联合国 A/64/129/Add.1

大 会

Distr.: General
9 September 2009
Chinese
Original: French/Spanish

第六十四届会议

临时议程* 项目 91

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

* A/64/150 及 Corr.1。

** 本文件所载资料是在主要报告提交后收到的。

09-50574 (C) 240909 250909

二. 从各国政府收到的答复

古巴

［原件：西班牙文］
［2009 年 7 月 2 日］

对“从国际安全的角度来看信息和电信领域的发展”决议的答复

1. 古巴完全赞同第 63/37 号决议表达的关切，即信息技术和媒体被用于不符合国际稳定与安全的目的，对国家完整产生不利影响，有害各国的民事和军事安全。该决议还适当强调，必须防止信息资源和技术被用于犯罪或恐怖主义目的。

2. 古巴重申，无论是抱着公开的还是不可告人的目的，为颠覆国家政治和法律制度敌对性地使用电信，是违反这方面国际公认准则的行为，也是不负责任地使用这种媒体的负面表现，其后果可能造成紧张关系和不利于国际和平与安全的局势，从而破坏《联合国宪章》阐述的宗旨和原则。

3. 古巴关切地提请注意，信息和电信系统如果被设计和(或)用于破坏一个国家的基础设施，就可以成为武器，从而可能危及国际和平与安全。

4. 在这方面应重申，古巴共和国在各种国际论坛已经谴责历届美国政府对古巴的广播和电视战攻势升级，公然违反管理无线电领域的现行国际法规。

5. 美国政府没有弥补可能对国际和平与安全造成的破坏，而是制造危险局势，如不经古巴同意，用军用飞机向古巴播放电视信号。这种态度与一个联合国安理会常任理事国是不相称的。

6. 从美国领土对古巴的无线电侵略，违反了关于国家之间关系的国际法，以及国际电信联盟关于其成员国行为守则的法律规章。

7. 截至 2009 年 5 月底，美国每周通过 30 个频率对古巴的非法广播共计 1 924 小时。其中若干电台所属的或服务的组织，与美国境内的知名反古巴恐怖分子有联系；这些人播放煽动破坏、政治刺杀和暗杀的节目以及其他典型的无线电恐怖主义题材。

8. 针对古巴的这些挑衅播放构成违反下列国际准则：

- 《国际电信联盟公约》序言所述的基本原则，即电信对维护和平与各国经济和社会发展发挥更大作用，以促进各国人民之间的和平关系与国际合作，并通过电信的良好运作推动社会经济发展。美国政府对古巴播放电视节目的内容是颠覆、破坏和误导性的，违背了这些原则。
- 《国际电信联盟公约》CS 197 和 CS 198 条款规定，所有电台，无论其目的，其设立和操作均不得对其他会员国的无线电通讯或服务造成有害干扰。

- 2007 年 11 月举行的世界无线电通信大会第九届全会的协议，其中第 6.1 段(g)分段规定：“航空器上运营的任何广播站，如系专门向他国政府领土播放而未经该国政府许可，则构成违反《无线电规章》”。

- 国际电信联盟《无线电规章》第 8 条第 8.3 款规定，其他国家政府在分配本国频率时，应考虑到已经分配和登记并得到国际承认的频率，以避免有害干扰。

- 国际电信联盟《无线电规章》第 42 条第 4.2 款，禁止在海面或其上空的航空器站进行任何无线电广播业务。

- 《无线电规章》委员会在 2004 年 12 月第 35 次会议上提出的意见指出，213 兆赫的转播对古巴节目造成有害干扰，并要求美国政府采取适当措施取消转播。自 2006 年 9 月以来，《无线电规章》委员会还一直要求美国政府采取措施，消除在 509 兆赫的干扰，但其至今没有答复。2009 年 3 月 20 日，该委员会第 50 次及其决定概要(RRB09-1/5 号文件)再次重申，这些广播是非法的，并要求美国采取一切必要措施，消除这两宗干扰古巴电视节目的情况。

- 《无线电规章》国际电信联盟第 23 条第 23.3 款限制国家境外的电视播放。2009 年 1 月美国政府问责局(美国官方机构)发表的报告承认，美国政府对古巴的广播和电视节目构成违反国际法和国内法。

