|  |  |
| --- | --- |
| **Conseil 2018Genève, 17-27 avril 2018** | **logo_F_** |
|  |  |
|  |  |
| **Point de l'ordre du jour: PL 1.5** | **Document C18/18-F** |
| **8 février 2018** |
| **Original: anglais** |
| Rapport du Secrétaire général |
| Activités de l'UIT relatives au renforcement du rôle de l'union dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication |

|  |
| --- |
| RésuméLe présent rapport résume les activités menées par l'UIT depuis la session de 2017 du Conseil au titre de la Résolution 130 (Rév. Busan, 2014) de la Conférence de plénipotentiaires, du rôle de l'UIT en tant que coordonnateur unique pour la grande orientation C5 du SMSI et des autres décisions prises par les membres concernant le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC).Suite à donnerLe Conseil est invité à **prendre note** du présent rapport.\_\_\_\_\_\_\_\_\_\_\_\_Références*Résolutions* [*71*](http://www.itu.int/en/council/planning/Documents/PP-14_Res71.pdf)*,* [*130*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20130.pdf)*,* [*140*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20140.pdf)*,* [*174*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20174.pdf)*,* [*179*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20179.pdf) *(Rév. Busan, 2014) et* [*181*](http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf) *(Guadalajara, 2010) de la Conférence de plénipotentiaires, Règlement des télécommunications internationales (Rév.Dubaï, 2012),* [*Résolution 1306*](https://www.itu.int/md/S15-CL-C-0109/en) *du Conseil, Résolutions*[*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf) *(Rév.Dubaï, 2014) et* [*2, 67 et 69 (Rév.Buenos Aires, 2017)*](https://www.itu.int/md/D14-WTDC17-C-0115/en) *de la CMDT, Objectif 2/Produit 2.2 de l'UIT-D (*[*Plan d'action de Buenos Aires*](https://www.itu.int/md/D14-WTDC17-C-0115/en)*), Résolutions* [*50*](https://www.itu.int/pub/T-RES-T.50-2016)*,* [*52*](https://www.itu.int/pub/T-RES-T.52-2016)*,* [*75*](https://www.itu.int/pub/T-RES-T.75-2016) *(Rév.Hammamet, 2016) et* [*58*](https://www.itu.int/pub/T-RES-T.58-2016) *(Rév.Dubaï, 2012) de l'AMNT, Documents*[*C05/32*](http://www.itu.int/md/S05-CL-C-0032/en)*,* [*C05/INF/10*](https://www.itu.int/md/S05-CL-INF-0010/en)*,* [*C06/4*](http://www.itu.int/md/S06-CL-C-0004/en)*,* [*C07/21*](http://www.itu.int/md/S07-CL-C-0021/en)*,* [*C08/33*](http://www.itu.int/md/S08-CL-C-0033/en)*,* [*C09/50*](http://www.itu.int/md/S09-CL-C-0050/en)*,* [*C10/12*](http://www.itu.int/md/S10-CL-C-0012/en)*,* [*C11/54*](http://www.itu.int/md/S11-CL-C-0054/en)*,* [*C12/29*](http://www.itu.int/md/S12-CL-C-0029/en)*,* [*C13/23*](http://www.itu.int/md/S13-CL-C-0023/en)*,* [*C14/23*](http://www.itu.int/md/S14-CL-C-0023/en)*,* [*C15/18*](http://www.itu.int/md/S15-CL-C-0018/en)*,* [*C16/18*](https://www.itu.int/md/S16-CL-C-0018/en) *et* [*C17/18*](https://www.itu.int/md/S17-CL-C-0018/en) *du Conseil* |

# 1 Activités relatives à la cybersécurité et à la lutte contre le spam

1.1 Le développement des TIC, étayé par la sécurité et la confiance, est reconnu comme un facteur essentiel du développement durable. Le présent rapport, qui s'articule autour des cinq piliers du [Programme mondial cybersécurité (GCA)](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx), fait apparaître la complémentarité des programmes de travail existants de l'UIT et vise à faciliter la mise en oeuvre des activités menées par le BDT, le TSB et le BR dans ce domaine.

