|  |  |  |
| --- | --- | --- |
|  | **世界电信标准化全会（WTSA-24）**2024年10月15-24日，新德里 |  |
|  |
|  |  |
| 全体会议 | 文件 37 (Add.10)-C |
|  | 2024年9月22日 |
|  | 原文：英文 |
|  |
| 亚太电信组织各成员国主管部门 |
| 第50号决议的拟议修改 |
|  |
|  |

|  |  |
| --- | --- |
| **摘要：** | 本文件包含修改WTSA第50号决议“网络安全”的提案。 |
| **联系人：** | 亚太电信组织秘书长Masanori Kondo先生 | 电子邮件：aptwtsa@apt.int |

引言

安全对于当今的电信/ICT基础设施而言变得越来越重要。ITU-T可以在为支持树立使用ICT的信心、信任以及提高安全性的关键技术，制定建议书方面发挥作用。利用ICT提供安全性和确保ICT的安全是两个主要研究领域。

应在系统/网络/应用的整个生命周期中考虑安全问题，否则将导致系统/网络/应用充满安全漏洞，需要大量修补工作。

鉴于安全标准化活动有助于防止恶意网络活动造成的破坏，因此应继续开展安全工作。此外，ITU-T的研究组，特别是第17研究组，应当研究已确定的新兴安全技术，如人工智能（AI）安全、元宇宙安全、零信任安全、软件供应链安全等。

本次修改的主要目的是澄清并加强第17研究组作为安全问题牵头研究组的作用。

提案

基于上述背景，亚太电信组织（APT）成员国主管部门建议WTSA-24考虑修订WTSA第50号决议“网络安全”。

MOD APT/37A10/1

第50号决议（2024年，新德里，修订版）

网络安全

（2004年，弗洛里亚诺波利斯；2008年，约翰内斯堡；2012年，迪拜；
2016年，哈马马特；2022年，日内瓦；2024年，新德里）

世界电信标准化全会（2024年，新德里），

忆及

*a)* 全权代表大会第130号决议（2022年，布加勒斯特，修订版）– 加强国际电联在树立使用信息通信技术（ICT）的信心和提高安全性方面的作用；

*b)* 全权代表大会第174号决议（2018年，迪拜，修订版）– 国际电联在防范非法使用ICT的风险的国际公共政策问题上的作用；

*c)* 全权代表大会第179号决议（2022年，布加勒斯特，修订版）– 国际电联在保护上网儿童方面的作用；

*d)* 全权代表大会第181号决议（2010年，瓜达拉哈拉）– 有关树立使用ICT的信心和提高安全性的定义和术语；

*e)* 有关建立打击非法滥用信息技术法律框架的联合国大会（UNGA）第55/63号和第56/121号决议；

*f)* 联大有关培育全球网络安全文化的第57/239号决议；

*g)* 有关培育全球网络安全文化及保护重要信息基础设施的UNGA第58/199号决议；

*h)* 联大有关数字时代隐私权的第68/167号决议申明，“人们在线下享有的各种权利，包括隐私权，在网上也须受到保护”；

*i)* 有关从外层空间遥感地球原则的UNGA第41/65号决议；

*j)* 联大关于全面审查信息社会世界高峰会议（WSIS）成果落实情况的大会高级别会议成果文件的第70/125号决议；

*k)* 世界电信发展大会（WTDC）有关加强在网络安全（包括抵制和打击垃圾信息）领域合作机制的第45号决议（2014年，迪拜，修订版）；

*l)* 世界电信标准化全会有关抵制和打击垃圾信息的第52号决议（2016年，哈马马特，修订版）；

*m)* 本届全会（2022年，日内瓦，修订版）有关重点鼓励发展中国家[[1]](#footnote-1)1建立国家计算机事件响应组的第58号决议；

*n)* 国际电联是《信息社会突尼斯议程》WSIS C5行动方面（树立使用ICT的信心并提高安全性）的主要推进方；

*o)* WSIS成果中与网络安全相关的条款，

考虑到

*a)* 电信/ICT基础设施和应用对于各种形式的社会和经济活动至关重要；

*b)* 传统的公共交换电话网由于其分层结构和内在的管理系统而具备一定程度的固有安全属性；

*c)* 如果在安全设计和管理方面没有足够当心，互联网协议（IP）网络会减少用户组件和网络组件之间的分离；

*d)* 因此，如果融合的传统网络和IP网络的安全设计和管理未得到充分重视，这些网络将更易受到入侵；

*e)* 网络安全是一个跨领域问题，网络安全格局既复杂又分散，涉及国家、区域和全球层面负责识别、审查和响应与树立使用ICT的信心、信任并提高其安全性相关的问题的许多不同利益攸关方；

