世界电信标准化全会
新德里，2024年10月15-24日

第50号决议 – 网络安全

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电联的常设机构，负责研究技术、操作和资费问题，并发布有关上述内容的建议书，以便在世界范围内实现电信标准化。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的课题，再由各研究组制定有关这些课题的建议书。

世界电信标准化全会第1号决议规定了批准ITU-T建议书所须遵循的程序。

属ITU-T研究范围的一些信息技术领域的必要标准是与国际标准化组织（ISO）和国际电工技术委员会（IEC）协作制定的。

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) 全权代表大会关于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的第130号决议（2022年，布加勒斯特，修订版）；

b) 全权代表大会关于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的第174号决议（2014年，釜山，修订版）；

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

d) 全权代表大会关于树立使用ICT的信心和提高安全性的定义和术语的第181号决议（2010年，瓜达拉哈拉）；

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

f) 联大关于培育全球网络安全文化的第57/239号决议；

g) 联大关于培育全球网络安全文化及清点各国为保护重要信息基础设施开展的工作的第64/211号决议；

h) 联大关于从外层空间遥感地球原则的第41/65号决议；

i) 联大关于从国际安全的角度看待信息和电信领域发展并推进在信息通信技术使用方面负责人的国家行为的第76/19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）关于加强在网络安全（包括抵制和打击垃圾信息）领域合作机制的第45号决议（2022年，基加利，修订版）；

l) 本届全会关于抵制和打击垃圾信息的第52号决议（2024年，新德里，修订版）；

m) 本届全会关于重点鼓励发展中国家[1]建立和加强国家计算机事件响应团队（CIRT）的第58号决议（2024年，新德里，修订版）；

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电信/ICT的信心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，特别是关键电信/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它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) 标准可为所有电信/ICT的安全问题提供支持；

j) 确保新兴电信/ICT的安全对于网络空间的安全至关重要，因此，制定安全标准必不可少；

[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。

k) 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，以针对网络安全事件做好防范、准备、响应和恢复工作；

l) 国际电联按照WTDC（2022年，基加利）通过的《基加利行动计划》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；

m) 针对本决议*考虑到k)*，ITU-T在其职权和能力范围内发挥作用，

进一步考虑到

a) ITU-T X.1205建议书提供了定义、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.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）、以及若干联盟和标准制定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；

d) 将电信/ICT使用中的安全性视为一个持续和迭代过程的重要性，从一开始就内置于产品中并贯穿产品生命周期的每个阶段；

e) 一种迭代的、基于风险的方法结合了技术、流程和人为因素，是加强电信/ICT使用的安全性和弹性的关键 – 通过按需制定和应用网络安全做法，以应对不断演进的威胁和漏洞 – 同时支持创新和新兴电信/ICT，

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（普遍连接：促成和促进对价格可承受、高质量和安全的电信/ICT的普遍接入），根据该决议，国际电联将重点实现普遍可接入、价格可承受、高质量、可互操作且安全的电信/ICT基础设施、服务和应用；

c) 标准是国际电联全球网络安全议程（GCA）有关技术和程序措施的支柱2的关键组成部分，GCA旨在促进有关国际合作，提出解决方案战略，以增强使用电信/ICT的信心和安全性，并在标准制定过程的整个生命周期中考虑到安全方面的问题；

d) 各国，尤其是发展中国家，在树立使用电信/ICT的信心和提高安全性方面所面对的挑战，

进一步认识到

a) 诸如网络钓鱼、欺骗、扫描/入侵、分布式拒绝服务、网页篡改和非授权访问等网络攻击的范围和多样性日益增加，各种攻击不断出现、演变并产生重大影响；

b) 一系列载体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、及时进行软硬件更新和适当的访问权限分配以防止攻击；

e) 确保数据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；

f) 网络安全是树立使用电信/ICT的信心和提高其安全性的根本要素；

g) 世界范围内对电信/ICT的访问日益增加、特别是互联网，以及未成年人使用互联网，

注意到

a) ITU-T安全和身份管理问题的领导研究组ITU-T第17研究组及其它标准化机构（包括全球标准协作组）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) 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；

c) 除其它网络威胁外，网络安全中的数据和个人身份信息（PII）保护方面已成为各成员国面临的一个重大问题；

d) 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电信/ICT的信心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电信/ICT的信心和提高安全性达成共识；

2 ITU-T研究组将继续依据本届全会第2号决议（2024年，新德里，修订版）规定的职责范围，评估现有的和不断演进的ITU-T建议书，将有关安全问题提交ITU-T第17研究组审议，包括其设计和操作的稳健性以及被恶意行为方利用的可能性等，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；

