联合国 A/69/112

大会

Distr.: General
30 June 2014
Chinese
Original: English/Spanish

第六十九届会议

暂定项目表* 项目 92

从国际安全角度看信息和电信领域的发展

从国际安全角度看信息和电信领域的发展

秘书长的报告

目录

* A/69/50。

14-56479 (C) 250714 280714

一. 导言

1. 2013 年 12 月 27 日，大会通过了题为“从国际安全角度看信息和电信领域的发展”的第 68/243 号决议。在决议第 3 段中，大会邀请所有会员国在考虑到关于从国际安全角度看信息和电信领域发展政府专家组的报告(A/68/98)所载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 2014 年 2 月 19 日向会员国发出普通照会，请它们就此事项提供信息。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。

二. 从各国政府收到的答复

澳大利亚

[原件：英文]
[2014 年 5 月 30 日]

澳大利亚认为，现行国际法为国家在网络空间中的行为和对国家从事非法网上行动作出适当应对提供了框架。这包括，在适用的情况下，国际人道主义法、关于使用武力的法律、国际人权法和关于国家责任的国际法。在制订任何新的或新增加的国家网络空间行为规范时必须符合国际法。

关于从国际安全角度看信息和电信领域发展政府专家组的协商一致报告(A/68/98)对各国具有重大指导意义；该报告申明，国际法，尤其是《联合国宪章》，适用于国家对网络空间的使用，是维护和平与稳定所不可或缺的。澳大利亚认为这一结论具有根本性意义。澳大利亚认为，各国应个别和集体地公开重申其理解，即国际法适用于国家在网络空间的行为，并承诺按照其对国际法的理解在网络空间采取行动。

报告认识到，需要进一步讨论和阐述如何将国际法应用于国家对网络空间的使用，并建议在这一领域作进一步研究。报告指出，随着时间的推移可以制订更多准则。澳大利亚认为，在承认所涉问题的复杂性的同时阐明如何将国际法应用于冲突和非冲突局势下国家在网络空间的行为，是国际社会的一项优先任务。

报告还就网络建立信任措施提出了开创性的建议。澳大利亚认识到，阐明如何将国际法应用于国家对网络空间的使用是一项长期任务。在短期内，有必要采取实际措施来处理和防止国家间可能因误解而产生并可能因误判和升级而导致冲突的问题。区域安全组织特别适合考虑、制订和实施网络建立信任措施。澳大利亚正在东南亚国家联盟(东盟)区域论坛带头作出努力，以推进这一重要议程；鉴于成员国的能力有差别，因此该议程应包括能力建设目标。

奥地利

[原件：英文]
[2014 年 5 月 19 日]

于 2013 年 3 月通过的《奥地利网络安全战略》为在确保人权的同时保护网络空间和虚拟空间中的民众提供了一个全面和积极主动的概念。它增强了奥地利网络空间基础设施和服务的安全和复原力。最重要的是，它有助于建立奥地利社会的认识和信心。

全球联络和国际合作对于《奥地利网络空间战略》至关重要。网络空间的安全是通过在国家和国际两级实行协调混合政策而得到保障的。奥地利将在欧洲联盟、联合国、欧洲安全与合作组织(欧安组织)、欧洲委员会、经济合作与发展组织(经合组织)和北大西洋公约组织(北约)伙伴关系的框架内，采用协调和有针对性的方法积极参与“网络外交政策”。

奥地利将大力促进执行《欧洲联盟网络安全战略》，全面参与欧洲联盟的战略和业务工作。各主管部委将采取必要措施，执行并充分利用《欧洲委员会预防网络犯罪公约》。奥地利倡导在国际一级的免费因特网。必须保障所有人权在虚拟空间得到自由行使；特别是，绝不能在因特网上不适当地限制表达和信息自由权。

奥地利将继续在北约伙伴关系的框架内开展双边合作，并积极支持编写一份欧安组织建立信任和安全具体措施清单。奥地利积极参与规划和实施跨国网络演习。所取得的经验将直接纳入规划和用于进一步发展业务合作。外交部协调与网络安全有关的外交政策措施。将酌情考虑缔结双边或国际协议。

