

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

世界电信标准化全会

日内瓦，2022年3月1-9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。

© ITU 2022年

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

第50号决议（2022年，日内瓦，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）

世界电信标准化全会（2022年，日内瓦），

忆及

- a) 全权代表大会第130号决议（2018年，迪拜，修订版）– 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（2018年，迪拜，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) 有关培育全球网络安全文化的UNGA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) 有关从外层空间遥感地球原则的UNGA第41/65号决议；
- i) 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UNGA第70/125号决议；
- j) 有关加强在网络安全（包括抵制和打击垃圾信息）领域合作机制的世界电信发展大会（WTDC）第45号决议（2014年，迪拜，修订版）；
- k) 有关抵制和打击垃圾信息的世界电信标准化全会第52号决议（2016年，哈马马特，修订版）；
- l) 有关重点鼓励发展中国家¹建立国家计算机事件响应组的本届全会第58号决议（2022年，日内瓦，修订版）；
- m) 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；
- n) WSIS成果中与网络安全相关的条款，

¹ 其中包括最不发达国家、小岛屿发展中国家、内陆发展中国家和经济转型国家。

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；
- 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）、以及诸如万维网联盟（W3C）、结构化信息标准促进组织（OASIS）、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；

d) 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（2018年，迪拜，修订版）的执行段落；

b) 全权代表大会第71号决议（2018年，迪拜，修订版）通过了《2020-2023年战略规划》，包括战略目标3（可持续性：管理电信/ICT快速增长带来的新风险、挑战和机遇），根据该决议，国际电联将重点加强网络和质量、可靠性、可持续性和复原力，以及树立使用电信/ICT的信心并提高安全性；

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，

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、非授权访问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进行及时漏洞管理和及时进行软硬件更新；

e) 确保数据安全性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一项因素，

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) 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) 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 所有ITU-T研究组均将继续依据本届全会第2号决议（2022年，日内瓦，修订版）规定的职责范围，评估现有的和不断演进的新建议书的设计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基础设施支持的新服务和新应用（包括但不限于，例如，基于电信/ICT网络的云计算和物联网）；
- 3 ITU-T继续在其职责和能力范围内提高人们对于加强和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，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、技术策略和标准框架的建议书和技术报告来提高全球ICT领域的安全意识；
- 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，以便制定建议书、增补和技术报告，帮助克服与安全相关的挑战；
- 7 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；
- 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信心和提高安全性方面的活动；
- 10 在ITU-T标准制定整个进程中均应考虑安全问题；
- 11 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ICT的信心；
- 12 第17研究组需要制定相互协作的安全分析和事件管理框架；
- 13 应将ICT网络和系统的韧性作为网络和基础设施建设工作的重点，

责成第17研究组

- 1 推进关于网络安全的研究，其中包括全球电信/ICT基础设施支持的新服务和新兴应用的安全；
- 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，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 发起安全联合协调活动，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安全联合协调活动；
- 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，以应对安全漏洞，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 为信息系统/网络/应用/数据生命周期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 设计一个或多个具有安全功能组件的安全架构参考框架，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，

责成电信标准化局主任

- 1 在有关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（2018年，迪拜，修订版）所规定的，就树立使用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ICT安全标准路线图活动所取得的进展；
- 4 继续承认在安全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的信心和安全性相关方面所开展的活动；

9 与BDT主任协作，通过组织培训项目、论坛、讲习班、研讨会等，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，以提高认识并确定需求，

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（2018年，迪拜，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ICT的信心并提高安全性，以便缓解风险和威胁；

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的信心并提高安全性；

4 利用相关ITU-T建议书及增补；

5 继续为第17研究组在网络风险管理方法方面的工作做出贡献。