*f)* 愈演愈烈的网络安全问题给电信/ICT系统用户带来显著且日益增多的损失，无一例外地给全世界所有发达国家和发展中国家敲响了警钟；

*g)* 以下事实：关键电信/ICT基础设施在全球层面的互连互通意味着，一国基础设施安全保障不充分会导致其它国家更易受害和面临更大风险，因此合作十分重要；

*h)* 我们愈来愈多地依赖于互联网及其他网络获取服务和信息的同时，网络威胁和网络攻击的数量和方法不断增多；

*i)* 标准可为物联网（IoT）和智慧城市与社区的安全提供支持，包括新技术和新兴技术的安全问题；

*j)* 为保护全球电信/ICT基础设施免受网络安全领域日益猖獗的威胁和挑战，需要协调国家、区域和国际层面的行动，以针对安全事件做好防范、准备、响应和恢复工作；

*k)* 国际电联按照WTDC（2014年，迪拜）通过的《迪拜行动计划》已经和正在开展的工作，其中包括国际电联电信标准化部门（ITU-T）第17研究组和国际电联电信发展部门（ITU-D）第2研究组已经和正在开展的工作以及ITU-D第1研究组第22/1-1号课题的最后报告；

*l)* ITU-T在其考虑到*j)*段的职责和能力范围内发挥作用，

进一步考虑到

*a)* ITU-T X.1205建议书为网络安全提供了定义、技术描述和网络保护原则；

*b)* ITU-T X.805建议书为识别安全漏洞提供了系统框架，ITU-T X.509建议书提供了公钥和属性证书框架，ITU-T X.1500建议书提供了网络安全信息交换（CYBEX）模型并探讨了可用来促进网络安全信息交流的技术；

*c)* ITU-T X.1060建议书为各组织建设和管理网络防御中心（CDC）提供了一个框架，以实现组织的安全，评估其实施安全服务的有效性并应对网络安全风险；

*d)* ITU-T和国际标准化组织（ISO）和国际电工技术委员会（IEC）的信息技术联合技术委员会（JTC 1）、以及诸如万维网联盟（W3C）、结构化信息标准促进组织（OASIS）、在线快速身份识别（FIDO）联盟、互联网工程任务组（IETF）和电子和电气工程师学会（IEEE）等若干联盟和标准实体已出版了大量资料并正在针对该议题开展大量的工作，这一点需得到考虑；

*e)* 在电子商务业务数据生命周期管理参考架构方面正在开展工作的重要性，

认识到

*a)* 责成电信标准化局（TSB）主任强化现有ITU-T各研究组内部工作的第130号决议（2022年，布加勒斯特，修订版）的执行段落；

*b)* 全权代表大会第71号决议（2022年，布加勒斯特，修订版）通过了《2024-2027年战略规划》，包括战略目标1（普遍互连互通：促成和推动对价格可承受、高质量且安全的电信/ICT的普遍接入），根据该决议，国际电联的目标是实现可普遍无障碍获取、价格可承受、高质量、可互操作和安全的电信/信息通信技术（ICT）基础设施、服务和应用；

*c)* 国际电联全球网络安全议程（GCA）促进旨在为增强ICT使用信心并提高安全性而寻找解决方案、制定战略的国际合作；

*d)* 各国，尤其是发展中国家，在树立使用ICT的信心和提高安全性方面所面对的挑战以及WTSA有关缩小发展中国家与发达国家之间标准化差距的第44号决议（2022年，日内瓦，修订版）；

*e)* 成员国，特别是发展中国家在为保护数据和个人可识别信息（PII）的技术与运营，建设可信且安全的电信/ICT基础设施及应用方面面临的挑战，

进一步认识到

*a)* 诸如网络钓鱼、垃圾信息、网址嫁接、扫描/入侵、分布式拒绝服务、高级持续威胁、网页篡改、非授权访问、恶意软件、数据下毒、欺骗等网络攻击形式不断出现并带来严重后果；

*b)* 僵尸网络正在用于传播僵尸恶意软件和进行网络攻击；

*c)* 攻击来源有时难以确定；

*d)* 软件和硬件所面对的重大网络安全威胁可能需要及时进行漏洞管理和及时进行软硬件更新以及适当的访问权限分配，从而防止终端设备攻击；

*e)* 勒索软件攻击继续增长；

*f)* 随着全球电信/ICT基础设施的不断演进，新技术的应用对电信/ICT安全以及数据和PII保护的技术和操作方面提出了新的挑战和更高要求，这可能会影响网络安全架构；

