联合国

裁军

33

研究丛刊

从国际安全的角度来看信息和电信领域发展

裁军事务厅

从国际安全的角度来看信息和电信领域发展的政府专家组的报告

联 合 国
2012年，纽约

用户指南

这份出版物是用正式语文在联合国裁军宣传方案项下作为一种便于使用的参考工具印发的，内容是秘书长关于核查的一切方面，包括联合国在核查领域的作用的报告。

与先前的研究丛刊略有不同的是，本出版物不仅载有政府专家组的报告，而且还载有与出版报告相关的其他材料。

这项出版是裁军研究丛刊的延续(第44页载有全部“蓝皮书”丛刊的名单)，它对公共图书馆和大学图书馆的参考部门、常驻代表团、研究机构和专门性的非政府组织提供了有用的材料。

本研究丛刊所载全部材料的电子版本，见www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/。

联合国文件都用英文大写字母附加数字编号。凡是提到这种编号，就是指联合国的某一份文件。

联合国出版物

目　　录

导　言

1998年，俄罗斯联邦在联合国大会第一委员会上介绍了一项决议，该决议未经表决通过，自此，“从国际安全的角度来看信息和电信领域发展”问题就被列入联合国议程。

此后，秘书长每年都向大会提交报告，联合国会员国在报告中表达各自对该重要问题的看法，强调必须开展集体行动。

迄今为止，已经成立了两个政府专家组，第一个小组在2004年和2005年举行了会议。第二个小组于2009年开始工作，并在2010年结束讨论。两个小组均审查了来自网络空间的现有和潜在威胁，并坚持致力于探索可能的合作措施以应对威胁。由于网络空间相对“新鲜”，涉及的问题较为复杂，因此第一小组无法就最后报告达成共识。最近成立的第二个小组能够就2010年发布的富有成果的报告取得一致意见。

在写给第二个政府专家组报告的前言中，联合国秘书长注意到“大会在加强国家和国际两级的信息技术和电信安全方面可以发挥重要作用”。他还说：“会员国间对话是形成共同看法的关键。务实合作也至关重要，以分享最佳做法、交流信息和建设发展中国家的能力，并减少误解的危险。误解会妨碍国际社会管理网络空间重大事件的能力。”

2010年，大会一致通过了一项呼吁对最后一个小组采取后续行动的决议。该政府专家组将于2012年开始工作，将继续研究信息安全领域现有和潜在的威胁，以及应对威胁的可能的合作措施，同时考虑到2010年报告中所载的评估和建议。第三个政府专家组将于2013年9月向大会第六十八届会议报告。

该研究系列侧重于2009/2010年政府专家组报告。还包括两份载有会员国意见的秘书长的说明。

第一部分

A/65/201

从国际安全的角度来看信息和电信领域发展的政府专家组的报告

摘　要

信息安全领域现有和潜在的威胁是二十一世纪最严峻的挑战之一。这种威胁的来源多种多样，表现形式是针对个人、企业、国家基础设施和政府的破坏性活动。其结果给公共安全、国家安全和整个全球链接的国际社会的稳定带来重大危险。

重要基础设施越来越多地使用信息和通信技术（信通技术），这就造成了新的脆弱性和破坏机会。由于电信和因特网复杂的互连性，任何信通技术装置都可以成为手段日益高超的滥用的来源或目标。由于信通技术固有的双重用途性质，支持繁荣电子商业的技术也可以用来威胁国际和平与国家安全。

破坏的起源、犯罪人身份或动机可能会难以确定。这种犯罪人往往只能从目标、效果或其他间接证据来推断，他们可以在几乎任何地方采取行动。这些特点便利使用信通技术从事破坏性活动。犯罪归属的不确定和缺乏共同理解，造成不稳定和误解的危险。

更多报道说，各国正在将信通技术发展成战争和情报工具，并用于政治目的。日益令人关注的是，有个人、团体和组织，包括犯罪组织代替别人从事破坏性在线活动。犯罪手段越来越高超，范围越来越大，提高了有害行动的潜力。尽管很少有迹象显示恐怖分子利用信通技术实施破坏性活动，但今后可能会增多。

应对二十一世纪的挑战有赖于志同道合伙伴之间的成功合作。各国之间以及国家、私营部门和民间社会之间的协作很重要。改进信息安全的措施必须有广泛的国际合作才能有效。政府专家组的报告就各国之间进一步对话以减少风险和保护国家和国际重要基础设施提出了建议。

秘书长的前言

十年前，我们无法预见信息技术和电信会如何深入我们的日常生活，或我们对它们的依赖会有多大。这些技术创造了一个全球链接的国际社会。这种链接虽然带来了巨大好处，但也带来了脆弱性和风险。

在应对新技术的影响方面取得了相当大的进展。但是任务是艰巨的，我们刚刚开始制定新信息环境所需的规范、法律和合作方式。

考虑到这一点，我任命了一个由来自15个国家的专家组成的政府专家组，研究这个领域现有和潜在的威胁，并建议应对方法。我感谢专家组组长和各位专家，他们勤奋和认真工作产生了这份报告，其中扼要说明了问题所在和今后可能的步骤。

大会在加强国家和国际两级的信息技术和电信安全方面可以发挥重要作用。会员国间对话是形成共同看法的关键。务实合作也至关重要，以分享最佳做法、交流信息和建设发展中国家的能力，并减少误解的危险。误解会妨碍国际社会管理网络空间重大事件的能力。

这是今后工作的充实议程。本报告是要朝向建设这些新技术所需的国际安全与稳定框架迈出第一步。我向会员国和广大全球受众推荐这份报告的分析和建议。

送　文　函

［2010年7月16日］

谨此提交从国际安全的角度来看信息和电信领域的发展政府专家组的报告。专家组是根据大会第60/45号决议第4段在2009年设立的。作为专家组组长，我很高兴地告诉你，就报告达成了协商一致。

在题为“从国际安全的角度来看信息和电信领域的发展”的该决议中，大会要求按公平地域分配于2009年设立一个政府专家组，继续研究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，以及旨在加强全球信息和电信系统安全的概念。还要求秘书长向大会第六十五届会议提交关于这一研究结果的报告。

按照该决议的规定，任命了来自15个国家的专家：白俄罗斯、巴西、中国、爱沙尼亚、法国、德国、印度、以色列、意大利、卡塔尔、大韩民国、俄罗斯联邦、南非、大不列颠及北爱尔兰联合王国和美利坚合众国。专家名单载列于附件。

政府专家组举行了四次会议：第一次是2009年11月24日至26日在日内瓦，第二次是2010年1月11日至15日在联合国总部，第三次是2010年6月21日至25日在日内瓦，第四次是7月12日至16日在联合国总部。

专家组就从国际安全的角度来看信息和电信领域的发展进行了全面深入的意见交流。此外，专家组考虑到在会员国对大会分别题为“从国际安全的角度来看信息和电信领域的发展”的第60/45、61/54、62/17和63/37号决议提交的答复以及专家组个别成员提供的投入和背景文件中表达的看法。

专家组希望对联合国裁军研究所的投入表示赞赏。该研究所担任了专家组的顾问，其代表是James Lewis和Kerstin Vignard。专家组还希望对担任专家组秘书的秘书处裁军事务厅新闻和外联处新闻干事Ewen Buchanan及协助专家组的秘书处其他官员表示感谢。

专家组组长

安德烈·**克鲁茨基赫**（签名）

一、导言

1. 信息安全领域现有和潜在的威胁是二十一世纪最严峻的挑战之一。这种威胁可以给经济及国家和国际安全造成很大损害。威胁的来源多种多样，其表现形式是针对个人、企业、国家基础设施和政府的破坏性活动。其结果给公共安全、国家安全和整个全球链接的国际社会的稳定带来重大危险。

2. 信息和通信技术（信通技术）具有独特属性，使各国和其他用户难以应对可能面临的威胁。信通技术无处不在，可以广泛获取。它们本身既不专属民用，也不专属军用，其使用目的主要取决于用户的动机。在许多情况下，网络由私营部门或个人拥有和经营。由于电

信和互联网复杂的互连性，任何信通技术装置都可以是手段日益高超的滥用的来源和目标。信通技术的恶意使用很容易隐藏。破坏活动的起源、犯罪人身份或动机可能会难以确定。这种犯罪人往往只能从目标、效果或其他间接证据来推断。威胁行为人可以在几乎任何地方采取行动而在很大程度上不受惩罚。这些特点便利使用信通技术从事破坏性活动。

3. 考虑到这些事态发展对国际安全的影响，联合国大会要求秘书长在政府专家的协助下，研究信息安全领域的现存威胁和潜在威胁以及有关的国际概念，并建议可能的合作措施以加强全球信息和通信系统的安全。

二、威胁、风险和脆弱性

4. 全球信通技术网络已成为破坏性活动的舞台。破坏动机十分不同，从单纯展示技术实力，到偷窃金钱或信息，或作为国家冲突的延伸。这些威胁的来源包括犯罪分子和可能的恐怖分子之类非国家行为体，以及国家本身。信通技术可用来破坏信息资源和基础设施。由于其固有的双重用途性质，支持强大电子商务的信通技术也可以用来威胁国际和平与国家安全。

5. 许多恶意的工具和方法起源于犯罪分子和黑客的活动。犯罪活动的手段日趋高超，范围越来越大，增加了有害行动的潜力。

6. 到目前为止，很少有迹象显示恐怖分子企图损坏或瘫痪信通技术基础设施或利用信通技术实施行动，但今后可能会增多。目前，恐怖分子大多依靠这些技术来沟通、收集信息、招募、组织、宣传其思想和行动及募捐，但最终可能会利用信通技术实施攻击。

7. 更多报道说，各国正在开发信通技术作为战争和情报工具，并为政治目的服务。犯罪归属的不确定性以及在可接受的国家行为方面缺乏共同理解，可能造成不稳定和误解的危险。

8. 日益令人关注的是，有个人、团体和组织，包括犯罪组织代替别人从事破坏性在线活动。这些代理人，无论动机是经济利益还是其他原因，都可能向国家和非国家行为体提供一系列恶意服务。

9. 重大基础设施越来越多地使用信通技术创造了新的脆弱性和破坏机会。越来越多地使用移动通信设备和网络运行服务也是这样。

10. 各国还担心，信通技术供应链会受到影响或破坏而妨碍正常、安全、可靠地使用信通技术。在信通技术中安装恶意隐蔽功能会破坏对产品和服务的信心，削弱商业信任，并影响国家安全。

11. 不同国家之间不同程度的信通技术能力和安全，增加了全球网络的脆弱性。国家法律和做法的差异会给实现一个安全和抵御力强的数字环境带来挑战。

三、合作措施

12. 与全球互联网络相关的风险需要协调一致的反应。会员国在过去十年中多次申明，有必要为抵御信通技术安全领域的威胁开展国际合作，以打击犯罪性滥用信息技术的行为，建立全球网络空间安全文化并促进可以降低风险的其他重要措施。

13. 在过去十年中，国际社会特别是以下组织为打击网络犯罪威胁做出了努力：上海合作组织、美洲国家组织、亚太经合组织论坛、东南亚国家联盟(东盟)区域论坛、西非国家经济共同体、非洲联盟、欧洲联盟、欧洲安全与合作组织和欧洲委员会。各国还为此做出了双边努力。

14. 跨国关注的非犯罪领域应该得到适当的注意，其中包括对与国家利用信通技术有关的国际准则缺乏共识而造成的误解危险，这可能会影响发生重大事故时的危机管理。这要求制订争取在可能的领域加强合作的措施。还可以制订旨在分享最佳做法、管理事故、建立信任、减少风险及提高透明度和稳定性的措施。

