et complète. Ce problème est exacerbé par les solutions multi-nuage.

- Le verrouillage technologique, à cause duquel les clients rencontrent des difficultés pour migrer vers un autre fournisseur de solutions d'informatique en nuage, peut poser de sérieux risques de sécurité. Les utilisateurs devraient inclure des plans de changement de fournisseur dans leurs stratégies de continuité des activités et devraient stocker toutes les données dans un format standard facilement transférable.
- Selon l'Autorité de régulation des communications de Namibie, le stockage des données des clients dans des centres de données de services en nuage situés en dehors des frontières nationales est un problème urgent. Dans les pays où les serveurs de données sont hébergés, les régulateurs n'ont aucune compétence et peu de possibilités de surveillance pour traiter les questions relatives à la protection des clients et à la cybersécurité lorsque des cyberattaques se produisent. Ces attaques peuvent entraîner une usurpation d'identité, une fuite d'informations personnelles et, dans certains cas, une perte potentielle de recettes. En outre, la législation des pays hôtes peut différer en ce qui concerne l'accès à l'information, la protection des données et l'interception légale, ce qui peut exposer les clients à un accès non autorisé aux données à caractère personnel[119].

Internet des objets

La diffusion d'une culture de sécurité par conception n'en étant qu'à ses débuts, la connectivité croissante est l'une des tendances les plus préoccupantes en matière de risque et elle pose des problèmes de sécurité considérables[120]:

- Les objets intelligents – qui vont des caméras, des portes et des systèmes de réfrigération aux systèmes de climatisation et aux dispositifs à porter sur soi – collectent une énorme quantité d'informations (à la fois des données et des métadonnées). Les attaquants peuvent en apprendre beaucoup sur la vie de leur cible en captant les données détectées par les objets intelligents de la cible.
- Une nouvelle menace pour l'IoT est celle des rançongiciels. Les dispositifs intelligents offrent un environnement d'extorsion attrayant pour les attaquants, non seulement en raison du grand nombre de cibles faciles à atteindre, mais aussi parce que les attaques de ce type peuvent perturber le fonctionnement des dispositifs, ce qui incommode la cible et l'oblige à payer la rançon[121].
- Les dispositifs IoT sont particulièrement vulnérables aux attaques DoS et DDoS, car la plupart d'entre eux ont des capacités techniques limitées (mémoire, stockage, unité centrale, etc.). Les attaquants peuvent facilement submerger leurs ressources limitées, provoquant des interruptions de service.
- La limitation des ressources des dispositifs IoT constitue un défi crucial lorsqu'il s'agit d'inclure des mesures de sécurité, qui peuvent nécessiter beaucoup de calculs[122].
- L'un des principaux problèmes de sécurité de l'IoT réside dans son niveau de complexité. Les appareils fusionnent différentes technologies comme la virtualisation, l'informatique en nuage, les capteurs et les réseaux, qui présentent leurs propres vulnérabilités. Sécuriser l'IoT signifie sécuriser l'ensemble de la chaîne de ces composants. De même, l'IoT a des applications dans plusieurs domaines (domotique, soins de santé, dispositifs à porter sur soi, etc.), qui ont des besoins de sécurité différents et sont soumis à des menaces différentes.

---

119 Document SG2RGQ/75 (Namibie) de la CE 2 de l'UIT-D.
120 Amit Ashbel, The rise of IoT and the associated security risks, 7 juillet 2016.
121 Syed Rameem Zahra et Mohammad Ahsan Chishti, RansomWare and Internet of Things: A New Security Nightmare. *Proceedings of the 9th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, Uttar Pradesh (Inde), 10-11 janvier 2019.
122 Ammar Rayes et Samer Salam, Internet of Things From Hype to Reality: The Road to Digitization, Springer International Publishing, 2019.

- Bien que les attaques via Internet soient les plus courantes, les dispositifs IoT peuvent également être visés par des attaques physiques. Dans les zones peu ou pas surveillées, les attaquants peuvent facilement atteindre et altérer les dispositifs IoT.
- Les dispositifs IoT peuvent également être utilisés comme vecteurs pour lancer des attaques DDoS. En 2016, par exemple, un célèbre fournisseur de systèmes de noms de domaine a été victime d'une attaque DDoS provenant de dizaines de millions d'adresses IP, la majorité du trafic malveillant provenant de dispositifs IoT tels que des imprimantes, des routeurs et des caméras[123].

5G

La cinquième génération de technologie de communication, connue sous le nom de 5G, offrira une connexion plus fiable et de haute qualité fondée sur des vitesses élevées et une faible latence, ce qui permettra de maximiser le rendement des applications technologiques émergentes dans des domaines comme l'énergie, la santé et l'industrie manufacturière. Ces atouts constituent une cible attrayante pour les attaquants, et leurs vulnérabilités intrinsèques rendent la cybersécurité particulièrement difficile à assurer. En outre, comme les solutions 5G sont encore en phase pilote, les renseignements et les données sur les cyberattaques font défaut, ce qui rend encore plus difficile la compréhension de la menace potentielle[124]:

- Le paysage des menaces sur la 5G est large et hétérogène; en associant diverses technologies, il hérite également de leurs vulnérabilités et de leurs menaces. En particulier, les réseaux et les actifs 5G peuvent être ciblés en tirant parti des insécurités héritées des technologies de deuxième, troisième et quatrième génération, des faiblesses traditionnelles fondées sur l'IP et des flux introduits par la technologie de virtualisation. Les attaquants peuvent également cibler des actifs spécifiques à la 5G comme le cœur, les points d'accès et les éléments de périphérie.
- Les attaques contre les technologies 5G peuvent inclure des tentatives de vol, de manipulation ou de destruction de données, d'interception ou de perturbation des communications, de dommages aux biens physiques ou de perturbation de la fourniture de services. La 5G reliera une large gamme de secteurs et de secteurs verticaux, ce qui modifiera très probablement le paysage de la cybersécurité, entraînant de nouvelles vulnérabilités.
- Un facteur de menace critique provient de la chaîne d'approvisionnement, en particulier des fournisseurs et des prestataires de services compromis. Le risque est qu'un fournisseur puisse intégrer de façon malveillante dans ses produits des portes dérobées, des logiciels ou des défauts critiques cachés. La mise en œuvre de mises à jour automatiques (et non contrôlées) et la manipulation des fonctionnalités posent également des problèmes de sécurité. La relation entre la 5G et la sécurité nationale est évidente, et les fournisseurs doivent être sélectionnés avec soin sur la base d'une approche axée sur les risques.

Intelligence artificielle

La prolifération des solutions d'intelligence artificielle dans différents secteurs de la société aura plusieurs répercussions sur le paysage de la cybersécurité. Ces moyens peuvent être ciblés par des acteurs malveillants ou utilisés par des adversaires et des défenseurs:

- Les ressources de l'IA peuvent être manipulées en modifiant les décisions et les comportements automatisés, en particulier par l'empoisonnement des données,

[123] Nicole Perlroth, Hackers Used New Weapons to Disrupt Major Websites Across U.S., *The New York Times*, 21 octobre 2016.
[124] ENISA, ENISA threat landscape for 5G Networks, novembre 2019.

l'altération des modèles de caractérisation et les portes dérobées[125]. Toutes ces méthodes exploitent la capacité d'apprentissage du système afin de modifier négativement les résultats en alimentant le système avec des données et des informations erronées[126].

- Les pirates se tournent vers les solutions d'IA pour améliorer leur portée et leurs capacités. L'IA peut être utilisée pour fournir des logiciels malveillants capables de contourner les mesures défensives de manière autonome, d'adapter leurs stratégies en fonction des succès remportés et d'améliorer constamment leur fonctionnement.
- L'IA est aussi une ressource défensive importante. Elle peut accroître considérablement la résilience d'un système en renforçant les activités défensives type comme la détection des menaces et des anomalies, la réaction aux incidents et l'analyse des menaces.

5.2.2 Menaces vues sous l'angle de l'industrie 4.0

Le modèle de l'industrie 4.0 nécessite d'appliquer l'automatisation, l'IoT, des solutions de virtualisation, l'analyse et l'IA à différents secteurs verticaux. Ces technologies permettent de recueillir, stocker, partager et interpréter d'énormes quantités de données et peuvent apporter des améliorations sensibles en matière de rapidité, d'efficacité, de rentabilité et de fourniture de services. L'industrie 4.0 peut être appliquée à divers secteurs, chacun d'entre eux étant susceptible de faire l'objet de menaces et de risques de sécurité particuliers.

