



大会

Distr.: General
2 July 2007
Chinese
Original: Arabic/Chinese/English/
French/Spanish

第六十二届会议

暂定项目表 * 项目 95

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. 从各国收到的答复	2
文莱达鲁萨兰国	2
布基纳法索	5
智利	6
中国	6
古巴	7
黎巴嫩	9
墨西哥	12

* A/62/150。



一. 引言

1. 在关于从国际安全的角度来看信息和电信领域的发展的第 61/54 号决议第 3 段中，大会请所有会员国继续向秘书长通报它们对以下问题的看法和评估意见：
(a) 对于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相关国际概念的具体内容；及(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. 2007 年 2 月 23 日，向会员国送交了一份普通照会，请各国向秘书长通报其对于这个问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的增编印发。

二. 从各国收到的答复

文莱达鲁萨兰国

[原件：英文]
[2007 年 6 月 25 日]

文莱达鲁萨兰国提交了文莱皇家警察部队提供的以下报告：

一. 引言

(关于信息安全问题的一般性意见)

1. 信息技术涵盖信息和电信领域的所有发展，在各个社会部门发挥着重要作用。信息技术正在改变着我们创造、收集、处理、管理和分享信息的方式。电子交易和电子记录成为主流模式，对于从商业到医疗卫生等各个行业非常重要。计算机网络建设正在推动这些变革。因特网和因特网用户逐年激增，说明了向网络社会的这种过渡。
2. 为此，信息安全已经成为信息技术的重要组成部分，特别是在信息社会背景下。但这是个复杂问题，适当的措施在很大程度上往往取决于信息技术设备及其基础设施的类型和所处位置。
3. 计算机网络建设是很多变革背后的推动力量，而这些变革也引发了人们对于网络化信息的安全和私密性的新的忧虑。假如得不到妥善处理，这些忧虑可能会从参与性和实用性两个方面限制人们充分发挥网络建设的潜能。多种个人、版权、敏感和产权信息都需要得到适当的机制和技术保障。

4. 需要针对具体情况审慎评估潜在的安全威胁和风险；让相关各方都了解影响到他们以及他们能够控制的威胁和风险，是至关重要的。只有做到这一点，相关各方才能充分理解并应用适当的安全程序。
5. 重点将是保护网络中的非机密信息、保障网络安全和防护能力以及网络服务的可靠性，确保能够获取信息。
6. 有三大领域需要研究：(a) 密码政策，这包括政府信息处理标准和控制手段；(b) 保护政府机构非机密信息的指南；及(c) 法律问题和信息安全，这包括电子商务、隐私和知识产权。
7. 信息保障，特别是使用密码的信息保障工作的重要性日益增强。适当的保障措施（反措施）必须阐释并预测将信息保障责任日益转嫁给终端用户的技术、体制和社会变革。假如不解决密码政策问题，在更广泛的领域内保护网络信息的工作就会遇到阻碍。要在政府机构或其他组织内部针对网络信息实施适当的保护措施，最重要的一步是由最高管理层确定该机构的总体目标，制订并执行能够反映出这些目标的机构安全政策。只有最高管理层有能力加强有效保护网络信息所需的共识，并运用所需资源。
8. 这种观点力图在信息技术环境下评估犯罪行为造成的威胁和风险，并建议警方可以制订安全程序和计算机犯罪预防措施。信息系统的隐患可能源自蓄意或无意的行为，可能来自内部或外部。

二. 关切

9. 文莱皇家警察部队对于电子政务倡议的国家发展工作缺乏安全筹备表示关切。
10. 迄今为止，文莱皇家警察部队尚未被邀参与或参与过面向信息时代的国家筹备工作。近三年来通过了多项立法，为国家进入信息时代做好准备。并建立了多个政府规范机构，负责率先推行电子政务倡议。
11. 执法准备工作中的安全问题既没有得到积极处理，也没有获得同国家议程中的其他项目同等的优先地位。文莱皇家警察部队认为，安全对于实现文莱进入信息社会的国家期望发挥着重要作用。
12. 安全对于信息社会十分重要，建设安全、可靠的基础设施的重要意义绝不容小觑。