15. 随着利用信息和通信技术进行的破坏活动变得越来越复杂和危险，明显的是，没有一个国家能够单独应对这些威胁。面对二十一世纪的挑战有赖于志同道合的伙伴之间的成功合作。各国之间以及国家、私营部门和民间社会之间的协作非常重要，改进信息安全的措施需要广泛的国际合作才能有效。因此，国际社会应审查是否需要合作行动和机制。

16. 现有的协议纳入了与国家使用信通技术有关的准则。鉴于信通技术的独特属性，可以与时俱进逐渐制订更多的准则。

17. 能力建设对于成功确保全球信通技术安全，协助发展中国家努力加强其重大国家信息基础设施的安全，以及缩小目前的信通技术鸿沟至关重要。必须开展密切的国际合作，才能建设在应对信通技术安全方面可能需要援助的国家的能力。

四、建议

18. 考虑到信息安全领域现有和潜在的威胁、风险和脆弱性，政府专家组认为有必要建议进一步的建立信任措施和其他措施，以减少信通技术受到干扰所造成的误解风险：

(一) 各国之间的进一步对话，以讨论与国家使用信通技术有关的准则，降低集体风险并保护关键的国家和国际基础设施；

(二) 建立信任、稳定和减少风险的措施，以应对国家使用信通技术的影响，包括在冲突中使用信通技术交换国家看法；

(三) 就国家立法及国家信息和通信技术安全战略和技术、政策和最佳做法进行信息交流；

(四) 确定支持欠发达国家能力建设的措施；

(五) 寻求制定与大会第64/25号决议有关的共同术语和定义的可能性。

从国际安全的角度来看信息和电信领域的发展政府专家组成员名单

白俄罗斯外交部国际安全和军控司司长
Vladimir N. Gerasimovich先生

白俄罗斯共和国常驻联合国日内瓦办事处代表团参赞
Aleksandr Ponomarev先生（第三次会议）

巴西国防部政策、战略和国际事务秘书处
巴西海军陆战队、巴西海军中校
Alexandre Mariano Feitosa先生

中国外交部军控司副司长
李松先生（第一和第二次会议）

中国外交部军控司副司长
康勇先生（第三和第四次会议）

爱沙尼亚信息技术大学副教授
Linnar Viik先生

法国国防和国家安全总秘书处
国家信息系统安全局
国际关系
Aymeric Simon先生

德国联邦外交部常规武器控制司司长
Gregor Koebel先生

印度信息技术部印度计算机应急小组高级主任
B. J. Srinath先生

以色列外交部军控司司长
Rodica Radian-Gordon女士

意大利部长理事会主席团通信安全部门主任
Vincenzo Della Corte先生（第一和第三次会议）

意大利部长理事会主席团通信安全部门
Walter Mecchia先生（第二和第四次会议）

卡塔尔埃米里通信兵部队
陆军信号连连长
Rashid A. Al-Mohannadi先生（第一次会议）

卡塔尔国防部（工兵）中校
Saad M.R.Al-Kaabi先生

大韩民国外交和贸易部大使
Lew Kwang-chul先生

俄罗斯联邦外交部新挑战和威胁司副司长
Andrey V. Krutskikh先生

南非通信部因特网治理副主任
Palesa Banda女士（第一次会议）

南非国防部政府信息技术干事
Mario Silvino Brazzoli少将

大不列颠及北爱尔兰联合王国国家信息保证技术局国际关系小组
Gavin Willis先生

美利坚合众国国务院网络事务办公室高级政策顾问
Michele G. Markoff女士

第二部分

背景资料

一、A/RES/63/37

从国际安全的角度来看信息和电信领域的发展

大会，

*回顾*其1998年12月4日第53/70号、1999年12月1日第54/49号、2000年11月20日第55/28号、2001年11月29日第56/19号、2002年11月22日第57/53号、2003年12月8日第58/32号、2004年12月3日第59/61号、2005年12月8日第60/45号、2006年12月6日第61/54号和2007年12月5日第62/17号决议，

*又回顾*其关于科学和技术在国际安全领域的作用的各项决议，除其他外，确认科学和技术的发展可以有民用和军事两种用途，需要维持和鼓励民用科学和技术的进展，

*注意到*在发展和应用最新的信息技术和电信手段方面取得了显著进展，

*申明*大会认为这一进程带来最大的机会，有利于推动文明的进一步发展，增加为所有国家的共同利益开展合作的机会，增强人类的创造潜力，并进一步改善全球社会的信息流通，

*为此回顾*1996年5月13日至15日在南非米德郎德举行的信息社会与发展会议提出的做法和原则，

*铭记*1996年7月30日在巴黎举行的恐怖主义问题部长级会议的结果及会议提出的建议，[1]

*又铭记*信息社会世界首脑会议（第一阶段——2003年12月10日至12日，日内瓦；第二阶段——2005年11月16日至18日，突尼斯）的结果，[2]

*注意到*信息技术和手段的传播和使用影响到整个国际社会的利益，广泛开展国际合作有助于取得最佳效益，

---

[1] 见A/51/261，附件。

[2] 见A/C.2/59/3和A/60/687。

*表示关切*这些技术和手段可能会被用于不符合维护国际稳定与安全宗旨的目的，可能对各国基础设施的完整性产生不利影响，损害其民用和军事领域的安全，

*认为*有必要防止为犯罪或恐怖主义目的利用信息资源或技术，

*注意到*那些按照第53/70、54/49、55/28、56/19、57/53、58/32、59/61、60/45、61/54和62/17号决议第1至3段的要求向秘书长提交它们对信息安全问题的评估意见的会员国所作的贡献，

*注意到*载有这些评估意见的秘书长的报告，[3]

*欢迎*秘书处和联合国裁军研究所采取主动，于1999年8月和2008年4月在日内瓦召开关于从国际安全的角度来看信息和电信领域发展的国际专家会议，并欢迎这些会议的成果，

*认为*秘书长报告中的会员国评估意见以及国际专家会议有助于进一步了解国际信息安全问题的实质内涵和有关概念，

*铭记*秘书长为执行第58/32号决议在2004年设立了政府专家小组，该小组按照其任务规定，审议了信息安全领域的现有威胁和潜在威胁，以及为消除这些威胁可以采取的合作措施，并对国际上旨在加强全球信息和电信系统安全的有关概念进行了研究，

*注意到*秘书长根据信息和电信领域的发展与国际安全问题政府专家组的工作结果编写的有关该小组的报告，[4]

1. *吁请*会员国进一步推动多边审议信息安全领域的现有威胁和潜在威胁，并审议为遏制这一领域新出现的威胁可以采取的措施，但须顾及维护信息自由流通的需要；

2. *认为*研究旨在加强全球信息和电信系统安全的有关国际概念可有助于实现这些措施要达到的目的；

3. *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) 上文第2段所述概念的内容；

(d) 国际社会为加强全球一级的信息安全可能采取的措施；

4. *请*秘书长在2009年按公平地域分配原则设立的政府专家组协助下，继续研究信息安全领域的现有威胁和潜在威胁、为消除这些威胁可以采取的合作措施及上文第2段提及的概念，并向大会第六十五届会议提交关于这一研究结果的报告；

---

[3] A/54/213，A/55/140和Corr.1及Add.1，A/56/164和Add.1，A/57/166和Add.1，A/58/373，A/59/116和Add.1，A/60/95和Add.1，A/61/161和Add.1及A/62/98和Add.1。

[4] A/60/202。

5. *决定*将题为“从国际安全的角度来看信息和电信领域的发展”的项目列入大会第六十四届会议临时议程。

2008年12月2日
第61次全体会议

二、A/RES/66/24

从国际安全的角度来看信息和电信领域的发展

大会，

*回顾*其1998年12月4日第53/70号、1999年12月1日第54/49号、2000年11月20日第55/28号、2001年11月29日第56/19号、2002年11月22日第57/53号、2003年12月8日第58/32号、2004年12月3日第59/61号、2005年12月8日第60/45号、2006年12月6日第61/54号、2007年12月5日第62/17号、2008年12月2日第63/37号、2009年12月2日第64/25号和2010年12月8日第65/41号决议，

*又回顾*其关于科学和技术在国际安全领域的作用的各项决议，除其他外，确认科学和技术的发展可以有民用和军事两种用途，需要维持和鼓励民用科学和技术的进展，

*注意到*在发展和应用最新的信息技术和电信手段方面取得了显著进展，

*申明*大会认为这一进程带来最大的机会，有利于推动文明的进一步发展，增加为所有国家的共同利益开展合作的机会，增强人类的创造潜力，并进一步改善全球社会的信息流通，

*为此回顾*1996年5月13日至15日在南非米德兰特举行的信息社会与发展会议提出的做法和原则，

*铭记*1996年7月30日在巴黎举行的恐怖主义问题部长级会议的结果及会议提出的建议，[1]

*又铭记*信息社会世界首脑会议（第一阶段——2003年12月10日至12日，日内瓦；第二阶段——2005年11月16日至18日，突尼斯）的结果，[2]

*注意到*信息技术和手段的传播和使用影响到整个国际社会的利益，广泛开展国际合作有助于取得最佳效益，

*表示关切*这些技术和手段可能会被用于不符合维护国际稳定与安全宗旨的目的，可能对各国基础设施的完整性产生不利影响，损害其民用和军事领域的安全，

*认为*有必要防止为犯罪或恐怖主义目的利用信息资源或技术，

---

[1] 见A/51/261，附件。

[2] 见A/C.2/59/3，附件；A/60/687。

*注意到*已经按照第53/70、54/49、55/28、56/19、57/53、58/32、59/61、60/45、61/54、62/17、63/37、64/25和65/41号决议第1至3段的要求向秘书长提交对信息安全问题的评估意见的会员国所作的贡献，

*表示注意到*载有这些评估意见的秘书长的报告，[3]

*欢迎*秘书处和联合国裁军研究所采取主动，于1999年8月和2008年4月在日内瓦召开关于从国际安全的角度来看信息和电信领域发展的国际专家会议，并欢迎这些会议的成果，

*认为*秘书长报告中的会员国评估意见以及国际专家会议有助于进一步了解国际信息安全问题的实质内涵和有关概念，

*铭记*秘书长为执行第60/45号决议，在2009年按公平地域分配原则设立了政府专家组，该专家组按照其任务规定，审议了信息安全领域的现有威胁和潜在威胁，以及为消除这些威胁可以采取的合作措施，并对国际上旨在加强全球信息和电信系统安全的有关概念进行了研究，

*欢迎*从国际安全的角度来看信息和电信领域的发展政府专家组的有效工作及秘书长转递的相关报告，[4]

*注意到*政府专家组报告的评估意见和建议，

1. *吁请*会员国进一步推动多边审议信息安全领域的现有威胁和潜在威胁，并审议为遏制这一领域新出现的威胁可以采取的战略，但须顾及维护信息自由流通的需要；

2. *认为*进一步研究旨在加强全球信息和电信系统安全的有关国际概念可有助于实现这些措施要达到的目的；

3. *邀请*所有会员国在考虑到从国际安全的角度来看信息和电信领域的发展政府专家组的报告所载评估意见和建议的情况下，[4]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) 上文第2段所述概念的内容；

(d) 国际社会为加强全球一级的信息安全可能采取的措施；

---

[3] A/54/213，A/55/140和Corr.1及Add.1，A/56/164和Add.1，A/57/166和Add.1，A/58/373，A/59/116和Add.1，A/60/95和Add.1，A/61/161和Add.1，A/62/98和Add.1，A/64/129和Add.1，A/65/154及A/66/152和Add.1。