# 2 Cadre législatif

2.1 Dans le cadre de l'Objectif 2.2 du Plan d'action de Buenos Aires, et compte tenu de la Question 3/2 (ancienne Question 22/1) de l'UIT-D, l'UIT aide les Etats Membres à comprendre les aspects juridiques de la cybersécurité, en mettant à leur disposition ses [ressources sur la législation relative à la cybercriminalité](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx), afin de contribuer à l'harmonisation de leurs cadres juridiques.

2.2 En ce qui concerne le cadre législatif, l'UIT collabore étroitement avec des partenaires tels que l'Office des Nations Unies contre la drogue et le crime (ONUDC) et d'autres partenaires bénéficiant de compétences spécialisées dans ce domaine.

# 3 Mesures techniques et procédures

3.1 La [Commission d'études 17 (CE 17)](http://www.itu.int/ITU-T/studygroups/com17/) de l'UIT-T, en sa qualité de commission d'études directrice chargée de la sécurité et de la gestion d'identité (IdM), continue de contribuer aux études et à la normalisation dans les domaines de la cybersécurité, de la lutte contre le spam, de la gestion d'identité, des certificats UIT-T X.509, de la gestion de la sécurité de l'information, des réseaux de capteurs ubiquitaires, de la télébiométrie, de la sécurité mobile, de la sécurité de la virtualisation dans l'optique de la sécurité de l'informatique en nuage, de la protection des informations d'identification personnelle ainsi que de l'architecture de la sécurité et de la sécurité des applications, souvent en coopération avec des organisations et des consortiums de normalisation extérieurs.

3.2 [A la réunion qu'elle a tenue du 29 août au 6 septembre 2017](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx), la CE 17 de l'UIT‑T a décidé de formuler une nouvelle Question 14/17 intitulée "Aspects sécurité des technologies de registres numériques distribués" et a approuvé les nouvelles Recommandations suivantes: UIT-T X.1040 "Architecture de référence de sécurité pour la gestion, tout au long de leur cycle de vie, des données sur les transactions de commerce électronique", UIT-T X.1053 "Code de bonne pratique pour les contrôles de sécurité de l'information sur la base de la Recommandation UIT-T X.1051 pour les petites et moyennes organisations de télécommunication", UIT-T X.1146 "Lignes directrices pour garantir la protection des services à valeur ajoutée fournis par les opérateurs de télécommunication", UIT-T X.1213 "Capacités requises en matière de sécurité pour lutter contre les réseaux zombies (ou botnets) ciblant des smartphones", UIT-T X.1248 "Exigences techniques pour lutter contre le spam par messagerie instantanée (SPIM)" et UIT-T X.1541 (révisée) "Format d'échange de description d'objet incident (version 2)".

3.3 La CE 17 de l'UIT-T a approuvé trois Suppléments aux Recommandations UIT-T de la série X, à savoir: Supplément 29 aux Recommandations de la série X – "Supplément à la Recommandation UIT-T X.1242 – Lignes directrices sur les mesures de rétorsion à prendre pour lutter contre les attaques par hameçonnage par le service de messages courts (SMS)"; Supplément 30 aux Recommandations de la série X – "Supplément à la Recommandation UIT‑T X.805 – Lignes directrices sur la sécurité pour les opérateurs de réseaux virtuels mobiles (MVNO)" et Supplément 31 aux Recommandations de la série X – "Supplément à la Recommandation UIT-T X.660 – Lignes directrices relatives à l'utilisation des identificateurs d'objet pour l'Internet des objets".