三. 文莱皇家警察部队的举措

（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）

13. 作为国家牵头执法机构，文莱皇家警察部队愿意在国家全面进入信息时代需要率先解决的安全问题方面提供协助。

14. 为此，已经派出多名警员赴海外接受关于因特网相关犯罪、特别是网络犯罪和跨国犯罪方面的培训。起初由于缺乏经费，在为调查计算机系统中的违法行为购置必要的信息技术设备和软件方面没有取得任何进展。文莱皇家警察部队目前已经有能力针对网络犯罪案件展开调查。

15. 文莱皇家警察部队积极参与关于加强执法能力的各项论坛，采取措施深化这一领域的国际合作。文莱皇家警察部队同区域及国际执法计算机网络建立了联系，从而进一步提高了抓捕逃犯的能力。

四. 文莱皇家警察部队的提案和建议

（国际社会为加强全球一级的信息社会和信息安全可能采取的措施）

16. 文莱皇家警察部队提出几点，作为推进和改善信息社会安全问题的出发点：

(A) 报告并监测威胁和弱点：

(1) 2004 年成立了文莱达鲁萨兰国计算机应急小组，已经有了某种形式的控制。但该小组同文莱皇家警察部队之间没有任何联系，也没有快速反应机制（例如监测或阻截实时入侵等），这种控制还不够完善。

(B) 促进安全计算机的教育和安全机制：

(1) 支持为全体用户编制关于网络的教材与课程，可以开展关于因特网安全做法与行为的早期培训；

(2) 投资开展宣传运动，强调应该为系统管理员、网络经理和首席信息干事开展安全培训；

(3) 协助开发并应用网络信息安全机制，这种机制让交易各方都能够确定各自需要采纳的预防措施和限制。

(C) 研究和开发：

(1) 为采用集散控制的无边界网络系统结构的安全和防护能力领域的研发工作拨付经费；

(2) 制订综合性工具包，支持网络管理员运行安全系统；

(3) 开发相关技术，用于全面、持续的风险识别和减轻风险项目。

(D) 标准的应用：

(1) 制订并鼓励各方接受软件安全标准，通过这种短期方法推动加强因特网产品安全；

- (2) 制订政府政策，规定由政府采购的计算机设备和软件必须达到特定安全标准，其中要求提供安全警报服务，向用户告知系统弱点并予以修复。

(E) 法律和执法：

- (1) 支持网络警察并为执法机构适当划拨经费，用于支持处理所报告的网络犯罪所需的培训、物力和人力；
- (2) 确保国家政策能够反映出应开展国际执法协作，解决网络犯罪问题，并在制订国际紧急追捕协定时支持执法工作；
- (3) 确保公共政策能够推进广泛使用加密方法，保护网络信息和网络用户。

布基纳法索

[原件： 法文]
[2007 年 6 月 20 日]

1. 布基纳法索早就表示开发信息和通信新技术的政治意愿，认为信息和通信新技术是加强善治以及经济和社会发展的战略手段。
2. 布基纳法索从 1996 年开始对信息和通信新技术的开发进行通盘考虑，以使信息技术促进公共服务现代化，提高行政效力。
3. 1999 年，布基纳法索制定了 2001-2005 年度国家信息和通信基础设施计划，以推动制定国家电讯、信息和通信手段综合政策。
4. 2004 年，布基纳法索政府通过了国家信息和通信基础设施开发计划执行战略。政府通过这项计划，确保信息和通信技术融入整个社会，使之为社会各阶层所用，并挖掘社会潜力推动国家发展战略。
5. 但是，鉴于信息系统应用所产生的风险，政府为保护信息、确保信息系统安全、保护基本人权、建立企业和行政部门的信任制定了一整套法规。
6. 在此期间，关于保护私人数据的 010-2004/AN 号法律于 2004 年 4 月 20 日获得通过。此项法律旨在保护个人的基本权利和自由，保护不论是否经过信息化处理的含有个人数据的信息的隐私。在这一法律实施过程中，布基纳法索通过 2007 年 5 月 18 日 2007-283/PRES/PM/MPDH 号法令成立了信息技术与自由委员会。该委员会作为独立的行政机构，负责监督公私营部门按照此项法律对涉及个人具体资料的信息的自动化处理。它拥有监管和处罚权，可以通过事先通知和声明并通过控制和处罚，对信息处理进行全面监管。

