联合国 A/70/172

大会

Distr.: General
22 July 2015
Chinese
Original: Arabic/English/Spanish

第七十届会议

临时议程* 项目 93

从国际安全角度看信息和通信领域的发展

秘书长的报告

目录

* A/70/150。

15-12333 (C) 130815 140815

一. 导言

1. 2014 年 12 月 2 日，大会通过了第 69/28 号决议，题为“从国际安全的角度来看信息和电信领域的发展”。大会在决议第 3 段中，请所有会员国在考虑到从国际安全角度看信息和电信领域的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，继续向秘书长通报他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. 按照这项要求，2015 年 2 月 2 日向各会员国发出一份普通照会，请它们就此提供资料。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

加拿大

[原件：英文]
[2015 年 6 月 4 日]

网络空间加强了社会互动，转变了产业和政府，继续成为经济增长、创新与社会发展的引擎。但网络空间也为我们的社会带来了新的威胁和挑战。

加拿大重申，各国在 2013 年《从国际安全角度看信息和电信领域的发展政府专家组的报告》中明确确认，国际法适用于网络空间，是各国负责任行为规范和原则的基石，并鼓励就和平时期的此类规范开展进一步工作。

加拿大还认为，处理信息与通信技术安全问题必须与尊重人权和基本自由同步进行。人们平常享有的权利在网上也必须得到保护。

加拿大致力于通过以下措施实现自由、公开、安全的因特网：

(a) 执行加拿大网络安全战略和行动计划仍然是国家层面工作的重中之重。这帮助我们确保加拿大的空间系统安全，通过与重大基础设施部门(如金融、交通和能源)的积极协作，保护加拿大人的网络安全；

(b) 加拿大建立了网络事件管理框架，以全国统一的方式管理和协调处理潜在或既有的网络威胁和事件的工作；

(c) 加拿大新颁布的反垃圾邮件立法有助于明确法律权利和义务，明确政府机构各自的责任，加强执法方面的法律规定与国际合作；

(d) 在国际上，加拿大投入了 800 万加元，支持开展网络安全能力建设项目，主要是在美洲和东南亚。加拿大还通过美洲国家组织提供了 360 多万加元，以供在 2007 至 2016 年间在美洲国家组织成员国开展能力建设，包括设立计算机安全事件反应小组。加拿大还加入了网络专门知识全球论坛，是论坛的创始成员之一；

(e) 加拿大支持北大西洋公约组织和各盟国为加强网络安全联盟所做的努力；

(f) 加拿大与东南亚国家联盟(东盟)区域论坛合作开展能力建设，突出建立信任措施和提高透明度措施对实现网络空间稳定的重要意义；

(g) 通过加拿大与美利坚合众国的网络安全行动计划，加拿大与美国合作，加强本国网络基础设施的抗御能力，在业务和战略层面加强互动、协作和信息共享；

(h) 加拿大还参与了七国集团、联合国毒品和犯罪问题办公室、美洲国家组织和东盟的打击网络犯罪举措，还是打击儿童网络性虐待全球联盟的成员；

(i) 加拿大建议有志于加强网络安全、防止网络犯罪的所有会员国参阅欧洲委员会的网络犯罪公约。

加拿大答复的全文可查阅 www.un.org/disarmament/topics/informationsecurity/。

古巴

[原件：西班牙文]
[2015 年 5 月 26 日]

第 69/28 号决议中表示关切的是，信息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。古巴也对此表示关切。

第 69/28 号决议还强调要防止为犯罪或恐怖主义目的利用信息资源或技术。

在这方面，古巴十分关注个人、组织和国家秘密、非法使用其他国家的计算机系统来攻击第三国的情况，因为这可能引发国际冲突。

所有国家开展合作是防止和应对这些新威胁、避免网络空间变成军事行动场所的唯一途径。

利用电信手段公开或秘密破坏各国的法律和政治秩序的做法违反这方面的国际公认准则，可导致紧张局势和情况，不利于国际和平与安全。

拉丁美洲和加勒比各国国家元首和政府首脑在 2014 年 1 月在哈瓦那举行的第二次拉丁美洲和加勒比国家共同体(拉加共同体)首脑会议上宣布拉丁美洲和加勒比地区为和平区，以促进彼此之间以及同其他国家之间的合作和友好关系，不论其政治、经济、社会制度和发展水平有何差别，力行容恕，和平共存，善邻友好。

