|  |  |  |  |
| --- | --- | --- | --- |
|  | **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.13)-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58号决议的拟议修改 | | | |
|  | | | |
|  | | | |

|  |  |  |
| --- | --- | --- |
| **摘要：** | 随着针对全球电信/ICT基础设施的网络威胁和攻击不断增加和演进，有必要在所有国家都做出适当程度的网络安全应急响应，计算机事件响应团队（CIRT）的作用变得比以往任何时候都更加重要。本文件提议对WTSA第58号决议进行一些修正。 | |
| **联系人：** | 亚太电信组织秘书长 Masanori Kondo先生 | 电子邮件： [aptwtsa@apt.int](mailto:aptwtsa@apt.int) |

引言

随着电信/ICT基础设施业务和技术的技术演进，网络威胁和攻击也在不断演进。网络威胁不仅可以通过计算机传播，还可以通过移动设备、服务器、网络甚至运营技术传播。同时，网络攻击越来越多地针对关键的电信/ICT基础设施和重要数据。

随着网络威胁和攻击之数量、严重性和复杂性的迅速增长，安全继续成为一个全球关切的问题，有必要帮助各国，特别是发展中国家，保护其电信/ICT网络免受网络威胁和攻击。计算机事件响应团队（CIRT）的作用对以适当的方式对事件做出响应而言至关重要，应予加强。然而，在许多国家，特别是发展中国家，应对网络安全事件的准备就绪水平仍然很低。因此，有必要在国家层面建立CIRT，并在政府和其他利益攸关方之间就网络安全事件响应加强信息共享和协作。起草建议书和增补有助于创建CIRT并推广CIRT运作框架，例如，关于“创建和运营网络防御中心的框架”的ITU-T X.1060建议书就如何确保组织准备好网络防御能力以及有效的安全业务（包括网络安全事件响应）提供了指导原则。

WTSA-20更新了第58号决议，它提出迫切需要在所有国家建立国家CIRT，重点是缩小发展中国家与发达国家之间的网络安全差距。本决议旨在反映更新后的全权代表大会第130号决议（2022年，布加勒斯特，修订版）有关CIRT的推广和运作框架。

修改第58号决议的主要目的是帮助提高全球网络安全应急响应水平。

提案

APT成员国主管部门提议修订WTSA第58号决议。

MOD APT/37A13/1

第58号决议（2024年，新德里，修订版）

鼓励建立国家计算机事件响应团队，尤其是在发展中国家[[1]](#footnote-1)1

（2008年，约翰内斯堡；2012年，迪拜；2022年，日内瓦；2024年，新德里）

世界电信标准化全会（2024年，新德里），

考虑到

*a)* 全权代表大会有关加强国际电联在树立使用信息通信技术（ICT）的信心并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)* 全权代表大会第123号决议（2018年，迪拜，修订版）责成秘书长和三个局的主任密切合作，开展帮助缩小发展中国家与发达国家之间标准化工作差距的举措，

进一步考虑到

ITU-T X.1060建议书为创建和运行网络防御中心提供了一个框架，

认识到

*a)* 世界电信标准化全会第54号决议（2016年，哈马马特，修订版）框架内采取的区域性做法取得了令人高度满意的结果；

*b)* ITU-T根据其能力和专业特长，在其内部高度优先开展的有关第50号决议（2024年，新德里，修订版）的工作，包括促进各国政府和其他利益攸关方在国家、区域和国际层面就树立使用ICT的信心并提高安全性达成共识；

*c)* 发展中国家数字化转型的水平和对信息通信技术（ICT）的依赖程度日益提高；

*d)* 网络威胁和对电信/ICT基础设施攻击之数量、严重性和复杂性的迅速增长，以及管理网络防御基础设施、工具、人员和安全业务的复杂性；

*e)* 随着电信/ICT基础设施业务和技术的不断演进，网络威胁和攻击也在不断演进，网络威胁不仅可以通过计算机传播，还可以通过移动设备、服务器、网络甚至运行技术传播，同时，网络攻击越来越针对关键的电信/ICT基础设施和重要数据；

*f)* 国际电联电信发展部门（ITU-D）第1研究组原第22/1号课题和ITU-D第2研究组现第3/2号课题在该议题方面开展的工作，

注意到

*a)* 许多国家，尤其是发展中国家的网络安全应急准备水平依然很低；

*b)* 高度互连的ICT网络可能会受到来自疏于防范国家和区域的网络的攻击；

*c)* 所有国家均达到适当水平的网络安全应急准备至关重要；

*d)* 有必要建立国家层面的CIRT（计算机事件响应团队/网络安全事件响应团队/网络事件响应团队），而且在国家和区域内部和之间与现有的CIRT进行协调十分重要；

e) CIRT（计算机事件响应团队/网络安全事件响应团队/网络事件响应团队）有几个同义词：CERT（计算机应急响应团队）、计算机安全事件响应团队（CSIRT）、CIRC（计算机事件响应中心）或CDC（网络防御中心）；

*f)* 国际电联电信标准化部门（ITU-T）第17研究组输出文件中包含的该研究组尤其为发展中国家在国家CIRT领域开展的工作，以及各团队之间的合作，例如，关于“创建和运行网络防御中心的框架”的ITU-T X.1060建议书，以确保各组织以具有有效的安全服务的网络防御能力做好准备，从而防止网络攻击和安全威胁，

铭记

发展中国家运行良好的CIRT将加强这些国家对全球网络安全应急响应活动的参与并有助于实现全球ICT基础设施的有效和安全运转，

做出决议

1 支持在需要、但目前没有创建CIRT的国际电联成员国创建国家CIRT，在设立CIRT的成员国中推广相关CIRT运行框架（如适用）；

2 支持电信发展局（BDT）主任通过提供技术建议书和增补，推广建立CIRT的国家、区域和国际最佳做法，

责成第17研究组

1 继续起草有助于创建CIRT和推广CIRT运行框架的建议书和增补；

2 促进对网络防御中心相关框架的研究，以期通过针对全球电信/ICT基础设施的有效检测以及响应流程和程序、安全业务技术和评估指标，最大限度地降低网络风险并减少安全漏洞的影响；

3 支持电信标准化局主任为CDC提出的、有助于缩小发展中国家与发达国家之间标准化工作差距的举措，其中应包括CDC安全相关标准化工作的工作项目，并作为安全牵头小组的使命与ITU-D相关组分享；

4 促进国际电联所有相关研究组和焦点组和其他SDO之间关于CDC的联合协调活动；

5 继续定义一系列有关CDC的能力，包括基础设施、组织，并通过设计实现电信/ICT基础设施CDC的安全性（即从设计阶段就可获得的安全能力和特征），

责成电信标准化局主任与电信发展局主任协作

1 按照国际电联工具包，确定建立和推广CIRT有关运行框架的最佳做法；

2 确定需要建立国家CIRT的国家，尤其是在发展中国家，并鼓励建立此类团队；

3 与国际专家和机构协作，建立国家CIRT；

4 在现有预算资源范围内酌情提供支持；

5 在适当框架范围内推进国家CIRT之间的协作，如开展能力建设和信息交流；

6 采取必要行动，推动本决议的实施，

请成员国

1 高度优先考虑创建国家CIRT；

2 与其它成员国和部门成员开展协作，

请成员国和部门成员

在此方面与ITU-T和ITU-D密切合作。

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)