3 ITU-T继续在其职权和能力范围内，通过制定建议书和技术报告，提高全球对于电信/ICT安全的认识，支持关于保护电信/ICT免受网络威胁和恶意网络活动影响的重要性的网络安全程序、技术政策和标准框架，以加强组织的人员安全能力建设，并继续促进适当的国际和区域性组织之间的合作，以加强电信/ICT安全领域技术信息的交流，目的是管理网络安全风险并保护电信/ICT；

4 ITU-T在制定用于促进电信/ICT相关新兴技术的网络安全的输出成果时，应考虑到用户和开发人员的需求；

5 ITU-T应考虑能力建设的重要性，以促进采用支持网络安全的标准，特别是针对（但不限于）发展中国家；

6 ITU-T应在这些方面与ITU-D进行协调与合作，包括ITU-D第3/2号研究课题（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），以及电信发展局（BDT）的能力建设工作范畴；

7 ITU-T的相关研究组应根据其职权，跟上新兴通信/ICT服务和技术的发展步伐，以便提醒ITU-T第17研究组哪些领域可能需要新的ITU-T建议书、增补和技术报告，以应对与网络安全相关的挑战以及数据和PII的保护问题；

8 ITU-T继续为制定和完善有关树立使用电信/ICT的信心和提高安全性的术语和定义（包括术语“网络安全”）开展工作；

9 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；

10 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电信/ICT信心和提高安全性方面的活动；

11 在ITU-T标准制定整个进程中均应考虑安全问题；

12 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；

13 电信/ICT网络和系统的网络弹性应被视为电信/ICT网络基础设施建设和应用开发的优先事项，

责成国际电联电信标准化部门第17研究组

1 酌情制定ITU-T建议书、增补和技术报告，推进关于网络安全的研究，包括其对新兴电信/ICT服务和技术的数据与PII保护方面，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网络安全及其数据和PII保护相关标准化工作的工作项目，以及应包含ITU-T建议书、术语和定义清单的安全纲要，并作为ITU-T安全方面的领导研究组的任务与国际电联无线电通信部门和ITU-D相关研究组共享；

3 酌情领导国际电联所有相关研究组和其它标准制定组织之间关于信任和安全的联合协调活动；

4 与ITU-T的所有其它研究组密切协作，制定一项行动计划，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威胁和漏洞，增进电信/ICT网络在遭受网络攻击时的弹性，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/服务产品的开发生命周期的每个阶段，包括需求、设计、实施、验证、发布与维护（包括组织人员之间的安全能力开发），定义一套总体/通用的安全能力，以便从一开始就能实现系统/网络/应用的安全性（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互操作性，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ITU-T建议书的质量并为全球电信/ICT基础设施中的潜在应用提供安全设计参考；

7 继续开发并支持相互协作的网络安全分析和事件管理工具，以支持CIRT的工作，特别是在发展中国家；

8 考虑满足既定要求，制定技术标准，以支持加强未成年人网络安全的工作；

9 考虑电信/ICT的持续变化，定期审查并修订网络安全相关现有ITU-T建议书，以适应新的安全要求，应对新的网络安全威胁；

10 为不断发展的电信/ICT基础设施提供评估和改进网络安全（包括其数据和PII保护问题）的最佳实践；

11 从网络安全角度对新兴电信/ICT的影响进行评估，确定差距并就安全采用和使用的策略提出建议，

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 继续承认在网络安全标准领域（特别是数据和PII保护方面），具有经验和特长的其它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其它组织和所有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BDT主任监督ITU-T建议书和可能的其它工具的制定工作，使成员国，特别是发展中国家能够在重大事件发生时预先做出快速响应，并酌情根据要求帮助这些机构利用适当框架提出行动计划，加大保护力度，同时顾及各种机制和伙伴关系；

8 支持ITU-T第17研究组在增强和树立使用电信/ICT的信心和安全性相关方面所开展的活动，并使该项工作与ITU-D研究组的工作和相关项目活动协调一致；

9 酌情为政策制定者、监管机构、运营商和其它利益攸关方，特别是来自发展中国家的利益攸关方，组织关于ITU-T建议书和实施指南的培训项目、论坛、讲习班、研讨会等，向所有利益攸关方传播与网络安全有关的信息，提高其对网络安全的认识，并与BDT主任协作，以提高认识并确定需求；

10 与区域性电信组织合作，更有效地向更广泛的受众传播知识和专长；

11 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，或酌情与BDT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和支持，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，以树立使用电信/ICT的信心并提高安全性；

4 利用相关ITU-T建议书、技术报告及增补；

5 继续在国际电联职权范围，为ITU-T第17研究组在网络安全风险和网络防护管理方法方面的工作做出贡献；

6 继续参与鼓励女性积极参与ITU-T网络安全相关活动和发挥领导作用的各项举措；

7 对其管辖范围内新的和新兴电信/ICT采取和支持实施网络安全措施，鼓励为所有用户提供安全且有弹性的环境。