联合国 A/C.2/64/L.8

大 会

Distr.: Limited
22 October 2009
Chinese
Original: English

第六十四届会议

第二委员会

议程项目 55(c)

全球化和相互依存：科学和技术促进发展

澳大利亚、加拿大、以色列、日本、马绍尔群岛和美利坚合众国：决议草案

创造全球网络安全文化以及评估各国保护重要信息基础设施的努力

大会，

回顾其 2000 年 12 月 4 日和 2001 年 12 月 19 日关于打击非法滥用信息技术的第 55/63 号和第 56/121 号、2002 年 12 月 20 日关于创造全球网络安全文化的第 57/239 号和 2003 年 12 月 23 日关于创造全球网络安全文化及保护重要信息基础设施的第 58/199 号决议，

又回顾关于从国际安全角度看信息和电信领域发展的 1998 年 12 月 4 日第 53/70 号、1999 年 12 月 1 日第 54/49 号、2000 年 11 月 20 日第 55/28 号、2001 年 11 月 29 日第 56/19 号、2002 年 11 月 22 日第 57/53 号、2003 年 12 月 8 日第 58/32 号、2004 年 12 月 3 日第 59/61 号、2005 年 12 月 8 日第 60/45 号、2006 年 12 月 6 日第 61/54 号、2007 年 12 月 5 日第 62/17 号和 2008 年 12 月 2 日第 63/37 号决议，

还回顾信息社会世界首脑会议 2003 年 12 月 10 日至 12 日日内瓦会议(第一期会议)和 2005 年 11 月 16 日至 18 日突尼斯会议(第二期会议)的成果，[1] 各国在成果中确认，言论自由和信息、思想和知识的自由流通对于今天的信息社会至关重要且有益于发展，而且，使各方有信心和安全地使用信息和通信技术是信息社会的两大支柱，因此，必须鼓励、推动、发展和大力落实全球网络安全文化，

[1] 见 A/C.2/59/3 和 A/60/687。

*认识到*网络信息技术对于日常生活、商业、提供物资和服务、研究、创新和创业等活动的多数重要功能以及对于个人、组织和政府之间的信息自由流通日益重要，不可或缺，

*注意到*政府、工商企业、民间社会和个人日益依赖全球信息基础设施网络，而且这种依赖将与日俱增，

*又注意到*各国在获取和利用信息技术方面存在的差距可能减损其社会经济繁荣程度，并特别注意到欠发达国家在网络安全最佳做法和培训方面的需要，

*表示关切*重要信息基础设施的可靠运作和网路所载信息的完整性正受到日益复杂和严重的威胁，这种威胁影响到家庭、国家和国际福祉，

*确认*重要信息基础设施安全是各国政府必须负责系统地处理的问题，是其必须与各有关利益攸关方协调，在国家一级发挥领导作用的领域，各有关利益攸关方也必须意识到有关风险，以适合各自角色的方式采取预防措施，作出有效应对，

*认识到*应该在国家、区域和国际各级分享信息和进行协作，以支持各国的努力，有效地处理这些威胁日益明显的跨国性质，

*注意到*有关区域组织和国际组织已开展的加强网络安全工作，特别是这些组织鼓励各国进行努力，并且促进了国际合作，

*又注意到*国际电信联盟 2009 年题为“确保信息和通信网络安全：发展网络安全文化的最佳做法”的报告，其中重点讨论了在言论自由、信息自由流通和适当法律程序基础上处理网络安全的全面国家做法，

*认识到*定期评估各国保护重要信息基础设施的努力有助于这些努力，

1. *邀请*各会员国自愿提供其网络安全和保护重要信息基础设施重要举措简介，以彰显各国的成就和最佳做法，指出经验教训和需要进一步采取行动的领域；

2. *提供*所附各会员国在这方面可使用的国家网络安全自我评估表，作为在审查国家网络安全和保护重要信息基础设施努力时可酌情利用的工具；

3. *邀请*已制定网络安全和保护重要信息基础设施战略的所有会员国最迟于大会第六十五届会议期间向秘书长介绍最佳做法和措施，以协助其他会员国、区域和国际组织、私营部门和民间社会各利益攸关方努力创造全球网络安全文化。