在 2015 年 1 月 28 日和 29 日在哥斯达黎加拉加 Belén 举行的拉加共同体第三次首脑会议上，成员国强调包括因特网在内的信息和通信技术及创新十分重要，有助于和平，增进福祉、人类发展、知识、社会包容，促进经济增长，有助于扩大社会服务的覆盖范围、提高服务质量。会议还重申，应根据《联合国宪章》和国际法和平利用信息和通信技术，并强调绝不应使用这些技术颠覆社会或造成可能导致国家间冲突的情况。

然而，美国政府不断传播攻击古巴的无线电和电视广播，使上述努力受到威胁。这违反了《联合国宪章》的宗旨和原则，违反了国际电信联盟的各种规章。此外，同样重要的是，这些广播侵犯了古巴的主权。

古巴重申，使用信息作为政治宣传工具或为造成不稳定、颠覆其他国家的内部秩序，侵犯其主权、插手和干涉他国内部事务是非法行为，必须得到制止。

我们重申，我们最强烈地反对以违背国际法的方式使用信息和通信技术，反对所有此类性质的行动。我们强调，必须确保这些技术的使用完全符合《联合国宪章》和国际法的宗旨和原则，特别是主权、不干涉内政以及国际公认的国家间和平共处标准。

古巴重申，国际合作对消除滥用信息和通信技术造成的危险至关重要。古巴还强调国际电信联盟在有关网络安全问题的政府间辩论中的重要作用。

古巴希望，劳尔·卡斯特罗·鲁斯总统和巴拉克·奥巴马总统 2014 年 12 月 17 日公布的古巴和美国双边关系新态势(包括决定恢复两国之间外交关系)将启动实现关系正常化的进程，结束这些激进政策，取消对古巴人民造成严重损害的经济、商业和金融封锁。禁运对信息和通信领域及古巴人民日常生活的其他方面造成了有害影响。

作为古巴计算机化方案的部分内容，于 2015 年 2 月 18 日至 20 日在古巴举行了第一次全国电脑和网络安全讨论会，主题是“建设计算机化的社会”。来自全国各地的 11 500 多名信息和通信技术专业人员参加了会议。安全、监测和处理信息和通信技术问题是会议讨论的议题之一。

古巴设立了计算机和网络安全理事会，受国家最高机关——政府和古巴共产党指导。该理事会的任务是为这一进程建议、协调和监督全面政策和战略。设立古巴计算机用户联盟的工作也已进行。

古巴支持第 69/28 号决议，将继续促进在全球和平发展信息和电信技术，为全人类造福。

萨尔瓦多

[原件：西班牙文]
[2015 年 4 月 21 日]

萨尔瓦多武装部队为加强信息和电信安全，对公共网络独立音频、视频和数据通信实行统一管理，组建并设置了周边信息安全工作队，此外还通过加密系统处理官方资料，以保护所有信息，防止任何外部人员企图渗透系统进行侵袭，防止网络攻击。

格鲁吉亚

[原件：英文]
[2015 年 5 月 26 日]

格鲁吉亚政府特别考虑到全国普遍开展的电子政务改革以及关键基础设施对信息与通信技术工具越来越强的依赖性，将信息和网络安全放在政治议程中的重要位置，认为应对网络威胁是国家和安全政策中必不可少的一部分。格鲁吉亚政府提出了这些关切，为了加强信息安全，采取了若干战略、法律、组织和体制措施。

2013 至 2015 年网络安全战略和行动计划是在全国层面处理网络安全问题的第一个战略，也是概述网络安全领域国家政策的主要文件，其中包括战略目标和指导原则，并阐述了具体行动和任务。网络安全是国家安全政策的主要优先事项，保护网络安全对于国家安全来说，与保护土地、水域和领空同样重要。