在国内，一个指导小组正在制订一项执行计划，以执行《奥地利网络安全战略》规定的横向措施。在指导小组的协调下，各主管机构负责在各自任务范围内执行这些措施。各机构将根据《奥地利网络安全战略》就各自负责的领域制订次级战略。参加指导小组的各部委承担的一项任务是，每年向联邦政府提交两次执行计划。在起草计划的同时将审查《奥地利网络安全战略》，并在必要时加以修订和更新。

哥伦比亚

[原件：西班牙文]
[2014 年 5 月 23 日]

对信息安全问题的一般看法

近年来在发展和应用信息和通信技术方面取得了重大进展，所带来的变化和裨益对许多国家的发展作出了很大贡献，同时促进了在传播信息方面的国际合作。

但是，这些技术进步也令人深切关注如下可能性：这些进步有可能被用于破坏国际稳定与安全，对国家基础设施的完整性产生不利影响，以致削弱国家民事和军事安全。

因此，哥伦比亚极为关切利用新技术形成计算机威胁的问题和在网络空间现有的犯罪威胁问题，并认为这类问题对本国非常重要。

哥伦比亚因而必须确定政策和战略，以防止信息技术被用于恐怖主义或犯罪目的。

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

立法和体制应对行动

哥伦比亚在 2005 年实施了 ISO 27001 标准，作为为国家实体信息安全规定质量标准的管理系统，并主张维护信息的保密性、完整性和可用性。[1]

四年后，即 2009 年，哥伦比亚共和国国会颁布了修正《刑法》的第 1273 号法令，设立了一个新的受法律保护的利益，即“信息和数据保护”。该修正案为相关当局起诉和审判与信息技术相关的罪行设定了国家法律框架。

哥伦比亚根据这一框架，除其他外，将以下行为定为犯罪行为：非法进入、非法拦截、攻击数据的完整性、攻击系统完整性、滥用装置、计算机伪造、计算机欺诈、儿童色情制品及侵犯知识产权和相关权利的罪行。

哥伦比亚在 2011 年通过 CONPES 3701 号文件推出了国家网络防御和网络安全政策，其基础为三个基本支柱：

(a) 为预防、协调和监测目的，采用适当的机构间框架，并为解决可能出现的任何威胁和风险提出建议；

(b) 拟订关于信息安全的专业培训方案；

(c) 加强有关这些事项的立法和国际合作，并在该框架内，加快哥伦比亚加入各种国际文书的进程，包括《布达佩斯公约》。

[1] 保密性：防止信息被未经授权的个人或程序所利用。完整性：确保对组织有价值的一切东西的准确性和完整性。可用性：确保经授权的实体需要时可获取并使用相关信息。

为了全面实现上述战略方针，哥伦比亚拟定并成立了四个部门：

1. 跨部门委员会，负责提出信息化管理的战略前景和制定公共信息技术基础设施、网络安全和网络防御方面管理的政策指导原则；

2. 哥伦比亚计算机应急小组，是网络安全和网络防御事项上的国家协调机构；

3. 武装部队联合网络指挥部，其任务是防止和打击任何影响到国家价值和利益的网络威胁或攻击；

4. 网络警务中心，负责哥伦比亚的网络安全，提供信息、支持并防止网络犯罪。

同样，哥伦比亚通过 2012 年第 1581 号法和对该法起部分规范作用的 2013 年第 1377 号法令设立了用于保护个人数据的法律框架。 此外，在工业和贸易监管局下设立了个人数据保护司。

信息技术和通信部还制定并实施了含有对实体采用信息安全管理系统的要求的政府在线战略。同样，该部自 2008 年以来已就与信息技术管理相关的程序培训了约 6 300 名公务员。

还应当指出的是，在能力领域里在查明重要基础设施方面正在取得进展(如果受损有可能导致人命损失、经济损失或削弱国家治理能力的基础设施)，以维护这些地点的网络安全。

国际合作

哥伦比亚在 2013 年正式申请加入《欧洲预防网络犯罪公约》；该公约确立了国际网络安全问题协定和对相应罪行实施惩罚原则，其中的主要目的是进行适当立法和开展国际合作，以保护社会免遭网络犯罪破坏。

此外，哥伦比亚在 2012 年加入了与世界经济论坛的一项多边协定，称为“促进网络复原力伙伴关系”，目的是查明和处理因人、程序和物体之间日益加深的连通性而带来的全球系统性风险。

