Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

ASSEMBLÉE MONDIALE DE NORMALISATION DES TÉLÉCOMMUNICATIONS

Genève, 1-9 mars 2022

Résolution 50 – Cybersécurité

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

RÉSOLUTION 50 (Rév. Genève, 2022)

Cybersécurité

(Florianópolis, 2004; Johannesburg, 2008; Dubaï, 2012; Hammamet, 2016; Genève, 2022)

L'Assemblée mondiale de normalisation des télécommunications (Genève, 2022),

rappelant

a) la Résolution 130 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires, sur le 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);

b) la Résolution 174 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires, sur le rôle de l'UIT concernant les questions de politiques publiques internationales ayant trait aux risques d'utilisation des TIC à des fins illicites;

c) la Résolution 179 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires, sur le rôle de l'UIT dans la protection en ligne des enfants;

d) la Résolution 181 (Guadalajara, 2010) de la Conférence de plénipotentiaires, sur les définitions et termes relatifs à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

e) les Résolutions 55/63 et 56/121 de l'Assemblée générale des Nations Unies, par lesquelles a été établi le cadre juridique pour la lutte contre l'exploitation des technologies de l'information à des fins criminelles;

f) la Résolution 57/239 de l'Assemblée générale des Nations Unies, relative à la création d'une culture mondiale de la cybersécurité;

g) la Résolution 58/199 de l'Assemblée générale des Nations Unies, relative à la création d'une culture mondiale de la cybersécurité et à la protection des infrastructures essentielles de l'information;

h) la Résolution 41/65 de l'Assemblée générale des Nations Unies, relative aux principes concernant la télédétection de la Terre depuis l'espace extra-atmosphérique;

i) la Résolution 70/125 de l'Assemblée générale des Nations Unies – "Document final de la réunion de haut niveau de l'Assemblée générale sur l'examen d'ensemble de la mise en œuvre des textes issus du Sommet mondial sur la société de l'information";

j) la Résolution 45 (Rév. Dubaï, 2014) de la Conférence mondiale de développement des télécommunications (CMDT), sur les mécanismes propres à améliorer la coopération en matière de cybersécurité, y compris la lutte contre le spam;

k) la Résolution 52 (Rév. Hammamet, 2016) de l'Assemblée mondiale de normalisation des télécommunications, "Lutter contre le spam";

l) la Résolution 58 (Rév. Genève, 2022) de la présente Assemblée, "Encourager la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement[1]";

m) que l'UIT joue le rôle de coordonnateur principal pour la grande orientation C5 de l'Agenda de Tunis pour la société de l'information (Établir la confiance et la sécurité dans l'utilisation des TIC) adopté par le SMSI;

n) les dispositions des résultats du SMSI relatives à la cybersécurité,

---

1 Les pays en développement comprennent aussi les pays les moins avancés, les petits États insulaires en développement, les pays en développement sans littoral et les pays dont l'économie est en transition.

considérant

a) l'importance cruciale que revêt l'infrastructure des télécommunications/TIC et ses applications pour pratiquement toutes les formes d'activités sociales et économiques;

b) que le réseau téléphonique public commuté traditionnel présente un certain niveau de sécurité intrinsèque du fait de sa structure hiérarchisée et de ses systèmes de gestion intégrés;

c) que les réseaux utilisant le protocole Internet (IP) n'assurent qu'une séparation réduite entre les éléments utilisateurs et les éléments réseaux si on n'accorde pas le soin voulu à la conception et à la gestion de la sécurité;

d) que les réseaux traditionnels et les réseaux IP post-convergence sont donc potentiellement plus vulnérables à l'intrusion si on n'accorde pas le soin voulu à la conception et à la gestion de la sécurité de ces réseaux;

e) que la question de la cybersécurité est intersectorielle, et que l'environnement de la cybersécurité est complexe et diversifié, et compte de nombreuses parties prenantes différentes aux niveaux national, régional et mondial chargées d'identifier, d'examiner et de résoudre les problèmes relatifs à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

f) que les pertes considérables et toujours plus importantes que les utilisateurs de systèmes de télécommunication/TIC ont subies en raison du problème toujours plus préoccupant de la cybercriminalité alarment tous les pays développés et les pays en développement du monde, sans exception;

g) que le fait, notamment, que les infrastructures essentielles des télécommunications/TIC sont interconnectées au niveau mondial signifie qu'une sécurité insuffisante des infrastructures dans un pays pourrait entraîner une vulnérabilité et des risques accrus dans d'autres pays, d'où l'importance de la coopération;

h) que le nombre de cybermenaces et de cyberattaques et les méthodes correspondantes sont en augmentation, tout comme la dépendance à l'égard de l'Internet et d'autres réseaux qui sont essentiels pour accéder aux services et à l'information;

