联合国 A/C.2/57/L.10/Rev.1

大 会

Distr.: Limited
10 December 2002
Chinese
Original: English

第五十七届会议

第二委员会

议程项目 84(c)

宏观经济政策问题：科学和技术促进发展

阿根廷、澳大利亚、保加利亚、加拿大、智利、克罗地亚、捷克共和国、丹麦、埃塞俄比亚、德国、印度、意大利、日本、新西兰、挪威、巴基斯坦、波兰、大韩民国、罗马尼亚、俄罗斯联邦、斯洛伐克、南非、瑞典、瑞士、突尼斯、土耳其、大不列颠及北爱尔兰联合王国和美利坚合众国：订正决议草案

创造全球网络安全文化

大会，

*注意到*各国政府、商业、其他组织和个人使用者日益依靠信息技术来提供基本货物和服务、经营商业和交流信息，

*认识到*随着各国愈来愈多地参与信息社会，确保网络安全的需要与日俱增，

*回顾*其关于为打击非法滥用信息技术制订法律基础的 2000 年 12 月 4 日第 55/63 号决议和 2001 年 12 月 19 日第 56/121 号决议，

*还回顾*其关于从国际安全的角度来看信息和电信领域的发展的第 53/70、54/49、55/28、56/19 和 57/53 号决议，

*意识到*有效的网络安全不仅是政府或执法惯例的问题，而是必须通过预防加以处理并得到整个社会支持的情事，

*还意识到*单单技术不能保证网络安全，整个社会必须优先考虑网络安全的规划和管理，

*认识到*各国政府、商业、其他组织和信息技术的个人拥有者和使用者，根据各自担任的角色，必须意识到相关的网络安全风险和预防措施，承担责任，并采取步骤增加这些信息技术的安全，

*认识到*各国在获得和利用信息技术方面存在差距会降低在打击非法滥用信息技术和在创造全球网络安全文化两方面开展国际合作的成效，并注意到需要促进特别是向发展中国家转让信息技术，

*确认*切须开展国际合作，通过支助各国旨在通过利用先进、可靠和安全的信息和通信技术及网络和通过促进其普遍取用来提高人的能力、增加学习和就业机会、改善公共服务和增进生活素质的努力，实现网络安全，

*注意到*由于互连性日增，信息系统和网络目前所遭受的威胁和暴露的脆弱性愈来愈多，形式也更为广泛，为所有人提出了新的安全问题，

*注意到*有关国际组织和区域组织在增进网络安全和信息技术安全方面的工作，

1. *注意到*本决议附件所列的各项要素，以期创造全球网络安全文化；

2. *请*所有有关国际组织审议特别是附件所列关于在今后任何有关网络安全的工作中创造全球网络安全文化的要素；

3. *邀请*各会员国致力在其社会中发展应用和使用信息技术方面的网络安全文化时特别考虑到这些要素；

4. *请*各会员国和所有有关国际组织在筹备将于 2003 年 12 月在日内瓦和 2005 年在突尼斯举行的信息社会问题世界首脑会议的工作时，特别考虑到这些要素和创造全球网络安全文化的必要性。

5. *强调*需要促进向发展中国家转让信息技术和能力建设，以便在网络安全方面采取措施。

附件

创造全球网络安全文化的要素

信息技术的迅速进步改变了研制、拥有、提供、管理、维修和使用信息系统和网络的各国政府、商业、其他组织和个别使用者（“参与者”）对待网络安全的方式。创造全球网络安全文化，所有参与者就必须注意下列九项相辅相成原则：

(a) *意识*。参与者应意识到信息系统和网络安全的必要性以及他们在增加安全方面能够做些什么；

(b) *责任*。参与者应以适合其个别角色的方式对信息系统和网络的安全负责。他们应定期审查各自的政策、惯例、措施和程序，并评估这些政策、惯例、措施和程序是否与其环境相称；

(c) **反应**。参与者应及时地协力预防和侦查安全事件并对这些事件作出反应。他们应酌情分享关于威胁和脆弱性的信息，实施开展迅速、有效合作的程序，预防和侦查安全事件并对这些事件作出反应。为此可能涉及跨边界的信息分享和合作；

(d) **道德**。鉴于信息系统和网络在现代社会的普遍性，参与者需要尊重别人的正当利益并认识到他们的行动或不行动可能危害别人；

(e) **民主**。应以符合民主社会所确认的价值观的方式实施安全，这些价值观包括交换想法和意见的自由、信息的自由流动、信息和通信的机密性、个人资料的适当保护、公开性和透明度；

(f) **风险评估**。所有参与者应定期进行风险评估，这些评估应：指出各种威胁和弱点；基础广泛，足以包含关键的内外因素，例如技术、物质和人的因素、政策和涉及安全问题的第三方服务；能够确定可接受的风险水平；协助选择适当的控制手段，根据所要保护的信息的性质和重要性，管理可能对信息系统和网络造成危害的风险；

(g) **安全设计和实施**。参与者应将安全视为信息系统和网络的规划和设计、操作及使用的一项基本要素；

(h) **安全管理**。参与者应以全面方式对待安全管理，这种方式基于动态的风险评估，其中包括参与者各级的活动及其业务的所有方面；

(i) **再行评估**。参与者应审查和再行评估信息系统和网络的安全，并对安全政策、惯例、措施和程序作出适当的修改，以便应付新的、不断变化的威胁和脆弱性。