[4] 见A/65/201。

4. *请*秘书长在将于2012年按公平地域分配原则设立的政府专家组协助下，根据上述报告中的评估意见和建议，继续研究信息安全领域的现有威胁和潜在威胁及为消除这些威胁可以采取的合作措施，包括国家在信息空间中负责任行为的规范、规则或原则和建立信任措施，以及上文第2段提及的概念，并向大会第六十八届会议提交关于这一研究结果的报告；

5. *决定*将题为“从国际安全的角度来看信息和电信领域的发展”的项目列入大会第六十七届会议临时议程。

2011年12月2日
第71次全体会议

三、A/66/152

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

一、导言

1. 大会在其第65/41号决议执行段落第3段中邀请所有会员国在考虑到从国际安全的角度来看信息和电信领域的发展政府专家组的报告[1]的评估意见和建议的情况下，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) 决议第2段所述概念的内容；

(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. 根据该要求，于2011年3月16日向会员国发出普通照会，请它们就该主题提供信息。下文第二节载有已收到的答复。以后收到的任何答复将作为本报告的增编印发。

[1] A/65/201。

二、已收到的各国政府的答复

澳大利亚

[原件：英文]
[2011年5月31日]

澳大利亚欢迎有机会根据大会关于从国际安全的角度来看信息和电信领域的发展的第65/41号决议提交本答复，表达我们的意见。

澳大利亚希望成为网络安全方面的世界领袖。我们认识到技术进步对全球数字经济和所有国家的安全所具有的重要性和裨益。澳大利亚力求利用自己的专门知识为所有国家创造最大程度的经济和安全收益。

随着技术越来越渗透进我们的生活之中，政府、企业和个人也就因各种目的和功能而越来越依赖于技术，如在线购买商品和服务、与别人交流、寻找信息和管理财务，甚至控制采矿和制造业中的设备等。要使因特网和数字经济带来的裨益最大化和增强全球网络安全，各国就必须一起努力，造就一个可靠、安全和有弹性的网络空间。澳大利亚努力成为主动参与者，为所有用户——国家、企业和个人——增强网络空间而发挥作用。

对信息安全问题的一般看法

澳大利亚认识到，网络安全属于国家最高安全优先事项。国际社会继续在经受网络犯罪规模不断扩大、复杂性不断增加和成功犯罪次数不断增多的情况。随着电子信息数量和价值的提高，罪犯和其他恶意行为者的努力也在增强；他们把因特网当作进行其活动的更为隐秘、便利和有利可图的途径。

在面对和管理这些风险时必须与包括隐私权在内的个人的公民自由权进行平衡，并需要促进效率和创新，以确保使澳大利亚实现数字经济的所有潜力。

澳大利亚及每一个国家的国家安全、经济繁荣和社会福祉都与各种信息和通信技术的可用性、完整性和保密性密不可分。据此，澳大利亚政府已投入大量资源，积极促进维护一个可靠、安全和有弹性的电子操作环境，以造福于所有用户。

尽管澳大利亚政府的网络安全政策主要侧重于澳大利亚信息和通信技术的可用性、完整性和保密性，但这一政策与其他相关政策和方案的网络安全政策是有协调的，例如网络安全着重于保护个人，特别是儿童，免受冒犯性内容、欺凌、为性剥削目的进行在线跟踪或诱骗等行为的侵扰。

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

为加强信息安全而做出的国内努力

澳大利亚认识到，要促进网络空间的国际合作就必须在国内模拟最佳做法。澳大利亚实施了一种以政府为主导的保护和加强网络安全的综合方法。在2009年，政府公布了首个网络

安全战略，阐述了澳大利亚政府网络安全政策的总目标和具体目标，规定了澳大利亚政府为实现这些目标所要完成的各项战略优先事项。该战略还说明了澳大利亚政府在为实现这些战略优先事项而展开的全面工作中将要采取的各项关键行动和措施。

澳大利亚网络安全政策的目标是维护一个能支持澳大利亚国家安全并能使数字经济的裨益最大化的可靠、安全和有弹性的电子操作环境。该战略的关键举措包括建立两个相互支持的组织：一个新的国家计算机应急小组和网络安全作业中心。国家计算机应急小组成立于2010年，为所有澳大利亚人和澳大利亚企业提供了网络安全信息方面的一个单一联络点，并确保使澳大利亚的因特网用户能得到关于网络威胁、其系统脆弱性的信息，以及有关如何更好地保护其信息和通信技术的信息。国家计算机应急小组与操纵着对澳大利亚国家利益具有重大意义的系统的各关键基础设施和企业的业主和运营商保持密切工作关系。该小组向这些企业提供有针对性的网络安全威胁和脆弱性信息，以协助更好地保护他们的信息和通信技术基础设施。同样成立于2010年的作业中心向澳大利亚政府提供所有来源网络态势情况，并能以更强的能力促进对具有国家重要性的网络安全事件做出业务反应。该中心确认和分析复杂的网络攻击，并协助应对发生于政府和关键私营部门系统和基础设施的网络事件。

该战略的一个关键优先事项是用信息、信心和实用工具教育和武装所有澳大利亚人，使他们上网时能保护自己。该战略的指导原则是共同责任原则，即所有用户在享受信息和通信技术裨益的同时，应采取合理步骤保护自己系统的安全，在交流和储存敏感信息时应谨慎小心，并有义务尊重其他用户的信息和系统。为使个人能在信息安全领域发挥积极作用，个人就必须知道和理解网络环境及其风险。为实现这一目标，澳大利亚现正开展一个提高认识方案，其中包括为澳大利亚家庭用户和小企业，包括为那些网络知识和技能有限的人建立了一个网络安全信息网站（见www.staysmartonline.gov.au），并与企业、消费者团体和社区组织合作开展了一个网络安全认识周。认识周帮助澳大利亚人了解网络安全风险，并教家庭和小企业用户用简单步骤保护其在线个人信息和财务信息。在2010年全国网络安全认识周期间，大约有150个政府机构、行业、社区和消费者组织合作在澳大利亚城市、区域和农村举办各种活动。在2011年，从5月30日至6月4日举行了认识周。

澳大利亚政府承认，网络空间安全是一项共同责任，因此主动与因特网业协会合作，以拟订一个创新的因特网服务提供商网络安全自愿业务守则，并于2010年12月开始实施。该业务守则为澳大利亚因特网服务提供商提供了一个在网络安全问题方面向其顾客提供信息、教育和保护的一致性做法。澳大利亚在多边论坛上介绍了成功实施该业务守则的情况，并分享了在拟订该守则过程中得到的经验教训。在2010年12月举行的经济合作与发展组织（经合组织）信息安全工作队会议、亚洲-太平洋经济合作组织电信和信息工作组会议和亚太地区电信组织会议上都作了介绍。澳大利亚渴望通过双边能力建设活动和多边论坛与其他国家分享这一守则，以协助其他国家更好地与因特网服务提供商进行协作，并使因特网服务提供商在教育和保护终端用户时更为负责。

促进国际合作

澳大利亚将有关网络安全的国际合作列为高度优先事项。鉴于因特网的跨国性质，要实现有效的网络安全就需要开展协调的全球行动，因此，澳大利亚对国际参与采取了一种积极和多层面的方法。除其他方面外，这包括以双边方式和通过多边论坛与外国政府和组织进行联系，以帮助促进国际最佳做法、分享经验教训、建设能力，以及促进协调的全球方法来消除网络安全威胁。

澳大利亚在联合国的参与包括担任关于下列问题的各项决议的共同提案国：创造全球网络安全文化以及评估各国保护重要信息基础设施的努力，和从国际安全的角度来看信息和电信领域的发展。澳大利亚还响应大会第64/211号决议，就保护包括信息和通信技术在内的关键信息基础设施的最佳做法提出了自己的意见，以促进改善全球网络安全。澳大利亚是国际电信联盟（国际电联）的成员，并向标准化和发展部门所属的研究小组做出贡献。澳大利亚向发展部门提供资金，以开展亚太区域的能力建设工作，包括网络安全举措。澳大利亚是经合组织信息安全和隐私问题工作队的积极贡献者及前任主席，目前是参与该工作队网络安全战略比较分析工作的志愿国。澳大利亚是拟订和执行《首尔-墨尔本关于亚太国家合作反垃圾邮件的协定》和作为在打击垃圾邮件方面的著名国际执法和合作网络的《伦敦行动计划》的当然领头国。

澳大利亚与其区域伙伴维持着协作关系，并致力于与他们一起工作。我们与本区域的其他国家在能力建设方面密切联系，以期实现一个可靠、有弹性和安全的网络空间。澳大利亚参与亚洲-太平洋经济合作组织电信和信息工作组的活动和东南亚国家联盟(东盟)区域论坛关于网络安全的工作。澳大利亚是亚洲-太平洋经济合作组织电信和信息工作组安全和繁荣问题指导小组的副召集国。澳大利亚目前正寻求担任东盟区域论坛工作计划下网络恐怖主义和跨国犯罪核心领域的共同牵头国。

在业务层面上，国家计算机应急小组与全球各国的国家计算机应急小组组织保持着密切的工作关系。在澳大利亚，该小组积极参与并促进在全球一级分享可靠和及时信息，包括威胁和脆弱性信息，以确保维持对态势的了解并对在线威胁做出一致和协调的全球应对。该小组积极促进能力建设举措，特别是在亚太地区，包括加入亚太计算机应急小组。该小组认识到信息安全不受地域限制，因此还通过加入事故对应和安全小组论坛和国际观察和警报网络与其他伙伴密切合作。

国际社会为加强全球一级的信息安全可能采取的措施

包括澳大利亚在内的所有国家都需继续寻找能加强信息安全的传统和创新措施。要迎接网络安全方面的全球性挑战就必须加强在多边论坛的努力，以改善可互操作网络的安全。这包括在联合国和国际电联内所作的努力，以及在类似亚洲-太平洋经济合作组织这样的区域论坛和具有更具体主题的国际小组（如事故对应和安全小组论坛和国际观察和警报网络）内所作的努力。

澳大利亚支持拟订关于网络空间负责任行为的国际原则，包括商定一套广泛的网络空间规范行为原则，以促进在网络方面进行更好的国际合作并加深信任，最终拟定商定的国际网

络空间规范。澳大利亚作为国际社会的一员将继续支持通过双边和多边论坛在这一问题上取得进展，以帮助实现一个更安全、更具有弹性和更可靠的网络环境。

国际社会为加强全球一级的信息安全可做出的具体努力包括：

(a) 拟订全球标准，包括商定一套广泛的网络空间规范行为原则，以促进进行更好的国际合作并加深信任；

(b) 扩大国际法律体系打击网络犯罪的能力，包括法律框架的一致性(例如，使更多的国家加入《欧洲委员会网络犯罪问题公约》，澳大利亚预计将在2011年底前达到其要求)，和加强执法合作，以使各国能有效制定国内法；

(c) 发展和推广对态势认识、战略预警和事件应对方面的最佳做法，包括发展各国的国家计算机应急小组，以在各国间开展和协调这类活动；

(d) 由经验丰富和机构健全的国家采取提高认识举措和开展能力建设活动，以协助发展中国家实现一个可造福于所有人的可靠、安全和有弹性的网络空间；

(e) 采用更为一致的方法与行业结成伙伴关系，以拟订网络空间的行为导则，如澳大利亚因特网行业业务守则。

有关国际概念

现行国际法为预防来自各种行为者的信息安全威胁提供了一个保护框架。各种现行国际法原则可适用于网络空间的使用，包括各国主权平等原则和禁止使用武力和禁止侵略行为，以及国际人道主义法。需要在各国间、国际和区域论坛继续进行讨论，以更确切地确定这些原则对来源于网络领域的威胁的适用范围和适用性。

