联合国 A/59/116

大会

Distr.: General
23 June 2004
Chinese
Original: Arabic/Chinese/English/
Spanish

第五十九届会议

临时议程* 项目 62

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

* A/59/50 和 Corr.1。

04-40703 (C) 210704 260704

一. 导言

1. 大会 2003 年 12 月 8 日关于从国际安全的角度来看信息和电信领域的发展的第 58/32 号决议第 3 段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) 有关信息安全的各种基本概念的定义，包括未经许可干扰或滥用信息和电信系统及信息资源；(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。大会同一决议第 4 段请秘书长考虑信息安全领域的现存威胁和潜在威胁及为对付这些威胁可能采取的合作措施，并在一个由秘书长根据公平地域分配原则任命成员、将于 2004 年设立的政府专家组的协助下，以及在有能力提供此种协助的会员国的帮助下，进行研究，并将研究结果向大会第六十届会议提出报告。关于从国际安全的角度来看信息和电信领域的发展的政府专家组于 2004 年 7 月开始工作。

2. 2004 年 2 月 18 日发出的普通照会请所有会员国向秘书长通报它们对这个主题的看法和评估意见。迄今收到七份答复，其内容转录在下面第二节。进一步收到的答复将作为本报告增编印发。

二. 从会员国收到的答复

阿根廷

[原件：西班牙文]
[2004 年 5 月 14 日]

目前的情况

1. 阿根廷共和国在数据的安全和保密方面取得了重大进展。在法律规范方面，《保护个人数据的第 25326 号法》是世界上这类法律中最新的之一，其监督工作将由司法部内专门为此目的成立的一个处来负责。另一方面，国家议会中正在审议若干有关信息犯罪的法案，并已接近完成。

2. 还在推动有关数字签字的立法，寻找使电子文件具有法律效力和技术保障，以期确保文件的作者身份和完整性。阿根廷是这方面的先锋，目前正在为执行国家公共编码基础设施做好最后的准备。

3. 具体而言，阿根廷在信息安全方面取得了重要进展。这方面国家信息技术处负有了解、协助和监督国家公共部门的数字和电子信息的安全和保密方面的主要责任。

4. 该处之下设有国家公共行政电信信息网紧急情况协调单位，对公共组织的网络发生的意外事件作出回应，它的主要目的是提高公共部门的安全标准。这方面它将设法处理报告的安全事故，发出预防和更正的警告，它已经开发出了特别的

安全工具，为公共部门的人员制定了这方面的课程，并正在为国家拟定示范安全政策。

对问题的总评价

5. 信息安全有各种不同的方面，它们的解决确实是对人们提出的一项挑战，技术的进步使得需要解决的问题变得日益复杂。

6. 主要的问题可以分为三类：

对信息本身的攻击

对信息资源的不正当使用

网络犯罪

7. 关于信息，新的技术使得信息的三个主要性质变得越来越难维持：保密性、完整性和供查阅性。关于信息本身的问题，有两大类问题需要特别处理：个人信息的管理需要十分谨慎，以保持个人的隐私；以及组织的信息，即商业的、工业的或公营机关或机构的信息，它们的传播、修改或遗失可能会对经济、社会、政治等方面造成损失。

8. 往往被低估的另一个问题是信息资源的不正当使用。不正当使用指将特定资源用于未经授权的目的或以造成滥用或浪费的不合理方式进行使用。譬如，目前通过因特网造成的病毒大规模传播，或其他类型的入侵，以及必须采取的应对措施，它们带来的额外开支远远超过了达到原来的目的所需要的费用。这方面的预防措施将可以节省大量的资源和精力。

9. 最后，新的技术产生了新的犯罪渠道，除了传统的方式之外，现在还得到了新技术的支撑，技术的进展带来了新的形式。

中国

[原件：中文]
[2004 年 5 月 24 日]

中国对信息安全问题的看法

1. 信息和电信领域的飞速发展是当今世界科技进步的一个重要标志。在安全威胁日益多元化、非传统安全因素上升、国际恐怖主义活动日趋猖獗的新形势下，信息安全已成为国际安全领域面临的一项重要课题。中国支持国际社会在维护各国信息安全方面作出的努力，赞成联合国成立信息安全政府专家组讨论和处理信息安全问题。