同时，美洲国家组织美洲反恐怖主义委员会(美洲反恐委)秘书处制定了一个用于在成员国中在网络安全领域开展能力建设的全面方法。秘书处的主要成就是建立国家“警戒、观察和警告”小组(又称为“计算机安全事故应急小组”)，担负并具备应对危机、事件和对网络安全的威胁的任务和能力。

哥伦比亚在这一框架内并同美洲反恐委合作设立了“警戒、观察和警告”小组，为拟订国家网络安全战略作出了贡献。哥伦比亚还参加了关于处理涉及网络安全、信息安全和网络犯罪事件的讲习班、培训班和会议。

还应指出的是，哥伦比亚已同一些从事信息和通信行业的国际企业和组织达成了协议，特别是同微软公司达成了能进入类似“预防网络犯罪中心”这样的机

构和其他网络安全方案的协议；同“反网络欺诈行为工作组”达成一项协议，目的是加入正在努力建立更有效的网络事件警戒和应对机制的全球法律当局、工业企业和政府实体联盟。

为加强信息安全而采取的国际措施

网络安全并不完全是政府的问题，也不能仅靠政府来解决：需要其他行为体即学术界、行业和民间社会，提供支持，以有效解决因各部门越来越密集地使用信息和通信技术所带来的风险。

哥伦比亚认为，为在全球一级加强国际信息安全，国际社会必须：

- 寻找机制，以使每一个国家的社会、民选官员和实体认识到必须创造一种信息安全文化，并认识到国际合作打击网络犯罪的重要性。
- 促进各国为加强国家在网络安全和网络防御领域的能力而制定战略。
- 敦促各国查明重要基础设施并制定一项专门用于增强其安全和复原力的方案。
- 鼓励将国内法律框架同网络安全领域的现行国际文书保持一致。改善不同国家之间的协调将使各国更容易建立用于预防、调查和起诉网络犯罪的合作渠道。

这类协调应有助于确定与技术相关的犯罪和设定明确的管辖权和起诉权规则。

- 促进确立要求各国及公共和私营国家实体保存计算机记录以供以后作调查和审判之用的义务。
- 编制一个刑事司法系统官员普遍不太熟悉的与网络犯罪相关的计算机术语集，以确保系统、网络和计算机数据的保密性和完整性。
- 促进交流网络防御和网络安全领域的经验和最佳做法，以及建立专门的培训网络。
- 敦促各国加入网络事件警戒网络。

古巴

[原件：西班牙文]
[2014 年 5 月 27 日]

古巴完全赞同第 68/243 号决议表达的关切，即担心信息技术和电信手段被用于会影响国际稳定与安全、危及国家完整性和损害国家民事和军事领域安全的目的。这项决议还正确地强调有必要防止为犯罪或恐怖主义目的使用信息资料和技术。

在这方面，古巴表示极为关切个人、组织和国家秘密和非法使用别国计算机系统对第三国实施攻击的问题，因为这种做法有可能会触发国际冲突。一些政府

甚至说，可用常规武器应对此类攻击。预防和应对这类新型威胁及避免网络空间成为军事行动区的唯一方法就是所有国家展开共同合作。

利用电信恶意地公开或秘密破坏各国的法律和政治秩序，这种行为违反这一领域公认的国际准则，产生的影响可能会造成紧张局势并无益于国际和平与安全。

因此，古巴再次谴责美利坚合众国政府对古巴展开违反关于无线电领域现行国际法规的广播和电视战。在实施这一侵略时根本不顾因制造危险局势而对国际和平与安全可能造成的损害。

对古巴的非法电台和电视广播旨在促进非法移徙，鼓励和煽动暴力、蔑视宪法秩序和实施恐怖主义行为。为颠覆其他国家的内部秩序、侵犯其主权及插手和干涉他国内部事务的目的而使用信息是非法的。

对古巴的广播违反了现行《国际电信联盟组织法》所载的国际规范，其序言确认电信对维护和平及对所有国家的经济和社会发展具有越来越大的重要性，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、国际合作及促进经济社会发展的目标。

美利坚合众国政府继续每天 24 小时在商业中波频带上播放音频广播。这一频带不向其他国家开放服务。其他商业广播电台向反古巴组织提供服务，播放旨在颠覆国内秩序和误导古巴人民的广播。