为进一步实现信息安全的制度化，格鲁吉亚司法部于 2010 年成立了数据交换局，作为负责制定和执行信息与网络安全政策及标准的中央政府机构，特别是完成以下任务：

- 在公共部门和核心基础设施领域采用并执行新信息安全政策和标准
- 成立国家计算机应急反应小组，执行网络安全任务
- 提供信息与网络安全咨询服务，开展信息安全审计，提供网络安全服务
- 开展提高对信息与网络安全认识的活动

格鲁吉亚信息安全法律和监管框架包括在 2011 和 2012 年间颁布的信息安全法及补充该法的次级规范法。格鲁吉亚立法中使用的主要概念详细介绍了基于国际标准化组织 27 000 标准系列的信息安全政策。法律着重说明了在执行信息安全

政策的过程中有关核心基础设施的某些权利和义务，并建立了与国家政府计算机应急小组的合作机制。

格鲁吉亚采取了重要步骤，增强国际合作，与合作伙伴共享所积累的知识。其中一个值得注意的例子是，数据交换局与欧洲联盟军事参谋团(来自奥地利、爱沙尼亚、波兰等国)和邻国(阿塞拜疆、亚美尼亚、摩尔多瓦共和国、土耳其等国)签订了双边合作协议和谅解备忘录。

格鲁吉亚承认，为了应对信息安全挑战，区域和国际合作机制愈加重要。为此，应努力增加专门处理此类重要问题的国际活动的数量，增进与主要利益攸关方之间的信任，继续与国际社会合作确定战略原则和法律概念。

德国

[原件：英文]
[2015 年 5 月 27 日]

开放、自由、安全、可靠的因特网为经济增长、社会发展、科学进步、促进民主、善政和法治提供了大好机遇。与此同时，人们越来越关注网络空间造成的国际安全风险。近几个月来，针对媒体平台等十分引人瞩目的目标的恶意软件活动不断增加。特别是，对核心基础设施的攻击可能造成严重后果。

目前，全方位的“网络战争”似乎并不可能。但是，在较大规模的战争活动中有限地使用网络能力已经成为现实，在混合冲突中也是如此。此外，网络空间中的事件可能会升级为现实世界中的冲突。

在这种环境下，德国主张采用三管齐下的办法：就国家在网络空间中负责任行为的原则达成一致，参与建立信任的措施，加强网络防御能力。

联合国是建立网络空间中国家负责任行为规则的核心平台。2012 至 2013 年从国际安全角度看信息和电信领域的发展政府专家组达成了共识，认为国际法特别是《联合国宪章》可适用于网络空间，这是一个重要的起点。2014 至 2015 年政府专家组在此基础上继续开展工作，德国再次积极参与了专家组的工作。

对网络空间中负责任国家行为的规则、规范和原则达成一致理解可以提高国际透明度和可预测性，进而促进和平与稳定。例如，这有助于进一步达成共识，决定武装冲突法如何适用于军事网络空间能力的使用，而越来越多的国家正在发展这一能力。

关于能力建设问题，德国极为重视区域组织的作用。2013 年，欧洲安全与合作组织就一套初步的网络建立信任措施达成了共识。执行工作正在顺利开展，第二套措施正在谈判之中，主要处理建立信任与合作问题。德国即将担任欧洲安全与合作组织的主席，计划在这一过程中将网络安全作为优先工作。

德国正在筹备信息技术安全法，在国家层面加强网络抗御能力。法律草案界定了核心基础设施信息技术安全的最低要求。草案规定了报告重大事件的义务，以完善整体安全系统，在总体上更好地保护公众。德国还为其他国家提供支持，加强它们管理网络安全风险的能力。

德国答复的全文可查阅 www.un.org/disarmament/topics/informationsecurity/。

荷兰

[原件：英文]
[2015 年 5 月 29 日]