格鲁吉亚

[原件：英文]
[2011年6月1日]

就格鲁吉亚而言，信息安全问题在2008年8月之后得到了特别重视，因为当时俄罗斯联邦对格鲁吉亚展开了猛烈的分布式拒绝服务攻击。

根据对这些事件的评估并鉴于近期正在迅速大规模发展电子政务项目和服务，因此信息安全成了国家安全概念中的一个重要方面。为改善对信息安全的监管，格鲁吉亚政府近年来一直在采取一些重大举措。

2010年，格鲁吉亚司法部成立一个法律实体——数据交换机构，直接负责拟订和执行政府部门的信息安全政策。在成立数据交换机构之后，格鲁吉亚政府发展了可协调实现电子政务和信息安全的机构机制。

数据交换机构在法律及其《章程》规定的职能框架内与格鲁吉亚司法部合作，执行和引入符合(ISO)27000国际标准的信息安全政策。该机构还协调执行和引入国家和企业部门信

息安全所需的机制或标准，特别是开展具有各种意义的活动。在这些活动中，最重要的一项活动就是每年举行的格鲁吉亚信息技术创新会议；该会议的议程总是与信息和网络安全有关，并得到该机构授权可拟订和执行有关提高公众对信息和网络安全问题认识的政策。

就日常的网络安全问题而言，数据交换机构负责建立计算机应急小组及其运作；目前该小组在该机构之下发挥职能，管理格鲁吉亚网络空间的信息安全事件。该机构还监测格鲁吉亚政府网络的运作以保障其安全。

该机构在信息和通信技术方面的职能还包括提高专业教育水平(以培训信息安全专才)、起草建议、监测安全和发放数据签名证书。在专业教育方面，该机构计划在国际捐助方(如欧洲联盟和世界银行)的帮助下开展一些特别项目。这些项目将确保使专业教育达到适当水准。至于数字签名安全，该机构将在民事登记局开始发放公民电子身份证(印有数字签名)时履行这一职能。

除了作为信息安全牵头和协调机构的数据交换机构所开展的活动外，还应强调格鲁吉亚政府目前所采取的其他举措，而数据交换机构也积极参与了这些举措：

(a) 在格鲁吉亚国家安全委员会之下成立了负责网络安全战略和行动计划的专家工作组（将在下阶段做出具体定义）；

(b) 正在拟订一些立法倡议，包括行政法和国家保密法，计划在2011年提交议会。应特别提及数据交换机构现正拟订的关于“信息安全”的法案，计划在2011年提交议会审议；

(c) 2010年，格鲁吉亚司法部和格鲁吉亚财政部在该机构的帮助下拟订了信息安全内部条例（政策和导则），现正开始实施。计划在政府其他机构采取类似举措。

德　　国

[原件：英文]
[2011年6月6日]

近年来网络空间的安全态势发生了根本性变化。一方面，我们可以看到技术驱动的创新过程正在发挥作用：越来越多的业务流程管理实现了电子化和相互连通，有时直接或间接连上了因特网。信息技术系统的复杂性不断加深。创新周期越来越短。另一方面，有组织犯罪和其他非国家行为者正在不停地攻击信息技术网络、数据库和网站。在某些情况下，这类攻击产生的影响尚未得到实事求是的评估。

正是出于这个原因，联邦政府在2011年2月通过了一个新的网络安全战略。该战略的核心就是保护关键基础设施。所有涉及网络安全问题的政府机关都要密切合作，并通过新设立的网络应对中心与其他机关和私营部门直接联系，以期快速侦测和分析重大信息技术事故，提出有关保护性措施的建议。至于政策，新成立的国家部长一级的网络安全委员会负责处理关键的网络安全问题和形成德国对这些问题的立场。

这包括协调网络外交政策，包括外交、国防、经济和安全政策等各个方面。在网络空间的国际相互连通意味着必须在国际一级采取协调行动。因此，德国将在欧盟和国际组织大力倡导加强网络安全。

鉴于信息技术的全球连通性，德国在其网络安全战略中倡导拟订广泛、无争议、具有政治约束力的网络空间国家行为规范。这些规范应得到国际社会大部分成员的接受，并应包括能建立信任和增强安全的措施。

网络空间的信任和安全建设措施

网络空间是一项公益物和一个公共空间。因此，我们必须从基础设施的弹性及系统和数据的完整性和故障安全性的角度来考虑网络空间的安全。既然是公共空间，各国就必须促进网络空间的安全，特别是针对犯罪和恶意活动的安全性，保护那些选择使用真实性工具的人免遭身份盗窃，确保数据和网络的完整性和保密性。

网络空间是全球性的。要确保网络安全、执行权利和保护关键信息基础设施，国家就必须在国家一级并与国际伙伴合作做出重大努力。

在此背景下，德国准备就一整套涉及网络空间内国家对国家行为的行为规范展开工作，特别包括信任、透明度和安全建设措施，并希望得到尽可能多的国家的签署。

德国最近在2011年5月9日至10日举行的欧洲安全与合作组织（欧安组织）关于网络安全的会议上就这样一个关于国际规范的行为守则作了如下概述：

(a) 确认关于数据和网络可用性、保密性、竞争性、完整性和真实性、隐私和知识产权保护的一般性原则；

(b) 尊重保护关键基础设施的义务；

(c) 加强旨在建立信任、减少风险措施、透明度和稳定的合作，具体做法是：

- 交流与国际监管网络空间有关的国家战略、最佳做法和国家看法；
- 交流对与网络空间使用有关的国际法律规范的国家看法；
- 设立和通报联络点；
- 设立预警机制和加强各国计算机应急小组之间的合作；
- 将危机通信链升级以包含网络事故，支持拟订可促进建立稳健和安全的全球网络基础设施的技术建议；
- 在打击恐怖主义的责任中包含交流对付非国家行为者的做法并加强有关合作；
- 支持发展中国家的网络安全能力建设，为大型活动（如奥林匹克运动会）的网络安全支助工作拟订自愿措施。

此外，我们认为有必要就下列方面展开辩论：在确定网络攻击的归属方面进行国际合作，因为网络攻击的归属通常很难追踪；国家对于从其领土上发动的网络攻击在得到有关这类攻击的通报之后仍不采取行动结束这类攻击所应承担的责任；国家在不促成网络空间的无法无天状态方面所应承担的责任，例如在知情的情况下容忍在其领土上储存以非法手段收集的个人数据。

网络安全的军事层面

由于军队在所有指挥层级都越来越依赖信息技术以掌控日益复杂的情况，对信息的保护及处理信息的手段已成为首要任务。

但是，在军方的考虑中，信息安全面临的挑战不仅来自知道如何操纵武器实际摧毁信息基础设施的潜在对手，而且还来自不负责任的用户、技术故障、罪犯或单纯的意外事件。

因此，需要做出的努力包括提高每一个用户的认识，确保信息技术供应链的可靠性，采取对应性防御措施以抵御网络攻击，以及建立一个具有整体弹性的信息技术构架。

总之，需要进行全面风险管理，采取措施加强国家和全球层面上的信息安全。

德国联邦国防军在国防军所有部门建立了有弹性的指挥和控制架构、安全技术和程序，以及信息技术安全组织，包括一个独立的计算机应急小组，在出现关键性信息技术运作故障时可进行干预。使个人能力和技术能力适应日益严重的威胁是一项永久性任务。

德国联邦国防军与德国联邦内政部密切协作做出努力，大力支持加强北大西洋公约组织（北约）和欧盟的信息安全，并为此目的制定政策和建设能力。此外，德国联邦国防军与一些国家就政策层面和工作层面的信息安全问题进行定期交流。

德国联邦国防军欢迎提出倡议，并与德国联邦政府其他部门就国际行动进行合作，以进一步保护全世界信息网络的可用性，例如拟订网络空间的自愿国际行为守则。

北约的网络防御

北约将网络安全定为新兴的关键性安全挑战之一。2010年11月在里斯本举行的北约首脑会议上经国家元首和政府首脑通过的《战略概念》指出：“网络攻击……可达到一个威胁国家和欧洲–大西洋繁荣、安全和稳定的门槛。”

国家元首和政府首脑在《首脑会议宣言》中给北约理事会规定了如下任务，“尽量利用现有的国际结构并根据对我们目前政策的审查结果，在2011年6月底前完成拟订北约深入的网络防御政策，并为执行这项政策起草一份行动计划”。

作为新政策的第一步，北约国防部长于2011年3月通过了一个网络防御概念。

该概念侧重于保护北约的网络和与北约网络相连或处理北约信息的成员国国家网络（包括拟订共同原则和标准，以确保在所有成员国内实现最低限度的网络防御）。为减少来自网

络空间的全球性风险，北约打算与伙伴国、类似联合国和欧盟这样的有关国际机构、私营部门和学术界合作。

德国欢迎北约就网络安全做出承诺并积极支持有关讨论。

欧洲安全与合作组织的网络安全

欧洲安全与合作组织讨论网络安全问题已经有好几年了。在2010年在阿斯塔纳举行的欧安组织首脑会议上，欧安组织56个与会国的国家元首和政府首脑强调，“在面临新兴的国际威胁时，必须实现目的和行动更大程度的统一”。《阿斯塔纳纪念性宣言》把网络威胁称为这些新兴的国际威胁中的一个威胁。

德国积极参与了2011年5月9日至10日在维也纳举行的欧安组织全面应对网络安全：探索欧安组织未来作用的会议。在会议期间，讨论了有关欧安组织后续活动的具体建议。

德国将继续支持欧安组织展开讨论，以探索欧安组织在网络安全领域的未来作用。

希　　腊

[原件：英文]
[2011年6月6日]

对信息安全问题的讨论比以往任何时候都更为广泛。现正考虑对目前网络和系统全球化所带来的威胁采取何种反制措施。在国家和国际上研究并采取了维护信息自由流动的措施

目前的国际和多国概念得到追踪和研究。需要就风险评估进行国际指导。网络防御问题也应得到讨论。在全球分享信息方面应维护国家在信息安全上的主权权利。

应认识到，所有会员国都应继续向秘书长通报其对相关问题的看法和评估。在这方面，要注意以下几点：

(a)　所有信息安全相关问题都应置于高度优先地位；

(b)　跨越国家和国际边界研究和实行维护信息自由流动和规定必要程度的保密性、完整性、可用性的方法；

(c)　应在国家和国际一级起草和商定有关建设和分享能力的网络连通性概念。应推行网络连通性风险评估并提供相关国际指导。此外，由于各国一个非常严重的关切问题就是需要采取网络防御措施，因此就需要提供一致性的国际指导，以促进合作、效率和经济效益。最后但并非最不重要的是，不能忽视对国家维护其主权和维持其信息基地的要求，起草的每一个概念都应考虑到这一点；

(d)　国际社会为加强全球一级信息安全而可能采取的措施如下：

（一）详细阐明并商定有关国际概念；

（二）为统一的通用基础设施提出一个涵盖基本立法事项的指导计划，以为所有函件和短信的电子处理提供必要的信息安全，提供多种通信方式；

（三）应统一多国联盟和小国家集团遵循的概念，并扩大至全球一级施行。对任何设计好的复杂措施进行工程分析远不及就威胁的具体性质及其对人类的不利影响达成一致意见更为重要，因为对手也可能会利用这种分析结果；

（四）在进行上述所有工作的同时，应认识到，国家主权是任何全球化努力的基本参照物。应起草一个包含各种能反映所需的一体化程度假设情况的国际概念，以为国家信息交流网关提供定义，并作为在国家、多国和国际一级做出的所有努力的指南。

哈萨克斯坦

[原件：俄文]
[2011年6月7日]