7. 最后，为满足信息社会的安全需要，布基纳法索成立了各种监管机构，例如最高信息委员会以及邮电及信息技术部下属的信息和通信技术发展方案协调局。
8. 面对超越国界的信息社会，布基纳法索认为国际合作是确保信息系统安全的根本条件。除了数字鸿沟，南方国家在信息安全方面面临的风险与北方国家相同。因此，各国必须进行合作，确保国家、机构、企业和个人以及信息网络和系统的安全。只有加强国际合作，才能取得打击网络犯罪斗争的胜利。
9. 布基纳法索对联合国重视信息安全问题表示欢迎，并认为目前应着手制定一项保护信息安全和个人数据的国际文书。无论如何，信息和计算机通信的发展以及国际安全问题应在人权范畴内加以监管，以避免在全世界范围内出现一个为不人道的安全措施所控制的监视社会。

智利

[原件：西班牙文]

[2007 年 6 月 13 日]

1. 智利高度重视在国际安全框架内的信息安全。全球关切信息技术可能会被用于不符维护国际稳定与安全的目的，并对各国的基础设施产生不利影响，对此我们也感到关切。我们认为必须制止信息技术用于犯罪目的。
2. 在立法领域，我们在制定有关电子文件的安全和保密以及国家行政机关之间和这些机关与公民之间沟通的效率的法律法规和准则方面已取得进展。
3. 鉴于此题目的重要性，智利积极参加 2003 年 12 月在日内瓦和 2005 年 11 月在突尼斯举行的两次信息社会世界首脑会议。

中国

[原件：中文]

[2007 年 5 月 15 日]

1. 当前信息技术迅猛发展和广泛应用，对于各国经济和社会发展和人民生活的改善起到了积极的促进作用。同时，信息安全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。妥善解决这一问题，符合各国的共同利益，也是国际社会的共同责任。
2. 中方认为，信息安全问题不仅涉及信息基础设施的脆弱性、互联性带来的风险，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，上述两方面因素都应予以重视。
3. 中方认为，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

下，保障信息自由流动；各国享有根据国内法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，保障各国获得信息技术的自由。

4. 中国政府一直高度重视信息安全问题，制定并逐步实施国家信息安全战略，制定了一系列信息安全法律法规和标准，在加强网络安全事件监测、完善协调处置机制、开展网络安全技术研究、建设网络安全应急体系等方面做了大量工作，基础信息网络和重要信息系统的安全防护能力不断增强。

5. 中国积极参加信息安全领域的国际合作。2006 年 6 月，上海合作组织成员国元首签署了《上海合作组织成员国元首关于国际信息安全的声明》，决定建立国际信息安全专家组。中国以建设性态度参加了上述专家组工作。

6. 中方认为，联合国是探讨解决信息安全问题的适当场所。2004 年至 2005 年，信息安全政府专家组已就信息安全各方面问题进行了研讨并提出不少有益的建议，为国际社会今后继续探讨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，探讨有效的应对之策。中国将一如既往地支持和积极参与处理信息安全问题的国际努力。

古巴

[原件：西班牙文]

[2007 年 5 月 16 日]

1. 目前古巴在信息和通讯技术领域可以展现的结果是，高度优先重视其社会价值，与任何形式的消费主义完全无关；并培养新类型专家，他们专心致志，抱持道德价值观，完全没有那些鼓吹全球化和新自由主义世界老板的样貌。

2. 大幅度改善技术基础设施，从少年时期开始就广泛深入地进行人力资本开发，是古巴国家一级下大气力，加速社会信息化的一些例子，以改善生活质量，提高国家的效率和竞争力。