为确保网络空间保持开放、自由和安全，国际社会有共同利益，也承担着共同责任。荷兰认为，普遍接受并遵守一套负责任国家行为的规范有助于促进安全。从国际安全角度看信息和电信领域的发展政府专家组已经开展了很多工作。但是，还需要在下列领域开展进一步工作并采取具体措施：

- 使各国更深入地理解国家行为规则方面的既有国际法和和规范可如何适用于网络空间，特别是适用于达不到武装冲突程度的网络行动的国际法律框架
- 确定自我约束和互助方面的规范和额外措施，特别是为某些系统和网络建立特别标准保护措施，包括提供基本民用服务的核心基础设施，民间事件应急架构，以及全球因特网的某些关键组成部分
- 加强法律、外交和政策能力，加强在网络空间国际和平与安全领域最佳做法的交流。在网络空间第四次全球会议期间，在海牙建立的网络专门知识全球论坛可以在这方面发挥重要作用

由于因特网已成为我们所有人的战略资产，需要就有关问题进行广泛的国际讨论。荷兰将继续积极协助促进对话。

荷兰答复的全文可查阅 www.un.org/disarmament/topics/informationsecurity/。

巴拿马

[原件：西班牙文]
[2015 年 6 月 3 日]

今天，信息和通信技术正在迅速发展。因此，所有巴拿马人在日常生活中与技术和通信的接触与日俱增。

我们现在的生活与通信方式和信息处理方式的发展息息相关，这已成为一个事实。

巴拿马政府已按照这一趋势采取了行动，使其适应安全机构的具体需要。为此，政府一直在进行技术改进，实现更高效、更安全的连通。

在这些改进工作中，巴拿马政府逐步制定通信实施计划，其中包括网络、安全和电话技术方面的内容。有关制造商确认，这些内容符合国际标准。

巴拿马政府为保护其因特网、数据和电话信息的安全，建立了基于内部防火墙平台的基础设施，并与国家多方位服务网络相联。

巴拿马政府利用基于安全防火墙的数据会话，确保信息的保密性和保护。

我们认为，随着用于适应安全机构安保需求的通信解决方案日益先进，这些机构必须能够获得有助于促进信息领域和谐发展的工具，采取积极和预防性措施。安全机构应利用这一技术态势，因为我们有义务保护地方和国际社会的安全。

秘鲁

[原件：西班牙文]
[2015 年 6 月 30 日]

信息技术部对信息安全问题的一般看法

秘鲁国家警察通过各级组织和职能结构的各种不同系统安全政策来管制其企业数据网络。

- 在信息安全方面，企业数据网络已经通过托管安全服务外包，由一个安全运营中心运行。
- 角色和身份工程的工作已经在计划中；这将允许用户进行独特的访问控制，确保可追溯性并提供审计工具。

在国家层面采取措施加强信息安全

预防措施包括：

- 指定网络管理员
- 对工作人员进行信息技术方面的培训
- 国家警察数据中心服务器的软件授权
- 实施“私有云”
- 资料备份
- 备份电力系统(不间断电源)
- 升级配电板和电气连接

- 在系统遭受攻击或拒绝服务的情况下外包周边安全服务(外部)。

决议标题中提到概念的内容

更新国家警察技术平台和警察信息系统，以整合信息手段，有效改善国家公共安全，通过提供服务来确保国家之间的互操作性，从而促进国际安全。

国际社会为加强全球信息安全可采取的措施

- 传播媒介的标准化，包括设备和通信协议的类型
- 可保证高可用性的技术平台的标准化，以实现国际安全方面各国的互用适用性
- 信息安全机制的标准化
- 在“信息场”的概念中，每个参与国际安全的国家都面临风险因素，并有可能通过建立自动化信息机制，确定打击和(或)遏制何种问题的共同目标。例如，在秘鲁，将考虑的问题包括毒品贩运、恐怖主义、有组织犯罪、走私、洗钱和贩运等。

葡萄牙

[原件：英文]
[2015 年 4 月 24 日]