这类组织在短波频带上播放这类广播，而美国政府对此是完全知情的。

在 2013 年 4 月和 2014 年 4 月期间，每周用于播放具有颠覆内容的反古巴广播的平均小时数在 1 909 至 2 070 小时之间，使用 27 个频率。2013 年 9 月和 10 月，两个在佛罗里达南部播放节目、其信号可在古巴西部和中部接收到的北美电台开始播放具有反革命性质的节目。

马蒂电台和电视台继续通过美国国际和国内卫星系统播放反古巴广播。

此外，今年揭露了“ZunZuneo”案件；这是一个美国政府用几百万美元支持、利用社交网络上的短信服务促进在古巴开展颠覆活动的复杂阴谋。

这个到 2012 年才结束的非法方案的目的是在未经当事人同意的情况下收集古巴用户的私人数据，并按性别、年龄、喜好和各种所属关系处理用户特征资料，以用于政治目的。

正如其他颠覆活动一样，ZunZuneo 违反了古巴和美国法律，如美国国会于 2003 年 12 月通过的《2003 年控制主动提供的色情和产品推销邮件骚扰法》(第 108-187 号公法)，该法禁止未经收件人明示同意，向其发送商业或任何其他类型的短信。

这同样也违反了《国际电信联盟组织法》，因为对新技术、尤其是社交网络的这类使用明显无益于通过有效的电信服务手段实现和平关系和国际合作。

发送主动提供的邮件(垃圾邮件)这一有害做法一直是电信标准化局 10 多项建议的针对目标，违反了 2003 年在日内瓦举行的信息社会世界首脑会议《原则宣言》第 37 点。

美国政府应尊重国际法及《联合国宪章》的宗旨和原则；应停止其对古巴的非法和秘密行动，而这种行动遭到了古巴人民和国际公众舆论的谴责。

在这方面，拉丁美洲和加勒比国家共同体(拉加共同体)于 4 月 29 日通过一项公报，其中强调，非法使用新的信息和通信技术的做法对各国及其公民产生了不利影响。

拉加共同体在该公报中强烈表示反对以违反国际法的方式使用信通技术及一切具有这种性质的行动。它强调，必须确保对此种技术的使用应完全符合《联合国宪章》的宗旨和原则、国际法，特别是主权、不干涉内政及国际公认的国家间共处的标准。它重申致力于加强国际努力，保护网络空间并促进其使用完全是为了和平目的和作为促进经济和社会发展的媒介。

古巴支持第 68/243 号决议，并将为全球信息和通讯技术的和平发展及使之为全人类造福继续作出贡献。

萨尔瓦多

[原件：西班牙文]
[2014 年 5 月 26 日]

萨尔瓦多武装部队在信息安全和电信框架内建立了一个独立于公共网络的音频、视频和数据电信网络，目的是保护所有信息免遭任何外部人员的渗透和网络攻击。

格鲁吉亚

[原件：英文]
[2014 年 5 月 30 日]

执行摘要

2008 年对格鲁吉亚发动的网络战争使保护重要基础设施的工作放在了格鲁吉亚政府议程的重要地位。对重要基础设施和对政府在信息技术服务方面的迅速增长的依赖加深了遭受网络犯罪相关事件侵害的脆弱性。因此，充分保护重要基础设施免遭网络威胁是格鲁吉亚政府的优先事项之一。

2008 年网络攻击的第一批目标就是政府网站和新闻媒体网站。后来，袭击范围扩大至包括更多的政府网站、格鲁吉亚金融机构、商业协会、教育机构、更多的新闻媒体网站和一个格鲁吉亚黑客论坛。这些攻击的目的是要扰乱正常业务活动。除了两大银行外，与商业有关的目标主要是那些可被用于在不同企业之间进行沟通和协调反应的组织。

上述经验表明，国家和个人行为体对格鲁吉亚重要基础设施的网络攻击可对公营部门和私营部门造成严重的实物损坏和巨大的财务损失。因此，格鲁吉亚政府认为网络安全属于国家总体安全政策的组成部分，特别是因为政府越来越多地利用信息技术作为提供政府服务的一种工具。