为确保信息和通信技术的网络安全，哈萨克斯坦共和国于2010年成立了计算机应急小组。

在这方面，从哈萨克斯坦网用户处收到的在哈萨克斯坦网域或由哈萨克斯坦服务器提供服务的网站所发现的任何有关病毒、安全代码、软件机器人系统或非法要求（色情、暴力、侵犯版权等）的信息将送交计算机应急小组进行分析。

荷　　兰

[原件：英文]
[2011年6月6日]

对信息安全问题的一般看法

荷兰支持安全和可靠的信息和通信技术，支持保护一个能尊重人权的开放、自由的因特网。安全和可靠的信息和通信技术对我们的繁荣和福祉至关重要，是实现可持续经济增长的催化剂。

信息和通信技术提供了机会，但也使我们的社会变得更为脆弱。威胁的跨国界性质使得国际合作必不可少。许多措施只有在得到国际共同执行或协调的情况下才能有效。在这方面，荷兰极为重视公共部门与私营部门的伙伴关系，以及使用信息和通信技术的用户的个人责任。

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

荷兰正在国内和国际上做出努力，以建立一个安全的数字环境。在国家一级，荷兰政府于2011年2月提出了一个题为“通过合作得到加强”的国家网络安全战略。2011年7月作为该

战略的组成部分，政府将成立国家网络安全委员会，以确保在公共部门、私营部门和学术研究机构之间采取协作方法。政府还将设立国家网络安全中心，以确定趋势和威胁，并帮助管理事故和危机。中心的一个主要任务是根据来自公共和私营方面的信息进行网络威胁分析。中心将包括现有的政府计算机应急小组。

在国际上，荷兰积极协助欧盟、北约、因特网治理论坛、国际电联和其他伙伴关系做出努力。荷兰促进在各网络安全中心（包括国家计算机应急小组组织）之间进行实务合作，加强国际观察和警报网络。网络犯罪迅速增多，这就需要进行有效执法以维持对数字社会的信心。关于执法工作，荷兰意图鼓励来自其他欧洲国家及欧洲以外国家的执法机构进行更多的跨界调查。荷兰是《欧洲委员会网络犯罪问题公约》的缔约方，并鼓励其他国家加入该公约。

国际社会为加强全球一级的信息安全可能采取的措施

荷兰认识到，必须就旨在实现安全使用网络空间的国家行为标准的拟订工作继续进行对话。荷兰愿意对这一对话做出积极贡献。荷兰的出发点是，建立一个能促进创新、刺激经济增长和保障基本自由的开放的因特网。

荷兰认为，很有必要让私营部门和知识机构参与这一对话，并愿意与其他国家分享经验和最佳做法。要使网络空间更为安全和可靠，就必须在所有利益攸关方和各组织之间就知识和信息进行密集的国际交流。在施行现行国际法律框架方面的一致性是值得国际重视的另一个重要问题。

美利坚合众国

[原件：英文]
[2011年6月7日]

一、导言

信息和通信技术对于所有会员国的发展都至关重要。这些技术连接在一起创建了网络空间，有助于实现在2003年和2005年举行的信息社会世界首脑会议所设想的关于信息社会的共同愿景。信息和通信技术有益于日常生活的基本功能、商业及商品和服务的提供、研究、创新、创业，以及信息在个人、组织和政府之间的自由流动。这些技术是一项强大的新工具，促成电子政务，促进经济发展，便利提供人道主义援助，并使关键的民用、公共安全和国家安全基础设施发挥作用。此外，网络通信在减少国际了解和合作障碍方面所能发挥的潜在作用再怎样强调都不为过分。

尽管对信息和通信技术的依赖日益加深，但与这种依赖性相连的风险也在增加。各种天然和人为的事件和活动威胁着国家关键基础设施、全球网络的可靠运作，威胁着运行于或储存在这些设施和网络中的信息的完整性。人为威胁的数量、复杂性和严重程度都在加大。有一些是来自国家方面的，但许多来自非国家行为者，涉及犯罪或恐怖活动。动机各异，从盗窃钱财或信息、扰乱竞争对手，到民族主义和将国家冲突的传统形式延伸到网络空间，不一

而足。这些威胁行为者将个人、公司、国家关键基础设施和政府都当成目标，对各个国家和全球相连的整个国际社会的福祉和安全造成了严重后果。

不管各国政府为保护其信息网络在国内采取何种国家措施，就减少信息和通信技术风险的战略进行国际协作对于确保所有国家的安全而言都必不可少。各国政府必须有信心，相信支持其国家安全和经济繁荣的网络是安全和有弹性的。实现可靠的信息和通信技术基础设施将确保所有国家都实现信息革命的潜力。

这项任务并不容易。国际社会面临的挑战是，要维护一个既能促进效率、创新、经济繁荣和自由贸易同时又能促进安全、安保、公民自由权利和隐私权的环境。这项任务的困难因信息和通信技术的独特属性而难上加难：所有人都可利用、网络通常由私营部门而不是由政府拥有和营运。与传统武器不同的是，破坏性的信息技术工具是隐形的，无法看见的。对这类工具的使用可穿越许多国家，很难确定其起始点、身份和肇事者的赞助方。非国家行为者正不断发展能力，使国家或非国家行为者越来越有可能利用代理人参与网络空间的破坏活动。这些属性使传统战略，如类似用于军控的措施，失去控制或遏制威胁行为者的效力；因此，需要采用创造性的新方法来减少风险。尽管任务艰巨，但会员国仍须团结在共同目标之下，通过保障信息技术的安全和完整性来维护和加强信息技术可以做出的贡献。

会员国的任务有两个方面：国内的和国际的。确保国家信息基础设施的安全是政府在国内与有关民间社会利益攸关方协调下必须领头担负的责任。同时，国内的努力应得到在为解决对网络化信息系统的各种威胁的跨国性质而制定的战略方面的国际协作的支持。这些努力应包括关于事故管理、减少和应对、跨国犯罪调查和起诉方面的合作；关于改善网络基础设施稳健性的技术建议；以及确认国际共享的行为规范，同时采取旨在加强稳定和减少误解风险的建立信任措施。

二、威胁、风险、脆弱性

针对构成网络空间的系统网络和在网络空间中运行的信息的威胁是21世纪严重的全球挑战之一。国家和非国家行为者可通过信息和通信技术把普通公民、商业、关键工业基础设施和政府当作目标。信息和通信技术、因特网及其他基础设施的会集创造了前所未有的可使电信、电力、油管和炼油厂、金融网络和其他关键基础设施瘫痪的机会。

信息技术的独特特点便利将其用于破坏活动，严重挑战力求减少风险的各国政府。与传统军事技术不同，构成网络空间的网络不是由政府垄断的，在许多情况下是由私营部门拥有和运营的。信息技术本身是广泛可用的技术，不具有固有的民用或军用性质，如何使用这类技术完全取决于使用者的动机。

所有人都可免费获得可用于破坏的软件工具，至少可获得基础工具。只要掌握必要技能，任何人都可以开发更为复杂的方法。此外，这些工具变化迅速，可利用新发现的脆弱性。这类工具在传统意义上是看不见的，相当隐秘，可能带有易于模仿的隐性“签名”。由于因特网的性质，恶意代码在到达其目标之前可越过许多国家的领土，从而使确认其始发点的工作变得极为繁重、费时，往往需要大量跨国合作。即使发现了始发点，肇事者或赞助者

的身份仍可能无迹可寻。因此，恶意行为者可以而且几乎正从地球任何地方进行秘密运作，并在很大程度上可逃脱惩罚。

身份的模糊性因网络入侵动机的模糊性而变得更为复杂。有组织的犯罪分子和其他个人或团体可能为促进自身的利益而采取行动，但也有可能被国家和非国家行为者招募作为代理人。缺乏及时的高可信属性和哄骗的可能性可能对政府造成不确定性和混乱，从而加大在重大网络事故中危机不稳定性、误导反应和丧失升级控制的潜在可能。

对网络空间的可靠运作构成威胁的主要行为者包括：

(a) **犯罪分子**。很多恶意工具起源于有组织的犯罪分子和黑客所作的创业努力。犯罪活动的复杂性和范围日益加大，突显了网络空间恶意活动在影响国家竞争力、导致普遍减弱对因特网用于商业和贸易的信心，甚至致使民用基础设施瘫痪方面所具有的潜力。这些活动的数量和范围都在不断加大；

(b) **国家**。有越来越多的传闻性公开报道，说国家正在发展和利用将国家冲突传统形式延伸至、利用或通过网络空间的能力。但是，有关在普遍认为是国家赞助的事件背后的来源或意图的确凿证据仍然无处可寻。通常的情况是，只能从涉及某一事件的目标、效果和其他旁证来推断肇事者的身份和动机；

(c) **恐怖分子**。恐怖分子目前尚不具有破坏信息网络或通过使用信息和通信技术实施具有物理效应的作业的能力，但不能排除今后出现这种能力的可能性。大多数专家认为，恐怖分子目前依赖信息和通信技术来招募人员、进行组织活动和筹集资金。因恐怖分子利用因特网而产生的具体威胁可能包括利用因特网来组织和展开具体的动能恐怖攻击；

(d) **代理人**。让人越来越感到关切的是出于金钱利益或民族主义或其他政治动机而代表其他人，不管是国家还是非国家行为者，从事在线恶意活动的个人或团体。据报告，“软件机器人大师”可向出价最高的人提供各种恶意服务。信息技术的独特属性向这类行为者提供了高度的匿名性，有效地掩盖了与赞助者的任何关系，使赞助者可做出听起来可信的否认。

国家在应对这类威胁时所面临的挑战很艰巨。信息和通信技术的属性意味着，这些威胁行为者的每一个行动可能只能从其效果中才能看到。因此，无法及时得到肇事者的高可信身份属性（如果有的话），是否能成功往往依赖高度的跨国合作。代理人的作用越来越大使分析属性的程序进一步复杂化，因为受害方不仅必须确认肇事者，而且还必须确认赞助者，这就使得这一挑战在今后变得更为麻烦。

要迎接这类挑战，各国政府就需要在国内组织和领头做出努力，为通信和信息基础设施发展和部署具有弹性的分层防御，而不管威胁的来源在何方。同时，这些威胁的复杂跨国性使国际协作成为必要，以便在全球基础上实施解决各种风险的战略。

三、行为原则、规则和规范

A. 国家在保证网络安全方面的责任

过去10年中，会员国已经认识到本国有责任在国内采取系统性步骤，保护自己免受网络安全威胁，并确认有必要进行国际合作。联合国大会有5项决议提请注意各国政府可采取用于减少其安全风险的基本防御措施。虽然这些决议的目的是为了提高认识，但同时也为了网络安全而推动一些涉及个人和国家行为的有用规范：

(a) 大会在关于打击非法滥用信息技术的第55/63号决议中强调，需要有现代化的有效国家法律来充分起诉网络犯罪并促进及时进行跨国调查合作；

(b) 大会在第56/21号决议中特别提及国际和区域组织在打击高技术犯罪方面的工作，包括欧洲委员会在拟订《网络犯罪问题公约》方面的工作：

> 联合国和其他组织一直在该领域展开密集活动。关注非法滥用因特网问题的联合国主要组织包括联合国毒品和犯罪问题办公室、预防犯罪和刑事司法委员会、联合国预防犯罪和刑事司法大会、国际电信联盟和其他组织；

(c) 大会在第57/239号决议中特别强调会员国在为创造全球网络安全文化和保护关键信息基础设施所作努力时应考虑的行动。可将这些行动视作政府应采用的一整套规范，这些规范为促进国际协作减少风险提供了基本基础或前提；

