



第六十一届会议

临时议程* 项目 82

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

目录

	页次
一. 导言	2
二. 从各国政府收到的答复	2
玻利维亚	2
中国	3
约旦	4
黎巴嫩	4
卡塔尔	5
阿拉伯联合酋长国	5

* A/61/150。



一. 引言

1. 大会在题为“从国际安全的角度来看信息和电信领域的发展”的第60/45号决议第3段中请所有会员国继续向秘书长通报它们对下列问题的看法和评估意见：(a) 对信息安全问题的一般看法；(b) 国家一级为加强信息安全和促进这一领域的国际合作所作的努力；(c) 旨在加强全球信息和电信系统安全的有关国际概念的内容；(d) 国际社会为加强全球一级的信息安全可能采取的措施。
2. 2006年2月23日，向会员国寄送了一份普通照会，请它们向秘书长通报它们对这个主题的看法和评估意见。收到的答复载于下文第二节。以后收到的其他答复将作为本报告增编印发。

二. 从各国政府收到的答复

玻利维亚

[原件：西班牙文]

[2006年6月13日]

联合国大会通过的第60/45号决议促进在多边一级分析信息安全领域的现存威胁和潜在威胁，以及为遏制这一领域新出现的威胁而可能采取的措施，但须顾及维护信息自由流动的需要。

对信息安全问题的一般评估意见

信息技术和电信手段、例如因特网电传和卫星移动电话的发展和应用取得了显著进展，在世界范围提供无歧视的、无限制的信息，这造成有可能取得机密信息。

但是，这一进程蕴含广阔的、建设性的机会，有利于推动文明的发展，扩大合作机会以促进所有国家的共同利益，实现促进人类利益的新目标。

从保障的观点来看，信息安全方面的处理较不受重视（取决于提供服务的公司）。在这方面没有内部安全政策。

在国家一级采取加强信息安全和促进这一领域国际合作的措施

关于应对信息和电信安全领域的现存威胁和潜在威胁的可能合作措施，规定了一种程序，把及时得到的信息通知信息部，并由电信局加以监控。

从保障的观点来看，所采取的安全措施不足，因为目前的技术很先进。

目前正在发展电信项目，这些项目考虑到最大程度的信息安全措施，使用加密传输结构，以减少和/或消除这种缺陷。

第 60/45 号决议第 2 段所述概念的内容

第 2 段措施的目的应有助于促进审查旨在加强全球信息和电信系统安全概念的有关国际概念。

国际社会为加强全球一级的信息安全可采取的措施

- 评估全球一级的信息和电信安全问题
- 确定信息和电信安全的基本标准和通过因特网未经许可进入或非法使用这些系统问题
- 制订加强全球信息和电信系统安全的国际原则，帮助打击恐怖主义和贩卖机密信息
- 关注这些工具和技术可能被用于与保障国家稳定和安全不符的目的
- 在军事和国际领域，采取符合世界技术先进情况的电信安全系统

建议

信息安全应视为国家政策，在电信法中落实由电信局规范和监督。

在国家一级的信息安全方面，应实施技术最先进的电信项目，采取最安全的措施，使其工作方案能安全地进行。

中国

[原件：中文]
[2006 年 5 月 24 日]

当前，信息技术迅猛发展，成为促进各国经济和社会发展、改善人民生活的重要积极因素。同时，信息技术的发展和广泛应用，也给国际和各国的安全带来了前所未有的挑战。信息安全问题已成为影响一国综合安全乃至全球安全与稳定的重要因素。妥善解决该问题，符合各国的共同利益，也是国际社会的共同责任。

中方认为，信息安全问题不仅涉及信息基础设施的脆弱性所引发的风险，还涉及滥用信息技术造成的政治、经济、军事、社会、文化等多方面问题。在研究信息安全问题时，上述两方面因素需予以同等重视。

