|  |  |  |
| --- | --- | --- |
| itu_logo | **世界电信标准化全会****（WTSA-16）2016年10月25日-11月3日，哈马马特** | Title: CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| **全体会议** | **文件 44(Add.13)-C** |
|  | **2016年10月3日** |
|  | **原文：英文** |
|  |
| 亚太电信组织各成员国主管部门 |
| 拟议修改WTSA-12第50号决议 – 网络安全 |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **摘要:** | 在此文件中，亚太电信组织各成员国主管部门建议修改第50号决议。 |  |

引言

自WTSA-12以来，ITU-T在网络安全相关活动中取得了长足进步。网络安全威胁方式有所变化，因此有必要在下一研究期（2017-2020年）加强这方面的活动并研究不断涌现的安全问题。

有必要更新第50号决议，以便体现自2012年以来发生的变化和进展。

提案

APT成员国主管部门建议按照附件修正有关网络安全的第50号决议。

MOD APT/44A13/1

第50号决议（2016年，哈马马特，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）

世界电信标准化全会（2016年，哈马马特），

忆及

*a)* 全权代表大会第130号决议（2014年，釜山，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；

*c)* 联合国大会有关创造全球网络安全文化和保护基本信息基础设施的相关决议，其中包括第57/239、58/199和64/211号决议；

*d)* 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）领域合作的机制的第45号决议（2014年，迪拜）；

*e)* 本届全会有关抵制和打击垃圾信息的第52号决议（2012年，迪拜，修订版）；

*f)* 本届全会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（2012年，迪拜，修订版），

考虑到

*a)* ICT基础设施及其应用对于包括第四次工业革命（FIR）和物联网等新生事物在内的各种形式的社会和经济活动至关重要；

*b)* 网络威胁和网络攻击的数量不断增加，同时我们也愈来愈多地依赖互联网和其他网络获取服务和信息；

*c)* 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确定、审查树立使用ICT的信心并提高其安全性相关问题并对此做出响应的许多不同利益攸关方；

*d)* 国际电联电信标准化部门（ITU-T）已通过约300项与树立使用ICT的信心和提高安全性相关的标准；

*e)* 国际电联电信发展部门（ITU-D）关于第21-1/1号课题（保证信息通信网络的安全：培育网络安全文化的最佳做法）的最后报告；

*f)* 与影响互联网用户安全的物联网（IoT）和智慧城市与社区（SCC）应用相关的安全问题标准化工作；

*g)* 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、区域和国际行动，以便针对安全事件做好防范、准备、响应和恢复工作，ITU-T凭借其职责和能力在此方面大有作为；

*h)* 在蓬勃发展的全球经济中，由电子和计算设备供应构成的厂商生态系统在很大程度上有具有分散性，严重关系到网络安全威胁的管理；

*i*) 国际电联（包括ITU-T第17研究组、ITU-D第2研究组）按照世界电信发展大会迪拜行动计划（2014年，迪拜）已经和正在开展的工作；

*j)* 国际电联电信标准化部门（ITU-T）在其有关树立使用ICT的信心和提高安全性方面和考虑到*g)*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建议书为识别安全隐患提供了系统框架，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方便网络安全信息交流的技术；

*c)* ITU-T和国际标准化组织（ISO）/国际电工技术委员会（IEC）的信息技术联合技术委员会（JTC 1）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，

意识到

*a)* 国际电联及其他国际组织通过开展各种活动，正在审议与树立使用ICT的信心和提高安全性有关的问题，包括稳定性和打击垃圾信息、恶意软件、假冒设备等的措施，并保护个人可识别信息；

*b)* ITU第17研究组、ITU-D第1和第2研究组及国际电联其他相关研究组根据第50和第52号决议（2012年，迪拜，修订版）以及第45号决议和第69号决议（2014年，迪拜，修订版），继续研究有关信息通信网络安全的技术手段；

*c)* ITU-T亦在帮助发展中国家树立使用信息通信技术的信心并提高安全性，支持其成立CIRT（包括负责政府与政府之间合作的CIRT），且在所有相关组织间进行协调亦很重要，

认识到

*a)* 信息社会世界高峰会议（WSIS）在相关成果中将国际电联确定为C5行动方面（树立使用ICT的信心并提高安全性）的推进方和协调方，联合国大会高级别会议于2015年12月对在WSIS成果落实的全面审查对此予以确认；

