联合国 A/C.2/58/L.74

大 会

Distr.: Limited
10 December 2003
Chinese
Original: English

第五十八届会议

第二委员会

议程项目 91(b)

宏观经济政策问题：科学和技术促进发展

委员会副主席亨利·劳本海默先生（南非）根据就决议草案 A/C.2/58/L.19 进行的非正式协商而提出的决议草案

创造一个全球网络安全文化及保护重要的信息基础设施

大会，

回顾其关于创造全球网络安全文化的 2002 年 12 月 20 日第 57/239 号决议；

关于为打击非法滥用信息技术奠定法律基础的 2000 年 12 月 4 日第 55/63 号和 2001 年 12 月 19 日第 56/121 号决议；关于从国际安全角度来看信息和电信领域的发展的 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 号和 2002 年 11 月 22 日第 57/53 号决议，

认识到信息技术对于促进社会经济发展，对于向各国政府、企业界、其他组织和个人使用者提供基本的货物和服务以及对于他们经营业务和交流信息都日益重要，

还注意到大多数国家的重要基础设施（例如除其它外，用于能源的发生、传送和分配、空中和海上运输、银行和金融服务、电子商务、供水、食品分配和公共卫生等领域的基础设施）与互联日增并影响其运作的重要信息基础设施之间的联系日益密切，

认识到每一个国家都将确定自己的重要信息基础设施，

认识到这一不断增强的技术相互依存关系有赖于一个由各重要信息基础设施部分组成的复杂网络，

注意到由于互联日增，重要信息基础设施如今所面临的威胁和暴露的弱点日益增加，形式也更为广泛，提出了新的安全问题，

注意到有效的重要基础设施保护工作除其它外，包括查清重要信息基础设施面临的威胁，降低脆弱性，在出现损害和攻击时将损害程度和恢复时间减到最低限度，并找出损害原因或攻击源头，

认识到有效的保护工作需要所有利益有关者在国家和国际两级开展交流与合作，并认识到国家一级的努力需要由利益有关者在国际和区域两级开展的有效实质性合作提供支持，

还认识到各国在获得和利用信息技术方面的差距会削减合作打击非法滥用信息技术和创造全球网络安全文化的成效，并注意到需要促进信息技术的转让，尤其是向发展中国家转让，

又认识到必须开展国际合作，支持各国进行努力，通过利用先进、可靠及安全的信息和通讯技术和网络，并通过促进其普遍利用，提高人类能力、增加学习和就业机会、改善公共服务及提高生活质量，从而实现网络安全，保护重要的信息基础设施，

又注意到相关国际组织和区域组织在增强重要信息基础设施安全方面的工作，

承认在进行保护重要信息基础设施的努力时应该适当考虑国家有关保护隐私的适用法律以及其他的有关立法；

1. 注意到本决议附件所列的保护重要信息基础设施的各点；

2. **邀请**所有相关国际组织，包括联合国有关机构，在今后关于网络安全或关于保护重要基础设施的任何工作中酌情考虑这些要点及其它；

3. **邀请**各会员国在按照国家法律和条例拟订其减少重要信息基础设施风险的战略时，考虑到这些要点及其他；

4. **邀请**各会员国和所有相关国际组织在筹备定于 2005 年在突尼斯举行的信息社会世界首脑会议第二阶段的工作时，特别考虑到这些要点以及保护重要信息基础设施的必要性；

5. **鼓励已经制定网络安全和保护重要基础设施战略的会员国及有关区域组织和国际组织交流其可以帮助其他会员国争取实现网络安全工作的最佳做法和措施；**

6. **着重指出必须加强努力，通过便利特别向发展中国家，尤其是最不发达国家转让信息技术和建设能力而缩小数字鸿沟，普及信息和通信技术，并保护重要的信息基础设施，从而使所有的国家都能充分地从信息和通信技术中获益，促进社会经济发展；**

附件

保护重要信息基础设施的要点

1. 建立有关网络脆弱性、威胁和事故的紧急警报网。

2. 加强宣传，以便利益有关者了解其重要信息基础设施的性质和范围及其在保护工作中必须发挥的作用。

3. 检查基础设施，确定其中的相互依存关系，以便加强对此类设施的保护。

4. 推动公共和私营部门的利益有关者建立伙伴关系，交流和分析重要基础设施信息，以便预防、调查和应对此类基础设施受到的损害或攻击。

5. 建立、维持和测试应急通信网，确保它们在紧急情况中保持安全和稳定状态。

6. 确保关于提供数据的政策考虑到保护重要信息基础设施的必要性。

7. 为追查攻击重要信息基础设施活动提供方便，并酌情向其他国家披露追查情报。

8. 开展培训和演习活动以增强应对能力，测试信息基础设施受到攻击时的连续性能和应急计划，并应鼓励利益有关者参与类似活动。

9. 具有充分的实体法和程序法以及训练有素的人员，以使他们能够调查和起诉攻击重要信息基础设施的行为，并酌情与其他国家协调此类调查。

10. 酌情参与国际合作以保障重要信息基础设施的安全，合作方式包括拟订和协调紧急警报系统，交流和分析有关脆弱性、威胁和事故的情报，并根据国内法律协作调查攻击此类基础设施的活动。

11. 促进国家和国际两级的研究和开发，鼓励采用那些符合国际标准的安全技术。