9. 古巴还回顾，2007 年 10 月 22 日至 11 月 16 日在瑞士日内瓦举行的世界无线电通信大会通过的结论文件认定，美国从航空器对古巴的无线电播放不符合《无线电规章》。全体会议通过的结论明文规定：“航空器上运营的任何广播站，如系专门向他国政府领土播放而未经该国政府许可，则构成违反《无线电规章》”。这些结论是世界无线电通信大会全会通过的，对国际电信联盟的工作具有法律效力。因此，世界无线电通信大会通过了 1990 年由当时的国际频率登记委员会所做的声明，即对航空气球上对古巴领土播放电视节目构成违反《规章》的规定。

10. 美国政府对古巴的敌对在其近 50 年来的经济、商业和金融封锁中彰显无疑，这一封锁也影响到信息和电信领域，见下面部分事例：

- 古巴无法获得许多网站提供的服务，只要链接被看出来自古巴.cu 域名的互联网地址(IP)，就会遭到拒绝。

- 在没有事先通知的情况下，封锁与古巴有联系的.com 域名；外国资产管制处(外资管制处)最近就采取过这种行为。

- 特别能说明这一点的是，2009 年 5 月微软技术集团公开宣布，因遵守美国法律义务，暂停其对古巴和其他一些国家的“Windows Live Messenger IM”聊天服务。”连接到这个工具时可以看到：“微软已经取消了对受美

国禁运国家客户的 Windows Live Messenger IM 服务，因此，微软将不在其国家提供 Windows Live 服务。”

- 其他的网页也有拒绝来自.cu域名访问的情况：思科系统(http://tools.cisco.com/RPF/register.do)连接技术，互联网接入服务器，甚至数字视频设备；SolidWorks(http://www.solidworks.com/sw/termsofuse.html)自动化设计；以及赛门铁克(http://www.symantec.com/about/profile/policies/legal)防病毒软件。

- 美国还倒打一耙，撒谎指责古巴防止其公民进入全球网络；而事实正相反，由于美国实施的封锁法，古巴不能连接到古巴群岛周围的光纤电缆，被迫支付昂贵的卫星服务。

- 2008 年 12 月以来，古巴电信公司主要由于无法从美国市场购买专用设备，已造成 53 769.8 美元的损失。因为被迫通过中间商寻找保障服务所需的产品，使价格被抬升了很多。

11. 美国的这一态度，破坏了世界各国在瑞士和突尼斯举行信息社会世界首脑会议时展现的精神意愿和取得的成果。信息社会世界首脑会议强烈敦促各国，在建设信息社会时采取必要措施，防止和避免采取不符合国际法和《联合国宪章》以及阻碍受影响国家人口充分实现经济社会发展和破坏其公民福利的单方面措施。

12. 2009 年 5 月 25 日至 29 日在日内瓦举行的科学和技术促进发展委员会第 12 届会议，审查了实施和监测信息社会世界首脑会议成果方面所得的进展；在这个重要论坛上，古巴重申谴责美国政府的封锁政策，特别是对开发通信技术和获取信息的单方面强制性措施以及对古巴无线电领域的侵略，这些都违反了两次首脑会议做出的规定。

13. 联合国大会关于从国际安全的角度来看信息和电信领域发展的讨论很有意义，其时效性和重要性与日俱增。以上指出的美国对古巴的具体事例，说明了这一辩论很有必要，迫切需要采取行动制止这种国家恐怖主义的表现。

14. 古巴坚决支持联合国大会这一行动，因此与 178 个成员国共同对 63/37 号决议投了赞成票，而作为唯一投反对票的国家，美国采取的一贯立场与此形成鲜明对比。

15. 古巴将继续尽最大努力，促进全球和平发展信息技术和电信，并用之为全人类造福。古巴愿与包括美国在内的其他国家齐心协力，为解决阻碍实现这些目标的障碍找到解决办法。

马里

［原件：法文］
［2009 年 7 月 9 日］

对执行“从国际安全的角度来看信息和电信领域的发展”决议的意见和评论

信息安全的一般问题

1. 拒绝服务(以使计算机系统停止运作)和入侵转移信息，是攻击计算机系统的主要形式。

2. 敏感政府或企业系统受到的威胁是，威胁或事故影响重要信息基础设施的完整性、保密性或可用性。

3. 这些因素包括：

- 由外国政府、恐怖分子或极端分子为政治动机策划的威胁
- 为间谍、破坏、外来干涉或者政治性暴力(恐怖主义)实施的威胁

4. 用信息技术替代较为传统的方法，如破坏、电磁辐射、实物侵入或内部信息源控制。

5. 电脑攻击可能针对个人和企业或公共机构。涉及国防或国家安全的攻击，使战略或敏感领域的政府部门、关键性经营者和企业尤其受到影响。然而，根据其目标是向公众开放的站点或服务、操作系统还是直接掌握敏感信息的个人，这些攻击的后果不尽相同。