Les maisons intelligentes

Les maisons intelligentes sont l'un des nombreux secteurs verticaux dans lesquels l'industrie 4.0 peut être appliquée, notamment en matière de consommation d'énergie, d'éclairage et de chauffage intelligents. Les maisons intelligentes contiennent une grande variété d'objets intelligents qui utilisent des capteurs et des actionneurs et sont gérés à distance via l'Internet[127]. La connexion de dispositifs à l'Internet crée un certain nombre de risques pour la sécurité:

- Les maisons intelligentes génèrent d'énormes quantités de données qui sont vulnérables aux attaques. Comme le relève le Ministère des postes et des nouvelles technologies de l'information et de la communication du Tchad, les objets connectés (y compris les téléviseurs intelligents) sont exposés aux menaces de sécurité du système d'information. Par exemple, l'utilisation des téléviseurs connectés peut favoriser l'accès aux informations privées via le web à des personnes non autorisées et faciliter le vol d'identité via le net. Les équipements connectés sont vulnérables au même titre qu'un ordinateur personnel relié à un réseau informatique. Ils sont aussi exposés aux logiciels malveillants[128].
- Les appareils intelligents sont peu sécurisés et peuvent facilement être détournés. Les attaquants qui prennent le contrôle de l'appareil peuvent se déplacer latéralement dans le réseau domestique afin de prendre le contrôle d'autres nœuds.
- Les appareils intelligents disposent généralement de faibles ressources de calcul, ce qui les rend particulièrement vulnérables aux attaques DoS et DDoS qui rendent l'appareil ou le réseau temporairement indisponible pour l'utilisateur auquel il est destiné.

---

125 Battista Biggio et Fabio Roli, Wild patterns: Ten years after the rise of adversarial machine learning, *Pattern Recognition*, vol. 84, décembre 2018, pp. 317-31.

126 Matthew Jagielski et al, Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning. *IEEE Symposium on Security and Privacy (SP), 2018.*

127 Ado Adamou Abba Ari et al, Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics*, 31 juillet 2020.

128 Document 2/140 (Tchad) de la CE 2 de l'UIT-D.

Les villes intelligentes

Les villes intelligentes associent les nouvelles technologies à l'intégration des données et à l'automatisation des tâches pour optimiser l'organisation des villes et offrir de meilleurs services. Les villes intelligentes reposent sur des flux de données importants partagés entre des services essentiels comme les transports, l'approvisionnement en énergie et les soins de santé, qui sont de plus en plus interconnectés. L'ampleur des données produites et le rôle qu'elles jouent dans le fonctionnement des villes intelligentes font naître un besoin crucial de cybersécurité afin de protéger la confidentialité des informations et l'intégrité des biens numériques contre diverses menaces de sécurité:

- ***Cybersanté***: la dépendance à la technologie et le volume des données de santé ne cessant de croître, les prestataires de soins de santé doivent protéger les informations sensibles et assurer la fourniture de services. Bien qu'aucun incident connu ne soit encore survenu, des simulations ont démontré qu'il est possible de désactiver par voie hertzienne des défibrillateurs cardiaques implantables[129], de pirater des pompes à insuline pour qu'elles libèrent des doses mortelles[130] et même d'infiltrer des systèmes de surveillance des patients pour modifier leurs signes vitaux en temps réel[131].
- ***Les réseaux intelligents***: il s'agit d'un élément clé des villes intelligentes. Ils utilisent des dispositifs bidirectionnels comme des capteurs, des actionneurs et des compteurs qui permettent de maintenir un équilibre et une surveillance continus des flux d'énergie des producteurs aux consommateurs[132]. Comme les réseaux intelligents reposent sur des protocoles TIC et des connexions Internet, ils sont vulnérables aux cyberattaques[133]. Les réseaux intelligents constituent une cible tentante pour les attaques; cependant, les réseaux intelligents ont une architecture complexe et causer des dommages à grande échelle nécessite des ressources techniques et organisationnelles de haut niveau. À ce jour, il n'y a eu que deux cas connus de pannes de courant majeures causées par des cyberattaques, à savoir les attaques BlackEnergy3 et Crashoverride, qui auraient toutes deux été menées par des acteurs étatiques[134].
- ***Le transport intelligent***: les moyens numériques, les systèmes physiques, les réseaux de communication et l'automatisation peuvent être appliqués aux infrastructures de transport pour en optimiser la qualité et l'efficacité. En modifiant les données et les informations, les attaquants peuvent entraver la circulation et même provoquer des incidents. En outre, les systèmes de transport intelligents supposent un flux important d'informations personnelles et sensibles qui doit être sécurisé.

L'Internet des objets industriel

L'Internet des objets industriel (IIoT) adapte le modèle de l'IoT au paysage industriel. Associé à la robotique et à l'automatisation, il peut apporter de précieux avantages aux entreprises industrielles, notamment en améliorant la qualité, la rentabilité et la maintenance du processus de production. Ces systèmes cyberphysiques présentent des caractéristiques et des exigences

---

129 Daniel Halperin et al, Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. *IEEE Symposium on Security and Privacy (SP), 2008.*

130 Arundhati Parmar, Hacker shows off vulnerabilities of wireless insulin pumps, *MedCityNews,* 1er mars 2012; David Klonoff. Cybersecurity for Connected Diabetes Devices, *Journal of Diabetes Science and Technology* 9, vol. 9, N° 5, 16 avril 2015.

131 Douglas McKee, 80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals, McAfee, 11 août 2018.

132 Lindah Kotut et Luay A. Wahsheh, Survey of Cyber Security Challenges and Solutions in Smart Grids, *2016 Cybersecurity Symposium (CYBERSEC).*

133 Muhammed Zekeriya Gunduz et Resul Das. Cyber-security on smart grid: Threats and potential solutions, *Computer Networks*, vol. 169, 14 mars 2020.

134 Dragos, Inc, CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids. 12 juin 2017.

particulières qui rendent la transposition des mesures de cybersécurité traditionnelles particulièrement problématique.

Les systèmes cyberphysiques sont des environnements durs en temps réel avec un niveau élevé de déterminisme, dans lesquels la disponibilité des données est importante par rapport à l'intégrité et à la confidentialité[135]. Dans ces systèmes, les composants numériques échangent avec les processus physiques comme les mouvements des objets, les réactions chimiques, la libération de substances et les processus de refroidissement, et les flux de données servent d'intrants pour l'exécution des tâches. Dans de tels contextes, l'adoption de contrôles de sécurité courants comme les logiciels antivirus, le chiffrement ou les pare-feu pourrait ralentir le flux de données et porter atteinte au déroulement des activités, entraînant des retards qui, bien que quantitativement peu importants, pourraient affecter considérablement les opérations[136].

De plus, la plupart des équipements des systèmes cyberphysiques ne peuvent pas prendre en charge des mesures de sécurité ou des mises à jour perfectionnées, ce qui fait que les ressources connectées à Internet sont potentiellement vulnérables. Les cyberattaques contre les systèmes cyberphysiques industriels peuvent causer de graves dommages économiques en perturbant le fonctionnement et, par conséquent, la production d'une usine.

Toutefois, la principale préoccupation est que, en manipulant le flux de données, les cyberattaquants pourraient modifier le fonctionnement d'un système jusqu'à ce qu'il atteigne un point de rupture mécanique, entraînant un impact cinétique qui pourrait avoir de graves conséquences pour la sécurité publique. Par exemple, si un attaquant fournit au système des chiffres modifiés qui indiquent au contrôleur qu'une température baisse trop rapidement, le contrôleur compensera automatiquement en augmentant le chauffage, ce qui entraînera une surchauffe non détectée[137]. Par exemple, en 2014, une aciérie allemande a été piratée avec succès, et les attaquants, en empêchant l'arrêt correct d'un four, ont pu causer des dommages physiques massifs à des composants critiques[138].

Les cyberopérations offensives ayant des effets physiques sont extrêmement complexes et nécessitent non seulement une bonne compréhension des ressources numériques utilisées, mais aussi une connaissance approfondie du processus physique visé et une compréhension détaillée des différentes variables. C'est pourquoi les menaces persistantes avancées et les mandataires parrainés par l'État ont le plus de chances de disposer des ressources techniques et organisationnelles nécessaires pour exécuter des opérations de ce type.