国家安全委员会和一个由政府不同机构组成的特别工作组在表达这些关切的同时，作为国家安全审查工作的组成部分，在 2011 年拟定了《格鲁吉亚国家网络安全战略》。《网络安全战略》及其实施行动计划于 2012 年 3 月提交公众供讨论 ，最后于 2013 年 1 月获得通过。

迈出的另外一步就是在 2010 年建立了格鲁吉亚司法部数据交换局，作为中央政府负责制订和执行电子政务政策和解决办法的一个实体。该局的一个重要任务就是维护公共部门和私营部门的信息安全，包括：

- 通过和执行公共部门和重要基础设施方面的信息安全政策和标准
- 提供信息安全领域的咨询服务和执行信息安全审计
- 对公众和民间部门开展关于信息安全问题的提高认识活动
- 通过国家计算机应急小组履行网络安全任务。

格鲁吉亚提交的文件全文可上 http://www.un.org/disarmament/topics/informationsecurity/ 查阅。

德国

[原件：英文]
[2014 年 5 月 30 日]

执行摘要

信息和通讯技术给工业化国家和发展中国家带来了史无前例的机会。同时也存在着脆弱性和系统性弱点。

现在有一种难以发现、复杂和针对高价值目标的恶意活动的趋势。可能产生严重后果。对关键基础设施的网络攻击会比孤立的暴力攻击造成更多破坏，有时会对其他联网实体造成无法预料的后果。

尽管有这些风险，但看起来暂时不可能发生全面“网络战争”。更可能发生的情况可能是有限使用网络能力作为规模更大的作战努力的一部分。最后，存在着网络事故可能升级为“真实”冲突的危险。

在这种情况下，增强网络复原力、商定适用于使用信息和通信技术的法律和规则，以及参与建立信任措施就变得比以往任何时候都更为重要了。

2013 年取得了可喜的进展：关于从国际安全角度看信息和电信领域发展政府专家组的最新报告表明，国际法适用于网络空间。专家组还认为，国家主权和源

自主权的国际规范和原则适用于国家进行的信通技术活动，以及国家在其领土内对信通技术基础设施的管辖权。德国期待看到新的政府专家组扩大这些成果。

关于建立信任措施，欧安组织取得了重要进展：通过了用于提高国家间合作、透明度、可预测性和稳定性的第一批步骤，以期减少源自使用信息和通信技术的误解风险、升级和冲突。欧安组织的这一协议可作为其他区域组织可效仿的模式。

德国的网络安全战略(2011 年)是基于以下认识而制定的：网络空间的提供和网络空间数据的完整性、真实性和保密性已变得极其重要了。确保网络安全已成为对国家、企业和社会的一项中心挑战。各方需一起采取行动，包括在国家一级和与国际伙伴进行合作。德国的网络安全战略确定了下列目标和措施：

- 保护重要信息基础设施
- 确保信息技术系统的安全
- 加强公共行政方面的信息技术安全
- 管理国家网络应急中心
- 设立国家网络安全委员会
- 有效控制网络空间犯罪
- 采取有效协调行动，确保欧洲和世界各地的网络安全
- 利用可靠和值得信赖的信息技术
- 联邦当局的人员发展
- 用于应对网络攻击的工具。

在 2013 年 9 月的德国大选后，按照联合协议，网络安全已置于政府议程的重要地位。数据隐私标准将得到提高。今后四年的首要主题包括如何更好地保护消费者、修订刑法以更好地保护个人、通过一项信息技术安全法以对重要基础设施规定强制性最低信息技术安全标准，以及所有联邦当局都有义务将其信息技术预算的 10%用于改善其系统的安全。

由于关切非法或任意监测和/或侦听通讯及第三方非法或任意收集个人数据的问题，德国政府强烈鼓励信息技术服务供应商将电信加密，并且不向外国情报机构转送电信数据。

德国提交的文件全文可上 http://www.un.org/disarmament/topics/informationsecurity/查阅。

葡萄牙

[原件：英文]
[2014 年 5 月 20 日]

关于上述主题的大会第 68/243 号决议回顾科学和技术在国际安全方面的重要作用，并认识到这些领域的发展可具有民用和军事用途，还认识到应维持和鼓励这类进展。信息和电信领域的进展意味着为以下各方面增加了机会：文明的发展、国家之间的合作、促进人的创造力，以及信息在整个社会里的流通。