附件

国家保护重要信息基础设施努力的自我评估工具

评估网络安全需要和战略

1. 评价信息和通信技术在贵国国民经济、国家安全、重要基础设施(如运输、水和食品供应、大众保健、能源、金融、应急服务)以及民间社会中的作用。

2. 确定必须管理的贵国经济、国家安全、重要基础设施和民间社会在网络安全和重要信息基础设施保护方面所面临的风险。

3. 了解已投入使用网络的弱点、每个部门目前所面临威胁的相对程度和现行管理计划；说明经济环境、国家安全优先事项以及民间社会需求等因素的变化如何影响这些评估。

4. 确定贵国网络安全和保护重要信息基础设施战略的目标，叙述该战略的目标、目前的实施程度、衡量进展情况的措施、该战略与其他国家政策目标的关系以及该战略在各区域和国际举措中的作用。

利益攸关方的角色和责任

5. 确定在网络安全和保护重要信息基础设施方面可以发挥作用的关键利益攸关方，并叙述每个利益攸关方在制定有关政策和开展有关行动方面的作用，包括：

- 国家政府各部委或机构，并指出主要联系人和各部委或机构的责任；
- 其他(地方和地区)政府参与方；
- 非政府行动者，包括工商界、民间社会和学术界；
- 公民，并指出因特网普通用户是否可获得避免网上威胁的基本训练，是否已开展关于网络安全的国家提高认识运动。

政策过程和参与

6. 确认政府和各行业在制定网络安全和保护重要信息基础设施政策和开展这项活动方面现有的正式和非正式协作渠道；确定参与方、各方的作用和目标、获取和处理投入的方法以及这些投入是否足以实现相关的网络安全和保护重要信息基础设施目标。

7. 确认可能需要的其他论坛或结构，以整合必要的政府和非政府观点和知识，实现国家网络安全和保护重要信息基础设施目标。

公私合作

8. 收集所有已采取的行动和发展政府与私营部门合作的计划，包括分享信息和事件管理的任何安排。

9. 收集促进共同依赖相同互联重要基础设施的重要基础设施参与方和私营部门行动者共同利益和处理其共同挑战的所有现行举措和计划采取的举措。

事件管理和恢复

10. 确认贵国政府中担任事件管理协调者的机构，包括监视、预警、应变和恢复等功能的能力；参与合作的政府机构；参与合作的非政府参与方，包括工商界和其他合作伙伴；已作出的合作和可信任信息共享安排。

11. 另外，确认贵国国家一级计算机事件应变能力，包括确认国家级电子计算机事件应变小组及其作用和责任，包括保护政府计算机网络的现有工具和程序以及传播事件管理信息的现有工具和程序。

12. 确认可增强事件应对和应急规划能力的国际合作网络和进程，同时酌情确认各合作伙伴和各种安排，以促进双边和多边合作。

法律框架

13. 审查和更新由于新信息和通信技术迅速发展并且由于依赖这些新技术而可能过时或失效的法律依据(包括有关网络犯罪、隐私、数据保护、商业法、数字签名和加密的法律依据)，在审查过程中利用区域和国际公约、安排和先例。确定贵国是否为布达佩斯《网络犯罪公约》缔约国或是否计划加入该公约，或是否计划制定相应的法律。

14. 确定贵国有关网络犯罪的依据和程序、包括法律依据的现状以及国家防止网络犯罪部门的现状，并确认检察官、法官和议员对网络犯罪问题的认识程度。

15. 评估现行法规和法律依据是否足以处理网络犯罪以及更广泛的网络空间当前和未来的挑战。

16. 检查贵国是否参与了国际社会打击网络犯罪的努力，例如是否参加了打击赛博犯罪 24/7 联络点网络，并确定参加这些努力在何种程度上促进了本国网络安全目标。

17. 确定在基础设施设在贵国境内或罪犯居住在贵国境内、但受害者却居住在其他地方的情形下，贵国执法机构要求满足哪些条件，才与国际同行合作调查跨国网络犯罪。

发展全球网络安全文化

18. 总结为发展联合国大会第57/239号和第58/199号决议所提及国家网络安全文化而采取的行动和将执行的计划，包括政府运作系统网络安全计划、对儿童和个人用户等方面开展的国家提高认识方案和外联方案的执行情况和国家网络安全和保护重要信息基础设施的培训要求。