大会在关于从国际安全角度看信息和电信领域的发展的第 69/28 号决议中回顾了科学和技术在国际安全方面的作用，认识到这些领域的发展可以用于民用和军事用途。虽然信息和电信领域的发展意味着有更多的机会实现文明进步和国家间合作，增强人类的创造潜力，加强全球社会中的信息流通，但另一方面，我们发现这些技术和手段可能会被用于不利于国际稳定与安全的目的，可能会对国家完整造成不利影响。

在同一决议中，大会呼吁会员国考虑到关于从国际安全的角度看信息和电信领域的发展政府专家组的报告(A/68/98)，在以下四个领域作出贡献：

(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) 旨在加强全球信息和电信系统安全的有关概念的内容；

(d) 国际社会为加强全球一级的信息安全可能采取的措施。

政府专家组的报告载有以下领域的建议：负责任国家行为的规范、规则和原则；建立信任措施和信息交流；能力建设措施。

根据这些建议，我们可以对我国情况作如下说明：

界定负责任国家行为的规范、规则和原则

葡萄牙认为，网络信息的安全十分重要，这种安全性一直在提高。

我们必须强调，我们已加大力度执行网络安全和完整性方面的立法，为此采用了风险评估方法，这需要在技术和组织层面采取适当的安全合作措施，报告对服务提供产生重大影响的安全违规或完整性损失事件。

在概念层面，必须深刻认识到，监管条例应当主要源自国际规则。

在国际一级，必须加强信息共享，在边境地区开展实地培训活动。

建立信任措施和信息共享

考虑到全球化的大背景，促进所有利益攸关方(包括公共和私营部门)之间的共享信息至关重要。

在国家一级，我们集中努力开展公共和私营实体都参与的联合活动、促进技术标准化并举行会议和研讨会，其中部分会议有国际发言者参与。

能力建设措施

采取能力建设措施十分重要。然而，培训和维持有关活动的人力资源面临困难。

有必要在安全等若干领域促进所有主要利益攸关方获取知识，促进集体培训活动。

卡塔尔

[原件：阿拉伯文]
[2015 年 6 月 24 日]

卡塔尔国继续监测信息安全领域中现有和潜在的威胁。卡塔尔国制定了战略，应对这种威胁，同时又符合保持信息自由流动的需要。卡塔尔国认为，信息安全对国家和全球安全至关重要。为维护信息安全，卡塔尔国采取了一系列措施，以升级相关技术，完善立法、监管和执法。卡塔尔国还在其国内法律允许的情况下，在区域和国际层面就有关问题协调和合作。

卡塔尔国认为，国际社会应继续努力制定一份具有约束力、保障信息安全的国际文书，从而促进信息安全。此类文书应规定开发防黑客程序，保持信息系统的连贯性。

大韩民国

[原件：英文]
[2015 年 6 月 11 日]

今天，网络空间开辟了新领域，带来了无尽的可能性，提供了前所未有的经济和社会效益。然而，因其开放、匿名、不分国界的性质，网络威胁正在对国际安全造成严重挑战。

大韩民国经历了一系列网络攻击，包括最近在 2014 年对核电站运营商的攻击。为了更有效地应对网络威胁，大韩民国在 2015 年 3 月颁布了综合计划来加强网络安全态势，设立了网络安全事务总统秘书职位。大韩民国坚信，必须商定一套适用于网络空间的国际准则，实施建立信任和建设网络能力的措施。

在这方面，大韩民国对关于从国际安全的角度看信息和电信领域的发展政府专家组 2013 年报告的结论表示欢迎。该报告确认对国家在网络空间中行为适用国际法的可能性，并期待进一步讨论商定原则将如何适用于网络空间中的国家行为。大韩民国 2014 年与联合国裁军研究所共同主办了亚洲-太平洋国际法与网络空间国家行为区域研讨会，使该区域各国有机会讨论与网络安全有关的事项。

大韩民国政府还致力于加强与主要国家的双边和三边合作，并积极参加网络问题区域和国际论坛，如东南亚国家联盟和联合国政府专家组区域论坛。作为 2013 年首尔网络空间会议的东道国，大韩民国与荷兰密切合作，筹备 2015 年在海牙举行的全球网络空间会议，并将继续促进伦敦进程会议。