(d) 大会在第58/199号决议中特别强调会员国在为创造全球网络安全文化和保护关键信息基础设施所作努力时应考虑的行动。可将这些行动视作政府应采用的一整套规范，这些规范为促进国际协作减少风险提供了基本基础或前提；

(e) 大会在第64/211号决议中邀请所有会员国利用所附的自我评估工具详细评估本国至今在上述领域及其他领域所作的努力，并分享那些可协助其他会员国做出努力的成功措施和最佳做法。

B. 在敌对行动情况下可适用的规范

尽管信息和通信技术的属性独特，但仍可以现行的国际法原则作为适当框架来确定和分析应用于制约敌对行动情况下网络空间使用的规则和规范。在这方面可考虑两个不同但相关的法律体系：*诉诸战争权和战时法*。前面一个体系提供的框架可用于考虑在网络空间发生的事件是否上升为可触发一国采用自卫权的武力使用水平。后一个体系提供的框架可用于确定应用于制约武装冲突情况下网络空间使用的规则。

诉诸战争法。制约使用武力和自卫的法律框架的大部分内容来源于《联合国宪章》的三项规定：

(a) 《宪章》第二条第四款规定，“各会员国在其国际关系上不得使用威胁或武力……，侵害任何…国家之领土完整或政治独立”；

(b) 《宪章》第三十九条将安全理事会定为仲裁者，负责断定是否发生了威胁和平、破坏和平的情况或侵略行为，并要安全理事会提出建议或做出决定，以根据《宪章》第四十一条或第四十二条采取适当的对应措施；

(c) 《宪章》第五十一条认可并加强了如下原则："联合国任何会员国受武力攻击时，在安全理事会采取必要办法，以维持国际和平及安全以前，本宪章不得认为禁止行使单独或集体自卫之自然权利。"

要就一项在网络空间发生的破坏活动是否构成可触发自卫权的武装攻击达成一个明确的法律结论可能会很困难。例如，当威胁行为者和动机不明、作用的结果也未直接造成大量死亡或实际破坏时，有可能会对是否发生了武装攻击做出不同的结论。但是，这种模糊不清和出现分歧的可能性并不意味着需要拟订一个专用于网络空间的新的法律框架。相反，它们只反映出在施行《宪章》时所出现的挑战，而这类挑战在许多情况下早已存在。然而，在某些情况下，在网络空间发生的一项破坏活动可能构成武装攻击。在这种情况下，应适用以下既定原则：

(a) 对迫在眉睫或实际发生的武装攻击应用自卫权，不管攻击者是国家行为者还是非国家行为者；

(b) 自卫时的武力使用必须限于为解决迫在眉睫或实际发生的武装攻击所必需的，并必须与所面临的威胁相对称；

(c) 各国需采取一切必要措施，确保其领土不被其他国家或非国家行为者用于针对另外国家及其利益的武装活动的目的，包括策划、威胁、实施或为武装攻击提供物资支持。

战时法。武装冲突法规定了适用于进行武装冲突的规则，即战时法，包括在武装冲突情况下信息技术工具的使用。特别是，武装冲突法的下列关键原则在判断武装冲突时网络攻击的合法性方面发挥重要作用：

(a) 区分原则要求将攻击局限于合理的军事目标，民用物体不应成为攻击对象；

(b) 对胡乱攻击的禁止包括禁止实施采用无法合理指向特定军事目标的作战手段或方法的攻击；

(c) 对称性原则禁止实施预期可能造成平民生命附带损失、平民受伤害或民用物体受破坏并在程度上超过所预期的具体和直接军事优势的攻击。

这些原则禁止攻击纯粹的民用基础设施，因为干扰或摧毁这些设施并不会带来有意义的军事优势。此外，在攻击一个军事目标之前必须评估附带损害的潜在性。换句话说，对信息技术攻击也必须做目标设定分析，就像传统上为使用动能（常规和战略）武器的攻击所作的分析一样。

虽然上述原则已确立并适用于网络空间的情况，但在网络空间活动的情况下解释这些法律体系确实会出现新的独特挑战，需要在各国间进行协商与合作。这并非不寻常。当新技术得到开发时，它们经常给现行法律体系的应用带来挑战。

C. 代理人的使用

信息和通信技术的独特属性给各国带来了新的挑战，使用代理人从事破坏行动就是其中一个例子。通过代理人采取行动极大地提高了国家参与攻击而又可听起来可信地进行否认的能力。虽然现行国际法有关于使用雇佣军的规定，但是在网络空间使用代理人的做法引起了具有广泛影响的新的重大问题。各国需要共同努力，制订解决该问题的有效方法。

D. 允许信息自由流动的责任

有关言论自由和信息自由流动的权利载于《世界人权宣言》和《公民及政治权利国际公约》；这些权利普遍规定，除受某些限制外，每个人都有言论自由的权利，包括不受干扰地保持看法的自由，以及通过任何媒介和超越国界寻找、接收和传授信息的自由。这些原则已在众多的国际论坛上得到确认，包括大会、国际电信联盟和信息社会世界首脑会议等。

E. 打击恐怖主义的责任

现在至少有16项安全理事会决议呼吁各国打击恐怖主义。这些义务全面适用于恐怖分子或恐怖主义协助者利用网络空间招募人员、筹资、转移资金、购买武器或策划攻击的情况。所有国家都有义务在尊重其他国家主权及本国在允许信息自由流动方面的责任的情况下，分享有关在线恐怖主义融资、招募人员、策划和协助活动的信息，并采取应对行动。

四、 透明性、稳定和减少风险及合作措施

正如上文所概述的，会员国面临着管理一个高度多样化和复杂的威胁环境的挑战。过去10年中，国际上展开了打击网络犯罪威胁的广泛努力。美洲国家组织、亚洲-太平洋经济合作组织、西非国家经济共同体、非洲联盟和欧洲委员会等展开了调查和起诉网络犯罪方面的培训工作。通过《网络犯罪问题公约》及通过受害国之间的双边努力，在调查和起诉网络犯罪方面实现了广泛的国际合作；在应对犯罪活动对信息和通信技术的威胁时，国际合作仍然是最有效的方法。

受到跨国关切的其他领域亦须得到类似的关注。这些领域包括因对与国家在网络空间的行为有关的国际规范缺乏共同理解而出现误解的风险，这将影响出现重大网络事件时的危机管理工作。这就需要拟订措施，以加强合作和建立信任，减少风险或加强透明性和稳定：

透明性措施

- 交流国家网络安全战略和最佳做法（已获得的经验教训）；
- 交流国家对关于使用网络空间的国际规范的看法；
- 交流专门负责网络安全的国家组织结构和联络点。

稳定和减少风险措施

- 建立或更新通信链及相关协议，以纳入网络事件；
- 加强合作以应对有组织的非国家行为者（罪犯、恐怖分子、代理人）；
- 建立程序，以允许在国家计算机安全事件应对小组之间进行日常信息交流。

合作措施

- 支持在较不发达国家进行网络安全方面的能力建设。

四、A/65/154

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

一、导言

1. 大会在第64/25号决议第3段，邀请所有会员国继续向秘书长通报其对下列问题的看法和评估意见：

(a) 对信息安全的一般看法；

(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) 该决议第2段所述概念的内容；

(d) 国际社会为加强全球一级信息安全可能采取的措施。

2. 按照这项要求，2010年2月26日向各会员国寄发了一份普通照会，请它们就这一主题提供资料。所收到的答复载于下文第二节。以后再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

古　　巴

[原件：西班牙文]
[2010年5月27日]

1. 古巴完全赞同大会第64/25号决议中所表达的关于以下方面的关切：信息技术和媒体可能会被用于不符合维护国际稳定与安全宗旨的目的，可能对别国基础设施的完整性产生不利影响，损害其民用和军事领域的安全。该决议还适当地强调了有必要防止为犯罪或恐怖主义目的利用信息资源或技术。

2. 古巴重申，充满敌意地使用电信并公开或隐蔽地意图破坏别国的法律和政治秩序的做法，违反了有关此问题的国际公认准则，也是负面和不负责任的，可能会引起紧张局势和不利于国际和平与安全的情况，从而破坏《联合国宪章》所体现的原则和宗旨。

3. 古巴关切地提请关注下列事实，即当信息和电信系统被设计和/或被用于破坏别国基础设施时，这些系统就可能变成武器，从而危及国际安全与和平。

4. 在这方面，古巴重申其在不同国际论坛上表达过的谴责，即谴责历届美国政府通过对古巴开展广播和电视战，使这一侵略不断升级。这明显违反现行的管理无线电频谱的国际规则。

5. 美国政府毫不顾忌其可能对国际和平与安全造成危害，比如通过制造危险状况如未经协议而使用军用飞机向古巴传送电视信号。

6. 从美国领土对古巴发动广播-电子侵略违反了规范国家间关系的国际法以及国际电信联盟（国际电联）的准则和规章，这些法律法规规定了联合国系统这一专门机构的成员国应该采取的行动。

7. 每个星期，位于美国领土的广播电台在34个不同的中波、短波、调频和电视频率，传送上千小时的广播和电视节目。2010年3月，每星期非法传送2 156个小时的节目。其中一些广播公司属于与广为人知的恐怖分子有关联的组织或为其提供服务，这些恐怖分子住在美国领土并同美国当局达成全面协议，从事反对古巴的活动。

8. 针对古巴的非法广播和电视节目并不提供新闻；相反，是为了颠覆目的，而捏造和歪曲新闻。对于这种行为，美国国会每年从联邦资金中核准3 000万美元的预算。自两家广播公司开始活动以来，美国政府已为此目的花费6 598亿美元。

9. 对古巴的挑衅性广播违反了以下国际原则：

- 《国际电信联盟章程》序言部分的基本原则，即电信对于维护和平及所有国家的经济社会发展日益重要，通过有效的电信服务手段，实现促进各国人民间的和平关系与国际合作以及促进经济社会发展的目标。美利坚合众国政府对古巴播出的电视节目内容，具有颠覆性、破坏性和欺骗性，是与以上原则相抵触的。
- 《国际电信联盟章程》第197条和第198条规定，所有电视台都必须在不对其他成员国广播服务或通信造成有害干扰的情况下，有效建立和运行。
- 2007年11月举行的世界无线电通信大会第九届全会协议第6.1段(g)分段规定：“航空器运营的任何广播站，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8.3条规定，其他国家政府在分配本国频率时，应考虑到已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42.4条，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。
- 国际电信联盟无线电规章委员会在2004年12月第35次会议上提出的裁决指出，美国在213兆赫的广播对古巴节目服务造成有害干扰，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

政府采取有关措施，消除在509兆赫的干扰，但至今没有答复。2009年3月20日，该委员会第五十次会议及其决定概要（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。国际电信联盟无线电规章委员会在2010年3月26日第五十三次会议上，重申其结论，即从美国从事的广播对包括在国际频率登记册上的古巴广播电台造成有害干扰，并敦促美国当局消除该有害干扰，要求无线电通信局监测有关情况，并按《无线电规章》规定的程序采取行动。

– 国际电信联盟《无线电规章》第23.3条限制向国外播放电视节目。

10. 2009年1月美利坚合众国政府问责局（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违反了国际法准则和国内立法。

– 该报告回顾，国际电信联盟在2004年和2006年认定，美国在13和20频道的播放对古巴电台造成了有害干扰，而美国国务院没有采取任何行动回应国际电联的裁决。报告还指出，2007年11月举行的世界无线电通信大会认为，从航空器播放的做法不符合国际电联规章。

– 该报告指出，尽管美国法律禁止在国内传播这种类型的广播节目，但在美国领土内、主要在迈阿密均能接收到这类的广播和电视转播，一些合同广播电视台播送政治广告和提供性服务产业的广告。另外，报告还注意到，对古巴的广播没有遵守新闻的平衡和客观标准，使用了煽动性和攻击性的语言。