但是，这些技术和手段可能会被用于与国际稳定与安全不相符的目的，对国家在民用和军事领域的国家完整性产生不利影响。

大会第 68/243 号决议回顾政府专家组的报告(A/68/98)，要求会员国在四个领域作出贡献：

1. 对信息安全问题的一般看法；

2. 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；

3. 旨在加强全球信息和电信系统安全的相关概念的内容；

4. 国际社会为加强全球一级的信息安全可能采取的措施。

该报告就下列领域提出了一些建议：国家负责任行为的规范、规则和原则；建立信任措施和交换信息；能力建设措施。

我们可以根据这些建议来阐明我国的举措：

㈠ 具有国家负责任行为特点的规范、规则和原则

1. 葡萄牙认为，网络信息安全是重要的并越来越重要；

2. 我们必须强调要努力落实关于网络安全和完整性的法规，采用控制风险的方法，而这就需要在技术和组织层面采用适当的安全措施，以及要求报告对服务运行产生重大影响的安全违规或完整性损失事件。同样重要的还有由国家安全违规或完整性损失事件通报中心所实施的安全领域审计程序；

3. 关于保护个人数据和隐私，必须强调已发生的变化，例如强制报告个人数据违规事件；

4. 在概念层面，必须加强如下看法：法规应遵从国际规则；

5. 在国际层面，必须加强信息共享和落实在边境地区的实地培训工作。

㈡ 用于加强信心和信息共享的措施

1. 必须在考虑到范围更为广泛的全球化的情况下促进信息共享；

2. 在国家层面，我们的工作专注于实现公共和私营部门都参与的联合项目，促进技术标准化，以及组办会议和研讨会，有时还邀请国际人士参加、发表演讲。

㈢ 能力建设措施

1. 必须拟定能力建设措施。但是，在培训和维持与这些活动相关的人力资源方面存在着困难；

2. 需要为获得知识提供便利；

3. 高级别机构未充分认识到其在这些事项上的责任。

塞尔维亚

[原件：英文]
[2014 年 5 月 28 日]

考虑到信息安全在全球和国家两级的高度重要性，塞尔维亚共和国已开展一些活动，以便制定有效的国家政策和设立有效的安全机制。塞尔维亚共和国政府于 2010 年通过的《2020 年之前塞尔维亚共和国信息社会发展战略》宣布，信息安全是六个优先领域之一。塞尔维亚没有一项专门针对信息安全的国家战略，但有若干其他文件涉及这个问题。在 2013 年 10 月成立了一个特别工作组，其任务就是起草一项关于信息安全的法律。该法律符合相关的国际和欧洲联盟法律框架，并就下列方面作出了规定：信息安全的体制框架；为增强塞尔维亚共和国信通技术系统安全需采取的措施，包括公共机构和企业的信通技术系统；在信通技术系统安全风险方面的预防协调工作的规范；设立国家计算机应急小组；适用于国家机构信息系统的具体安全措施和先决条件；信通技术系统中保密数据的安全；密码安全和为免遭破坏性电磁发射而采取的保护措施。

共和国机构联合事务管理局信通技术司负责开展与保护信息安全、数据保护和实施规定的国家机构信息系统安全标准有关的活动。管理局的年度报告指出，根据其所承担的保护国家信通技术系统的任务，管理局每天都针对网络攻击提供保护，因为网络每天都遭受到攻击。

塞尔维亚共和国学术网络负责开展塞尔维亚共和国教育和科研机构的计算机安全事件应对活动。学术网络 2013 年年度报告指出，同 2012 年相比，相关事件的发生次数增加了。该报告确认，旧设备是导致遭受攻击次数增多的原因之一。

只有得到社会各级都接受的完善的国家信息安全文化才能在当地有效地加强国家信息和电信系统的安全。同样，只有这类完善的国家信息安全系统才能成为国际信息安全概念应用的组成部分，以用于加强全球信息和电信系统安全。