5.3 Solutions existantes et nouvelles

Une proportion importante des dispositifs IoT ne comportent pas de fonctions de cybersécurité de base. En octobre 2018, après 18 mois de collaboration avec des représentants du secteur privé et des experts du Centre national de cybersécurité, le ministère britannique du numérique, de la culture, des médias et des sports a publié le Code de bonne pratique pour la sécurité des

[135] Roberto Setola et al, Cyber threats for operational technologies, *International Journal of System of Systems Engineering*, vol. 10, N° 2, 2020.
[136] Roberto Setola et al, An overview of Cyber Attack to Industrial Control System, *Chemical Engineering Transactions*, vol. 77, 2019.
[137] Stephen McLaughlin et al, The Cybersecurity Landscape in Industrial Control Systems, *Proceedings of the IEEE*, vol. 104, numéro 5, mai 2016.
[138] Robert Lee et al, German Steel Mill Cyber Attack, Industrial Control Systems Defense Use Case, 30 décembre 2014.

consommateurs en matière d'IoT[139]. Les 13 lignes directrices volontaires du code fournissent une base de référence pour les dispositifs IoT que les fabricants devraient intégrer dans leurs produits pour les rendre "sûrs par conception". Le code a contribué à l'élaboration de la première norme applicable au niveau mondial en matière de sécurité de l'IoT, ETSI TS 103 645[140].

Algérie Télécom a également souligné l'importance de fournir des guides et des recommandations sur la sécurisation des nouvelles technologies comme le nuage et l'IoT qui sont appelées à devenir le moteur essentiel du développement des systèmes d'information et de l'économie numérique[141].

Les **Tableaux 1** et **2** fournissent une liste des Recommandations de l'UIT-T qui sont pertinentes pour la protection de l'informatique en nuage et de l'IoT respectivement, en matière d'infrastructure, d'applications, de données et de confidentialité.

Tableau 1: Architecture de sécurité de l'informatique en nuage pour la protection de l'infrastructure, des applications, des données et de la vie privée

Titre	Sujet	Institution	Lien
Aperçu de la sécurité de l'informatique en nuage			
UIT-T X.1601	Cadre de sécurité applicable à l'informatique en nuage	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12613
Conception de la sécurité de l'informatique en nuage			
UIT-T X.1602	Exigences de sécurité pour l'environnement des applications de logiciel en tant que service	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12615
UIT-T X.1603	Exigences de sécurité des données pour le service de surveillance de l'informatique en nuage	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13406
UIT-T X.1604	Exigences de sécurité relatives au réseau en tant que service (NaaS) dans l'informatique en nuage	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14093
UIT-T X.1605	Exigences de sécurité pour les infrastructures en tant que service (IaaS) publiques dans l'informatique en nuage	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14094

[139] Royaume-Uni, Ministère du numérique, de la culture, des médias et des sports, Code of Practice for Consumer IoT Security, octobre 2018.
[140] Institut européen des normes de télécommunication (ETSI), ETSI TS 103 645 V1.1.1 (2019-02), Cyber Security for Consumer Internet of Things.
[141] Document 2/66 (Algérie Télécom SPA (Algérie)) de la CE 2 de l'UIT-D.

Tableau 1: Architecture de sécurité de l'informatique en nuage pour la protection de l'infrastructure, des applications, des données et de la vie privée (suite)

Titre	Sujet	Institution	Lien
UIT-T X.1631	Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information fondés sur la norme ISO/CEI 27002 pour les services en nuage	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12490
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage			
UIT-T X.1641	Lignes directrices pour la sécurité des données des clients de services en nuage	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12853
UIT-T X.1642	Lignes directrices relatives à la sécurité opérationnelle de l'informatique en nuage	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12616

Tableau 2: Architecture de sécurité de l'IoT pour la protection de l'infrastructure, des applications, des données et de la vie privée

Titre	Sujet	Institution	Lien
Sécurité de l'Internet des objets (IoT)			
UIT-T X.1361	Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13607
UIT-T X.1362	Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT)	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13196
UIT-T X.1364	Exigences et cadre de sécurité applicables à l'Internet des objets à bande étroite	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14088
UIT-T X.1365	Méthode de sécurité applicable à l'utilisation de la cryptographie fondée sur l'identité à l'appui des services de l'Internet des objets fournis sur les réseaux de télécommunication	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14089
UIT-T X Suppl. 31	UIT-T X.660 – Supplément sur les lignes directrices relatives à l'utilisation des identificateurs d'objet pour l'Internet des objets	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13411

Autres techniques et cadres de sécurité nouveaux

- Les applications d'IA, y compris l'apprentissage machine et l'apprentissage approfondi, peuvent apporter des avantages considérables aux stratégies de cybersécurité en matière d'efficacité et de rentabilité. Ces solutions utilisent la régression, la classification et le regroupement pour détecter des anomalies, identifier différentes typologies d'attaque et élaborer des mesures potentielles de correction. Les systèmes d'intelligence artificielle peuvent également renforcer les interventions en cas d'incident en suggérant des mesures spécifiques en réponse à des incidents particuliers. Ils peuvent aussi améliorer les activités de gestion des risques en attribuant automatiquement des valeurs de risque aux nouvelles vulnérabilités et aux mauvaises configurations sur la base de leurs descriptions et prévenir de manière proactive les attaques en accélérant considérablement l'extraction, l'élaboration et l'application des données sur les menaces, les acteurs, les attaques, les logiciels malveillants, les vulnérabilités et les indicateurs de compromission[142].
- Les caractéristiques particulières de la technologie des registres distribués (DLT) sont également prometteuses pour les applications de sécurité[143]. Tout d'abord, le stockage fondé sur la technologie DLT est décentralisé, ce qui réduit considérablement le risque de violations importantes des données, car les attaquants ne peuvent plus accéder à toutes les données détenues par un seul point d'accès. De même, la décentralisation apporte des avantages essentiels en matière de sécurité aux réseaux IoT, qui sont traditionnellement organisés selon la logique du modèle client-serveur, dans lequel une autorité centrale gère les données et les appareils au sein du réseau. Grâce aux applications DLT, les dispositifs IoT peuvent identifier les anomalies et isoler les nœuds qui se comportent de manière inhabituelle. En outre, les applications DLT peuvent créer un climat de confiance dans les réseaux IoT, en garantissant que la disponibilité, la vérifiabilité, la responsabilité, l'intégrité et la confidentialité des données échangées restent constantes[144].
- La méthode SOAR (Security Orchestration, Automation and Response) (orchestration, automatisation et intervention en matière de sécurité) consiste en des solutions qui connectent les outils et les systèmes de sécurité afin de réaliser des activités comme la gestion des vulnérabilités, l'intervention en cas d'incident et l'automatisation des opérations de sécurité de manière intégrée et organique. L'automatisation des processus de sécurité permet au système de mettre en œuvre des mesures correctives et des activités de maintenance (analyse des vulnérabilités, surveillance des accès et des journaux) sans intervention humaine.
- Une autre option est celle des modèles de confiance zéro, dans lesquels les environnements de réseau sont segmentés en interne et les accès sont administrés selon le principe du moindre privilège. Cela signifie que chaque module, y compris les utilisateurs, les dispositifs, les interfaces de programmation d'applications et les dispositifs IoT, ne peuvent accéder qu'aux ressources, données et actifs nécessaires à leur fonction légitime. Les modèles de confiance zéro augmentent considérablement la sécurité interne, car ils rendent les mouvements latéraux et l'escalade des privilèges plus difficiles pour les attaquants qui, pour accéder à l'ensemble du réseau, devront cibler plusieurs dispositifs.
- Les courtiers en sécurité de l'accès au nuage sont des points d'application des politiques qui opèrent entre les utilisateurs et les fournisseurs de services en nuage. Par exemple, les politiques de sécurité appliquées peuvent comprendre l'authentification, l'authentification unique, l'autorisation, la correspondance des justificatifs d'identité, le profilage des dispositifs, le chiffrement, la segmentation en unités, la journalisation, l'alerte et la détection/prévention des logiciels malveillants[145].

---

142 Padmavathi Ganapathi et D. Shanmugapriya, Handbook of Research on Machine and Deep Learning Applications for Cyber Security, *IGI Global*, 2019; et Dave Shackleford, Who's Using Cyberthreat Intelligence and How?, *SANS,* 12 février 2015.

143 Nir Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, *Telecommunications Policy*, vol.41, numéro 10, novembre 2017.