6. 识别网络攻击来源是特别困难的。所采用的方法往往查出可以在几个不同的国家和地区的一系列计算机。要逐级往上查寻这些计算机，需要很长时间的调查，并且依赖于国际司法合作的不定情况。隐蔽的方法很多，包括在主人不知情的情况下盗用其计算机和在网吧使用公共匿名计算机等等。

7. 然而，大部分政府部门和观察者指出，这些袭击背后藏着黑客团体，其手法似乎越来越精巧。

加强信息安全的国家努力和国际合作活动

(a) 国家一级

8. 马里目前没有关于信息安全的现行法律。

9. 建立一个法律和监管框架，是 2005 年 6 月政府通过的国家信息和通信技术战略计划的优先事项之一。

10. 马里政府已从国际发展协会获得一项信贷(4033 MLI)，以资助支持增长项目，并打算将这笔贷款的一部分，用于进行关于编写马里信息和通信技术法律和监管框架所需技术援助的咨询。

11. 为世界银行借款人征选顾问的工作，依照 2008 年 5 月信息和通信技术局所做规定，发出了 N° 001/2009/SPM/UCP-PAC 号意向书。

12. 在这个法律和监管框架中，将制定关于下列问题的法律：自由，商业，电子商务，知识产权，数据安全和保密，网络犯罪，免费使用公共信息和构成人类遗产的信息。

(b) 加强信息安全的国际合作活动

13. 电脑攻击超越边界，可以同时面向数个国家。为进行网络监测和对事件做出反应，需要开展国际合作和协助。更广泛地讲，保护信息系统不受非法活动侵害，现在已成为许多国家的共同关切。

14. 马里还选用了区域电信部门改革办法，在 2006 年批准了西非经货联盟的指导准则，并在 2007 年批准了西非国家经济共同体其他法规。

15. 国际电信联盟正在建立一个促进网络安全(全球网络安全方案)，马里政府对此很感兴趣。在这项促进网络安全的工作中，设立了一个高级专家小组，负责提出一项长远的战略，包括法律措施和补救软件产品漏洞的技术措施，并预防和侦查电脑攻击和管理危机。

加强信息和电信安全的国际原则的内容

16. 国际信息安全应奉行现有的国际法(确定如何应对国际和平与安全受到的威胁)和国际人道主义法(涉及作战方法和手段、保护非冲突方国家以及受到或可能受到冲突影响的人员和财产)。

17. 《联合国宪章》是有关维持和平与安全的国际法的基石。

18. 所有国际法专家承认，这些规则建立了一个维护国际和平与安全的安全机制。虽然信息和通信技术已经被设计或用作破坏手段(即“信息武器”)，而国际社会尚未就信息安全在现有国际法中的地位达成一致意见，但是《联合国宪章》可以被解释为：允许国际行动者享有很大的自由，可使用信息和通信技术采取攻击行动以及解决国际冲突和争端。

19. 造成这一出人意料情况的原因是，国际法还没有象对常规武器敌对行动一样，对信息领域的敌对行动做出明文规定，虽然当今世界的互相联系及其对信息和通信技术的依赖意味着，这种攻击可能与常规攻击具有同等甚至更高的破坏性。由于对信息安全方面一些概念没有普遍接受的解释，如“侵略行为”(第 1 条)，“武力”(第 2 条第 4 款)和“武装侵略”(第 51 条)，就更增加了难度。

20. 1974 年 12 月 14 日大会第 3314(XXIX)号决议对侵略行为做出定义。

21. 虽然该决议没有得到协商一致通过，但其规定具有指导意义，可作为安全理事会和国际社会所有成员确定侵略行为的标准。

22. 如果受害国有理由相信，袭击由另一国的武装部队实施，目的是干扰军事设施运作、破坏国防或经济能力或侵犯国家在特定领土的主权，使用信息武器的行为即可理解为一种侵略行为。