*b)* 网络安全是树立使用电信/ICT的信心并提高安全性的要素之一；

*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，

进一步认识到

*a)* 网络安全事件数量庞大、种类繁多（包括但不局限于社交工程攻击、高级持续性威胁等）并继续随着时间的推移而变化，而且，有时难以辨别网络安全攻击的来源；

*b)* 网络安全威胁源于严重关乎国家基础设施，甚至危及人生安全的代码、软件和硬件缺陷，需要及时进行缺陷管理并在必要时发布软件/硬件补丁；

*c)* 数据日益成为信息和电信网络的关键资产，也是网络安全攻击的主要目标，

注意到

*a)* 有关安全和身份管理问题的牵头研究组第17研究组和其它标准化机构（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)* 有必要在尽量大的范围内协调国家、区域和国际战略，避免重复工作并优化资源的使用；

*c)* ITU-D有责任帮助发展中国家开展网络安全能力建设活动以便做到因地制宜并满足各国的需求；

*d)* 在研究安全问题的各个组织之间开展合作和协作，可以推进工作进展并为培育和保护网络安全文化做出贡献，

做出决议

1 根据国际电联的能力和专业特长，继续在ITU-T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研究组继续针对现有、不断演进和新的建议书的设计稳健性以及被恶意行为方利用的可能，尤其是由全球电信/ICT基础设施支持的新的服务和应用基础设施（如包括但不局限于基于电信/ICT（如IMT-2020）的大数据分析、云计算、智慧城市、数字金融服务、移动边缘计算、量子计算、第5代移动网络、电子卫生、物联网、软件定义网络、网络功能虚拟化、工业互联网、智慧电网和智能交通系统开展评估并酌情向TSAG做出报告；

3 ITU-T应着手就与大数据安全相关的标准开展研究，侧重于数据保护和整个数据生命周期的保护以及数据安全评估标准和做法；

4 ITU-T应继续在其职责和能力范围内提高人们对于防止信息和通信系统受到网络攻击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；

5 ITU-T应与ITU-D密切合作，特别是围绕第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做法；

6 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；

7 应促进建立全球一致的、可互操作程序，用于共享有关事件响应的信息；

8 第17研究组与ITU-T所有其它研究组密切协同，制订一份行动计划以评定ITU-T有关安全薄弱环节的现有、演进中和新的建议书并应继续定期向电信标准化顾问组（TSAG）提供有关电信/ICT安全的报告；

9 ITU-T各研究组应继续与活跃在该领域的标准制定组织和其它机构联络，这些机构包括ISO/IEC信息技术联合技术委员会（JTC1）、经济合作和发展组织（OECD）、亚太经济合作组织电信和信息工作组（APEC-TEL）和互联网工程任务组（IETF）；

10 ITU-T各研究组将处理涉及设备提供商、软件提供商、服务提供商和最终用户的网络安全威胁管理问题；确保网络威胁管理行之有效并明确规定多方在缓解网络安全威胁中的责任；

11 第17研究组继续就第130号决议（2010年，瓜达拉哈拉，修订版）提出的ICT网络安全技术手段，尤其是相关问题开展工作，

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，尽可能全面地清点国家、区域和国际性举措及活动，以便在世界范围内促进此重要领域战略和工作方法的统一；

2 按照第130号决议（2014年，釜山，修订版）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 按照第130号决议（2014年，釜山，修订版）的规定围绕“ICT安全标准路线图”向国际电联理事会提交年度活动进展报告并评估目前工作和未来工作计划、方向或路线图的有效性；

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，继续实施并跟进信息社会世界峰会有关树立使用ICT的信心和提高安全性的相关活动，从而共享有关国家、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；

6 就有关网络安全的任何事项，尤其是第45号决议（2014年，迪拜，修改版）的实施，与电信发展局合作；

7 继续按照《全球网络安全议程》（GCA）并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；

8 鼓励在网络安全管理框架和原则的制定中与ITU-D开展合作，以便为成员国作出榜样；

9 依据普遍采用的做法、导则和建议，确定并记录成员国可选择用于提高应对网络威胁与攻击的能力，强化旨在树立使用ICT的信心并提高安全性的国际合作的可行步骤，以便增强全球ICT使用的安全性，同时亦顾及国际电联的《全球网络安全议程》（GCA）和可用财务资源的限制；

请各成员国，部门成员、部门准成员和相关学术成员

1 在考虑到全权代表大会第130号决议（2014年，釜山，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 共同努力，制定网络安全标准和指导原则以防止受到网络攻击；

4 利用相关ITU-T建议书，特别是ITU-T X系列建议书及增补。

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

1. 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。 [↑](#footnote-ref-1)