3. 在此一政策基础上，古巴对广大社会的信息资源进行合理和有效的利用，包括设备和链接。优先部门包括卫生、教育、科学中心、文化机构和公司，从而确保国家的经济社会发展。

4. 然而，这一发展受到美利坚合众国残酷和长期施加的经济、商业和金融封锁，其现政府使这些行动愈演愈烈。

5. 古巴是从 1996 年开始与因特网连接的，当时美国政府给古巴发放了联网许可。然而，尽管目前国际光纤电缆离古巴海岸很近，但封锁的法律一直阻止与这些光纤电缆连接，这意味着古巴不得不使用卫星频道，分别仅以 65 兆位每秒

(Mbps) 和 124 兆位每秒 (Mbps) 的宽频进出。与光纤电缆连接, 不仅可加快链接, 而且还可大大降低费用。但有关法律规定, 增加新的频道或更改频道, 必须获得美国财政部的许可。

6. 至于技术基础设施, 美国对古巴的封锁不仅阻止古巴购买美国公司的设备和信息程序, 而且由于其治外法权的性质, 还压制古巴与其他国家公司进行的商业活动, 美国只要查明 IP 地址是古巴的, 就封锁其下载软件和信息 (包括免费下载的内容)。

7. 因特网是全球共享领域, 当然面临需要克服的挑战: 这不仅是指因特网供全人类使用, 并相应地由所有国家来加以管理, 而且还涉及消灭受到普遍谴责的罪恶, 例如散布色情、煽动恐怖主义和种族主义, 欺诈、散布法西斯意识形态以及任何形式的网络罪行。

8. 但是, 另一个巨大、富国闭口不提的挑战是, 必须消除其选择性和精英优越感的特征, 因为这种特征今天把现实世界的的不平等和鸿沟统统搬到网络空间, 形成所谓 “数字鸿沟”。

9. 世界上数以百万计的人民远远不能成为 “因特网网民”, 他们还不会读书写字, 他们每天最大的担忧是如何摆脱饥渴和疾病而活命。如果各国政府具有政治意愿, 进行国际合作, 并从所谓发达世界目前浪费在宣传、过度消费和军备竞赛中的资金中拿出少许, 就可以使因特网成为开展文化和教育革命的工具, 从而促进知识传播, 促进教育、文化、合作、团结和新世纪需要的伦理道德价值观, 倡导人类更崇高的情感, 摒弃不人道、自私和个人主义的行为。

10. 从另一个方面看, 一些安全机构也一直特别注意这个问题。其中大多数成为政府的顾问机构。它们获得大量资金, 研发了各种方法和方案, 以加强现有技术并开辟新的可能, 包括截取通讯, 进入系统和数据库, 研发识别及跟踪车辆以及个人的系统。这些复杂的网络包括天线系统、侦听站、雷达和卫星, 并得到潜艇和间谍飞机的支持, 所有这些都与超大型计算机和专门应用设备相链接。

11. 如果认为服务和技术供应公司在与上述机构合作时, 没有为它们的情报间谍工作提供便利, 那将是一种非常幼稚的观点。应铭记的是, 依照美利坚合众国的所谓 “爱国法案”, 政府有权要求任何机构提供情报 (无论机密与否), 只要政府认为符合国家安全利益就行。

12. 鉴于知识是全人类共同继承的财产这一前提, 信息资本的展现和分配必须实现民主化, 并为和平与发展事业服务, 因为这对于新的千年向前发展是至关重要的。

黎巴嫩

以下信函来自黎巴嫩常驻联合国代表团，是该团与黎巴嫩电信部、内务部和国防部之间的公文往来。

电信部

[原件：英文]

[2007年6月4日]

1. 我们正在公布一项新的、关于黎巴嫩信息和通讯技术部门的法律，该法目前处在议会最后核准阶段。该法将包括安全和有关信息犯罪的所有事项。
2. 一旦上述法律生效，电信部将与其他部委和所有有关负责人一道安排与 b、c 和 d 点有关的事项。