2. 中国认为，信息技术的使用应遵循《联合国宪章》和其他国际公认的基本准则，维护和促进国际和地区的和平、稳定和发展。在非传统安全威胁日益突出的

情况下，各国应高度重视信息犯罪和信息恐怖活动。鉴于各国在电信领域的发展不平衡，国际社会也应加强在信息技术的研究和利用方面的合作。

3. 中国认为，在联合国信息安全政府专家组框架内，各方应考察信息安全领域现存和潜在的威胁，并探讨各项具体应对之策。中国将以建设性的态度积极参与专家组工作，希望专家组工作能够取得积极成果。

哥斯达黎加

[原件：西班牙文]
[2004 年 3 月 15 日]

1. 哥斯达黎加政府必须指出，哥斯达黎加议会于 2001 年 10 月 24 日通过了以下《刑法》修正案，题为“《刑法》第 4573 号法增加新的第 196 之二、217 之二和 229 之二条，以期制止和惩罚信息犯罪”。上述修正是近年来哥斯达黎加在信息安全方面最重大的进展。

2. 上述修正将信息犯罪分成三类（违反电子通信、信息诈欺和更改数据和破坏信息），它是哥斯达黎加在这个领域上的一项重大进展，使它能适应当前的需要，保障信息安全。

谨附上整个修正案供参考（见附录）。

附录

《刑法》第 4573 号法增加新的第 196 之二、217 之二和 229 之二条，以期制止和惩罚信息犯罪

8148 号法

哥斯达黎加共和国立法大会

令

《刑法》第 4573 号法增加新的第 196 之二、217 之二和 229 之二条，以期制止和惩罚信息犯罪

单独一条 ——《刑法》1970 年 5 月 4 日第 4573 号法增加第 196 之二、217 之二和 229 之二条，条文如下：

第 196 条之二——违反电子通信

凡掌握、接入、利用、散播载于电子、信息学、磁、电信等媒介内的信息、数据和图像和改变它们的目的，以期未经他人同意，公开他人秘密和伤害他人隐私者得处以六个月至一年监禁。当犯下上段所述行为者为电子、信息学、磁和电信等媒介的负责人时，则应处以一年至三年监禁。

第 217 条之二——信息诈欺

凡为本人或为第三者获取财产利益的目的，通过计算机程序、使用错误或不完整数据、非法使用数据或以任何有关系统数据处理程序的其他行动，影响一个计算系统数据的处理程序或结果的人，将被处以一年至十年监禁。

第 229 条之二——改变数据和破坏信息

凡未经授权，通过任何手段，接入、取消、删除、更改一台计算机内注册的数据，或使其无法使用的人，将被处以一年至四年的监禁。

当上述行为导致一个计算机程序、一个数据库或一个信息系统遭到破坏或变得无法使用，则将处以三年至六年监禁。当该计算系统、数据库或信息系统载有公共性质的数据时，则可处以八年以下监禁。

古巴

[原件：西班牙文]
[2004 年 6 月 1 日]

古巴共和国按照题为“从国际安全的角度来看信息和电信领域的发展”的第 58/32 号决议第 3 段的要求提出的意见

1. 大会 2003 年 12 月 8 日关于从国际安全的角度来看信息和电信领域的发展的第 58/32 号决议第 3 段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) 有关信息安全的各种基本概念的定义，包括未经许可干扰或滥用信息和电信系统及信息资源；(c) 加强全球信息和电信系统安全的有关国际概念的内容。

2. 古巴认为，为了公开或秘密颠覆国家的法律或政治命令的目的，敌意地使用电信是对这一领域内国际公认的准则的一项侵犯，是消极和不负责任的使用那些工具的一种表现，可能会因此产生紧张关系和不利于国际和平与安全的局势，直接违背了《联合国宪章》的原则和宗旨。

3. 大会第 58/32 号决议序言部分第 8 段再次重申它关切“这些技术和手段可能会被用于不符维护国际稳定与安全宗旨的目的，对各国基础设施的完整性可产生不利影响，损害其民用和军事领域的安全”。古巴完全同意这一关切。

4. 当信息系统和电信系统被设计和（和）用来对一个国家的基础设施造成损害时，它们可以变成为武器。

5. 古巴重申，所有国家都必须尊重这个领域内现有的国际准则。必须按照国际合作协定，征得有关国家的许可，方可接入另一个国家的信息系统和电信系统。交流的形式和范围应尊重接入系统所属国家的立法。