i) que les normes peuvent prendre en compte les aspects liés à la sécurité de l'Internet des objets (IoT) et des villes et des communautés intelligentes;

j) que, pour protéger les infrastructures mondiales de télécommunication/TIC contre les menaces et les risques liés à l'évolution de l'environnement de la cybersécurité, il est nécessaire de prendre des mesures concertées au niveau national, régional et international, pour la prévention, la préparation, l'intervention et le rétablissement en cas d'incidents liés à la cybersécurité;

k) les travaux déjà entrepris et en cours à l'UIT, notamment au sein de la Commission d'études 17 du Secteur de la normalisation des télécommunications de l'UIT (UIT-T) et de la Commission d'études 2 du Secteur du développement des télécommunications (UIT-D), y compris le rapport final de la Commission d'études 1 de l'UIT-D au titre de la Question 22/1, et dans le cadre du Plan d'action de Dubaï, adopté par la CMDT (Dubaï, 2014);

l) que l'UIT-T a un rôle à jouer dans le cadre de son mandat et de ses compétences en ce qui concerne le point *j)* du *considérant*,

considérant en outre

a) que la Recommandation UIT-T X.1205 établit une définition, une description des technologies et les principes de protection des réseaux;

b) que la Recommandation UIT-T X.805 établit un cadre systématique pour déterminer les failles de sécurité et que la Recommandation UIT-T X.1500 donne un modèle d'échange d'informations sur la cybersécurité (CYBEX) et porte sur les techniques qui pourraient être utilisées pour faciliter l'échange d'informations sur la cybersécurité;

c) que l'UIT-T et le Comité technique mixte pour les technologies de l'information (JTC 1) de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI), ainsi que plusieurs consortiums et entités de normalisation comme le World Wide Web consortium (W3C), l'Organization for Advancement of Structured Information Standards (OASIS), le Groupe de travail sur l'ingénierie Internet et l'Institut des ingénieurs en électricité et en électronique, notamment, disposent déjà d'un important volume de documents publiés et ont des travaux en cours qui se rapportent directement à ce sujet, dont il faut tenir compte;

d) l'importance des travaux en cours sur une architecture de référence de sécurité pour la gestion, tout au long de leur cycle de vie, des données sur les transactions de commerce électronique,

reconnaissant

a) le paragraphe du dispositif de la Résolution 130 (Rév. Dubaï, 2018) chargeant le Directeur du TSB d'intensifier les travaux menés au sein des Commissions d'études existantes de l'UIT-T;

b) que, par sa Résolution 71 (Rév. Dubaï, 2018), la Conférence de plénipotentiaires a adopté le Plan stratégique pour la période 2020-2023, qui comprend le But stratégique 3 (Durabilité: Gérer les nouveaux risques, enjeux et perspectives résultant de l'essor rapide des télécommunications/TIC), au titre duquel l'Union s'emploiera en priorité à renforcer la qualité, la fiabilité, la pérennité et la résilience des réseaux et des systèmes ainsi qu'à instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC;

c) que le Programme mondial cybersécurité (GCA) de l'UIT encourage la coopération internationale dans le but de proposer des stratégies en vue de l'élaboration de solutions propres à accroître la confiance et la sécurité dans l'utilisation des TIC, compte tenu des aspects liés à la sécurité à toutes les étapes du processus d'élaboration des normes;

d) les problèmes auxquels les États, en particulier ceux des pays en développement, sont confrontés pour instaurer la confiance et la sécurité dans l'utilisation des TIC,

reconnaissant en outre

a) que des cyberattaques, telles que le hameçonnage, le détournement d'adresses, le balayage/l'intrusion, les dénis de services distribués, le détournement de sites web, l'accès non autorisé, etc., apparaissent et ont de graves conséquences;

b) que des réseaux zombis sont utilisés pour distribuer des logiciels malveillants et mener des cyberattaques;

c) que l'origine des attaques est parfois difficile à identifier;

d) que les menaces très importantes qui pèsent sur la cybersécurité des logiciels et des matériels nécessiteront peut-être une gestion des failles en temps voulu et l'actualisation des logiciels ou des matériels en temps utile;

e) que la sécurisation des données est un élément essentiel de la cybersécurité dans la mesure où les données sont souvent la cible des cyberattaques;

f) que la cybersécurité est l'un des éléments qui permettent d'instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC,

notant

a) l'activité et l'intérêt marqués pour l'élaboration de normes et de Recommandations sur la sécurité des télécommunications/TIC au sein de la Commission d'études 17, qui est la commission d'études directrice pour la sécurité et la gestion d'identité, et au sein d'autres organismes de normalisation, y compris le Groupe de collaboration pour la normalisation mondiale (GSC);

