|  |  |
| --- | --- |
| **Conseil 2017 Genève, 15-25 mai 2017** | **logo_F_** |
|  |  |
|  |  |
| **Point de l'ordre du jour: PL 1.5** | **Document C17/18-F** |
| **14 mars 2017** |
| **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 | |

|  |
| --- |
| Résumé  Le présent rapport résume les activités menées par l'UIT depuis la session de 2016 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 donner  Le Conseil est invité à **prendre note** du présent rapport.  \_\_\_\_\_\_\_\_\_\_\_\_  Références  [*Résolution 71 (Rév. Busan, 2014)*](http://www.itu.int/en/council/planning/Documents/PP-14_Res71.pdf)*,* [*Résolution 130 (Rév. Busan, 2014)*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20130.pdf)*,* [*Résolution 140 (Rév. Busan, 2014)*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20140.pdf)*,* [*Résolution 174 (Rév. Busan, 2014)*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20174.pdf) *et* [*Résolution 179 (Rév. Busan, 2014)*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20179.pdf) *de la Conférence de plénipotentiaires,* [*Résolution 181 (Guadalajara, 2010)*](http://www.itu.int/council/Basic-Texts/ResDecRec-PP10-e.docx#res181)*,* [*Règlement*](http://www.itu.int/pub/S-CONF-WCIT-2012/fr) *des télécommunications internationales (Rév.Dubaï, 2012),* [*Résolution 1306 du Conseil*](https://www.itu.int/md/S15-CL-C-0109/en)*, Résolutions* [*2*](https://www.itu.int/en/ITU-D/TIES_Protected/WTDC14/WTDC14-FinalReport-E.pdf)*,* [*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf)*,* [*67*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/67revDubai.pdf) *et*[*69*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/69revDubai.pdf) *(Rév. Dubaï, 2014) de la CMDT,* [*Objectif 3*](https://www.itu.int/en/ITU-D/TIES_Protected/WTDC14/WTDC14-FinalReport-E.pdf) *du Plan d'action de Dubaï (PAD) de la CMDT-14, Résolutions* [*50*](http://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2050.pdf)*,* [*52*](http://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2052.pdf) *et* [*75*](http://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2075.pdf) *(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*](http://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) *et* [*C16/18*](https://www.itu.int/md/S16-CL-C-0018/fr) *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 3 du Plan d'action de Dubaï, 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 à l'étude 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 de la TVIP, de la sécurité de la virtualisation dans l'optique de la sécurité de l'informatique en nuage 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 Depuis la session de 2016 du Conseil de l'UIT, la CE 17 a approuvé les Recommandations UIT‑T sur la cybersécurité suivantes: Recommandation UIT-T X.1038 "Exigences de sécurité et architecture de référence pour les réseaux pilotés par logiciel"; Recommandation UIT-T X.1039 "Mesures de sécurité techniques pour la mise en oeuvre des dimensions de sécurité UIT-T X.805"; Recommandation UIT-T X.1085 "Technologies de l'information – Techniques de sécurité – Cadre d'authentification télébiométrique utilisant un module matériel de sécurité biométrique"; Recommandation UIT-T X.1087 "Contremesures techniques et opérationnelles pour les applications de la télébiométrie utilisant des dispositifs mobiles"; Recommandation UIT-T X.1258 "Authentification d'entité améliorée basée sur des attributs agrégés"; Recommandation UIT-T X.1542 "Format d'échange de messages sur les informations de session"; Recommandation UIT-T X.1641 "Lignes directrices relatives à la sécurité des données des clients de services de nuage"; par ailleurs d'importantes modifications ont été apportées aux Recommandations UIT-T de la série X.500 "Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire".