6. 一国对另一国的信息系统和电信系统的侵袭可能会危害到国际和平与安全。遗憾的是，已有国家玩弄这种手段来推行敌对政策。

7. 将近 20 年来，古巴一直遭受到这种侵袭，这些侵袭是美国政府所唆使的、容许的、和执行的。美国政府分别于 1985 年和 1990 年非法设立了一个无线电台和一个电视台，自那时以来，它们就一直在影响和干扰着古巴的无线电和电视广播。

8. 每周，从美国向古巴播放 2 227 小时旨在破坏古巴宪法秩序的无线电和电视广播节目。有来自 18 个电台的 29 个中波、短波、调频和电视频道专门用来从事这个目的。

9. 那些频道每天总共播出 312 到 315 小时的政治煽动节目，它们与促进信息和思想的自由流通完全无关，它们传递的是虚假的指控——以欺诈、谎言和扭曲为手段所捏造的指控——它们传播的是旨在破坏古巴宪政秩序的信息。

10. 在这 18 个参与对古巴进行无线电和电视侵袭的电台中，15 个所属的组织与居住在美国境内并在美国联邦行政当局完全知情并同意的情况下在其境内作业和行动的众所周知的恐怖分子有关，或为那些恐怖分子所有。

11. 在这些广播电台中，有 12 个是专门为反对古巴而设立的。其中有恶名昭彰的 Martí电视台和电台。它们为美国政府所有，美国政府每年拨出 3 500 万美元向古巴发动无线电——电视战。

12. 美国政府于 2004 年 5 月宣布，它将部署“EC-130 单一指挥部”空中平台，并拨出额外经费以购买和重新装备一个专门向古巴播放所谓的 Martí电台和电视的空中平台，这是一个危险的新挑衅。

13. 在这些针对古巴的非法广播中，它们歪曲我们国家的真实情况，鼓励在危险的情况下进行非法移民，唆使人民不遵守秩序、发起暴动、采取恐怖行动和破坏在全民投票中得到 96%以上的古巴人支持的古巴共和国宪法所建立的体制和法律秩序。

14. 明目张胆地为了颠覆国家内部秩序、侵犯其主权和介入和干扰其内政的目的而使用信息是一项违反国际法、试图破坏人民行使自由决定权利的非法行动。

15. 这种广播不仅侵犯了古巴的主权，而且公然违反了国际电信联盟国际频率登记委员会所订立的各项准则，特别是其禁止电视广播超越国界的第 23.3 号无线电广播条例，因而是违反国际法的行动。

16. 这些电视广播也违反了《国际电信联盟组织法》的序言，因为这些活动并不在于通过电信的良好运作以促进各国人民间的和平关系和国际合作以及经济和社会的发展。

17. 古巴认为有必要再次呼吁各国注意到以下方面，这与充分使用电信作为加强国际合作与安全的手段密切相关：

(a) 各国必须停止单方面使用胁迫措施，违反国际法，限制受影响的国家取得信息和通信技术以及接入信息交换的国际网络，

(b) 基于威胁到国际和平与安全的理由而对任何国家取得电信技术或其他密切相关技术的证明和可能可以施加惩罚的制度应是个多边制度，并以国际社会公认的标准为基础。

(c) 应加强这个领域的国际合作，调动必要资源帮助发展中国家加强和扩大其电信系统。

(d) 应该立即在国家和国际两级采取立法和其他措施，制止电信以及信息和通信技术——以及其他信息和通信手段——的所有权和控制权过度集中在私人手中，以免对信息的必要多种来源造成不利影响，并用作破坏和平和煽动战争的宣传工具。

(e) 应该建立一个管理和监控因特网及其他国际信息和通信网的多边、政府间、民主和透明的系统。该监控系统必须是政府间性质的。

(f) 电信和其他国际通信监控系统应该是多边、透明、有明确责任和公共监督程序的系统，足以制止一些工业国家，尤其美国利用其全球监视系统侵犯许多国家的主权和安全，包括个人的隐私。

(g) 应促使各国发展有效保障，以保持文化的多样性，以及在国际电信系统传播的信息中消除一切形式歧视或挑起仇恨的内容。

格鲁吉亚

[原件：英文]
[2004 年 5 月 18 日]