b) qu'il est nécessaire d'harmoniser les stratégies et initiatives nationales, régionales et internationales dans toute la mesure du possible pour éviter les doubles emplois et optimaliser l'utilisation des ressources;

c) les efforts de collaboration importants déployés par et entre les gouvernements, le secteur privé, la société civile, les milieux techniques et universitaires, dans le cadre de leurs rôles et de leurs responsabilités, pour instaurer la confiance et la sécurité dans l'utilisation des TIC,

décide

1 de continuer d'accorder à ces travaux un rang de priorité élevé à l'UIT-T, conformément à ses compétences et à ses connaissances spécialisées, notamment en favorisant une compréhension commune, entre les gouvernements et les autres parties prenantes, de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC aux niveaux national, régional et international;

2 que toutes les commissions d'études de l'UIT-T doivent continuer à évaluer les Recommandations existantes et les nouvelles Recommandations en cours d'élaboration quant à la robustesse de leur conception et aux risques d'une exploitation par des acteurs malveillants, et tenir compte des nouveaux services et des nouvelles applications qui seront assurés par l'infrastructure mondiale des télécommunications/TIC (y compris, mais non exclusivement, par exemple, l'informatique en nuage et l'Internet des objets (IoT), qui sont fondés sur les réseaux de télécommunication/TIC), conformément à leurs mandats définis dans la Résolution 2 (Rév. Genève, 2022) de la présente Assemblée;

3 que l'UIT-T, dans le cadre de son mandat et de ses compétences, doit continuer à sensibiliser à la nécessité de renforcer et de défendre les systèmes d'information et de télécommunication contre les cybermenaces et les cyberactivités malveillantes, et à promouvoir la coopération entre les organisations internationales et régionales appropriées afin de renforcer l'échange d'informations techniques dans le domaine de la sécurité des réseaux d'information et de télécommunication;

4 que l'UIT-T devrait sensibiliser l'opinion à l'échelle mondiale en ce qui concerne la sécurité des TIC, en élaborant des Recommandations et des rapports techniques pour appuyer les procédures, les politiques techniques et les cadres normatifs en matière de cybersécurité;

5 que l'UIT-T devrait travailler en collaboration avec l'UIT-D, en particulier dans le contexte de 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);

6 que les commissions d'études concernées de l'UIT-T devront suivre le rythme de l'évolution des technologies nouvelles et émergentes, compte tenu de leurs mandats, pour élaborer des Recommandations, des Suppléments et des rapports techniques permettant de surmonter les difficultés que soulèvent ces technologies sur le plan de la sécurité;

7 que l'UIT-T doit poursuivre ses travaux sur l'élaboration et l'amélioration des termes et définitions relatifs à l'instauration de la confiance et de la sécurité dans l'utilisation des télécommunications/TIC, y compris en ce qui concerne le terme cybersécurité;

8 que l'adoption de procédures mondiales, cohérentes et interopérables pour échanger des informations sur les mesures prises en cas d'incident doit être encouragée;

9 que les commissions d'études de l'UIT-T doivent continuer d'assurer la liaison avec les organisations de normalisation et d'autres organismes travaillant dans ce domaine et encourager la participation d'experts aux activités de l'UIT dans le domaine de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

10 que les aspects liés à la sécurité devront être pris en considération tout au long du processus d'élaboration des normes de l'UIT-T;

11 que des réseaux et des services de télécommunication/TIC sécurisés, résilients et fiables devront être conçus et exploités afin de renforcer la confiance dans l'utilisation des TIC;

12 qu'il est nécessaire que la Commission d'études 17 procède à une analyse de la sécurité fondée sur la coopération et élabore des cadres de gestion des incidents;

13 que la résilience des réseaux et des systèmes TIC devra être considérée comme une priorité dans le développement des réseaux et des infrastructures,

charge la Commission d'études 17

1 d'encourager les études relatives à la cybersécurité, notamment en ce qui concerne la sécurité des nouveaux services et des nouvelles applications qui seront assurés par l'infrastructure mondiale des télécommunications/TIC;

2 d'aider le Directeur du TSB à tenir à jour la "Feuille de route relative aux normes de sécurité des TIC", qui devrait comprendre des sujets d'étude visant à faire progresser les travaux de normalisation relatifs à la sécurité, et de la communiquer, en sa qualité de commission d'études directrice pour la sécurité, aux commissions d'études concernées du Secteur des radiocommunications de l'UIT (UIT-R) et de l'UIT-D;

3 d'encourager les activités conjointes de coordination sur la sécurité entre toutes les commissions d'études et tous les groupes spécialisés concernés de l'UIT et les autres organisations de normalisation;