144 Ben Cole, The supply chain of trust inherent to IoT data security, *IoT Agenda*, 28 novembre 2016.

145 Gartner, Gartner Glossary, Cloud Access Security Brokers (CASBs).

- La gestion des accès privilégiés fait référence à un ensemble d'outils et de solutions pour la surveillance et la protection des comptes privilégiés comme les comptes d'administrateur utilisés pour accéder aux actifs, données et ressources critiques. Ces solutions isolent les comptes critiques dans un référentiel sécurisé et surveillé, réduisant ainsi le risque de vol de justificatifs d'identité.
- Les organisations devraient passer d'une approche de conception et d'exploitation (DevOps) à une approche de conception, de sécurité et d'exploitation (DevSecOps), qui intègre la sécurité comme partie intrinsèque de la conception et de l'exploitation. Dans les cadres et les outils DevSecOps, au lieu d'être intégrée aux produits finals (comme les logiciels et les applications), la sécurité est considérée comme une caractéristique intégrale et essentielle dès le premier stade de la conception. Cette approche rend la sécurité plus robuste, atténue les risques et réduit les coûts de mise en conformité.
- Le cadre CARTA (Continuous Adaptive Risk and Trust Assessment) (évaluation continue adaptative du risque et de la confiance) de Gartner propose une approche adaptative de la sécurité, dans laquelle les décisions sont fondées sur le risque et l'efficacité[146]. CARTA comporte trois phases: "run", qui se concentre sur l'analyse des principales menaces; "build", qui fait référence aux menaces et aux vulnérabilités identifiées pendant la conception des produits et de l'exploitation; et "plan", dans lequel les analyses sont utilisées pour déterminer les risques de sécurité et évaluer si leur atténuation aurait un effet négatif sur la productivité[147].

Solutions rentables

- Selon le ministère britannique du numérique, de la culture, des médias et des sports, en s'attachant à porter atteinte au retour sur investissement des attaques les plus courantes et peu sophistiquées, il est possible de commencer à lutter contre les effets des cyberattaques à une échelle qui présente des avantages importants au niveau mondial. Le programme de cyberdéfense active (ACD) a été mis au point pour augmenter le coût et le risque de monter des cyberattaques sur des produits de base contre le Royaume-Uni, réduisant ainsi le retour sur investissement pour les criminels[148]. En 2018, le dispositif a eu le plus grand effet grâce à son service de retrait, qui identifie les sites malveillants (qu'il s'agisse d'attaques ou d'infrastructures qui les soutiennent) et notifie à l'hôte ou au propriétaire qu'ils doivent être retirés de l'Internet: au total, 192 256 sites web frauduleux ont été retirés de cette manière, dont 64% dans les 24 heures. En outre, 22 133 campagnes d'hameçonnage hébergées dans l'espace IP délégué au Royaume-Uni (soit un total de 142 203 attaques individuelles) ont été supprimées, et 14 124 sites d'hameçonnage liés au gouvernement ont été retirés[149].
- Selon la société lituanienne NRD Cyber Security, afin d'obtenir des incidences positives significatives sur la sécurité de l'environnement numérique national, les équipes CSIRT nationales et sectorielles devraient travailler non seulement comme points de contact, coordonnateurs d'intervention en cas d'incident et analystes, mais aussi comme facilitateurs capables de servir de guide pour concevoir des capacités de cybersécurité indépendantes supplémentaires au sein du secteur privé, des communautés professionnelles, des centres d'éducation, des institutions de recherche, des manifestations, des réunions, des conférences et des équipes CSIRT privées et internes[150].
- Selon l'entreprise estonienne Guardtime, les cyberexercices sont essentiels pour atteindre une cyberrésistance durable car ils aident les équipes à comprendre les processus nécessaires pour atténuer une cybercrise. L'Estonie recommande d'élaborer un programme de gouvernance de la cyberrésilience qui couvre l'éducation, la formation

---

146 Gartner, The Gartner IT Security Approach for the Digital Age, 12 juin 2017.
147 Gartner, Gartner Keynote: Leverage Automation for Modern Security, 17 juin 2019.
148 Ian Levy et Maddy S, Active Cyber Defence (ACD) – The Second Year, United Kingdom National Cyber Security Centre, 15 juillet 2019.
149 Document SG2RGQ/175 (Royaume-Uni) de la CE 2 de l'UIT-D.
150 Document 2/172 (NRD Cyber Security (Lituanie)) de la CE 2 de l'UIT-D.

et les cyberexercices, allant de manifestations localisées à des exercices réguliers personnalisés à l'échelle nationale. Ces programmes devraient prendre en considération divers aspects de la structure d'organisation et de la situation socio-économique du pays, les rôles et responsabilités des différentes parties prenantes, l'environnement réglementaire national, les partenariats régionaux et internationaux du pays et les divers risques auxquels le pays est confronté dans le paysage évolutif des cybermenaces[151].

[151] Document SG2RGQ/32 (Guardtime AS (Estonie)) de la CE 2 de l'UIT-D.

Chapitre 6 – Comment la cybersécurité peut contribuer à la protection des données à caractères personnel

6.1 Introduction

Avec l'avènement des nouvelles technologies de l'information, divers services nouveaux et de plus en plus pratiques apparaissent pour une utilisation quotidienne. Néanmoins, l'avènement des nouvelles technologies de l'information modifie également, sur le plan bilatéral, les risques auxquels sont confrontés les individus en matière de protection de la vie privée et des données. Bien que de nouveaux dangers pour les données à caractère personnel continuent d'apparaître, diverses techniques peuvent être utilisées pour réduire ou éviter ces risques. C'est pourquoi il convient de mettre davantage l'accent sur la cybersécurité et les technologies de renforcement de la protection de la vie privée qui peuvent contribuer à la protection des données à caractère personnel, comme la pseudonymisation et l'intégration du respect de la vie privée dès la conception.

La pseudonymisation est une procédure de gestion des données et de désidentification par laquelle les champs d'informations personnelles identifiables dans un enregistrement de données sont remplacés par un ou plusieurs identifiants artificiels, ou pseudonymes. Un pseudonyme unique pour chaque champ remplacé ou pour chaque ensemble de champs remplacés rend l'enregistrement de données moins identifiable, tout en restant adapté à l'analyse et au traitement des données[152]. La pseudonymisation peut contribuer à protéger les informations personnelles identifiables et peut réduire la charge des entités qui recueillent et détiennent ces données.

Si le respect de la vie privée est intégré dès la conception, on n'attend pas la fin d'une violation de données pour prendre des mesures de sécurité. Au contraire, les concepteurs prévoient ou anticipent les menaces pour la vie privée ou les empêchent de se produire grâce à des mesures préventives comme la planification ou la conception des services[153]. La différence entre les deux approches est que, alors que la pseudonymisation nécessite certaines mesures techniques, l'intégration du respect de la vie privée dès la conception donne aux responsables du traitement des données une certaine souplesse pour déterminer quelles mesures techniques supplémentaires peuvent le mieux garantir la sécurité et la confidentialité des données.

---

[152] Wikipédia, https://fr.wikipedia.org/wiki/Pseudonymisation.

[153] Le concept de l'intégration de la vie privée dès la conception a été utilisé dans le domaine existant de l'architecture, mais il était secondaire. Il a commencé à gagner du terrain après avoir été mentionné par Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario, au Canada, au milieu des années 1990.

6.2 Environnement juridique et bonnes pratiques dans les États Membres

Au Brésil, la loi générale sur la protection des données récemment adoptée comprend des définitions des différents types de données personnelles et de traitement et prévoit les autorisations légales pour le traitement national et international, les droits fondamentaux des personnes concernées et la création d'une autorité nationale de protection des données[154]. La loi établit les principes de réduction des données au minimum, de prévention des violations de données et de sécurité des données et formule des règles particulière pour régir ces domaines. La loi englobe également l'intégration de la sécurité dès la conception, en stipulant que les mesures de sécurité visant à protéger les données à caractère personnel doivent être mises en œuvre dès la phase de conception du produit ou du service jusqu'à son exécution.

En 2017, la Chine a officiellement publié un ensemble de normes nationales sur les spécifications de sécurité des informations à caractère personnel dans les technologies de l'information, qui complètent les exigences de sécurité des informations à caractère personnel énoncées dans sa loi sur la cybersécurité. Ces normes fournissent des lignes directrices et des instructions d'exploitation. La Chine poursuit ses recherches et l'élaboration de normes sur la protection des informations à caractère personnel[155].

Les entreprises spécialisées dans la sécurité des données en Chine sont très actives dans le domaine de la recherche et du développement afin de pouvoir offrir des produits et services de sécurité, notamment pour prévenir les pertes de données, inspecter la sécurité des bases de données, détecter les fuites de données, chiffrer les bases de données et masquer des données. Elles proposent une aide de nature technique en matière de protection des données à caractère personnel.

La République de Corée a apporté un amendement notable à sa loi sur la protection des informations à caractère personnel afin de prévoir des mesures techniques pour protéger ces données[156]. L'amendement a intégré des modifications visant à rationaliser la surveillance réglementaire et à introduire le concept de "données pseudonymisées", qui permet aux responsables du traitement et aux sous-traitants de traiter les données de manière plus sûre, tout en réduisant au minimum le risque d'utilisation abusive et de violation des données grâce à d'autres mesures technologiques et d'organisation comme la protection des données dès la conception et par défaut.