3.4 Au cours de la prochaine réunion de la CE 17 qui se tiendra en mars 2018, trois projets de nouvelles Recommandations devraient être approuvés selon la procédure TAP. L'étude des autres thèmes ci-après, "Cadre technique pour lutter contre le spam publicitaire sur les applications mobiles, "Cadre de sécurité relatif à l'Internet des objets", "Cadre de sécurité pour l'exploitation des réseaux vocaux LTE (VoLTE, voice-over-long-term-evolution)", "Protocole de renforcement de la confiance – protocole d'amélioration de l'authentification et métadonnées – Version 1.0" devrait également être achevée et ces thèmes devraient être approuvés.

3.5 Un [Atelier de l'UIT sur les aspects sécurité de la chaîne de blocs](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Pages/default.aspx) s'est tenu le 21 mars 2017 à Genève (Suisse), pour examiner les possibilités qu'offre la chaîne de blocs pour renforcer la confiance dans l'utilisation des TIC. Une table ronde de spécialistes a rassemblé des associations professionnelles et des organismes de normalisation, qui ont réfléchi à la manière dont les travaux menés par la CE 17 de l'UIT‑T pourraient contribuer à la collaboration en matière de normalisation destinée à appuyer la chaîne de blocs.

3.6 La CE 17 de l'UIT-T a organisé un [Atelier sur les aspects sécurité des systèmes de transport intelligents](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Pages/default.aspx) le 28 août 2017 à Genève (Suisse), au cours duquel les participants ont examiné les besoins en matière de sécurité de tous les acteurs de la chaîne de valeur qui sous-tend les systèmes de transport intelligents (ITS) et souligné la nécessité de renforcer la collaboration entre les organismes concernés.

3.7 Le [Groupe régional de la CE 17 de l'UIT-T pour la région des Etats arabes](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/sg17rgarb/Pages/default.aspx) a tenu sa première réunion le 10 décembre 2017 à Mascate (Oman).

3.8 La CE 17 de l'UIT-T projette d'organiser un [atelier de l'UIT sur la sécurité de la 5G](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx) le 19 mars 2018, avant sa prochaine réunion de la CE 17 qui se tiendra du 20 au 29 mars 2018 à Genève (Suisse).

3.9 La CE 17 de l'UIT-T a poursuivi sa coordination avec la CE 20 de l'UIT-T, chargée de l'étude de: "L'Internet des objets et ses applications, y compris les villes et les communautés intelligentes (SC&C)" dans le domaine de la sécurité de l'IoT.

3.10 L'UIT-R poursuit ses travaux dans le domaine de la normalisation des radiocommunications, de façon à répondre à l'évolution constante des réseaux modernes de télécommunication. Ce secteur a défini des principes de sécurité précis concernant les réseaux IMT (3G, 4G et 5G) (Recommandations UIT-R M.1078, M.1223, M.1457, M.1645, M.2012 et M.2083). Il a également publié des Recommandations sur les questions de sécurité relatives à l'architecture de gestion des réseaux pour les systèmes numériques à satellites (Recommandation UIT-R S.1250) et sur l'amélioration de la qualité de fonctionnement du protocole de commande de transmission sur les réseaux à satellite (Recommandation UIT-R S.1711).

# 4 Structures organisationnelles

4.1 L'UIT continue de contribuer au renforcement des capacités aux niveaux régional et international. L'Union a procédé à des évaluations techniques pour faire le point sur l'état de préparation à la [création d'équipes d'intervention en cas d'incident informatique (CIRT)](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx) dans 68 pays, et poursuit ses activités en vue de prendre les mesures de suivi nécessaires. Des CIRT nationaux sont en cours de mise en place ou d'amélioration au Burundi, à Chypre, en Gambie, en Palestine et au Zimbabwe, les activités connexes ayant été menées à bonne fin dans 13 pays.