11. 古巴进一步回顾，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（WRC-07）通过的结论文件认定，美国从航空器对古巴的无线电播放违反了《无线电规章》。全体会议通过的结论规定：“从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，则被认定不符合《无线电规章》。”

12. 这些结论是2007年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，即对航空气球针对古巴领土播放电视节目构成违反《规章》的规定。

13. 美利坚合众国政府对古巴的敌对态度，在其近50年来的经济、商业和金融禁运中彰显无疑，这一禁运也影响到信息和电信领域：

– 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域名的因特网地址(IP)，就会遭到拒绝。

– 在没有事先通知的情况下，外国资产管制处(外资管制处)禁运了与古巴有联系的.com域名。

– 由于美利坚合众国政府实施经济、贸易和金融禁运的法律规定，古巴无法连接到围绕古巴群岛的光纤电缆，迫使古巴支付卫星服务，这种服务具有带宽的限制、获得必要技术的难题以及高昂的连接成本。

– 因特网被用来进行针对古巴的诽谤运动，以便颠覆和诋毁古巴。

14. 美国的这一态度，破坏了2003年和2005年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。

15. 该首脑会议强烈敦促各国，在建设信息社会时采取措施，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。

16. 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采取的行动，说明了这一辩论很有必要，迫切需要找到制止这种表现的办法。

17. 古巴坚决支持联合国大会这一行动，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。古巴愿与包括美利坚合众国在内的其他国家进行协作，找到克服阻碍实现这些目标障碍的解决办法。

希　　腊

[原件：英文]
[2010年6月28日]

1. 人们比过去任何时候都更广泛地讨论信息安全问题。随着全球化的到来，对于其固有的现代威胁的反措施当然也在考虑之列。还研究了维护信息自由流动的措施，以及在国内外采用这些措施的问题。

2. 遵循和研究了现有的国际和多国概念。需要提供评估风险的国际标准。应解决网络防卫的问题。应维护全球环境下，国家对信息安全的主权。

3. 据理解，所有会员国应继续向秘书长通报其对相关问题的意见和评估。在这方面，应注意下列几点：

(a) 所有信息安全问题均受到高度重视；

(b) 研究了采取何种方法维护信息的自由流通，提供必要程度的保密、完整性和可用性，并在国内外加以应用；

(c) 应草拟和商定国内国际分享网络链接的概念。必须进行网络链接风险评估，并提供有关国际指导准则。此外，由于各国一直严重关切采取措施保护网络安全的问题，必须制定统一的国际指导准则，以实现合作、效率和经济的目标。最后但并非最不重要的是，不能忽视一个国家维护其主权以及维护其信息基础的要求，起草的每一个概念均应考虑到这一点；

(d) 为加强全球一级信息安全，国际社会可能采取的措施如下：

(1) 详细拟定和商定有关国际概念；

(2) 可拟定统一的通用基础设施的指导性计划，其中涵盖基本立法事项，以便向注册用户提供电子处理所有往来邮件和短信所需的信息安全，并提供多种通信方式；

(3) 应统一和扩大多国联盟和小国群体所遵循的概念，并应用到全球。具体说明威胁及其负面影响的协定不应只是制定更复杂的措施，因为这些措施也可为对手所利用；

(4) 与所有上述情况同样重要的是，应把国家的主权理解为全球化努力的基本参考要素。应制定和作为指南应用一种国际概念，即在反映出适宜程度的一体化背景下，界定国家信息交换的网关，以利于国家、多国和国际三级的努力。

墨 西 哥

[原件：西班牙文]
[2010年5月18日]

信息安全问题概况

1. 墨西哥银行和金融机构以及联邦政府处理安全和国家安全的单位，都是在计算机安全领域做出最大努力的机构。联邦公共安全秘书处内设有网络犯罪股和网络警察股。

2. 另一方面，虽然政府这三个部门分别进行了打击网络犯罪的努力，但联邦政府没有指导打击墨西哥网络犯罪的网络安全政策，必须加强这方面的立法，法官在处理和惩治网络犯罪方面需要更多的工具，需要加强针对因特网服务提供者的条例，要求他们保持在其平台上所有活动的记录，一旦事件发生，可提供信息。还有必要就打击网络犯罪和破坏国家安全的网路恐怖主义签署国内协定并与其他国家做出合作安排。

国家一级采取措施加强信息安全和促进在这一领域的国际合作

3. 墨西哥目前正努力查明信息安全的情况：

(a) 惩治某些网络犯罪可援引以下法律：《联邦刑法典》；《联邦区刑法典》；《刑事诉讼法》；《科洛马数据保护联邦法》；阿瓜斯卡连特斯、锡那罗亚、塔瓦斯科和塔毛利帕斯等州的《刑法》；

(b) 2009年4月30日，墨西哥《政府公报》公布一项法令，在墨西哥合众国《政治宪法》第73条加入第XXIX-O节，授权国会就保护人民所拥有的个人数据进行立法；

(c) 2009年6月1日，公布了一项法令，为《宪法》第16条增加了第2款，其中确认所有人都有权保护其个人数据，有权以法律规定的方式，查阅、修改和删除这些数据并表达其反对意见。法律还提供了豁免以下原则的理由，即出于国家安全、法律和秩序、公众安全和健康或保护第三方权利的因素，指导数据处理工作的原则；

(d) 墨西哥国家自治大学计算机安全事故反应小组负责处理学术界安全问题，并在处理网络犯罪方面向墨西哥当局提供支持和技术咨询意见；

(e) 联邦警察部队设有网络警察单位，负责对公共安全犯罪行为进行后续调查工作；

(f) 政府正在编写一份关于网络脆弱性执行报告，以便通知政府高级部门全球网络事故的情况，从而组织和支持促进墨西哥网络安全的倡议；

(g) 计划在联邦政府内设立国家计算机安全事故应急小组(CSIRT)，[1]以协调打击国内外网络犯罪的努力；

(h) 网络脆弱性作为一个项目已列入国家风险议程；

(i) 在公共和私营部门的协调下，制定了提高普通公众对防止网络犯罪的认识的方案；

(j) 墨西哥参加了各种论坛，并与其他国家就网络犯罪问题签署了善意协定。

国际社会加强全球信息安全可采取的措施

4. 世界范围加强信息安全的措施如下：

(a) 通过适当的立法或根据需要更新现有立法，以保护网络空间的信息；

(b) 对法官进行网络安全问题的培训，使他们能够理解网络犯罪的性质，并做出适当判决；

(c) 成立国家计算机安全事故反应小组，以协调各项努力，处理好重大安全事件，并作为其他国家的联络部门；

(d) 各国计算机安全事故反应小组之间不断进行联络，使其在区域或全球发生事故之际能协调各自的应对措施；

(e) 组织论坛，以分享经验并培训作为国际社会成员的各个安全小组；

(f) 为合作打击网络犯罪做出国际安排，以便利调查并形成团结战线。

巴 拿 马

[原件：西班牙文]
[2010年6月21日]

1. 巴拿马共和国设有支持出于包括恐怖行为内的犯罪目的，不适当利用因特网的机构，其中包括国家安全委员会、法治和秩序部内法医研究所。

[1] 计算机安全事故应急小组。

2. 国家安全委员会从事的情报工作，是为了打击包括恐怖主义在内的有组织犯罪，以及有可能对财产和国家领土完整发动的攻击。

3. 根据2007年12月27日第69号法令，法医医学科学研究所设立了法律和秩序部，负责调查网络犯罪。

4. 我国《刑法典》规定利用因特网用于恐怖主义是犯罪行为，将予以镇压和惩治。第289条指出："任何人使用因特网，实施恐怖主义行为提供训练，或招募他人予以实施，都将处以5至10年监禁。"

5. 其他法律法规也惩处出于犯罪目的利用因特网的行为，并规定将进行刑事、民事和行政处罚，其中包括2007年5月18日第14号法令第八章；2008年7月22日第51号法令第一章（计算机安全罪），其中规范了电子文件及电子签名以及提供服务，并对电子贸易的发展做出了其他规定。1996年2月8日第38号法令颁布了指导巴拿马共和国电信业的规则。

卡 塔 尔

[原件：英文]
[2010年5月25日]

1. 卡塔尔国认为应按照《联合国宪章》和国际关系基本原则使用信息和通信技术。此外，保障信息的自由流通绝不应损害国家主权，同时应维护安全并尊重各国不同的文化、政治和道德。

2. 国家一级的努力基于通信安全的利益，以随时加强之并跟上国内国际的进展。

3. 国内努力可简述如下：

- 制定安全战略和政策，颁布法律，限制出于不符合保护安全稳定目标的目的运用信通技术。
- 建立加强信息安全的机制，确保保护卡塔尔敏感信息的基础设施。
- 因特网安全和情报办公室努力监测政府网络和国家网络，以应对通过因特网对卡塔尔国形成的威胁。
- 对因特网事件加以管理并协调解决事件的努力，其目的在于在最短的停机时间内，保证把上报的有关因特网问题解决好。在卡塔尔国，这项工作由卡塔尔计算机应急小组负责。
- 让信息发挥更有效的作用，意识到改善卡塔尔各机构雇员的技术技能水平和资格。
- 支持卡塔尔人处理好与因特网有关的问题。
- 采取后续行动，理解现代科学技术领域与因特网安全有关的最新进展。

- 促进国际关系，以处理与因特网有关的问题。卡塔尔国参加了事故对应和安全小组论坛以及Meridian进程。

4. 国际社会为促进国家一级的信息安全可采取的最重要措施如下：

- 联合国应继续领导这一讨论，并更多地澄清在电子战中使用信息、有线和无线通信技术的问题，现有国际法原则是否足以提供适当框架，以确定何为适当的在线行为，何为攻击性行径。
- 为建立有线和无线信息国际特设委员会，全面研究与此相关的问题。
- 卡塔尔国鼓励所有会员国建立工作队，在国家一级应对计算机紧急情况。
- 在通信领域，与专门的保安机构确定合同。
- 通过在地方和国际两级举行专题讨论会和会议，提高安全意识。
- 鼓励各国进行合作，以打击间谍活动和电子盗版活动。
- 使用加密和安全设备，以安全的方式转发信息和文件，以确保在交流时的保密性。
- 更新保护系统，定期举办讲习班，以盘点信息安全领域最新科技进展。

乌 克 兰

[原件：俄文]
[2010年5月12日]

从国际安全的角度来看信息技术和电信应用的成就

1. 信息技术在社会各种活动中的作用日益扩大，导致人们担忧信息的安全。随着先进的信息技术进入各国社会的日常生活，犯罪份子以及试图犯罪的人对信息和电信系统、对国家机构信息资源以及对商业实体的网络攻击越来越多。

2. 计算机犯罪案中有一半涉及未经授权获取计算机信息。为获利而实施计算机犯罪的行为也越来越多，这种行为造成的物质损失也越来越大。跨国黑客集团犯罪数量也在增加。

3. 计算机犯罪很少报告，确定这类罪行全部范围的努力往往受挫。受到这种攻击的政府和商业实体总是试图掩盖事实，以免承担失去其权威的风险，他们不愿意透露所遭受的损失及其信息保障系统的薄弱。因此，这类犯罪案件往往得不到报案，这说明有必要制定协调一致的防范和预防措施，这些措施是保护信息系统的核心。

4. 计算机犯罪通常只是一系列犯罪行为的第一步，这与盗窃、勒索、诈骗等传统类型的罪行如出一辙。这些罪行日益变得更加复杂和隐蔽，其实施方式也日益精湛，给世界上几乎所有国家均造成巨大的经济和政治危害。此外，大多数专家认为各国的信息主权与国家安全事务之间存在直接联系。