De plus, le Gouvernement de la République de Corée a publié des lignes directrices sur la protection du traitement automatique des données à caractère personnel. Si les nouvelles technologies comme l'analyse des mégadonnées fondée sur l'IA et les capteurs utilisés dans les dispositifs IoT pour recueillir les données rendent possibles des services innovants, il est difficile de comprendre le flux de traitement des données à caractère personnel et les limites des réponses de suivi. En ce qui concerne le traitement automatique des données à caractère personnel à partir de dispositifs IoT, les lignes directrices encouragent l'application du principe de respect de la vie privée dès la conception, selon lequel le risque de violation des données à caractère personnel est pris en compte dès les premières étapes de la planification et tout au long du cycle de vie des données.

---

154 Document SG2RGQ/143 (Brésil) de la CE 2 de l'UIT-D.
155 Document 2/156 (Chine) de la CE 2 de l'UIT-D.
156 Document 2/342 (République de Corée) de la CE 2 de l'UIT-D.

Les 10 règles de protection du traitement automatisé des données à caractère personnel incluses dans les lignes directrices sont les suivantes:

- Phase de planification
  - Règle 1: confirmation des données personnelles nécessaires aux services
  - Règle 2: confirmation du respect de la loi lors de la collecte de données à caractère personnel
- Phase de conception
  - Règle 3: réduction au minimum des données et traitement des seules données à caractère personnel nécessaires
  - Règle 4: application de mesures de sécurité appropriées à chaque étape du traitement des données à caractère personnel
  - Règle 5: diffusion transparente des procédures et méthodes de traitement des données à caractère personnel
  - Règle 6: garantie que les personnes concernées peuvent facilement exercer leurs droits
  - Règle 7: instructions claires à l'intention des personnes concernées lors de la fourniture et de la commande de données à caractère personnel à un tiers
  - Règle 8: destruction des données à caractère personnel et prévention de toute collecte ultérieure lors de la cessation des fonctions par la personne concernée
  - Règle 9: plans visant à garantir le droit des personnes concernées en cas de cessation d'activité
- Phase d'examen
  - Règle 10: examen des facteurs de risque liés aux violations de données à caractère personnel avant le lancement du service.

Compte tenu de la nécessité récente de suivre les cas confirmés de COVID-19 dans le monde, la République de Corée a pris diverses mesures institutionnelles et techniques pour protéger les données à caractère personnel. En plus de garantir la base juridique pour le suivi des patients confirmés en révisant la réglementation pertinente, des mesures techniques sont prises pour séparer et gérer les informations d'identification afin de prévenir d'éventuelles violations des données à caractère personnel. Des informations séparées ne sont utilisées pour les enquêtes épidémiologiques que lorsque des cas confirmés se produisent, et les informations sur les utilisateurs et visiteurs individuels sont gérées en toute sécurité, par exemple en étant automatiquement détruites quatre semaines après la génération[157].

Une société italienne a mis au point une méthodologie exclusive qui peut être facilement utilisée par les organisations pour dresser une liste des activités techniques permettant de mettre l'infrastructure en nuage (privée, publique ou hybride) en conformité avec la réglementation sur la protection de la vie privée[158]. La méthodologie comprend une proposition visant à définir des lignes directrices générales qui pourraient être utilisées par les États Membres pour créer leurs propres configurateurs nationaux afin de normaliser la conformité entre les différents

[157] Document SG2RGQ/268 (République de Corée) de la CE 2 de l'UIT-D.
[158] Document SG2RGQ/25 (Proge Software (Italie)) de la CE 2 de l'UIT-D.

pays de manière plus efficace et moins coûteuse, en utilisant le nuage comme une plate-forme puissante pour faciliter l'essor fulgurant de l'économie numérique.

Dans un autre cas de bonne pratique, l'Article 25 sur la protection des données par conception et par défaut du règlement général sur la protection des données de l'Union européenne (RGPD) reconnaît que la protection de la vie privée dès la conception est la méthode la plus appropriée pour prévenir les risques de protection des données à caractère personnel posés par les dispositifs IoT, les mégadonnées, l'IA et d'autres nouvelles technologies. Avec la notion de respect de la vie privée dès la conception, des mesures techniques et d'organisation appropriées visant à garantir la sécurité et la confidentialité des données personnelles sont intégrées dans le cycle de vie complet des produits, services, applications et procédures commerciales et techniques d'une organisation. Les mesures techniques peuvent inclure, sans s'y limiter, la pseudonymisation et la réduction des données[159].

L'Agence de l'Union européenne pour la cybersécurité (ENISA) a présenté huit stratégies clés pour aider les entreprises à appliquer le principe de respect de la vie privée dès la conception, dans le but d'examiner diverses méthodes d'approche, stratégies et facteurs techniques pour la protection des données à caractère personnel[160].

Tableau 3: Huit stratégies clés pour l'application du principe de respect de la vie privée dès la conception

	Principe	Contenu
1	Réduire	Réduire au minimum la quantité de données à caractère personnel traitées en les traitant selon des finalités claires en vue de réduire la possibilité d'atteintes à la vie privée
2	Cacher	Masquer la transmission en texte clair lors du traitement de données à caractère personnel afin d'empêcher tout accès de l'extérieur
3	Séparer	Séparer et stocker diverses données à caractère personnel afin d'éviter toute discrimination à l'encontre d'une seule personne dans la base de données
4	Agréger	Agréger de grandes quantités de données à caractère personnel afin de réduire au minimum la discrimination à l'égard des personnes et répartir en catégories les résultats du traitement pour rendre la discrimination impossible
5	Informer	Informer les personnes concernées de l'ensemble du processus de traitement des données à caractère personnel afin de permettre une compréhension transparente des finalités pour lesquelles les données sont utilisées
6	Contrôler	Contrôler l'utilisation des données à caractère personnel. Les personnes concernées doivent comprendre l'ensemble du processus de traitement des données à caractère personnel et être en mesure d'exercer leurs droits concernant l'utilisation abusive de leurs données à caractère personnel ou les niveaux de sécurité fondés sur la cinquième stratégie, "informer"

[159] Union européenne, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[160] ENISA, Privacy and Data Protection by Design – from policy to engineering, décembre 2014

Tableau 3: Huit stratégies clés pour l'application du principe de respect de la vie privée dès la conception (suite)

	Principe	Contenu
7	Appliquer	La politique interne de protection des données à caractère personnel doit refléter des obligations légales et systématiques et doit être appliquée
8	Démontrer	Démontrer le respect des obligations légales comme le fonctionnement efficace des politiques de protection des données à caractère personnel et l'intervention immédiate contre les incidents entraînant une fuite de données

L'ENISA a également fait des suggestions concernant les activités de protection de la vie privée et des données à entreprendre par les différentes parties prenantes. Elle recommande aux décideurs de promouvoir et de soutenir l'élaboration de nouvelles mesures d'incitation pour faire progresser les services de protection des données à caractère personnel et aux groupes de recherche et développement d'étudier les méthodes d'ingénierie pour la protection des données à caractère personnel par une approche interdisciplinaire et de diffuser les résultats de la recherche par l'intermédiaire des décideurs et des médias. Enfin, l'agence recommande que les concepteurs de logiciels fournissent une technologie capable de mettre à jour intuitivement les propriétés de protection de la vie privée et de soutenir la protection des données à caractère personnel dans le cadre de projets d'infrastructure publics et mutuellement établis.

Aux États-Unis, la Commission fédérale du commerce (FTC) met l'accent sur les principes pratiques et procéduraux de protection de la vie privée, comme le respect de la vie privée dès la conception et le choix simplifié du consommateur, et sur les principes de fond et de procédure comme la garantie de transparence. La commission insiste également sur la protection de la vie privée des consommateurs dans l'organisation des entreprises, les produits et toutes les étapes de la conception des services[161].

L'autorité espagnole de protection des données (AEPD) a publié un guide sur le respect de la vie privée dès la conception, dans lequel elle souligne la nécessité de prendre en compte la vie privée et les principes de protection des données dès le début de tout type de traitement. Le guide présente également les principes de base et les stratégies de traitement des données à caractère personnel[162].

Tableau 4: Lien entre les objectifs de protection de la vie privée et les stratégies de conception de la protection de la vie privée

Objectifs de protection de la vie privée	Stratégies de protection de la vie privée axées sur les données	Stratégies de protection de la vie privée axées sur les processus
Non-associativité	Réduire, abstraire, séparer, cacher	
Contrôle		Contrôler, appliquer, démontrer
Transparence		Informer

[161] FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy-makers, mars 2012.
[162] *Agencia Española Protección Datos (AEPD)*, A Guide to Privacy by Design, octobre 2019.

