大 会

Distr.: General
17 March 2010

第六十四届会议
议程项目 55(c)

2009 年 12 月 21 日大会决议

[根据第二委员会的报告(A/64/422/Add.3)通过]

64/211. 创建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，

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

又回顾其关于从国际安全角度看信息技术发展的 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 2003 年 12 月 10 日至 12 日在日内瓦(第一期)和 2005 年 11 月 16 日至 18 日在突尼斯(第二期)举行的信息社会世界首脑会议的成果，[1]

认识到可以放心安全地使用信息和通信技术是信息社会的一大支柱，必须鼓励、推动、发展和大力落实全球网络安全文化，

又认识到网络信息技术对于日常生活的很多重要功能、商业、商品和服务的提供、研究、创新和创业等活动以及对于个人、组织、政府、企业和民间社会之间的信息自由传播所起的作用越来越大，

[1] 见 A/C.2/59/3 和 A/60/687。

还认识到政府、企业、组织和信息技术的个人拥有者和使用者，必须根据各自担任的角色承担起责任，并采取步骤，加强这些信息技术的安全，

认识到开展多个利益攸关方对话的因特网治理论坛必须承担讨论各种问题的任务，包括讨论与互联网治理的关键要素有关的公共政策问题，以促进互联网的可持续性、可靠性、安全性和稳定性以及发展，重申各国政府在国际互联网治理以及确保互联网的稳定性、安全性和连续性方面应该平等发挥作用和承担责任，

重申仍然需要加强合作，使各国政府在有关互联网的国际公共政策问题上，而不是在不影响国际公共政策问题的日常技术和操作问题上，平等发挥作用和承担责任，

认识到每一个国家都将自行决定本国的重要信息基础设施，

重申有必要利用信息和通信技术的潜力，推动实现国际商定的发展目标，包括千年发展目标，认识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经济繁荣，并会削弱合作打击非法滥用信息技术和创建全球网络安全文化的成效，

强调指出必须加强努力，通过便利在网络安全最佳做法和培训方面向发展中国家，尤其是最不发达国家转让信息技术和能力建设，弥合数字鸿沟，普及信息和通信技术，保护重要的信息基础设施，

表示关切重要信息基础设施的可靠运作和网路所承载信息的完整性面临的威胁日益复杂和严重，影响到家庭、国家和国际福祉，

确认重要信息基础设施的安全是各国政府必须系统地承担的一项责任，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，而各有关利益攸关方则必须意识到有关风险以及根据各自所起作用应当采取的预防措施和有效应对办法，

认识到应当通过国际信息分享和协作支持各国的努力，以便有效应对这些威胁日具跨国性质的问题，

注意到有关区域组织和国际组织在加强网络安全方面所做的工作，重申它们在鼓励各国作出努力和促进国际合作方面发挥的作用，

又注意到国际电信联盟 2009 年关于确保信息和通信网络安全及发展网络安全文化的最佳做法的报告，其中重点讨论了各国以符合言论自由、信息自由传播和适当法律程序的方式全面处理网络安全的办法，

认识到定期评估各国保护重要信息基础设施工作的进展有助于此种努力，

1. **邀请**各会员国在其认为适当时利用所附国家保护重要信息基础设施努力自愿自我评估工具，协助评估本国在这方面以及为加强其网络安全作出的努力，以突出说明有待采取进一步行动的领域，目标是提升全球网络安全文化；

2. **鼓励**已制定网络安全和保护重要信息基础设施战略的会员国、相关区域和国际组织向秘书长提供此种信息，用于汇编和分发给会员国，以交流最佳做法和措施，协助其他会员国努力推动实现网络安全。

2009 年 12 月 21 日
第 66 次全体会议

附件

国家保护重要信息基础设施努力自愿自我评估工具 [2]

评估网络安全需要和战略

1. 评估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、水和食物供应、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面临并且必须加以管理的风险。

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严重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. 确定国家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、衡量进展情况的指标、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。

利益攸关方的作用和责任

5. 确定在网络安全和保护重要信息基础设施方面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，并说明主要联系人和各自的责任；
- 其他(地方和地区)政府参与方；

[2] 这是会员国认为适当时可以部分或全部采用的自愿工具，以协助它们努力保护国家重要的信息基础设施和加强国家网路安全。

- 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培训，是否已开展关于网络安全的全国提高认识运动。

政策制定过程和参与

6. 说明在政府-行业协作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；列明参与方、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. 说明可能需要进一步建立的其他论坛或结构，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. 汇集发展政府与私营部门合作方面所有已采取的行动和已制定的计划，包括任何信息分享和事件管理安排。

9. 汇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的共同利益和处理其共同挑战的所有现行举措和计划举措。

事件管理和恢复

10. 说明担任事件管理协调者的政府机构，包括监视、预警、应对和恢复等职能的能力；参与合作的政府机构；参与合作的非政府参与方，包括行业和其他合作伙伴；已作出的合作和可靠信息共享安排。

11. 另行说明国家一级计算机事件应对能力，包括确认国家级电子计算机事件应对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. 说明可增强事件应对和应急规划能力的国际合作网络和进程，同时酌情说明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。确定贵国是否制定了调查和起诉网络犯罪的必要立法，注意到现有框架，例如联合国大会关于打击非法滥用信息技术的第 55/63 号和第 56/121 号决议和包括欧洲委员会《网络犯罪问题公约》在内的区域倡议。

14. 确定贵国有关网络犯罪的依据和程序，包括法律依据和国家防止网络犯罪部门的现状，以及检察官、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. 检查贵国参与国际社会打击网络犯罪的努力，例如参加打击赛博犯罪全天候联络点网络的情形。

17. 确定在基础设施设在本国境内或罪犯居住在本国境内而受害者居住在其他地方的情形下，国家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. 总结为发展大会第 57/239 和 58/199 号决议所述国家网络安全文化而采取的行动和制定的计划，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全国提高认识方案和外联方案的执行情况以及国家网络安全和保护重要信息基础设施的培训要求。