从国际安全的角度来看信息和电信领域的发展

1. 格鲁吉亚电信的信息安全的目前状态

1.1 格鲁吉亚的信息安全系统正处于发展阶段。

1.2 国家信息安全系统的概念是由格鲁吉亚的基础设施和发展部和格鲁吉亚通信委员会制订的。

1.3 倡导小组是在没有指定用途的经费的情况下展开工作。

2. 任务状况

倡导小组包括以下成员：

- 格鲁吉亚基础设施和发展部：电信和信息技术政策处
- 格鲁吉亚国家通信委员会：技术处

3. 格鲁吉亚国家信息安全系统政策的基本原则如下：

3.1 信息安全的概念的共同方向是由格鲁吉亚信息化方案确定的。该方案处于发展阶段。

3.2 公司、政府和公共信息系统的信息安全战略以及适当的电信基础设施应以国家信息安全标准系统为基础。

3.3 格鲁吉亚的信息安全标准系统是在对国际标准化组织（ISO）、国际电信联盟（国际电联）和欧洲电信标准研究所的各项国际标准进行协调统一的基础上建立的。

3.4 在公司一级，信息安全的政策是通过按照 ISO 17799 标准进行自愿核证的方法性建议和规则予以实施的。

4. 格鲁吉亚对全球信息社会的参与应提供以下机遇：

4.1 随着格鲁吉亚对国际过程的参与，包括参与发展国际信息安全系统，它将建立起一个统一的信息空间和基础设施。

4.2 在国际信息标准的基础上进行综合全球化，它将与格鲁吉亚加入世界贸易组织、联合国和其他国际组织是相一致的。

4.3 在合作与信息开放的原则的基础上，加入全球后工业经济，克服格鲁吉亚与国际信息界之间的信息差距。

4.4 加强格鲁吉亚的信息安全。

5. 格鲁吉亚基础设施和发展部在信息安全领域的主要任务

5.1 界定电信标准方面的缺失，监测和研究各国际标准化组织的活动结果，质量核证系统，生态和信息安全。

5.2 按照国际组织的要求，协调国际和地方的信息发展方案和战略，并与各项国际倡议和区域安全项目合作。

6. 加强格鲁吉亚的国家信息安全

6.1 成功地实现信息方案和信息安全系统需要有一个指定目标的供资来源和国际支助。

6.2 国际组织的帮助在以下领域内十分重要：

- 电信基础设施的研究，以及它向新一代的网络转移；

- 对国家信息安全标准系统的条件和相容性的分析；
- 为各层次的经济和社会活动拟定信息安全的方案和开发这方面的技术。

7. 与国际组织的合作

- 国际电联和区域通信共同体
- 联合国
- 亚太经社会、贸发会议和世贸组织

8. 项目、研讨会和其他活动

8.1 国际电联：为格鲁吉亚基础设施和发展部建立防止未经授权接入的保护系统项目

组织者：国际电联电信发展局、“Utimaco”、保加利亚政府、电信和信息技术部

8.2 发展格鲁吉亚贸易融资基础设施培训班

- 在新的信息和通信技术的支持下建立一个公司系统的问题
- 电子商务、信息通信技术开发和贸易融资，开发电子贸易财务系统、电子银行系统和电子付款系统
- 讨论包括发展国家贸易财务基础设施在内的各种问题。

黎巴嫩

[原件：阿拉伯文]
[2004 年 5 月 27 日]

鉴于信息技术和电信工具的发展和应用，黎巴嫩感到关切的是，这些技术和工具不应被用于任何不符合国际稳定与安全概念的目标，并认为必须防止将信息资源或技术用于犯罪和恐怖主义目的。黎巴嫩将积极响应联合国旨在保护信息安全和机密并防止以任何方式予以滥用的各项决议，并为此进行合作。

大不列颠及北爱尔兰联合王国

[原件：英文]
[2004 年 5 月 14 日]

1. 联合王国欢迎联合国界参与解决我们日益依赖通信网络和信息系统所带来的问题，包括我们更容易受到各种威胁。信息安全对于全球经济的成长至关重要，信息社会世界高峰会议在其第一阶段结束时通过的各项原则和《行动计划》确认了这一重要性。

2. 通过的原则呼吁“与所有利益相关方和国际专业组织合作，促进、发展和落实一种全球性的网络安全文化”，并“通过加强国际合作支持”这方面的努力。联合王国坚信，促进高峰会议的原则和八国集团促进保护重要信息基础设施的原则和联合国大会第 58/199 号决议等所描述和提及的全球性的网络安全文化，将能使各国最有可能实现其各项安全目标。