3.3 Sept projets de Recommandation devraient être approuvés selon la procédure TAP en mars 2017, concernant la cybersécurité, la protection des informations d'identification personnelle, le contrôle d'accès, le chiffrement pour l'Internet des objets, la perception par l'utilisateur final des indicateurs de fiabilité et les capacités de mise à jour sécurisée des logiciels pour les systèmes de transport intelligents. Par ailleurs, huit autres projets de Recommandation devraient être achevés et soumis à la procédure d'approbation AAP, concernant les techniques structurées d'échange d'information sur la cybersécurité, la lutte contre les réseaux zombies utilisant des téléphones intelligents, la lutte contre le spam de messagerie instantanée (SPIM), le hameçonnage par SMS, les mesures contre le vol de téléphones mobiles et la sécurité des capacités ouvertes des services de télécommunication. Des travaux ont été entrepris en vue de l'élaboration de projets de Recommandation sur la lutte contre les escroqueries par service téléphonique, la sécurité des services de compteurs intelligents dans les réseaux de distribution intelligents, la mise en oeuvre de la désidentification, les mécanismes hybrides d'authentification et de gestion des clés dans le modèle client-serveur, l'analyse des mégadonnées dans les services Internet mobiles, la sécurité des mégadonnées en tant que service, des communications en tant que service et des réseaux en tant que service, l'authentification télébiométrique utilisant des bio-signaux, la détection télébiométrique des piratage et le profil de syntaxe de message cryptographique (CMS).

3.4 [Le Groupe régional de la CE 17 pour l'Afrique](http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/sg17rgafr/Pages/default.aspx) a tenu sa deuxième réunion les 27 et 28 juillet 2016 à Khartoum (République du Soudan).

3.5 La CE 17 a continué à travailler en coordination avec la nouvelle CE 20 de l'UIT-T: "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'Internet des objets (IoT).

3.6 L'UIT-R poursuit ses travaux dans le domaine de la normalisation des radiocommunications, de façon à répondre à l'évolution constante des réseaux de télécommunication modernes. Ce Secteur a défini des principes de sécurité clairs 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, en Gambie, à Chypre et au Kenya, les activités connexes ayant été menées à bonne fin dans douze 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.

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, afin de renforcer les capacités des équipes participantes en matière de communication et d'intervention en cas d'incident, et d'intensifier la coopération nationale et internationale dans le domaine de la lutte contre les cybermenaces. A ce jour, l'UIT a organisé seize cyberexercices, auxquels plus de 100 pays ont participé. Au cours de la période couverte par le présent rapport, des cyberexercices internationaux ont été organisés à Quito (Equateur) pour la [région Amériques](http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2016/15551.aspx) (27 juin – 1er juillet 2016), à Tunis (Tunisie) pour la [région des Etats arabes](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Tunisia_cyberdrill_2016.aspx) (23-27 mai 2016) et à Maurice pour la [région Afrique](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Mauritius_cyberdrill_2016.aspx) (4-8 avril 2016).

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 les 18 et 19 février 2016 au siège de l'UIT à Genève (Suisse), les 6 et 7 juin 2016 à la Saïd Business School de l'Université d'Oxford (Royaume-Uni) et les 13 et 14 octobre 2016 à Washington DC (Etats-Unis), à l'invitation de l'Organisation des Etats Américains (OEA). Ce kit pratique sera bientôt achevé et sera mis à la disposition du public d'ici à la fin de l'année 2017.

4.5 L'UIT a fourni une assistance au Népal concernant l'élaboration de sa stratégie nationale de cybersécurité et la protection en ligne des enfants, ce qui a permis d'améliorer la sensibilisation et de renforcer les capacités au sein d'une centaine de parties prenantes issues des secteurs public, réglementaire et privé. Elle a également mené avec succès une simulation de cybersécurité et renforcé la coopération avec l'Autorité des télécommunications du Népal (NTA).

4.6 Une enquête sur l'état de préparation en matière de cybersécurité a été menée dans plusieurs pays de la région Asie-Pacifique (2015-2016) sur la base des cinq piliers du Programme mondial cybersécurité (GCA).

# 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 de l'UIT-D ainsi que comme cadre opérationnel de coopération aux niveaux régional et international.

5.2La Commission d'études 2 de l'UIT-Dpoursuit ses travaux menés pendant la période d'études 2014-2018 sur 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).