*g)* 管理网络安全威胁和保护电信/ICT的技术取得进步；

*h)* 安全能力发展的需要，包括管理安全风险和技术人员能力的发展；

*i)* 确保数据和大数据基础设施安全是网络安全的核心组成部分，因为数据往往是网络攻击的目标而大数据技术的广泛应用使该目标在当今的网络行为中无处不在；

*j)* 网络安全是树立使用电信/ICT的信心、信任和提高其安全性的一项关键因素；

*k)* 安全性在系统、网络、应用和数据的整个生命周期中占据重要地位；

*l)* 安全架构和框架很重要，可被视为各种系统、网络、应用和数据安全架构设计的基础，

注意到

*a)* ITU-T安全和身份管理问题的牵头研究组第17研究组及其它标准化机构（包括全球标准协作（GSC）组）在制定电信/ICT安全标准和建议书方面所开展的积极活动和各方对此的关注；

*b)* 应评估不断演进的网络基础设施和开放网络基础设施发展快速创新的互操作性和安全性问题；

*c)* 除其他网络威胁外，保护数据和PII的技术和操作方面已成为成员国面临的一个大问题；

*d)* 有必要尽量协调国家、区域和国际战略和举措，避免重复工作并优化资源的使用；

*e)* 各国政府、私营部门、民间团体、技术社团和学术界在各自职责范围内为树立使用ICT的信心、信任并提高安全性付出的巨大努力与协作，

做出决议

1 根据ITU-T的能力和专业特长，继续在部门内部高度重视此项工作，包括促进各国政府和其它利益攸关方在国家、区域和国际层面就树立使用ICT的信心和提高安全性达成共识；

2 根据其在本届全会第2号决议（2022年，日内瓦，修订版）规定的职权，所有ITU-T研究组均要在制定ITU-T标准的整个过程中考虑安全问题，并将继续评估现有的和不断演进的新建议书的设计与操作的稳健性以及被恶意行为方利用的可能，同时考虑到由全球电信/ICT基础设施支持的新的和新兴电信/ICT服务和技术（包括但不局限于，例如，基于电信/ICT网络的云计算和物联网）；

3 ITU-T通过制定支持网络安全程序的建议书和技术报告，继续在其职责和能力范围内提高全球对于ICT安全的认识，同时加强防范针对信息和通信系统的恶意网络活动和网络威胁的必要性的认识，从而进一步提升个人的安全能力，并继续促进适当的国际和区域性组织之间的合作，以便加强信息和电信网络安全领域技术信息的交流；

4 ITU-T应通过制定支持网络安全程序、技术策略和框架的建议书和技术报告来提高全球ICT领域的安全意识，以便更好地管理网络安全风险并保护信息和电信网络；

5 ITU-T应与ITU-D合作，特别是围绕ITU-D第3/2号课题 – 保障信息和通信网络的安全：培育网络安全文化的最佳实践；

6 ITU-T的相关研究组应根据其职权，跟上新兴技术的发展步伐，以便提醒第17研究组哪些领域可能需要新建议书、增补和技术报告，以应对与安全相关的挑战并处理有关保护数据和PII的技术和操作问题；

7 ITU‑T继续为制定和完善有关树立使用电信/ICT的信心、信任（包括通过保护数据和个人可识别信息）和提高安全性的术语和定义（包括“网络安全”）开展工作；

8 应促进建立全球、一致且可相互操作的进程，用于共享事件响应相关信息；

9 ITU-T各研究组继续与活跃在该领域的标准组织及其它机构联络，并鼓励专家参与国际电联有关树立使用ICT信心、信任和提高安全性方面的活动；

10 应开发和维护安全、可信和适应力强的电信/ICT网络和服务，以增强对使用电信/ICT的信心和信任；

11 第17研究组需要制定相互协作的网络安全分析和事件管理框架；

12 应将ICT网络和系统的韧性作为电信/ICT网络基础设施和应用建设工作的重点，

责成第17研究组

1 酌情制定建议书、增补和技术报告，推进关于网络安全的研究，其中包括新服务和新兴服务以及技术的数据与PII的安全技术和操作方面，以应对全球电信/ICT基础设施使用中的漏洞；