5. 打击信息技术领域罪行的努力遇到许多具有法律性质的问题，因为计算机证据具有非物质以及经常是稍纵即逝的性质。在处理网络犯罪问题时所涉及的复杂问题使得国际合作更加重要。为此，所有国家最后还是要制定适当和相互兼容的法律、程序和规范类的工具。

6. 在实践中，对计算机犯罪的调查显示，迫切需要各国执法机构之间的合作。

7. 在国际实践中，通常采取联合措施调查计算机犯罪。乌克兰安全部门积极参与执法机构和特殊事务部门的联合行动，这也是打击通过因特网散播儿童色情制品以及国际恐怖主义诈骗罪的行动的一部分。

8. 此外，有必要加紧努力，进一步发展在提供信息安全方面的合作，维护共同利益和引进保护信息的措施，这主要是以双边和多边协议的形式。只有在各国政府机构有效合作的情况下，才能找到成功解决信息安全问题的办法，特别是因为所需的法律基础业已到位。

9. 鉴于有必要打击网络犯罪和网络恐怖主义的威胁，乌克兰安全局一直与外国执法机构保持接触。

10. 应指出，电脑犯罪分子往往选择政府办事处建立的网络作为其目标。此外，能否成功追查和惩治罪犯，取决于国际联系的质量，即是否已建立并优化了本国立法以符合当前的标准。

11. 考虑到计算机犯罪在全球持续增多，各国黑客集团之间存在联系以及网络威胁与国界无关，至关重要的是，应扩大在打击网络威胁的斗争中的合作。

12. 为执行信息社会世界首脑会议的各项决定（2003年12月10日至12日在日内瓦举行第一次会议；2005年11月16日至18日在突尼斯举行第二次会议），乌克兰通过了一项关于2007–2015年乌克兰信息社会发展的基本原则法令。该法的目的是，在更加安全的环境内运用最新的信息和通信技术。

13. 此外，已制定并通过了乌克兰电信发展计划。计划提供了后勤和技术保障，以确保乌克兰电信基础设施所有部门能安全运作，其中包括：

- 制定和逐步推行规范性和法律基础，以保护信息，通过技术手段和加密技术，保证符合欧洲和全球标准；
- 发展最新的信息保护方法，运用技术，全面解决保护电信网络资料的任务；
- 在法律允许的情况下，建立制度，合法拦截电信网络中的信息；
- 建立国家协调中心，协调公共信息和电信网络的安全，协助国家和非政府组织中心，回应和应对在这些网络上发生的事件。

14. 乌克兰对信息保护的规范性和法律依据还包括：国家安全的基本原则法令；信息法令；保护信息和电信系统的法令；总统和内阁成员关于从技术上保护乌克兰信息的发布令；信息、电信系统和网络的保护条例，与全球数据传输网络链接的程序。其中还包括了在司法部登记的大量规范性法规，宗旨是规范信息系统与全球数据传输网络的链接、特殊活动颁发执照的程序以及评估信息保护的程序。

15. 规范性和法律法规指出，只有使用受到保护的信息和通信技术系统，才能对信息提供必要的保护，换句话说，应该使用那些纳入了综合信息保护系统的信息，这个单一系统包括一系列旨在应对威胁的法律和后勤措施、软件和硬件。综合系统和它的信息保护组成部分必须经过认证以符合信息保护标准。

16. 为了规范综合信息保护系统的要求及其组成部分，乌克兰已制定并推出了约50个技术标准，规定了以下方面的准则：评估信息保护、信息和通信技术的分类、综合信息保护系统的每个组成部分达到信息保护要求的程序，这些均取决于所涉及各种不同的信息和通信技术、其最终目的、使用的领域和处理信息的类型。

17. 乌克兰也制定了本国评估信息技术安全的国家标准制度。该系统依据一系列规范文书，即保护信息和电信系统免遭未经授权的获取该系统的信息；这些文书已与欧洲联盟各国类似文书和国际标准统一，特别是国际标准化组织/国际电子技术委员会第15408号标准。

18. 此外，乌克兰还正在制定全国范围的组织和技术措施系统，以防止对国家机关、执法、海关和税务电信系统、信贷和金融机构等信息采取未经授权的行动，特别是企图通过因特网干扰其工作。

19. 按照《国家特别通信和信息保护局法》第16条第10和11款的具体规定，为了加强国家机构之间的协调，以侦测对信息和电信系统进行的威胁，为了应对此种威胁实施的后果，并组织在这些问题上的国际合作，在该局内设立了适当的计算机应急小组，并已投入运作。

20. 计算机应急小组反映了全球对快速反应设施的行动趋势，计算机应急小组就是要应对计算机紧急情况。这类机构活动的国际协调由事故对应和安全小组国际论坛提供，这个论坛是应对安全事件的小组的论坛。

21. 2009年7月13日，乌克兰计算机应急小组成为该论坛的正式成员(www.cert.gov.ua)。

22. 2009年，乌克兰应急小组处理了来自30个国家和地区计算机应急小组的461份报告（澳大利亚、奥地利、比利时、加拿大、中国、丹麦、芬兰、法国、爱沙尼亚、德国、匈牙利、印度、以色列、意大利、日本、韩国、立陶宛、马来西亚、荷兰、挪威、巴基斯坦、波兰、葡萄牙、罗马尼亚、俄罗斯联邦、沙特阿拉伯、西班牙、中国台湾、土耳其、美利坚合众国），其中涉及在乌克兰因特网从事的未经授权行为（分发有害软件、发动“拒绝服务”攻击及其他企图犯下的未经授权的行为）。

23. 还应指出的是，乌克兰建立了法律和监管框架，并努力确保国家特别通信和信息保护服务局与执法机构之间的合作，以采取措施，保障信息和电信系统中国家信息资源的安全，提高该系统的能力，以应对那些未经授权的针对信息资源的行为。

24. 因此，在乌克兰建立信息和电信系统的所有阶段及其综合信息保护系统中的信息现均可得到保护，无论处理的信息的种类重要性如何，以及无论信息和电信系统的种类和复杂性如何。此外，制定整个信息和电信系统的信息资源的要求、设计、开发、安全评估以及保护的所有基本办法，均符合联合国会员国以及欧洲联盟成员国的国家安全部门采用的方法。

25. 为了培训信息安全和计算机工程领域的专家，成立了信息保护研究所，这是国家信息和通信技术大学的一个学术和科学部门。

大不列颠及北爱尔兰联合王国

[原件：英文]
[2010年6月2日]

1. 联合王国高兴地对有关从国际安全的角度来看信息和电信领域的发展的联合国第64/25号决议，做出回应。

2. 我们认为这个问题极为重要，关系到每个国家在国际安全大环境中的商贸和对本国公民的保护。联合王国尽了相当大的努力，使网络空间对于所有国家而言，更为安全，我们欢迎在这一领域的国际活动，我们相信所有国家应进行合作，以促进网络空间有个安全、复原力强的环境。

对信息安全问题的一般看法

3. 我们相信，一个安全的网络空间对于当今世界非常重要。公民、商业、重要的国家基础设施和政府越来越多地依赖于因特网。影响某国因特网服务的任何事件都有可能对该国产生后果，也许还是严重的后果。遗憾的是，任何国家内外都可能出现若干威胁行动者，他们可能会出于某些原因，试图扰乱或操纵因特网服务。

在国家一级为加强信息安全和促进这一领域的国际合作而采取的努力

4. 联合王国将继续在国内外努力，以促进网络空间的安全。在国内，我们于2009年6月出版了《国家网络安全战略》。该文件加强了全国关于信息安全的努力。该《战略》要求成立2个新的组织，网络安全办公室和网络安全行动中心。这两个组织已经成立，并继续扩大。联合王国有3个计算机应急小组，向联合王国关键基础设施、军事和其他政府网络提供专家服务。在国际范围，我们也积极参与这项工作。我们在联合国的参与包括参加政府专家小组。我们是关于创建全球网络安全文化以及评估各国保护重要信息基础设施的努力的联合国决议的共同提案国。我们是国际电信联盟(国际电联)有关机构的成员。我们参加了欧洲安全与合作组织的各项活动。在我们的全力支持和参与下，欧盟已开始对保护欧盟各国重要的基础设施的若干倡议开展工作。我们参加了欧盟与东盟的接触，参加了东盟关于网络安全的区域论坛。同样，我们还参与了北约内部一些有关保护该组织网络的活动。联合王国一直是MERIDIAN进程（www.meridian2007.org）、事故对应和安全小组论坛（www.first.org）和欧盟各国计算机应急小组组织的牵头国家（www.egc-group.org）之一。

5. 联合王国国家网络安全战略可从内阁网页www.cabinetoffice.gov.uk下载。

国际社会为加强全球一级的信息安全可能采取的措施

6. 我们鼓励所有国家设立计算机应急小组。我们鼓励所有国家制定有关网络犯罪的有效的国内立法。我们相信，电子犯罪不是网络空间的唯一罪恶活动，但是最普遍的活动。我们认为减少犯罪活动将有利于所有人。我们认为，欧洲委员会《网络犯罪公约》代表了打击国际电子犯罪的合适工具。此外，我们相信，国际电联开发、联合国推广的工具包为各国提供了自我评估准备解决对重要的国内基础设施潜在攻击的良好基础。我们欢迎在多种场合，为促进信息安全最佳实践做出的努力。

有关国际概念

7. 主要的国际概念是国际法的概念。对现有国际法律是否适用于网络空间，有过相当多的辩论，尤其是在网络会议上。联合王国已研究过这个问题，我们的观点是，有关使用武力和武装冲突法的现有国际法原则，为查明和分析利用网络空间从事敌对行动，提供了合适的框架。

“蓝皮书”研究丛刊清单

编号		
33	2011年	从国际安全的角度来看信息和电信领域发展
32	2008年	核查的一切方面，包括联合国在核查领域的作用
31	2005年	在当前国际形势下的裁军和发展之间的关系
30	2003年	关于裁军和不扩散教育问题的研究
29	2003年	导弹问题的各个方面
28	1999年	小型武器
27	1994年	将建立信任措施用于外层空间的研究
26	1993年	关于防御性安全概念和政策的研究
25	1993年	将分配给军事活动的资源用于保护环境的努力的可能性
24	1992年	关于如何促进国际常规武器转让的透明度的研究
23	1991年	南非核弹头弹道导弹能力
22	1991年	可促成建立中东无核武器区的有效、可核查措施
21	1991年	核武器：全面研究报告
20	1991年	联合国在核查领域的作用
19	1989年	军备竞赛和军事支出的经济和社会后果研究
18	1989年	关于核战争的气候和其他全球性影响的研究
17	1987年	关于威慑的研究
16	1986年	海军军备竞赛
15	1986年	裁减军事预算
14	1986年	安全的概念
13	1985年	单方面核裁军措施
12	1985年	关于常规裁军的研究
11	1983年	军备竞赛和军事支出的经济和社会后果研究
10	1983年	裁减军事预算
9	1983年	设立国际卫星监测机构的意义
8	1982年	裁军和国际安全之间的关系
7	1982年	全面彻底裁军：建立信任的措施
6	1982年	以色列的核军备
5	1982年	裁军和发展之间的关系（另见第31号，2005年）
4	1981年	裁减军事预算
3	1981年	对区域裁军的一切方面的研究
2	1981年	南非在核领域的计划和能力
1	1981年	对核武器的全面研究（另见第21号，1991年）

可通过向当地书店询问或通过联合国网站获取印刷版本：https://unp.un.org。

裁军

研究丛刊 33

11-59425—May 2012