国家安全委员会和保密信息保护办公室(以下简称：国家安全委员会办公室)是塞尔维亚政府在国家一级负责协调实施国家和欧洲联盟安全政策的部门(国家安全局)。该部门的一部分具体工作就是通过信息保障措施和在政府机构和其他机构里协调落实这些措施，以保护保密信息。为此，在 2011 年通过了关于用于保护信息电信系统中保密信息的具体措施的法令(《塞尔维亚共和国政府公报》，第 53/2011 号)。在国际一级，自 2011 年以来，国家安全委员会办公室一直积极参加东南欧国家安全部门主任论坛。论坛的其中一个主要目标是，根据国际标准在区域各国加强信息保障和机密信息保护工作。国家安全委员会办公室是在东南欧国家安全部门框架内拟订区域网络防御概念的首席协调机构。

国家安全委员会办公室已编写并向其他专题工作组成员送交了若干相关提议，供其审查、统一和批准。这些提议载于下列文件中：㈠ 网络防御方案的目标；和㈡ 东南欧国家安全部门网络防御问题单。

塞尔维亚共和国国防部正在参与执行大会第 68/243 号决议。国防部各部门正积极参加负责起草信息安全法的工作组的工作。

此外，国防部正在组建一些将在信息安全和网络防御领域运作的部门。

瑞士

[原件：英文]
[2014 年 5 月 29 日]

A. 对信息安全问题的一般看法

信息和通信技术(信通技术)已成为社会、经济和政治活动一个不可或缺的驱动要素。瑞士决心抓住因利用信通技术而产生的机遇。瑞士考虑到与信通技术有关的新发展和挑战，以落实《瑞士联邦委员会信息社会战略》的方式积极参与塑造信息社会。

但是，信通技术的使用使信息和通信基础设施易被犯罪分子、情报人员、政治-军事人员或恐怖分子滥用或容易遭遇功能障碍。通过电子网络实施的动乱、操纵和特定攻击是信息社会面临的风险。在这一背景下，各国越来越多地参与一系列关于网络安全的区域和国际的政策讨论和辩论。这种参与是基于越来越感受到在计算机系统及相关技术脆弱性方面存在不安全因素，认识到它们可被用于恶意目的。

虽然自 1980 年代以来就一直记录着这种环境中的脆弱性和威胁情况，但将因利用信通技术而产生的威胁和脆弱性置于国家安全议程则是过去 7 年才发生的事。因此，瑞士联邦政府在 2010 年成立了一个专家组，以审查风险和提高国家应对这些威胁和脆弱性的能力。

瑞士作为一个整体系统的运作依赖于数量越来越多的相互联网的信息和通信设施(计算机和网络)。这种基础设施是脆弱的。全国范围的或长期的扰乱和攻击可能对瑞士的技术、经济和行政业绩产生严重不利影响。发动这类攻击的可以是各种肇事者和出于各种不同的动机：个人肇事者、政治活动分子、意图实施欺诈或讹诈的犯罪组织，以及想要扰乱国家和社会、破坏其稳定的恐怖分子或国家间谍。信通技术特别容易成为目标，这不仅是因为它们为滥用、操纵和破坏提供了许多可能性，而且还因为可以匿名方式很轻易地就能使用它们。保护信息和通信基础设施免遭这类扰乱和攻击行为的破坏符合瑞士国家利益。因此，我们欢迎关于从国际安全角度看信息和电信领域发展政府专家组得出关于国际法适用于信通技术的结论。

B. 在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

2012 年 6 月 27 日，瑞士联邦政府通过了保护瑞士免遭网络风险破坏国家战略，从而为采取综合、整体和统一办法解决网络风险奠定了基础。该战略力求改善对网络风险和新出现的威胁的早期侦测工作，使瑞士基础设施更能抵御网络攻击，以及全面减少网络风险。主要侧重点是网络犯罪、间谍和破坏活动。该战略的基本设想就是：需要建立一种网络安全文化，责任共享，以及需要采用一种基于风险的方法。该战略要求在政府一级加强协调工作，促进公私伙伴关系，以及加强国际领域的合作。

该战略由一整套 16 项措施组成，应在 2017 年全部到位。为确保有效及时落实这些措施，瑞士政府于 2013 年 5 月 15 日通过了一个详细的战略实施计划。瑞士政府还设立了一个指导委员会，负责实施每一项具体措施的牵头机构都派代表参加了该委员会。指导委员会的任务是确保协调、有的放矢地实施该战略。委员会的作用和职责范围包括确保在瑞士联邦相关部委[2] 和地方一级的相关机构中进行协调。在业务一级，政府已成立了一个协调单位，以支持指导委员会的工作。