4 de collaborer étroitement avec toutes les autres commissions d'études de l'UIT-T, d'élaborer un plan d'action visant à examiner les Recommandations UIT-T existantes, en cours d'élaboration ou nouvelles, pour lutter contre les failles de sécurité et de continuer de faire rapport périodiquement sur la sécurité des télécommunications/TIC au Groupe consultatif de la normalisation des télécommunications;

5 de définir un ensemble commun ou général de capacités de sécurité pour chaque étape du cycle de vie des systèmes d'information, réseaux ou applications, afin que la sécurité au stade de la conception (capacités et fonctionnalités de sécurité prévues dès la conception) soit assurée pour les systèmes, réseaux ou applications dès le premier jour;

6 de concevoir un ou plusieurs cadres de référence pour l'architecture de sécurité, dotés d'éléments fonctionnels de sécurité qui pourraient être considérés comme les bases de la conception d'architectures de sécurité pour différents systèmes, réseaux ou applications, afin d'améliorer la qualité des Recommandations relatives à la sécurité,

charge le Directeur du Bureau de la normalisation des télécommunications

1 de continuer de tenir à jour, compte tenu de la base d'informations associée à la "Feuille de route pour la normalisation de la sécurité des TIC" et des efforts consacrés par l'UIT-D à la cybersécurité, et avec l'assistance d'autres organisations compétentes, un inventaire des initiatives et activités nationales, régionales et internationales pour promouvoir, dans toute la mesure possible, l'harmonisation à l'échelle mondiale des stratégies et méthodologies dans ce domaine d'une importance cruciale, notamment par l'élaboration d'approches communes dans le domaine de la cybersécurité;

2 de contribuer à l'élaboration des rapports annuels à l'intention du Conseil de l'UIT sur l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, comme indiqué dans la Résolution 130 (Rév. Dubaï, 2018);

3 de soumettre au Conseil un rapport sur l'état d'avancement des activités menées au titre de la "Feuille de route pour la normalisation de la sécurité des TIC";

4 de continuer de reconnaître le rôle que jouent d'autres organisations possédant une expérience et des compétences dans le domaine des normes de sécurité et d'assurer une coordination avec ces organisations, selon qu'il conviendra;

5 de continuer d'assurer la mise en œuvre et le suivi des activités pertinentes du SMSI relatives à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, en collaboration avec les autres Secteurs de l'UIT et en coopération avec les parties prenantes compétentes, en vue de partager des informations et des bonnes pratiques au plan mondial sur les initiatives en matière de cybersécurité nationales, régionales et internationales, et non discriminatoires;

6 de coopérer avec le Programme mondial cybersécurité (GCA) du Secrétaire général et d'autres projets de portée mondiale ou régionale dans le domaine de la cybersécurité, selon qu'il conviendra, pour encourager le renforcement des capacités et nouer des relations et des partenariats avec diverses organisations et initiatives régionales ou internationales liées à la cybersécurité selon qu'il conviendra, et d'inviter tous les États Membres, en particulier les pays en développement, à participer à ces activités et à assurer une coordination et une coopération entre ces différentes activités;

7 d'apporter un appui au Directeur du Bureau de développement des télécommunications (BDT), en vue d'aider les États Membres à mettre en place un cadre approprié entre les pays en développement, permettant de réagir rapidement à des incidents majeurs et de proposer un plan d'action destiné à renforcer leur protection, compte tenu des mécanismes et des partenariats, selon le cas;

8 d'appuyer les activités menées par les commissions d'études concernées de l'UIT-T pour ce qui est du renforcement et de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

9 de diffuser auprès de toutes les parties prenantes des informations sur la cybersécurité, en organisant des programmes de formation, des forums, des ateliers, des séminaires, etc., à l'intention des décideurs, des régulateurs, des opérateurs et d'autres parties prenantes, en particulier dans les pays en développement, afin d'accroître la sensibilisation et de recenser les besoins, en collaboration avec le Directeur du BDT,

invite les États Membres, les Membres de Secteur, les Associés et les établissements universitaires, selon qu'il conviendra

1 à travailler en étroite collaboration en vue de renforcer la coopération aux niveaux régional et international, en tenant compte de la Résolution 130 (Rév. Dubaï, 2018), en vue de renforcer la confiance et la sécurité dans l'utilisation des TIC, de façon à réduire les risques et les menaces;

2 à coopérer et à participer activement à la mise en œuvre de la présente Résolution et des mesures connexes;

3 à participer aux activités menées par les commissions d'études concernées de l'UIT-T pour élaborer des normes et des lignes directrices en matière de cybersécurité, afin d'instaurer la confiance et la sécurité dans l'utilisation des TIC;

4 à utiliser les Recommandations UIT-T pertinentes et leurs suppléments;

5 à continuer de contribuer aux travaux de la Commission d'études 17 concernant les méthodes de gestion des cyberrisques.