4.2 L'UIT a travaillé en partenariat avec le Centre mondial des capacités de cybersécurité de l'Oxford Martin School, avec lequel elle a mené conjointement une évaluation des capacités de cybersécurité en Thaïlande, en Sierra Leone et à Madagascar. Dans le cadre d'un projet financé par le Gouvernement australien (DOCA), l'UIT procédera à des évaluations CIRT aux Samoa, au Tonga, à Vanuatu, et en Papouasie-Nouvelle-Guinée, après quoi elle mènera une évaluation des capacités de cybersécurité.

4.3 L'UIT continue d'organiser des [cyberexercices](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx) pour les pays partenaires. A ce jour, l'Union a organisé 19 cyberexercices, auxquels plus de 100 pays ont participé. Au cours de la période considérée, des cyberexercices internationaux ont été organisés à: a) [Paramaribo (Suriname](https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2017/20287.aspx)) pour la région des Caraïbes (3-7 juillet 2017); b) à [Dar Es Salaam (Tanzanie](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Tanzania_cyberdrill_2017.aspx)) pour la région Afrique et la région des Etats arabes (13-17 novembre 2017); et c) à [Chisinau (Moldova](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Moldova_cyberdrill_2017.aspx)) pour la région Europe et la région de la CEI (21-23 novembre 2017).

4.4 Un [kit pratique sur les stratégies nationales](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx) en matière de cybersécurité est en cours d'élaboration, dans le cadre d'une action coordonnée par l'UIT qui fait appel à de multiples parties prenantes. Pour faire avancer les travaux, trois ateliers réunissant les partenaires concernés ont été organisés en 2016 et une réunion de suivi a eu lieu à Washington DC (Etats-Unis) les 25 et 26 février 2018. Ce kit pratique sera bientôt achevé.

# 5 Renforcement des capacités

5.1 L'UIT continue d'organiser des [forums régionaux sur la cybersécurité](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) à l'intention de toutes ses régions, qu'elle utilise comme instrument de renforcement des capacités pour différents programmes et diverses activités du BDT ainsi que comme cadre opérationnel de coopération aux niveaux régional et international.

5.2Suite à la CMDT-17, les travaux au titre de la Question 3/2 ([Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité](http://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=1&sp=2014&rgq=D14-SG02-RGQ03.2&stg=2)) se poursuivront pendant la période d'études 2018-2021.

5.3 L'UIT, conjointement avec Africa CERT, a organisé un atelier de renforcement des capacités sur le thème "[Renseignement en matière de menace à l'intention des équipes CIRT](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Threat-intelligence-training-Benin-2017.aspx)" du 11 au 15 décembre 2017 à Cotonou (Benin), en collaboration avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI FRANCE).

5.4 A la suite de la présentation en 2014 des premiers résultats du projet relatif à [l'Indice de la cybersécurité dans le monde](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx) (GCI) et de leur prise en compte dans la Résolution 130 (Rév. Busan, 2014) de la Conférence de plénipotentiaires, les travaux relatifs à la seconde version de [l'Indice de la cybersécurité dans le monde (GCI) (2017)](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx) ont été achevés à partir des réponses de 134 pays et avec le concours de partenaires internationaux.

5.5 Un webinaire consacré au "[Rapport sur l'indice de cybersécurité dans le monde pour la région Europe](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2017/GCI/Webinar-on-New-Report-on-Global-Cybersecurity-Index-%28GCI%29-for-the-Europe-Region.aspx)" a été organisé le 18 décembre 2017. L'objectif de ce webinaire était de présenter le rapport sur l'indice GCI pour la région Europe, qui permet de mieux cerner et de mieux comprendre les conclusions relatives à la cybersécurité dans les 43 pays de la région Europe de l'UIT et qui contient notamment des exemples de pratiques suivies en Europe.

5.6 Il est prévu d'organiser un [Atelier régional de l'UIT pour l'Europe et la CEI sur la cybersécurité et la protection en ligne des enfants](https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Pages/EVENTS/2018/04_Odessa/04_Odessa.aspx) du 4 au 6 avril à Odessa (Ukraine).