内务部

[原件：阿拉伯文]

[2007年5月23日]

1. 在国家一级

内部安全部队各部门之间信息交流主要依靠电信手段（各区域业务中心的电话、传真）。这些手段继续遭受破坏，例如电信被截或电话被偷听，所以总局相当时间以来开始扩大在内部安全部队使用的 TETRA 网络，在黎巴嫩若干区域使用，然后再推广到全国。此外，按照部长理事会 2006 年 9 月 15 日第 47 号决定，安全部队最近还装设封闭式蜂窝电话网络。

2. 在国际一级

安全信息交流、特别是内部安全部队和国际机构之间的交流，由内部安全部队总局国际电信司负责，该司通过国际刑警组织贝鲁特局，设有发送和接收安全数据站。该站目前使用一种定期通信系统，其运作以因特网技术为基础，特点是信息流通快，和可以保护机密，它设有专门网络，同国际刑警组织保持联系；国际刑警组织负责监测这一系统的管理和改进。

- 关于(a)点问题，即对信息安全问题的一般看法(大会第 61/54 号决议)，内部安全部队在信息和电信安全领域致力使用有效的技术手段。在这一领域需要应付许多挑战，最重要的挑战是使安全结构和保护数据的环境标准化，达到适当的、令人满意的标准，以期建立、适用和加强管理安全信息系统以及管制这些系统。
- 关于(b)和(c)点问题，即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(同上)，我们在根据所掌握的信息网络现状评估受侵入危险方面，取得了实际的具体经验。我们在改进我们的数据网络安全

全条件方面取得了进展，我们在以下领域采取新的技术和采取解决办法和执行措施：对系统的保护；对系统免遭侵入和病毒的评估；制定计划，使在系统遭受攻击时工作可继续进行；培训人员使在每次发生紧急状况时都有能力介入。

- 关于(d)点问题，即国际社会为加强全球一级的信息安全可能采取的措施（同上），我们建议首先采取一种预防性政策，遏止个别侵入的活动并在这一领域进行国际合作；其次，制定防止破坏和侵入信息网络的行为的法律，将这些行为定为应受惩罚的犯罪行为；最后，会员国之间交流经验数据，以期从中得益，在这一领域取得质量上的进展。

在这方面，应该明确指出，总局就该计划采取了如下措施：

(a) 在内部安全部队总局内设立一个防止信息犯罪处，其主要任务特别是在指出信息罪行及其对数码数据安全构成威胁的危险，并对这些罪行的犯法者进行调查和起诉。

(b) 安全部队经由若干专业官员参加议会技术委员会拟订防止信息犯罪法律草案的工作。这个法律草案正待议会通过。

(c) 安全部队参加国际刑警组织的活动，并对国际刑警组织中东和北非防止信息犯罪委员会的工作作出贡献，该委员会的副主席及另一名成员是内部安全部队专门处理信息问题的官员。此外，防止信息犯罪处处长负责同国际刑警组织联系，处理信息安全和防止信息犯罪的问题，特别是影响到信息安全的犯罪行为。

考虑到国家一级和国际一级一般安全、特别是信息系统和通信系统安全遭受威胁的危险，必须拟订一项面对未来的战略，考虑到保护信息方面的技术进步，找出防止一切破坏的方法。在这方面，应指出如下几点：

1. 信息的动力及安全标准

由于技术进步，转移及保全数据的方法演变极快，但系统、工具、内容管制方面的困难，有必要采取措施在一切级别加以保护。已经订有管理信息安全的国际准则（ISO17799）。

2. 黎巴嫩与信息安全

在立法和行政方面，黎巴嫩确保保护信息环境的方法不足。没有任何法律或行政程序责成行政机构和公共机构执行这些准则（ISO17799）；中央银行和若干私营银行执行某些类似国际准则的指示。也没有关于私营通信网络编码基本原则的法律。

