



第五十九届会议

临时议程** 项目 60

从国际安全的角度来看信息和
电信领域的发展

从国际安全的角度来看信息和电信领域的发展

秘书长的报告**

增编

目录

	页次
从会员国收到的答复	2
墨西哥	2
美利坚合众国	3
委内瑞拉	6

* 由于技术原因重新印发。

** 所附的信息是在主报告提出后收到的。



从各国收到的答复

墨西哥

[原件: 西班牙文]

[2004年8月18日]

1. 在这个信息系统和电信技术突飞猛进的时代, 国际社会已日益认识到一个事实, 即随着这项进步而来的是, 这些系统的使用者相互连接的规模已经变得这样庞大, 性质是这样的多样化, 已经超越了国家的领土和司法的边界。
2. 随着此一高度连接而来的是成正比的国家和国际安全领域的脆弱性, 从而证实了电信系统和信息对国际和平与安全有巨大影响力的战略领域。
3. 鉴于以上各项原因, 墨西哥认为为限制这个领域正在出现的威胁而采取的手段, 除了要能够维护信息的自由流通和促进发展和平用途的那些工具之外, 必须在裁军及不扩散领域带来具体的好处, 拉近各国的距离, 促进这个领域更大的合作。
4. 墨西哥认为, 由于科技的快速发展已不可避免地在要遵守的标准和此种系统的实际能力之间造成了差距, 使到信息安全领域潜在的和实际的威胁立即增加了, 因此, 必须与时俱进地对其进行前瞻性的审视。
5. 鉴于这个问题是当前所关切的问题, 鉴于必须研究能够使大家更精确地谈这个现象、以便能够有效地对付它的那些概念, 因此, 墨西哥赞赏今年2月开展的工作——这些工作的目的是成立一个政府专家工作组, 就拟写报告探讨第58/32号决议第4和第2段分别提出的“信息安全领域的现存威胁和潜在威胁及对付这些威胁可能采取的合作措施”和“旨在加强全球信息和电信系统安全的有关国际概念”一事与联合国秘书长合作。在这方面, 墨西哥希望要向大会第六十届会议提交的报告将会有实质性的建议, 并会在这个问题的概念和法律定义方面带来进展。
6. 为此, 墨西哥认为, 有关这个问题的发展和讨论如能够在大会其他委员会的结构内发生将会是有用的, 而现行的国际文书中所载的有关条文规定, 还有其他国际组织如联合国教育、科学及文化组织(教科文组织)在国际安全、国际恐怖主义和信息等领域和在信息社会中所取得的进步, 也将是有用的。
7. 至于这个决议的第3段, 内容关于“有关信息安全的各种基本概念”, 特别是“未经许可干扰或滥用信息和电信系统及信息资源”, 墨西哥强调未经许可干扰这种概念可能造成混淆, 因为它有指某些国家援引有问题的人道主义理由或其他理由单独地或纠集其他国家来干涉他国内政的含义。
8. 因此, 这个概念或完全可以省略或以“未经许可的访问”或仅仅是“非法访问”来指某些人或实体对信息系统所做的行动。

9. 鉴于人们明显地关切控制一些国家的防卫计划的信息系统可能有安全隐患，关切电脑科学和电信有被恐怖主义者利用或被用来威慑，因此，墨西哥重申对话、谈判、国际合作和国际法是确保为了信息安全问题而订立的措施绝不会限制信息和通信自由的唯一途径。

美利坚合众国

[原件：英文]

[2004年7月13日]

1. 有效的信息网络和安全的基础设施对保障这些国家和全球信息网络的可靠性、服务和完整性至关重要，美国和美国人民越来越依靠这些信息网络获得必要的服务和经济安全。有待解决的问题是各国如何独自和集体行动，以加强信息网络和基础设施的安全，防止蓄意攻击。

2. 一些国家认为，这一目标可通过国际公约实现，由公约限制发展或使用各种各样的信息技术。这些提案意味着只要政府认为从外界传入国家境内的信息会扰乱政治、社会和文化，政府就有权批准或禁止这种信息。

3. 美利坚合众国并不认为这种做法有助于加强全球信息和通信系统这一目的，反而有违对各国的成长和发展极其重要的信息自由流通的原则。保障信息安全不应该侵犯任何人通过任何媒体（包括电子媒体）不分国界地搜寻、获得和传播信息与想法的自由，正如《世界人权宣言》第19条所规定的。

4. 相反，美利坚合众国认为，网络安全的一个最主要的威胁来自有组织的罪犯、骇客个人和非国家行为者（包括恐怖分子）不遗余力的犯罪攻击。从这一角度来看，保护网络空间益处的最好方法是着重由国家大力惩治滥用信息技术的行为，并着重在全国系统地贯彻旨在防止重要的信息基础设施受到破坏的措施，而不论这种威胁来自何处。这就是美利坚合众国所说的创建全球性的网络安全文化。按照这种观点，各方（政府、工商业、民间社会）都能明了各自的责任，并各行其是，保障网络安全。