6.3 Enseignements tirés et voie à suivre

Le taux de cyberattaques, de violations de données et d'utilisation non autorisée de données à caractère personnel augmente de manière exponentielle. Il est plus important que jamais, en particulier pour les organisations qui traitent des informations d'identification personnelle, de comprendre les droits et les obligations des individus et des organisations en matière d'informations personnelles.

Le présent chapitre a présenté un aperçu des changements juridiques et des mesures techniques de cybersécurité concernant la protection des données personnelles adoptés dans les États Membres. Il a également traité des bonnes pratiques pour aider les États Membres à se conformer aux exigences en constante évolution en matière de protection des données et a abordé le rôle des technologies de cybersécurité dans l'atténuation des risques et l'appui à la conformité.

Les enseignements suivants peuvent être tirés de l'examen des diverses technologies de cybersécurité et des bonnes pratiques suivies par les États Membres en matière de protection des informations personnelles:

- Les dispositions institutionnelles en matière de pseudonymisation, de protection de la vie privée dès la conception et d'autres mesures technologiques contribuent à créer un environnement plus sûr.
- Les entreprises qui recueillent et utilisent des informations personnelles doivent faire un véritable effort pour mettre en place des mesures techniques destinées à protéger les informations personnelles à un niveau plus fondamental.
- Les diverses parties prenantes, y compris les personnes concernées, la société civile, les milieux universitaires et les représentants du secteur privé, doivent examiner ensemble l'utilisation de la technologie et faire des efforts de sensibilisation et d'amélioration de la sécurité.

Chapitre 7 – L'avenir de la Question

La cybersécurité est une question importante pour toutes les parties prenantes, y compris les gouvernements et les consommateurs. Les travaux menés par l'UIT-D à cet égard contribuent à sensibiliser aux risques. Alors que les taux de connectivité et d'utilisation de l'Internet continuent d'augmenter dans le monde entier, la nécessité de protéger les consommateurs et les systèmes reste essentielle. Compte tenu de la nécessité constante de partager les informations sur les pratiques de cybersécurité à l'échelle mondiale, l'équipe de direction de la Question 3/2 de la Commission d'études 2 de l'UIT-D estime que cette Question consacrée à la cybersécurité devrait rester inchangée pour le prochain cycle d'études. Les thèmes abordés au cours de la présente période d'études restent pertinents et devraient être le point de départ pour la soumission de nouvelles contributions et la poursuite des travaux pendant la prochaine période d'études. Le cadre général de la Question devrait donc rester inchangé: étant donné que les questions de sécurité concernent toutes les technologies, la Question 3/2 continue de s'appliquer à toutes les technologies nouvelles et émergentes. Compte tenu de leur nature, ces questions doivent être prises en compte dès la phase de conception des technologies.

Annexes

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

Contributions on Question 3/2

Web	Received	Source	Title
2/407	2021-03-03	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/400	2021-03-01	United States	Update on Cyber Awareness Campaigns
2/385	2021-01-28	Bhutan	Survey findings on National Child Online Safety and Protection
RGQ2/278	2020-09-22	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs
RGQ2/268	2020-09-22	Republic of Korea	Protecting personal data in responding COVID-19 pandemic (Korea's experience)
RGQ2/261	2020-08-19	Togo	Draft text for Chapter 1 of the Final Report for Question 3/2 - Update on the status of spam and malware, including mitigation responses
RGQ2/241	2020-08-26	United Kingdom	Updated case study on securing consumer Internet of Things (IoT) devices in UK
RGQ2/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme
RGQ2/234	2020-08-20	United Kingdom	UK case study - reporting service for phishing emails
RGQ2/216	2020-07-27	Brazil	Brazilian National Cybersecurity Strategy (E-Ciber)
RGQ2/215	2020-07-27	Brazil	#SafeConnection (#ConexãoSegura) Awareness Campaigns
RGQ2/214	2020-07-27	Brazil	Brazilian National Cyberdrill - Cyber Guardian Exercise
2/344	2020-02-11	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/342	2020-02-11	Republic of Korea	Korea's major amendment to data protection law and its implication

(suite)

Web	Received	Source	Title
2/341	2020-02-11	Republic of Korea	Implementation plan for strengthening national cybersecurity of Korea
2/338	2020-02-11	Co-Rapporteur for Question 3/2	Draft table of contents (V1) for the Final Report of Q3/2
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility
2/328	2020-02-08	Deloitte (United States)	People with disabilities and the Internet of Things
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo
2/322	2020-02-07	Welchman Keen (Singapore)	Enhancing capacity and capability for critical national infrastructure in the Pacific Island Nations
2/321	2020-01-08	Sudan	WSIS project for consideration by Question 3/2
2/305	2020-01-15	Mexico	Perception on security and trust from Mexican users on fixed and/or mobile Internet
2/287	2020-01-07	China	Forum on network security technology development and international cooperation
2/286	2020-01-07	China	National Network Security Publicity Week and network security industrial park
2/272	2020-01-02	Niger	Cybersecurity best practices: case study and recommendation
2/264	2019-12-27	Russian Federation	Protecting children from information harmful to their health and development. Experience of the Russian Federation
RGQ2/TD/13 +Ann.1 (Rev.1)	2019-10-08	Forum of Incident Response and Security Teams (FIRST)	Introduction to incident response for policy makers
RGQ2/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills
RGQ2/179	2019-09-23	China	China's practice in protecting children's personal information
RGQ2/175	2019-09-19	United Kingdom	Follow up to "case study for the use of Active Cyber Defence on UK Government networks"

(suite)

Web	Received	Source	Title
RGQ2/156 +Ann.1-3	2019-09-04	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK
RGQ2/153 +Ann.1-2	2019-08-22	United States	Enhancing the resilience of the Internet and communications ecosystem against botnets and other automated, distributed threats
RGQ2/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1
RGQ2/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus
RGQ2/143	2019-08-23	Brazil	The adoption of the Brazilian General Data Protection Law
RGQ2/135	2019-07-30	Bhutan	Cybersecurity initiatives in Bhutan
RGQ2/134	2019-07-29	State of Palestine, which participates in ITU under Resolution 99 (Rev. Dubai, 2018)	Government Data Exchange
RGQ2/118	2019-06-21	Democratic Republic of the Congo	Securing information and communication networks: Best practices for developing a culture of cybersecurity
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire
2/199 (Rev.1)	2019-03-06	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combatting Cybercrime (PLCC)
2/172	2019-02-07	NRD Cyber Security (Lithuania)	National and sectorial CSIRT developments as means to strengthen cybersecurity environments, 2019 update
2/168	2019-02-07	Republic of Korea	2019 Comprehensive Cybersecurity Plan for the private sector
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies
2/165	2019-02-06	Mexico	Fixed and/or mobile Internet users' perception of cybersecurity
2/156	2019-02-05	China	Work experiences in personal information protection

(suite)

Web	Received	Source	Title
2/155	2019-02-05	China	Design of evaluation index for network security capability
2/154	2019-02-05	China	Experience of Internet governance with the coordinated participation of the whole of society
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin
2/141	2019-01-15	Chad	Digital dividend
2/140	2019-01-15	Chad	Vulnerability of connected TVs
2/136	2019-01-15	Chad	Status of cybersecurity in the Republic of Chad
RGQ2/TD/1	2018-09-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for ITU members
RGQ2/79	2018-09-18	Bhutan	Challenges, issues and recommendations from Bhutan: developing country perspective
RGQ2/75	2018-09-18	Namibia	Enforcement of cyber security challenged by cloud services
RGQ2/55	2018-09-10	United Kingdom	Case study for the use of Active Cyber Defence on UK government networks
RGQ2/47	2018-08-31	BDT Focal Point for Question 3/2	Information on two publications issued in 2017: regional review of national activities on child online protection in Europe; and mobile identification: implementation, challenges, and opportunities
RGQ2/39 +Ann.1	2018-08-20	High-Tech Bridge SA (Switzerland)	Cybersecurity awareness and other educative activities to members
RGQ2/32	2018-08-16	Guardtime AS (Estonia)	Towards cyber resilience - the role of national cyber exercises
RGQ2/30	2018-08-15	Brazil	Survey proposal
RGQ2/26	2018-08-14	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means of strengthen cybersecurity environments
RGQ2/25	2018-08-14	Proge-Software (Italy)	Data Privacy and Cloud.be compliant
2/91	2018-04-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/84	2018-04-23	Japan	Proposal for workshops in 2018-2021 study period