3. 但是，联合王国不认为需要制定一个多边文书，那将会限制某些民用和（或）军事技术的开发或利用。关于信息技术的军事应用，这样的文书是没有必要的。武装冲突法，特别是必要和比例的原则，适用于那些技术。此外，这种办法可能会阻碍信息的自由流通，而信息社会世界高峰会议也认为那是信息社会的关键原则。

基本构想和相关的概念

4. 我们必须看到网络和信息系统所面临的风险是因威胁和弱点的不同而异的。威胁不断在变化，但很清楚，最近几年来威胁已变得更加复杂。国家的行动者只是信息系统受到的威胁的一小部分。最近几年更受到人们关注的是恐怖分子、有组织的罪犯、和骇客的活动，他们设法以不适当的方式接入系统或攻击网络的正常运作。为了扩大全球的网络安全，我们需要确保通过刑法来处理对信息系统和网络的攻击。《欧洲委员会网络犯罪公约》是将网络罪行定为犯罪行为方面最好的模式。

5. 但是，对于威胁的分析只不过是网络安全的一个方面。联合王国相信，保护网络和信息系统在很大的程度上是同威胁的来源无关的。因此国际合作应直接以系统的弱点为焦点。系统的弱点可以是技术性的——软件和协议方面的弱点——但它们也可以来自使用者所犯的错误，譬如使用者受到“social engineering”和“phishing”伎俩的欺骗而提供了安全资料。改变网络文化，即开发、部署和使用网络和信息系统的方式，是我们面临的最大挑战。经济合作与发展组织（经合组织）的“信息系统和网络安全准则-建设安全文化”为开启这项文化变化提供了稳固的基础。

落实相关的概念：联合王国的做法

6. 2003 年，联合王国通过了一项关于信息安全的国家战略，其中涉及保护重要的信息系统和网络的复原能力。它把重点放在保护政府的信息资产和系统上，但它同时还确认到必须同私营部门合作，并应有一个对外接触的部分，不仅同工商部门还要同个别公民进行接触。它还确认到了同其他国家建立伙伴关系共同努力对于实现一个更安全的网络空间的重要性。

7. 在政府内已经建立了新的结构来执行这项战略，由内政、工业和国防等部积极参与，并在每一个国务部会内任命了一个指定的风险承担人。为支持这一政策，

还发展了政府专家在预期信息安全将面临的挑战和对它们作出回应等方面的技术能力。该政策还确认了研究和创新的重要性，并将于 2004 年 6 月发表一份关于网络安全长期办法的重大研究。

8. 联合王国的战略包括三个关键举措。在 1999 年，联合王国设立了国家基础设施安全协调中心，这是一个多机构的举措，目前它在保护重大基础设施方面享有很高的国际声望。它鼓励有关各界之间分享信息，它作为一个联络点，在同国际接触的基础上实时发布警告，并在查明和改正协议弱点方面发挥了主要作用。

9. 联合王国还对开发信息安全管理标准方面发挥了重大作用，包括拟定信息安全管理准则（ISO/IEC 17799）——它原先是一个英国的标准，但正迅速被人们接受为这个领域上最重要的标准。这些标准对信息安全采取了一种以弱点，和以风险为根据的办法，使各组织能把信息安全管理成为主流工作。

10. 对于处理网络罪行，联合王国正在开发一套电子罪行战略，其中将利用《欧洲委员会公约》和欧盟的各项立法。此外，联合王国执法界已经作好调整，以反映出网络罪行不断变化的性质，它成立了一个国家资源单位，国家高科技犯罪小组，并在各地的警察部队里成立了专家单位。

落实相关的概念：国际合作的潜力

11. 信息社会世界高峰会议强调了国际合作在使信息社会能发挥最大潜力方面的重要性。大会第 58/32 号决议为我们建立网络安全文化提供了机会，它通过尽量减少系统受到干扰的风险和保护信息的自由流通，保护了各国政府、工商业和人民的利益。经合组织准则为制定各项原则提供了有力的模式，它可以帮助促成网络安全文化，并为我们应如何实现网络安全发挥指导作用。

12. 联合王国欢迎联合国界参与解决信息安全的问题，它相信联合国可以为通过集中关注以下问题对发展网络安全文化作出贡献：

- 开发和交流最佳做法
- 建立基线办法，根据《欧洲委员会公约》将网络罪行定为犯罪行为
- 加强各国家当局之间在查明威胁、弱点和展开调查和起诉犯罪者等方面的实时协作
- 开发出一个更加协调一致的办法，以期消除信息系统的各种弱点。