国际社会可为加强全球信息安全采取的措施

23. 为加强全球一级的信息安全，应对为敌对目的使用信息和通信技术的威胁，国际社会必须在下列某些领域加强行动：

(a) 国家参与提高各方行为者(政府、企业和用户)对信息系统安全的认识和责任感；

在这种情况下，应注重国家之间协调对安全产品工业和科技基础的支持政策。国家和私营部门之间的协作也必须发挥突出作用；

(b) 加强国家能力，使其掌握监测必要的人力资源和技术专长，从而查出传输电脑攻击的异常流量；

(c) 调整信息系统安全领域各国际机构的政策，赋予每个机构具体职能；

(d) 制定计算机安全领域的指标，以帮助各国更好地管理信息和通信技术基础设施。这些指标可包括以下几方面：

- 发生灾害时恢复数据
- 使用标准(准则)
- 监测运行情况(制定基准)
- 电子传输
- 与国际刑警组织的合作
- 访问平台。

结论

24. 根据我们的意见，对计算机安全与恶意使用信息和通信技术的担心日益增加。这些技术虽然有无数优点，但也可能因其无度发展造成灾难的后果。

25. 这些技术发展带来的法律问题迄今没有得到令人满意的答案，因为各种规章往往不切有关情况。

26. 因此，各国应当致力于协调地建立有关工具，确保更好地迈向一个安全的信息社会。

西班牙

［原件：西班牙文］
［2009 年 7 月 8 日］

西班牙对从国际安全的角度来看信息和电信领域的发展的立场

导言

1. 信息安全是信息社会的重要方面。技术进步导致以多种格式处理和存储信息的能力持续快速增长；另一方面，通信领域可用的带宽大量增加，使人能够几乎实时传输和接收大量信息，而不需要特别复杂的基础设施。

2. 这些技术进步使人能更便利地获得各种信息，但也方便了为非法目的使用或获取信息，尤其是国家或跨国行动者之间将通信和信息系统用于敌对或犯罪目的，甚至用来实施恐怖行为或攻击。

3. 过去一年证实，犯罪组织、尤其是恐怖主义组织对互联网的利用呈增长趋势；它们主要利用了互联网的两个优点，即其全球性和充分保障匿名。

4. 因此，必须在社会和信息技术发展与国家和国际法规同期发展之间取得平衡；这些法规应当是适应新技术环境的最新现代法规，要能够应对需要保护信息以防止非法使用而不限制个人权利和自由的挑战。

滥用因特网进行恐怖主义活动

5. 今天，恐怖组织使用互联网产生的主要威胁如下：

(a) 利用互联网作为武器，即将其作为攻击重要基础设施的电脑系统或互联网基础设施本身的一种手段。这种类型的攻击在普通犯罪领域是比较常见的，但爱沙尼亚 2007 年受到的攻击表明，一国的信息基础设施也可能受到这类攻击的影响。与此类威胁直接相关的有，最近两年新出现的恶意软件大幅度增加，以及“僵尸”电脑网络被用于对计算机系统发起攻击。

(b) 以互联网为手段开展其他活动，主要有以下：

- 通信活动。犯罪组织以互联网取代固定电话或移动电话等其他手段进行通信。互联网通信最常用工具包括电子邮件、即时讯息程序和论坛。

- 散布与恐怖活动有关的宣传和材料。目前有数以千计涉及恐怖活动或煽动暴力的网站，随着博客现象的出现，这种趋势愈演愈烈。如何防止恐怖组织利用因特网是一个非常复杂的问题，因为这些网站很容易迁移。这是一个跨国现象，因为承载和管理网页的服务器可能在若干国家，而且可能不是在有关恐怖组织开展行动的国家。

- 招募活动。有时互联网被用来作为开展招募活动的手段，特别是通过聊天室和即时讯息程序。

- 筹资。互联网还为恐怖组织开展获取资金的活动提供了机会。特别值得注意的是，恐怖组织可通过互联网参与开展欺诈活动，以此为手段获取资金。

- 传播培训手册。恐怖组织通过互联网传播恐怖主义技术、制造爆炸物和武器操作手册。

- 收集信息实施攻击。互联网是一个非常重要的信息来源，经常被恐怖组织用来为其活动获取资料。

国家一级为打击恐怖组织利用互联网采取的措施。

立法措施

6. 在各国采取的措施中，西班牙近年来、特别是在 2007 年开展了大量工作，在其法律系统中增加了关于信息安全以及自由行使《世界人权宣言》和《西班牙宪法》所赋自由和权利的一系列法律。制定的广泛法律法规既包括纯粹国内内容，又包括欧洲联盟指定；为实现上述目标，这些法律法规实施了新的信息安全标准，认为要在维护信息保密性的同时实现适度保护，大多数情况下最重要的是保持信息的完整性和可用性。需要指出的有(按时间顺序排列)：

- 规管个人资料自动处理的 10 月 29 日第 5/1992 号组织法，基于想法是建立预防机制，防止信息处理造成侵犯隐私，及其各项衍生规定。

- 保护个人资料的 12 月 13 日第 15/1999 号组织法，目的是在处理个人资料中保障和保护公众自由和自然人的基本权利，特别是其荣誉与个人和家庭隐私，及其各项衍生规定。