(suite)

Web	Received	Source	Title
2/82	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	KOVA Project: A best practice for COP implemented in Iran
2/75	2018-04-14	A.S. Popov Odessa National Academy of Telecommunications (Ukraine)	ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection. Conclusions and Recommendations
2/74	2018-04-13	Korea Telecom (Republic of Korea)	Study topics for Question 3/2 in the current study period
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities
2/66	2018-04-08	Algérie Télécom SPA (Algeria)	Proposals on the content of the (Question 3/2) final report
2/49	2018-03-15	Burundi	Current situation with regard to the Burundian Penal Code in relation to efforts to combat cybercrime
2/41	2018-02-28	Burundi	Cybersecurity, Internet Exchange point and e-commerce in Burundi

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
RGQ2/242	2020-08-31	Council Working Group on Child Online Protection	Liaison statement from the Council Working Group on Child Online Protection (CWG-COP) to ITU-D SG2 on the outcome of the 15th and 16th Meetings of CWG-COP
RGQ2/174	2019-09-18	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on vulnerability of TVs
2/182 +Ann.1	2019-02-11	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D Study Group 2 Question 3/2 on Cybersecurity in Africa (overview and out-look), from Democratic Republic of Congo
RGQ2/62	2018-09-14	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison representative with ITU-D Question 3/2
RGQ2/43	2018-08-27	ITU-T Study Group 13	Liaison statement from ITU-T SG13 to ITU-D SG1 Q3/1 and ITU-D SG2 Q3/2 on inter-sec-tor coordination
RGQ2/3	2018-05-11	ITU-T JCA-IMT2020	Liaison Statement from JCA-IMT2020 to ITU-D Study Groups 1 and 2 on invitation to update the information in the IMT2020 roadmap

(suite)

Web	Received	Source	Title
2/73	2018-04-13	ITU-T JCA-AHF	Liaison Statement from ITU-T JCA-AHF to ITU-D Study Group 1 Q7/1 and Study Group 2 Q3/2 on JCA-AHF recent meeting reports
2/69	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison relationship with ITU-D Study Group 2 Question 3/2
2/68	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on best practices in Benin and Senegal
2/67 (Rev.1)	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/62	2018-04-03	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/46	2018-03-05	ITU-T JCA-IMT2020	Liaison Statement from ITU-T JCA-IMT2020 to ITU-D study groups on invitation to update the information in the IMT2020 roadmap
2/23	2017-11-24	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on an ongoing work item on technical framework for countering telephone service scam
2/10	2017-11-22	ITU-T Study Group 20	Liaison Statement from ITU-T SG20 to ITU-D study groups on work on the combat of counterfeit ICT devices and mobile device theft

Annex 2: List of lessons learned received on Question 3/2

Web	Received	Source	Title
SG2RGQ/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs

The UK Government provides targeted support to small and medium-sized enterprises (SMEs) to help them navigate complicated standards to better understand how to mitigate cyberrisk. This support is designed specifically for organizations who are not aware of the cyberthreat and have limited resources, both financially and in terms of technical capability. Lessons learned include the following:

- Clear and consistent cyberrisk management messaging is crucial. Critically, **awareness campaigns** should not just explain *what* businesses need to do and *how* they can actually carry out the action by pointing to government advice, guidance and support, but should draw attention to *why* they should do it.
- Advice and guidance is most effective when it is non-technical, size-specific and easy to access. Government and law enforcement should use national, regional and local networks, and work in partnership with key industry bodies, to identify levers and business touchpoints that can be used to amplify messaging, and ensure advice and guidance reaching SMEs.
- The creation of a government-backed **certification scheme** can be an effective intervention to support SMEs to improve their cybersecurity. The certification scheme can:
    - be quickly and effectively delivered by a single supplier if the government can outline the technical controls and/or minimum standards that should be covered;
    - evolve to continue to meet the needs of SMEs and address the changing threat landscape;
    - better ensure organizations remain compliant through having a certification expiry date and requiring annual recertification.

Web	Received	Source	Title
SG2RGQ/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme

Challenges

A range of interconnected challenges face governments in relation to traditional approaches to public procurement of ICTs, which is typically:

- neither understanding nor meeting the needs of users
- task oriented, risk averse and inflexible
- isolated from what happens:
  - 'before' (strategic planning, investment appraisals, early market engagement)
  - 'after' (service delivery, monitoring and evaluation, supplier relationship management)
- hidden from public scrutiny due to the poor quality, inconsistency, incompleteness and poor availability of data.

User-centred design approaches

Since GDS was established in 2011, it has incubated, embedded and mainstreamed new standards-based approaches to government transformation.

These approaches were first conceptualized by the Government Design Principles,[163] published in April 2012.

Since then, GDS and the government and UK public sector more broadly have been incrementally applying these principles to redesign and improve services, organizational structures, governance approaches, etc. This includes public procurement.

Social Purpose Digital Commissioning

Focus on culture, mindset, collaboration and capability, by:

- understanding users' needs
- being clear about the problems you are trying to overcome (e.g. legacy ICT, system vulnerabilities, capability and capacity, governance and accountability, etc.) to meet users' needs
- being outcome-oriented (rather than solution-oriented), experimental and flexible, making small incremental investments to try out different approaches to address users' problems, learning quickly and iteratively
- being multidisciplinary and collaborative coalition builders, advocating for systemic change through communities of practice
- engaging throughout the end-to-end lifecycle of delivery - the 'before' and 'after' of procurement
- being open to public scrutiny through deliberative participation of civil society, enabled by structured, quality, consistent, complete and published open data.

[163] UK Government. Guidance. Government Design Principles. April 2012.

Web	Received	Source	Title
SG2RGQ/215	2020-07-27	Brazil	*#ConexãoSegura* (#SafeConnection) Awareness Campaigns

The campaign around personal data protection on the Internet reinforced the importance of telling consumers how to protect themselves in the digital environment. The interactions of consumers on digital media and on the website revealed that many of them have a number of doubts about what is fraud or scam - especially when it involves cash prizes, in addition to not knowing what to do when they are victims of these situations. It is also important to advise people not to post or publish personal data (surprisingly many people do not know what can happen). In the next initiative, it would be interesting to expand the dissemination of materials further in order to reach a wider audience.

Web	Received	Source	Title
SG2RGQ/214	2020-07-27	Brazil	Brazilian National Cyberdrill - Cyber Guardian Exercise

The exercise started with two national critical infrastructure (NCI) sectors and evolved in its second edition to a broader and more complex exercise process. The exercise continues to evolve, and for its third edition (cancelled due to the COVID-19 pandemic) it was planned to include six NCI sectors and to add an international cooperation component to the exercise.

Web	Received	Source	Title
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo

Turn cybersecurity in the Democratic Republic of the Congo into a lever for integration, protection, good governance, economic growth and social progress.

This vision will make a significant contribution to building the country's capacity in its digital transformation (circulation of information, data economy, growth economy, transparency and traceability, interoperability of information systems, etc.). It will allow digitalization to become a key driver for modernizing the State, promoting economic growth and fostering social progress.

Web	Received	Source	Title
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK

A significant proportion of IoT devices do not have basic cybersecurity features built into them. Following 18 months of collaboration with industry and experts at the UK's National Cyber Security Centre (NCSC), the Department for Digital, Culture, Media and Sport (DCMS) published the Code of Practice (CoP) for Consumer IoT Security in October 2018. The 13 voluntary guidelines, as outlined in the 2018 CoP, provide a much-needed baseline for IoT devices that manufacturers should embed into their products to make them 'secure by design'.

These include:

- No default passwords
- Implement a vulnerability disclosure policy
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure personal data are protected
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data.

These guidelines are outcome-focused as opposed to being prescriptive, which gives companies the space to come up with innovative solutions and appropriate ways to secure their products. Some devices might require enhanced security that is not included on this list and, as such, retailers and manufacturers are encouraged to secure their devices accordingly and seek solutions beyond the 13 guidelines. Action on the first three guidelines will bring largest security benefits in the short term.

Web	Received	Source	Title
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility

This document describes the consideration and implementation of cybersecurity measures for persons with disabilities, especially those with hearing difficulties, such as telecommunication relay service and remote captioning, to enhance accessibility to information and communication services.

Web	Received	Source	Title
SG2RGQ/134	2019-07-29	State of Palestine	Government Data Exchange

The central server issues certificates to security servers and provides a list of authenticated certificates to the systems connected to the Government Data Exchange. In addition, the central security server maintains encrypted activity data (hash logs) from the security servers to enable a series of e-service uses to be built subsequently, if necessary. If one of the parties to the service denies sending or receiving certain information, the service provider and user logs are compared with the encrypted copy in the central server. This method allows the integrity of security server logs to be checked, as it is impossible to change the log without it subsequently being detected.