中国认为，信息技术的使用应遵循《联合国宪章》和国际关系基本准则；应在确保国家主权和安全、遵守各国法律、尊重各国历史、文化、政治差异的前提下，保障信息自由流动；各国享有根据国内法律管理本国网络空间的权利；鉴于各国在电信领域的发展不平衡，国际社会应加强在信息技术研究和利用方面的合作，切实保障各国获得信息技术的自由。

联合国是探讨解决信息安全问题的适当场所。2005 年信息安全政府专家组虽未能取得实质性成果，但各国专家就信息安全各方面问题深入交换了意见，提出不少宝贵建议，为国际社会今后继续探讨、解决信息安全问题打下了良好基础。中方支持联合国于 2009 年再次设立政府专家组，全面、深入研究信息安全领域面临的威胁和挑战，探讨各项应对之策。中国将一如既往地支持和参与处理信息安全问题的国际努力。

约旦

[原件：阿拉伯文]

[2006 年 6 月 5 日]

信息安全与国家安全相关，信息安全系统与电信安全直接关联，因为信息是通过有线或无线电信网络传递和交流的。为了保护和强化信息和电信安全，需要采取以下举措：

(a) 订立条例、法律和制度，以保护信息的保密性、完整性和供应，抗御对信息的攻击，并打击利用信息系统犯罪的行为；

(b) 在信息和网络部门行动者参与下订立国家计划，以强化信息、电信和网络安全功能。该计划应确保：

1. 保密性和可靠性：确保信息不被披露，不被未经授权者知晓；

2. 内容的完整性：确保信息内容健全，未被修改或处理过，在处理或交流过程中的任何阶段，信息内容都未被损坏、改动或修补，无论是在内部处理过程中还是通过非法干扰；

3. 信息或服务的持续可得性：确保信息系统的持续运作及信息互动持续能力，为信息站提供服务，确保信息用户不受阻碍地使用或获取信息；

4. 当事方无法否认其与信息相关的行动：确保参与信息方面行动或信息站活动的当事方无法否认其参与，因为可以证明某人在某时从事了某一行动；

(c) 订立信息安全战略，即一套规则，以便在信息系统输入部门处理技术和信息者以及与信息系统协作者和管理信息系统者加以适用。该战略的目标是：使使用者和管理者熟悉他们在保护计算机系统和网络以及保护输入、处理、储存、转移和检索各阶段一切形式的信息等方面的义务和职责。

黎巴嫩

[原件：阿拉伯文]

[2006 年 6 月 21 日]

国防部在回复有关国际安全背景下信息和电信领域发展情况的问题时表示如下：

关于信息安全问题的评估，军队的信息网络是封闭式网络，采用被动安全措施，因为信息保护先进技术代价高昂而没有能力采用。至于电信网络，其基础是全国的民用通信架构，适用的是普通法律，因此不适用安全措施。

在国家一级努力加强信息安全的工作中，信息技术方面与电信技术方面的诉讼程序大不相同，因为后者总是超前于法律。在此方面，黎巴嫩现有的法律是 1999 年 10 月 27 日第 140 号法律，事关保护通信保密权及司法或行政部门依据该法第 2 至 13 条的具体规定提出截获通信的要求的条件。在此值得一提的是，该法律不足以使安全机构与民用企业（ISP-GSM）之间进行协调，以使该领域的起诉、调查和防止潜在威胁等工作标准化。这突出表明需要在此领域开展国际合作，需要技术和法律专才以弥补黎巴嫩在法律和技术方面的差距。

卡塔尔

[原件：阿拉伯文]

[2006 年 6 月 12 日]

关于国际安全背景下电信领域的发展情况，卡塔尔国政府正在大力全面控制信息和电信安全，为此颁布了必要的法律，以期避免信息安全领域现有和潜在的危险。

卡塔尔最近设立了通信和信息技术最高委员会，其中包括一个法律部门，任务是完成国家电子法的起草，提交主管当局，确保该法得到批准并在今年生效。该法律草案的目的是防止把计算机硬件或技术用于犯罪或恐怖目的，让会员国全面了解，以便它们全面履行义务，并争取就那些尚未在国际上达成一致意见的概念订立标准定义，以便促进国际论坛上的讨论。