- 关于电子签名的 9 月 17 日第 14/1999 号皇家法令，以促进企业、公民和公共行政活动中迅速引进新的电子通信安全技术，将 1999 年 12 月 13 日欧洲议会第 1999/93/EC 号指令纳入西班牙公共法规，该指令制定了关于电子签名的欧盟框架。关于电子签名的 12 月 19 日第 59/2003 号法，根据实施皇家法令后积累的经验纳入修改内容，更新了这项框架。

- 规管国家情报中心的 5 月 6 日第 11/2002 号法以及后来规管国家情报中心的 3 月 12 日第 421/2004 号皇家法令，规定国家情况中心负责协调使用数字媒体和程序的各种行政机构的行动，保障这一领域的信息技术安全，并确保遵守关于保护机密信息的法规等等。

- 关于信息社会和电子商务的 7 月 11 日第 34/2002 号法，将关于信息社会服务某些方面、特别是内部市场电子商务的 6 月 8 日 2000/31/CE 号指令(电子商务指令)纳入西班牙法律。该法还纳入了欧洲议会和理事会

关于保护消费者权益方面中止行为的 5 月 19 日 98/27/CE 指令的部分内容，规定可依其规定，对违反该法规定的行为采取中止行动。

- 11 月 13 日第 32/2003 号一般电信法，规管网络运营和提供电信服务
- 关于电子签名的 12 月 19 日第 59/2003 号法，如上。
- 关于公民电子获得公共服务的 6 月 22 日第 11/2007 号法，规管公民与公共行政之间通过使用和应用电子、计算机及通信技术和媒体进行交流。
- 规管警方从脱氧核糖核酸(DNA)获得的身份查验数据库的 10 月 8 日第 10/2007 号组织法，建立统一收集国家安全部门储藏身份查验数据文件的数据库，这些数据是在刑事调查、尸体鉴定程序或失踪人员调查中通过 DNA 分析取得的。
- 关于电子通信和公共通信网络的数据保存的10月18日第25/2007号法，对在这一领域进行的研究有积极影响。
- 12 月 21 日第 1720/2007 号皇家法令，批准了 12 月 13 日第 15/1999 号个人数据保护法的实施法。
- 12 月 28 日第 56/2007 号法，推动信息社会的措施
- 对下列有关恐怖组织活动的因特网犯罪的刑事定罪：
  - 电脑破坏，刑法第 264 条
  - 威胁，刑法第 169 条及以下
  - 宣扬称颂恐怖主义，刑法第 578 条

其他措施

- 成立打击犯罪集团使用互联网的专门执法小组
- 参加欧洲刑警组织开发的“检查网络”项目
- 建立快速反应中心，以加强公共行政部门的计算机系统安全
- 设立保护关键性基础设施国家中心。

国际社会可为加强全球信息安全采取的措施

- 使用互联网恐怖组织是一个跨国的现象，往往需要在不同国家共同进行调查。因此，调查和防止互联网上的恐怖活动，在很大程度上取决于国际协定和其他国际合作工具的存在。在这方面，应统一立法，以便能够更有效地打击这些犯罪集团在网络中的存在。国际警务合作也是一个关键问题，因为由于电子证据的不持久性，速度是这类调查的关键。

- 使私营部门参与打击网络犯罪。私营部门的合作是必不可少的，因为大多数互联网服务由私营部门掌握。私营部门长期以来一直面临互联网上存在的威胁，其知识和经验可在这方面发挥很大价值。

- 教育最终用户注意其计算机系统的安全。更深刻地认识这个问题，可减少被犯罪分子用来开展活动(特别是“僵尸电脑网络”方面活动)的电脑数量。

- 关于国际社会可为加强全球信息安全采取的措施，各国家之间应签署一项协议(类似于《海上人命安全公约》等)，承诺统一法律以便对网络犯罪进行追查，尽量避免匿名、缺少立法和经济利益使网络成为犯罪和恐怖主义的理想温床。所有这些应与信息自由和自由获取信息保持平衡。

- 根据各国法律，强化国际司法和警务合作，以便能够针对互联网的分散性和链接记录的不持久性，快速高效地追查刑事罪行。

7. 总之，国际社会应采取保护信息所需的措施，从统一的战略远景出发，并在可能情况下建立统一导向，为所有国家树立共同的标准和准则，制定平衡和全面的具体保护措施，并协调有关各国和各国际组织的政策和行动。