执行问题

电信部关于保全数据流通档案的 2005 年 12 月 19 日第 4/2 号通告没有得到遵守。没有任何法律管理网吧的工作，对卫星通信的管制也没有效力。

在这方面，应指出，美利坚合众国在 9 月 11 日恐怖主义袭击之后，建立了国内安全部，对全国各地的一切网络建立管制系统，进行分析和监测。另外也订有关于数据编码和网络进出的严格法律。

3. 防止和预防方法

事实显示，按照通信协议（传输控制协议/因特网协议），网络空间是受管理网络，但这个空间很脆弱，并不安全，犯罪团体可加以攻击、甚至予以摧毁，原因是网络空间的目的主要在于销售和商业化。此外，网络犯罪的特点是迅速和不受管制和限制，而防止措施很慢，协调根本不存在，而所订的法律不充分。

对因特网协议的运作，曾作出许多改进，同时涉及使用者和编码（特别是因特网协议 6），并进行认真研究，以制定信息网络的安全技术，甚至打击侵入和摧毁。

防止网络犯罪的国际协议，特别是布达佩斯公约，规定国家间迅速合作，这导致：

- 建立一个通信网络（7/24），这个网络与国际刑警组织的网络类似，专门处理信息犯罪问题；
- 设立一个常设委员会和若干区域工作组，促进技术合作，加强防止信息犯罪处的职能。

但这个公约似乎不能确保迅速立即防止可能对网络发动的病毒攻击。

4. 建议

- 执行和改进关于信息安全的法律，同时执行保护信息安全的准则；
- 重新发动和改进各主管部门内的安全措施，以保护信息手段和系统；
- 使电信部内各专业部门展开运作，并使它们与公私部门及机构取得联系，以建立一个对信息系统安全的环境；
- 密切注意世界上特别是在执行因特网协议（例如因特网协议 6）方面取得的进展，并利用必要的技术手段以认识任何侵入因特网的人的身份，以及采用数码身份系统（数码身份证）；

- 加强信息安全领域保护权利各部门之间的协调，订定划一的国际技术准则，以促进监测、管制和协调，并尽可能划一立法系统，以保全国安全，同时符合国际安全的需要。

公共安全总局指出，它有关安全的通信只在黎巴嫩领土内部进行，没有对外通信。关于内部通信，正在若干友好安全机构主管单位的帮助下，改进保护系统。但是，由于财政和技术资源不足，必要的设备仍未到位。

国防部

[原件：阿拉伯文]

[2007年5月1日]

国防部通知如下：

- 黎巴嫩保证不利用信息技术和电信手段从事与国际稳定和安全概念不符的目的；
- 黎巴嫩在国家一级采取必要措施（改进有关系统和相关立法并使之现代化）以加强信息安全，并鼓励各有关方面彼此间交流所掌握的数据；
- 黎巴嫩尊重联合国的决议，这些决议的目的在于保护信息安全及其机密性，防止以任何方式滥用信息，并禁止使用信息来源或信息技术从事犯罪目的或恐怖主义目的。

墨西哥

[原件：西班牙文]

[2007年5月22日]

1. 墨西哥支持俄罗斯联邦在联合国大会提出的“从国际安全的角度来看信息和电信领域的发展”的决议，并认为就该题目和相关概念促进广泛的意见交流至关重要。墨方认为可利用第一委员会和其他裁军论坛的工作，由专家就该题目作出陈述或讨论。
2. 国际法律文书或出口管制政治协定所建立的大部分国际核查机制都使用信息和电信手段以促进其有效操作，因此在这些领域首先必须审查相关进展情况。另一方面，弹道导弹系统发展和核武器现代化需要相关信息和电信发展。此外，在外层空间和卫星技术领域的发展肯定与国际安全有关。
3. 墨西哥在裁军谈判会议框架内经常指出应紧急通过一个工作方案，纳入一个主题，即“防止外层空间的军备竞赛”，该主题被视为与空间信息和通信技术的脆弱性有关。

4. 墨西哥认为按照第 58/32 号决议就该主题设立的政府专家组继续进行工作，并于 2009 年重新设立很重要。为此，墨西哥认为应一直促进广泛讨论。
-