大韩民国答复的全文可查阅 www.un.org/disarmament/topics/informationsecurity/。

西班牙

[原件：西班牙文]
[2015 年 5 月 26 日]

西班牙认为，信息和通信技术为全世界所有社会提供了重要支持，但此类技术的全球化带来严重风险和威胁，如网络间谍活动、网络恐怖主义、黑客行为和网络战争。

在设立国家网络安全理事会之后，西班牙继续取得进展，制定了基于国家网络安全战略的计划，以加强预防、保护、探测、分析、应对、恢复和协调能力，更好地应对网络威胁。

西班牙继续在欧洲联盟和欧洲安全与合作组织、北大西洋公约组织、欧洲委员会等主要的国际论坛积极参与促进国际合作，密切监测所有影响到网络安全的战略举措。

西班牙继续认为联合国可为就网络安全问题达成国际共识发挥重要作用，并支持举行包括其他国际论坛在内的制度化对话，以此促进区域合作，建立全球标准、最佳做法、国家行为守则和建立信任措施，最终确保和平、安全利用信息技术。

西班牙认为，各国应当在四个领域达成共识。首先，应制定合作性质的建立信任措施，最终目标是促进各国在网络安全领域的透明度，加强各国能力，消除任何发现是来自第三国的可能袭击。

第二，西班牙认为，各国应当继续思考国际法原则和规范如何解释和适用于网络空间；特别是涉及使用武力或以武力相威胁、人道主义法、保护个人基本权利和自由的原则和规范。

第三，西班牙认为，应加强国际合作，为此改善沟通渠道，建立计算机应急小组的协调机制，开展联合演习和其他类似行动，促进司法和警察合作机制。

最后，应继续鼓励和协助受援国开展必要的能力建设，协助其制定确定网络安全标准的国家法律。

西班牙答复的全文可查阅 http://www.un.org/disarmament/topics/informationsecurity/。

大不列颠及北爱尔兰联合王国

[原件：英文]
[2015 年 5 月 29 日]

大不列颠及北爱尔兰联合王国欢迎有机会对大会题为“从国际安全角度看信息和电信领域的发展”的第 69/28 号决议作出回应。本次回应是以对 2013 年第 68/243 号决议的回应为基础的。鉴于在此背景下对“信息安全”一语有不同的解释，联合王国在回应全文中均采用其偏好的术语“网络安全”及相关概念，以避免混淆。

联合王国承认，网络安全是国家和国际关键基础设施的基本要素，是在线经济活动和社会活动的重要基础。网络空间活动构成的实际威胁和潜在威胁值得严重关切。我们在回应中详述了在国家和国际层面为加强该领域安全并促进合作已经采取及将要采取的措施。这些措施是根据联合王国 2011 年 11 月公布的网络安全战略采取的。

联合王国继续在国际网络安全辩论中发挥领头作用。我们为所有四个关于从国际安全的角度看信息和电信领域的发展政府专家组提供了专家。我们认为，前一个专家组的协商一致报告显示，在就网络空间国家行为规范达成共同谅解以及在确认国际法在网络空间的可适用性方面已取得了很有价值的进展。我们期待收到现有专家组 2015 年 6 月讨论的结果。联合王国还对欧洲安全与合作组织在 2013

年谈判成果的基础上关于网络空间今后可能的建立信任措施的讨论表示欢迎，并对其他区域组织的类似工作表示欢迎。

本次回应概述联合王国支持和改进网络安全及交流最佳做法的工作，包括在国内外开展的工作，也包括与国际组织合作应对网络犯罪和主要事件以及建设网络容量和能力的工作。联合王国期待在所有这些领域取得更大进展。联合王国有幸积极参与处理这些重要问题，并希望进一步参与加强网络安全能力和国际合作。

联合王国答复的全文可查阅 www.un.org/disarmament/topics/informationsecurity/。