5. 至于信息技术的军事应用问题，完全没有必要为此制定一项国际公约。武装冲突法及其必要性、相称性、减少附带损害的原则已经对这种技术的使用作了规定。

通过预防途径保障网络安全

6. 国家自行行动并进行国际合作加强其重要的信息基础设施的安全是实现网络安全目标的最佳途径。每个国家都应该建立一个国家方案，期能：

- (a) 教育并提高关于信息网络和基础设施安全最佳做法的认识；
- (b) 有效地惩治滥用信息技术的行为；

(c) 加强政府与工业界之间的伙伴关系，提供奖励措施，确保国家系统的安全；

(d) 建立国家的事事故警告和反应能力，并建立在国内和国际这两个级别交流信息的程序。

7. 每个国家应该着重在所有的利益有关者（包括政府、工商业和平民）中建立网络安全文化，并在国家之间为全球的网络安全文化进行国际合作。

8. 政府专家组的报告应该强调大会题为“打击非法滥用信息技术”的 2000 年 12 月 4 日第 55/63 号决议和 2001 年 12 月 19 日第 56/121 号决议以及题为“创造全球网络安全文化”的 2002 年 12 月 20 日第 57/239 号决议中的做法。报告可发扬这种做法，在措辞中进一步倡导会员国已经采取的网络安全原则。最近为加强区域的网络安全而进行的多边努力（诸如亚洲-太平洋经济合作组织电信论坛、美洲国家组织、信息社会世界首脑会议和八国集团所作的努力）也可以指导这种工作。

9. 对国家和全球的信息基础设施的完整性和服务造成巨额威胁的主要是犯罪性滥用。在美利坚合众国看来，更重要的是政府应采取步骤，确保有效调查和起诉从事这种活动的人。为此，美利坚合众国和其他 34 个国家已经签署欧洲委员会 2001 年 11 月 23 日关于赛博犯罪的公约，该公约为国家立法和跨国执法合作提供了指导方针。欧洲委员会预期将会按其惯例和公约第 37 条，向不属于欧洲委员会的国家开放该公约。事实上，所有国家，无论有否签署该公约，都可以立即将此公约作为范本，起草针对赛博犯罪的有效国内法。

10. 此外，无论攻击来自何处或出于何种动机，其使用的手段和信息系统遭到的破坏都具有类似的性质。因此，更为重要的是，所有国家都应采取系统的步骤，减少其系统的薄弱环节，并在国民中灌输网络安全文化，即旨在保障其信息基础设施安全的一套做法和习惯。

11. 保护重要的网络和信息基础设施的措施包括减少这种基础设施容易受到各种打击的薄弱环节，以便一旦遭到破坏，能够最大限度地减少损失，且能尽快恢复。

12. 有效的保护还要求各利益有关者（工业、学术界、私营部门和政府实体，包括保护基础设施的机构和执法机构）之间在国家 and 国际两级进行交流、协调与合作。在进行这种努力时，应该适当注意信息的安全以及关于提供法律互助和保护隐私的适用的法律。在推动这些目标的过程中，应该鼓励会员国在制定战略以减少重要的信息基础设施所面临的风险时，实施八国集团成员国重大信息基础设施保护专家所起草的、其后由八国集团司法和内政部长于 2003 年 5 月通过的下列十一项原则：

(a) 各国应该建有紧急警告网络，提醒网络的薄弱环节、威胁和事故；

(b) 各国应该提高利益有关者的认识，帮助他们了解重要信息基础设施的性质和范围，以及各方为保护这种基础设施必须发挥的作用；

(c) 各国应该检查他们的基础设施，找出相互之间的依存关系，进而加强对这些基础设施的保护；

(d) 各国应该促进公私利益有关者之间的伙伴关系，交流和分析重要的基础设施信息，以便防止和调查这些基础设施受到的破坏或攻击，并对此作出反应；

(e) 各国应该创建和维持通报危机的网络，并对其进行测试，保证它们在紧急情况中的安全与稳定；

(f) 各国应该确保提供数据的政策考虑到保护重要信息基础设施这一需要；

(g) 各国应该协助追查攻击重要的信息基础设施的行为，并酌情将追查信息通告给其他国家；

(h) 各国应该进行培训和演习，以提高反应能力，并测试在发生攻击信息基础设施事件时的持续运作计划和应急计划，并鼓励利益有关者参与类似活动；

(i) 各国应该确保制定充分的实体法和程序法，诸如欧洲委员会关于赛博犯罪的公约中所概述的那些法律，并确保配备训练有素的人员，使其能调查和起诉攻击重要信息基础设施的行为，并酌情同其他国家协调这类调查；

(j) 各国应该酌情开展国际合作，保障重要的信息基础设施的安全，包括发展和协调紧急预警系统，交流和分析关于薄弱环节、威胁和事故的信息，并按本国法律，协调调查攻击这种基础设施的行为；

(k) 各国应该促进国家和国际的研究与发展工作，并鼓励运用根据国际标准核证的安全技术。

13. 教育和培训、政策与法律以及国际合作均可有效地加强网络与信息基础设施的安全，对此技术也可助一臂之力。

14. 应该支持联合国和其他多边组织的努力，鼓励会员国：

(a) 评估国家重要网络和信息基础设施的安全，包括了解其薄弱环节和相互依存关系；

(b) 进行教育并提高全国对信息网络和基础设施安全最佳做法的认识；

(c) 有效惩治滥用信息技术的行为，并协助对赛博犯罪进行的跨界调查；

(d) 促进政府与工业之间的伙伴关系，提供奖励措施，确保国家系统的安全；

(e) 建立全国的事故预警和反应能力，并建立在国家和国际这两个级别上交流信息的程序。

委内瑞拉

[原件：西班牙文]

[2004年6月28日]

1. 委内瑞拉玻利瓦尔共和国政府认为任何破坏信息安全的行为皆违反国家充分行使主权的合法权利。因此，利用信息技术和媒体进行政治经济颠覆是违反民主的基本规则的。
2. 因此，信息安全具有双重性质，因为它既与保证保护和捍卫信息有关，又与其正当使用及真实性有关。而不当使用及故意不使用信息及电信系统或信息来源以进行颠覆，是破坏国际安全的因素。
3. 委内瑞拉支持订立国际原则来加强全球信息和电信系统的安全，因为有了这些系统才能够对抗及支援信息领域的反恐、反犯罪而不损害国家主权。