The terms of the data-sharing process are defined by a memorandum of understanding signed by the two parties sharing the data and the Ministry of Telecommunications and Information Technology (MTIT), as third-party system operator. The memorandum includes an annex on the obligations of the parties, an annex on controls, standards and the duties and rights of each party, and an annex on the data which the two parties agree to share.

The system allows a connected ministry to determine which other connected institutions may access and read its data and the level of data that may be accessed. This is done by means of a control window on the ministry's own security server, enabling it to grant access rights to any of its services to the institutions it wishes.

Encrypted data are shared directly through secure servers from one information system to another. They do not pass through the central system and cannot be displayed there. The central system only has statistical information on the data shared.

Using this approach, the system facilitates the secure sharing of data between institutions, enabling them to share data between one another. It has also made it easier for the public to access services currently available G2G, by only going to one institution where the service involves more than one. MTIT is currently working to develop this mechanism and to provide services to the public directly via applications being developed.

Web	Received	Source	Title
SG2RGQ/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus

- Enhancing international cooperation, particularly between developed and developing countries.
- The school's regional nature helps to enhance cooperation among African countries.
- Covering all aspects of cybersecurity in both initial and continuing training.
- As cybersecurity is a prerequisite for the Digital Senegal 2025 Strategy (SN2025), classes have begun at the offices of the National School of Administration (ENA) while construction of the school's own premises is being completed at Diamniadio, 20 km from Dakar.
- The school will be the final element in the system for information system security and cybersecurity already in place.
- Boosting the fight against cybercrime in Africa.

Web	Received	Source	Title
SG2RGQ/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1

The recent update process to develop Version 1.1 of the Framework demonstrates an example of a good process for stakeholder engagement to ensure the Framework remains a useful tool for managing cybersecurity risk.

Web	Received	Source	Title
SG2RGQ/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK

A recent advisory on ransomware from the National Cyber Security Centre (NCSC) recommends the following risk-mitigation techniques:

- Keep devices and networks up to date (e.g. prompt updating and patching, and regular scans)
- Prevent and detect lateral movement in your enterprise network
- Segment networks
- Set up a security monitoring capability
- Whitelist applications
- Use antivirus
- Back up files.

The full advisory and detailed list of recommendations can be found at: https://www.ncsc.gov.uk/news/ongoing-threat-organisations-ransomware

Protecting your organization from ransomware: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Mitigating malware: https://www.ncsc.gov.uk/guidance/mitigating-malware

Unfortunately, it is not a question of 'if' but 'when' a cyberattack will occur. In the event an attack does take place, cooperation between the public and private sectors is key to understanding the threat and coordinating a quick and effective response to mitigate the impact of an attack. In the event of an attack, organizations are advised to contact the National Crime Agency, NCSC's Cyber Incident Response, or Cyber Security Information Sharing Partnership (CiSP). NCSC led the UK's response to the WannaCry attack and worked in collaboration with the National Crime Agency (NCA). Over the course of an incident, NCSC publishes statements and guidance for large organizations as well as home users and small businesses. Up-to-date information is announced via the NCSC Twitter account (@NCSC).

Web	Received	Source	Title
SG2RGQ/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills

This contribution recommends the use of cyberrange technology (cloud-based – public or private cloud) and competency frameworks in the development and delivery of new generation cyberdrills.

Web	Received	Source	Title
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire

- De-dramatize prevention by banishing the anxiety-provoking approach. Internet prevention can be part of a fear culture. However, this increases the anxiety of parents who are already worried about a technology they do not understand well, thereby undermining the extraordinary learning tool that is the Internet.
- Encourage educational programmes aimed at developing best practices in content management and raising children's awareness of responsible use of the Internet.
- Put an Internet portal online in order to provide children, adolescents, parents and teachers with an educational base.
- Involve all stakeholders in community-awareness activities: government agencies, the private Internet sector, NGOs, community groups and the general public.

Web	Received	Source	Title
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire

Statistics should be collected on complaints and damages (financial, moral).

Web	Received	Source	Title
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combating Cybercrime (PLCC)

- Development of partnerships between bodies responsible for combating cybercrime and the police in developing countries
- Awareness-raising in schools
- Collaboration with equivalent organizations in other countries.

Web	Received	Source	Title
SG2RGQ/262/172	2018-08-14 2019-02-07	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means to strengthen cybersecurity environments (2018 +2019 update)

For national digital security success, CSIRTs should focus substantial energy on broad facilitation for developing additional independent capabilities – in industries, professional communities, education centres, research, events, meet-ups and conferences, private and internal CSIRTs.

Web	Received	Source	Title
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies

- Establish and adopt situation awareness and threat intelligence policies.
- Develop incident analysis and response capabilities - establish CERTs.
- Develop collaboration with the private sector and information-sharing policies (public-private partnerships).

Web	Received	Source	Title
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin

Benin calls on ITU-D Study Group 2 to support:

- the establishment of a national CERT in Benin to enhance the level of trust in cyberspace;
- the building up of a common African security and defence policy;
- the creation of a panel of eminent personalities to reflect on Africa's role in regard to security;
- the establishment of a CERT-AFR (for Africa) along the lines of CERT-EU (for the European Union);
- a coordinated effort to avoid disparities between the strategies adopted and means deployed by Member States in terms of military cyberdefence capabilities;
- regulators and ICT authorities as they seek to:
    - adopt measures designed to enhance the security of information systems and networks;
    - create reliable digital identities;
    - protect minors and vulnerable groups; and
    - foster transparency.

Web	Received	Source	Title
SG2RGQ/25	2018-08-14	Proge-Software [*SME pilot*] (Italy)	Data Privacy and Cloud - be compliant

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) (EU) 2016/679 governs data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying regulation within the EU. Superseding Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personally identifiable information (personal data) of individuals (formally called data subjects in the GDPR) inside the European Union, and applies to an enterprise that is established in the EU or – regardless of its location and the data subjects' citizenship – that is processing the personal data of people inside the EU. Controllers of personal data must put in place appropriate technical and organizational measures to implement the data-protection principles. Severe penalties are applied to violators.

Cloud computing

In computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or how it is transported. Periodically they pay for what they have consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power or specially crafted development environments without having to worry how these work internally. Cloud computing is usually Internet-based computing. According to a paper published by IEEE Internet Computing in 2008, "*Cloud computing is a paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include computers, laptops, handhelds, sensors, etc.*".

Web	Received	Source	Title
SG2RGQ/32	2018-08-16	Guardtime AS [*SME pilot*] (Estonia)	Towards cyber resilience – the role of national cyber exercises

Cyberexercises are essential to achieving sustainable cyberresilience. Cyberexercises are different from training, and must be customized, realistic and engaging. Governments should consider developing a programme to govern cyberresilience, covering education, training and cyberexercises ranging from localized events to customized national-scale exercises conducted on a regular basis.

Web	Received	Source	Title
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities

1. Contact the service provider to inform it of the highjacking of your e-mail address.
2. Try to give information on the spammer's/hacker's contact details with an example e-mail, e.g. by forwarding the suspect e-mail to its fraud section.
3. Ask to have your violated e-mail blocked.
4. Change your e-mail address.
5. Let your friends and contacts know you have been hacked and give them the new address.
6. Do not click on any web addresses unless you have verified it is in fact from a known source.

Web	Received	Source	Title
2/41	2018-02-28	Burundi	Cybersecurity, Internet exchange point and e-commerce in Burundi

Security of IT data and of communication networks in order to ensure high-quality services is the pillar of ICT-sector development. A legal and regulatory framework for cybersecurity in our country is an essential tool for implementing all aspects of data security. The introduction of an Internet exchange point facilitates local communications and reduces latency times and associated costs. Lastly, domain name management provides facilities for investors. Data security will thus enable us to ensure reliable e-transactions and retain our customers.

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 des Almadies
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
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Courriel: itu-harare@itu.int
Tél.: +263 4 77 5939
Tél.: +263 4 77 5941
Fax: +263 4 77 1257

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
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailande

Adresse postale:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Courriel: ituasiapacificregion@itu.int
Tél.: +66 2 575 0055
Fax: +66 2 575 3507

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

Adresse postale:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Courriel: ituasiapacificregion@itu.int
Tél.: +62 21 381 3572
Tél.: +62 21 380 2322/2324
Fax: +62 21 389 5521

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: itumoscow@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: 978-92-61-34102-2

9 789261 341022

Publié en Suisse
Genève, 2021