5.3 Un atelier sur le thème ["Stratégie de la cybersécurité dans les pays d'Afrique"](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Pages/default.aspx) a été organisé conjointement par l'UIT et l'UAT avec l'appui du TSB et du BDT, du 24 au 26 juillet 2016, au siège de la National Telecommunication Corporation (NTC) à Khartoum (République du Soudan).

5.4 Pour la première fois, l'UIT a travaillé officiellement en partenariat avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour organiser un [Forum régional conjoint UIT-ENISA sur la cybersécurité](http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/RCYBF/Regional-Cybersecurity-Forum.aspx), les 29 et 30 novembre 2016 à Sofia (Bulgarie).

5.5 La 4ème édition de la ["Plate-forme de dialogue entre secteur public et secteur privé sur la cybersécurité en Europe centrale"](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/CYBR/Cyber-Security-in-Romania.aspx) a eu lieu du 14 au 16 septembre 2016 à Sibiu (Roumanie).

5.6 A la suite de la présentation en 2014 des premiers résultats du projet relatif à l'Indice de la [cybersécurité dans le monde (GCI)](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx), une [nouvelle version du GCI](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2016.aspx), comprenant un index amélioré et un groupe de partenaires, est en cours d'élaboration. A ce jour, 136 pays ont répondu au questionnaire et l'analyse des réponses est en cours.

5.7 En 2016, l'UIT a aidé au renforcement des compétences techniques pour aider les intervenants en cas d'incident au Myanmar, au Viet Nam, en République démocratique populaire Lao et au Cambodge.

# 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 SCIRT/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 2016 du SMSI](https://www.itu.int/net4/wsis/forum/2016/), 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.

6.3 Pendant le Forum d'ITU Telecom 2016, l'UIT, en collaboration avec l'EastWest Institute (EWI), a organisé une séance de discussion sur le thème ["Confiance dans les TIC, innovation et commerce"](http://www.itu.int/net4/Telecom/webs/TelecomWorld/session/description/C-00001734).

6.4 L'UIT a participé à la [conférence internationale multi-parties prenantes "Cyberespace, énergie et développement – Protection des infrastructures énergétiques essentielles"](https://www.energypact.org/energypact-foundation_conferences/) organisée par le Gouvernement de l'Autriche, l'EnergyPact Foundation et l'Institut autrichien de la technologie, avec le concours de la CEI, de l'ONUDC et de l'UIT, à Vienne (Autriche) le 16 février 2017.

6.5 [195 profils par pays](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx) sont toujours à la disposition du public sur le site web de l'UIT. Ces profils sont des représentations factuelles non analytiques de la situation en matière de cybersécurité de chaque pays, qui reposent sur les [cinq piliers du programme GCA](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx). Il s'agit de documents évolutifs qui continuent d'être mis à jour à mesure que de nouvelles données concernant les pays sont disponibles.

# 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 C17/15](https://www.itu.int/md/S17-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 Lors des deux précédentes réunions du GTC-COP, Child Helpline International (CHI) a présenté les résultats de la campagne "[Oeuvrer en partenariat pour protéger les enfants et les jeunes](http://www.itu.int/en/cop/Pages/consultation-may2016.aspx)" menée conjointement par l'UIT et CHI. Les résultats finals de cette campagne, qui avait été lancée en mai 2016, ont été présentés le 15 novembre 2016 à l'occasion d'ITU Telecom World 2016 et de nouvelles méthodes pour développer les services des permanences téléphoniques pour les enfants ont été présentées aux participants. L'accent a été mis sur la collaboration entre les membres de l'UIT et les permanences téléphoniques. Les membres du GTC-COP ont salué cette campagne et le Président a encouragé le Secrétariat à poursuivre cette initiative afin d'avancer vers la réalisation de l'Objectif de développement durable 16.

7.4 Les bureaux régionaux de l'UIT continuent de fournir une assistance aux Etats Membres concernant l'analyse de leur cadre de protection en ligne des enfants, l'objectif étant d'élaborer et de proposer un cadre viable pouvant être mis en oeuvre sur une longue période.

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