2 支持TSB主任维护ICT安全标准路线图，该路线图应包括推进安全相关标准化工作的工作项目，数据和PII保护的技术和操作问题，以及应包含建议书、术语和定义清单的安全纲要，并作为安全领导小组的任务与国际电联无线电通信部门（ITU-R）和ITU-D相关研究组共享；

3 在国际电联和其他标准制定组织的所有相关研究组和焦点组之间发起信心、信任和安全联合协调活动，包括有关保护上网儿童的联合协调活动及其差距分析；

4 与ITU-T的所有其他研究组密切协作，制定行动计划，评估现有的、演进的和新的ITU-T建议书，以应对不断演进的安全问题、威胁和漏洞，从而确保ICT网络在遭受网络攻击时的韧性，并继续向电信标准化顾问组提供关于电信/ICT安全的定期报告；

5 继续为信息系统/网络/应用/数据生命周期，包括发展个能安全能力的每个阶段定义一套总体/通用的安全能力，以便从第一天起就能实现系统/网络/应用的内在安全性（可通过设计来获得的安全能力和特征）；

6 继续设计一个或多个具有安全功能组件的安全框架或参考架构，包括考虑到不同类型系统之间的安全协作，这些组件可被视为各种系统/网络/应用的安全架构设计的基础，以提高安全相关建议书的质量并为新兴技术在全球电信/ICT基础设施中的潜在应用提供安全设计参考；

7 考虑ICT技术和业务的不断变化，定期审查网络安全建议书并修订现有建议书，以适应新的安全要求并应对新的网络安全威胁；

8 为评估和改进不断发展的电信/ICT基础设施的数据和PII保护的安全性，以及相关的技术和操作提供最佳做法，

责成电信标准化局主任

1 在有关电信/ICT安全标准路线图和ITU-D所开展的网络安全相关努力的基础上，在其它相关组织的帮助下，继续维持国家、区域和国际性举措及活动的清单并继续加以完善和更新，以便尽最大可能在世界范围内促进此重要领域战略和工作方法的统一，其中包括出台网络安全领域的通用方法；

2 如同第130号决议（2022年，布加勒斯特，修订版）所规定的，就树立使用电信/ICT的信心和提高安全性向国际电联理事会提交年度报告；

3 向国际电联理事会汇报电信/ICT安全标准路线图活动所取得的进展；

4 继续承认在安全、数据保护、PII标准领域具有经验和特长的其他组织发挥的作用并酌情与这些组织开展协调；

5 通过与国际电联其它部门协作并与相关利益攸关方合作，继续实施并跟进有关树立使用电信/ICT的信心和提高安全性的相关WSIS活动，从而分享有关国家、区域和国际以及全球有关网络安全的非歧视性举措的信息和最佳实践；

6 与秘书长提出的GCA及其它全球或区域性网络安全项目开展适当合作，酌情推进能力建设以及与各区域性和国际网络安全相关组织和举措发展良好关系和伙伴关系，并请所有成员国，特别是发展中国家参加这些活动，同时与这些不同活动进行协调与合作；

7 支持电信发展局（BDT）主任协助成员国在发展中国家之间建立适当的框架，以便在重大事件发生时做出快速响应，并提出行动计划，加大保护力度，同时酌情顾及各种机制和伙伴关系；

8 支持相关ITU-T研究组在增强和树立使用ICT的信心、信任和安全性相关方面所开展的活动；

9 通过组织培训项目、论坛、讲习班、研讨会等并酌情通过ITU-T建议书和实施导则，向所有利益攸关方，其中包括政策制定机构、监管机构、运营商和其他利益攸关方，特别是来自发展中国家的利益攸关方，传播与网络安全有关的信息并提高利益攸关方对此的认识；

10 考虑尽可能通过与ITU-T研究组各区域组会议同期举办讲习班，或与电信发展局主任和国际电联区域代表处协调和协作举办活动的方式提高认识，

请各成员国，部门成员、部门准成员和相关学术成员

1 在考虑到第130号决议（2022年，布加勒斯特，修订版）的情况下，通过密切协同加强区域和国际合作，从而增强使用电信/ICT的信心并提高安全性，以便缓解风险和应对威胁；

2 开展合作并积极参与本决议的实施工作和相关行动；

3 参加相关ITU-T研究组的活动，制定网络安全标准和导则，以树立使用ICT的信心、信任并提高安全性；

4 利用相关ITU-T建议书、技术报告及增补；

5 继续为第17研究组在网络风险和网络防护管理方法方面的工作做出贡献。

1. 1 这些国家包括最不发达国家、小岛屿发展中国家、内陆发展中国家和经济转型国家。 [↑](#footnote-ref-1)