阿拉伯联合酋长国

[原件：英文]

[2006 年 6 月 17 日]

阿拉伯联合酋长国理解网络犯罪越来越大的危险，并认识到此种网络空间犯罪不以传统的国家边界为限。现代化的信息和通信系统使人有可能从任何地点和针对任何人实施非法活动。

为了成功地打击网络犯罪，必须在国家一级和国际一级采取有效行动。

阿拉伯联合酋长国作出了重大努力，加强国家一级的信息安全，包括：

- **阿拉伯联合酋长国防止网络犯罪法**

防止网络犯罪法于 2006 年初通过并公布，涵盖如下内容：

- 进入罪（未经许可进入、病毒散播、黑客攻击、身份窃盗）
- 数据罪（拦截、更改、盗窃、隐私）
- 网络罪（干扰、更改、毁坏）
- 其他相关罪行（使人能够实施犯罪行为、贩毒、贩运人口、洗钱、恐怖主义行为）。

这个法律也处理检查和不合适材料问题。违反防止网络犯罪法可处徒刑或罚金，或两者兼处。

- **建立国家电脑紧急应对工作队**

阿拉伯联合酋长国电信管理局正考虑建立国家电脑紧急应对工作队，以加强安全，应对网络攻击，提供关于网络威胁的预警和信息协调一切事故的应对活动，并通过培训和教育提高国内公众的认识。

- **因特网服务提供者行为守则**

阿拉伯联合酋长国即将拟订一项强制执行的因特网服务提供者行为守则，规定因特网服务提供者必须切实和更主动积极地减少可能载有病毒的群发电子邮件。因特网服务提供者必须主动积极地检查网络流通，查找用于发送垃圾邮件的公开转发、僵尸网络、已被侵入的个人电脑因特网服务提供者还必须在其中列入条款，容许他切断用户，如果用户故意或无意地转发垃圾邮件。违反守则的任何部分，将予惩处。

此因特网行为守则的目的在于要求服务提供者遵守因特网服务提供者行业的高水平行为标准和商业做法。

- **双边协定**

阿拉伯联合酋长国内的因特网服务提供者同邻近国家积极缔订打击垃圾邮件的双边协定，已成功地减少垃圾邮件转发国外的数量。阿拉伯联合酋长国促进和鼓励国际合作打击网络犯罪，支持研究制订谅解备忘录，实施信息共享和支持跨边界执法。

- **提高认识宣传/教育**

政府/电信管理局和业界合作，促进人民对这一技术给他们带来的好处以及网络犯罪的危险的认识。

例如，电信管理局最近印发了“Wireless Security Guidelines”和“Web Hosting policy”两个册子。前者详细说明如何建立无线网络及成功安全运作应采取的步骤。后者扼要说明使用服务的准则，包括：使用政策；垃圾邮件政策；关于违反知识产权的处理政策；关于非法内容的处理政策。

- **国际安全技术措施的重要性**

目前已存在一些促进网络空间安全的技术措施，包括：

- 建立公开密钥基础设施和拟订安全协议；
- 开发优质软件、防火墙、防止病毒方案、电子权利管理系统、加密等等；
- 使用智能卡、生理特征身份证、电子签名、基于角色的技术等等。

但是，网络空间越来越复杂，其组成部分越来越精细，以致出现了新的和未预料到的威胁。所以，必须加大力度发展安全技术，在任何新技术设计进程之初不忘考虑安全问题。

- **在全球一级加强信息安全的可能措施**

- 国际合作是必要的，因为网络犯罪是一种无边界的犯罪，不能以常规方法管制；
- 建立共同法律构架，以使各国顺利交流信息，促进国家间合作。此外，必须考虑订立网络犯罪的统一定义问题，同时考虑到各国的具体定义不同；
- 执法当局应熟悉处理网络空间犯罪问题。它们应该能够搜索和没收电脑储存的数据，以免犯罪证据被毁灭。