这套措施包括风险和脆弱性分析、对威胁状况的分析、连续性和危机管理及能力建设措施，以及国际合作和倡议。

这 16 项措施可分为四个主要领域：

- 预防(即风险和脆弱性及威胁状况分析)；
- 反应(即事件处理、积极措施和执法)；
- 连续性(即连续性和危机管理)；
- 支助进程(即国际合作、教育和研究、法律基础等)。

[2] 相当于一个部。

C. 大会第 68/243 号决议第 2 段所述概念的内容

国际合作是通过瑞士国家网络战略需要加强的一个行动领域。瑞士决心在国际安全政策一级进行合作，以便同其他国家和国际组织一起应对网络空间威胁。瑞士致力于监测和塑造在外交一级的相关发展，并在国际会议和其他外交举措的框架内促进政治交流。

在这一背景下，瑞士参与了旨在发展全球机制的各种国际进程。欧安组织通过了在网络安全领域的建立信任措施。瑞士认为这一进程是至关重要的。因此，通过采用“双轨”，瑞士将专注于落实第一套建立信心措施和发展进一步措施。此外，瑞士参与的另一个重要进程就是《伦敦议程》。最后，虽然瑞士不是政府专家组成员，但仍对专家组发布的报告感兴趣。在这方面，我们特别支持如下要求：除其他外，继续研究包括《联合国宪章》及国际人权法和国际人道主义法在内的国际法如何适用于信通技术的使用。

就双边关系而言，瑞士同各国就与网络相关的问题举行定期政治磋商会议。

瑞士是 2012 年 1 月 1 日生效的《欧洲委员会预防网络犯罪公约》的签署国。

D. 国际社会为加强全球一级的信息安全可能采取的措施

必须将重点放在能增强国家间的信任和增进国家间相互了解和信心的倡议和措施上。在双边一级，各国和其他相关利益攸关方之间关于网络安全问题的轨道 1、1.5 和 2 对话已证明是有效的。必须进一步发展和加强关于网络安全问题的对话。

可以设立联合机制以防止武装冲突升级的方式在全球一级加强信息安全。因此，可在技术和政策层面设立直接沟通渠道。通过在最高级别上保持经常接触，网络空间的安全是可以得到改进的。

大不列颠及北爱尔兰联合王国

[原件：英文]
[2014 年 5 月 29 日]

执行摘要

大不列颠及北爱尔兰联合王国很高兴有机会对题为“从国际安全角度看信息和电信领域的发展”的大会第 68/243 号决议作出答复，这次答复是在 2013 年对第 67/27 号决议答复的基础上作出的。联合王国在答复中采用自己喜欢的术语“网络安全”及相关概念以避免混淆，因为对这方面所采用的词语“信息安全”有不同解释。

联合王国认识到网络空间是国家和国际重要基础设施的一个基本要素，是在线经济和社会活动的一个根本性基础。网络空间活动构成的实际威胁和潜在威胁

令人极为关注。我们的答复详细说明了为加强这一领域安全和促进相关合作而已采取和将要采取的国家方法和国际方法。这些方法的依据就是于 2011 年 11 月公布的《联合王国国家网络安全战略》。

联合王国一直积极和建设性地参与关于网络安全的国际辩论。我们为所有三个政府专家组都提供了专家，并欢迎最后一个专家组的协商一致报告；这个报告在就国家在网络空间中的行为规范达成共同谅解方面取得了宝贵进展并确认国际法适用于网络空间。联合王国还欢迎通过了在欧安组织成功谈判达成的第一套区域网络空间建立信任措施。我们的答复概述了联合王国在分享全球最佳做法方面的工作；首先是同国际伙伴合作应对网络犯罪和重大事件，其次是致力于建设网络能力。

联合王国期待看到所有这些领域取得进一步进展。这包括即将组成的政府专家组、在欧安组织落实建立信任措施和在欧安组织和其他区域集团发展进一步建立信任措施、设立计算机应急小组并加强它们之间的合作、加强关于网络犯罪的执法合作，以及推广多方利益攸关方办法。

联合王国很高兴能够积极参与处理这些重要问题，并期待进一步参与加强网络安全方面的能力和国际合作。

联合王国提交的文件全文可上 http://www.un.org/disarmament/topics/informationsecurity/ 查阅。