# 6 Coopération internationale

6.1 L'UIT continue de nouer des relations et des [partenariats](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) avec diverses organisations et initiatives régionales et internationales, notamment la Commonwealth Cybercrime Initiative, l'ENISA, INTERPOL, la CEDEAO, la Banque mondiale le Forum FIRST et les associations régionales d'équipes CSIRT/CERT, comme AP CERT, AFRICA CERT et OIC CERT.

6.2 En tant que coordonnateur principal de la grande orientation C5 du SMSI, l'UIT a organisé plusieurs manifestations à l'occasion du [Forum 2017 du SMSI](https://www.itu.int/net4/wsis/forum/2017/), qui ont permis à tous les groupes de parties prenantes d'échanger des données d'expérience dans le cadre de leur action au niveau mondial en vue d'instaurer la confiance et la sécurité dans l'utilisation des TIC. Il est prévu d'organiser plusieurs manifestations de haut niveau à l'occasion du Forum 2018 du SMSI, dans le cadre du 10ème anniversaire du lancement du Programme mondial cybersécurité (GCA) et de l'initiative pour la protection en ligne des enfants.

6.3 L'UIT a participé à la [Conférence internationale multi-parties prenantes "Semaine de la cybersécurité 2018 – Vienne – Protection des infrastructures énergétiques essentielles"](https://www.energypact.org/energypact-foundation-events18/) organisée par le Gouvernement autrichien, l'EnergyPact Foundation et l'Institut autrichien de la technologie, avec le concours de la CEI, de l'OSCE et de l'UIT, du 29 janvier au 2 février 2018 à Vienne (Autriche).

# 7 Protection en ligne des enfants (COP)

7.1 Le [Groupe de travail du Conseil sur la protection en ligne des enfants](http://www.itu.int/en/council/cwg-cop/Pages/default.aspx) (GTC-COP) a tenu deux réunions depuis la dernière période considérée, et a notamment organisé des consultations ouvertes en ligne avec des jeunes sur différents thèmes. On trouvera davantage de renseignements dans le [Document C18/15](https://www.itu.int/md/S18-CL-C-0015/fr).

7.2 L'UIT et ses partenaires continuent de travailler en étroite coopération afin de progresser vers la réalisation des Objectifs de développement durable (ODD), en particulier l'ODD 16.2 "Mettre un terme à la maltraitance, à l'exploitation et à la traite, et à toutes les formes de violence et de torture dont sont victimes les enfants".

7.3 En juin 2017, l'UIT et l'UNICEF ont organisé un atelier thématique intitulé "De la sécurité en ligne des enfants à l'inclusion numérique: rôle des partenariats mondiaux multi‑parties prenantes", au cours duquel il a été question de la participation des enfants aux délibérations précédant la prise de décisions et de l'importance d'utiliser une terminologie définie d'un commun accord pour déceler les lacunes et déterminer les mesures à prendre.

7.4 L'UIT a participé à la septième Consultation régionale et au troisième Dialogue sur les politiques à suivre concernant les permanences téléphoniques pour enfants en Europe. Plusieurs membres ont estimé qu'il était nécessaire de disposer d'un numéro régional harmonisé pour les permanences téléphoniques pour enfants et les décideurs ainsi que les institutions régionales ont été encouragés à intensifier leur action en la matière.

7.5 L'UIT a participé au Sommet mondial Aqdar, qui s'est tenu à Abu Dhabi (Emirats arabes unis) du 21 au 23 novembre 2017. Les participants ont abordé plusieurs questions liées au rôle de l'éducation morale dans les établissements universitaires, tant au niveau régional qu'au niveau international, pour trouver une solution aux menaces qui pèsent sur le monde. L'UIT a présenté les travaux menés par le GTC-COP et souligné la nécessité de sensibiliser les jeunes enfants à l'utilisation sûre et responsable des technologies.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_