联合国 A/71/172

大会

Distr.: General
19 July 2016
Chinese
Original: Arabic/English/French/
Russian/Spanish

第七十一届会议

临时议程* 项目 94

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/71/150。

16-12486 (C) 110816 150816

一. 导言

1. 2015 年 12 月 23 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 70/237 号决议。在该决议第 4 段中，大会邀请所有会员国结合从国际安全角度看信息和电信领域发展政府专家组报告(A/70/174)所载评估意见和建议，继续向秘书长通报本国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该领域国际合作所作的努力；

(c) 决议第 3 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采取的措施。

2. 根据这一要求，2015 年 2 月 15 日向所有会员国发出了普通照会，邀请各国就此提供资料。截至本报告编写之时收到的回复载于第二节。此后收到的任何其他回复，将作为本报告增编印发。所有呈件的全文，可查阅 www.un.org/disarmament/topics/informationsecurity。

二. 各国政府的回复

阿尔巴尼亚

[原件：英文]
[2016 年 4 月 15 日]

阿尔巴尼亚在机密信息安全和保护领域的主要优先事项是签署阿尔巴尼亚共和国政府与欧洲联盟之间关于交换和保护机密信息的安全程序协议。上述协议已于 2016 年 3 月 3 日在地拉那签署，预计阿尔巴尼亚共和国议会将适时予以批准。

在采取并执行适当措施方面，为了加强信息安全和促进相关国际合作，阿尔巴尼亚对法律规章作了修订。

- 部长会议 2015 年 3 月 4 日第 188 号决定，“核准确保工作人员安全的规则”
- 部长会议 2015 年 3 月 4 日第 189 号决定，“确保被标示为‘国家秘密’的机密信息及北约信息的实物安全”
- 部长会议 2015 年 3 月 4 日第 190 号决定，“对部长会议第 80 号决定‘确定销毁机密信息的标准和程序’的几处修改和补充”
- 部长会议 2014 年 10 月 22 日第 701 号决定，“核准确保工业领域机密信息安全的规则”

在机密信息的实物保护方面，阿尔巴尼亚拥有更加全面的法律规章。考虑到机密信息的不同等级，阿尔巴尼亚对“安全领域”作了重新定义和定位。

继通过关于工作人员安全的新决定之后，机构间合作、监督和国家机构检查最终有所增加。国家机构开始修订工作人员职责清单，并根据责任领域发放相关安全证书。

关于工业安全，阿尔巴尼亚着重审查了信息安全政策，包括部长会议通过2014 年 10 月 22 日第 701 号决定采取的做法。

阿尔巴尼亚强调的另一个重要步骤是拟订一部处理机密信息的新法律，该法律将保持高效、现代且符合欧洲高标准。对这一领域国家立法的审查已经完成，考虑到了欧洲联盟的既有成果，特别是关于保护欧盟机密信息安全规则的第2013/488/EU 号理事会决定。

澳大利亚

[原件：英文]
[2016 年 5 月 31 日]

应大会第 70/237 号决议的要求，澳大利亚谨就国际安全背景下信息和电信领域的发展发表看法。本呈件以澳大利亚针对 2014 年第 68/243 号决议和 2011 年第 65/41 号决议提供的资料为基础。

网络安全与创新和国家安全都有着本质联系。网络安全是创新、增长和繁荣的基础，也是一个全球机遇，政府、私营部门和社区都投资其中，同时又都能够从中获益。

全球社会要准确了解网络安全。每一个人，包括政府、企业和个人，都要合力打造值得信任的网络环境。不仅仅是为了保护关键信息，还要提供让创新茁壮成长的环境，使技术产业能够蓬勃发展。要利用不断增长的全球需求，推出更好的网络安全解决方案、设备和技能人员。

澳大利亚确认，强大的网络安全是全球经济增长和繁荣的基本要素。2015 年，澳大利亚审查了本国处理网络安全的办法，并于 2016 年 4 月 21 日推出了新的网络安全战略。

澳大利亚认为，国际社会的优先要务是阐述如何将国际法适用于国家在网络空间的行为，特别是非冲突情况下的行为。考虑到我们在保护因特网全球性方面的共同利益，有必要作出进一步努力，阐明如何将主权和管辖权等关键概念适用于网络空间。2015 年政府专家组的报告就关键基础设施保护、计算机应急小组、国家提供协助的责任、针对网络犯罪开展合作以及防止恶意网络工具和技术扩散等问题提出的自愿准则，拥有进一步发展的空间。重要的是，将建立信任措施工作从促进提高透明度转为落实合作措施。

加拿大

[原件：英文]
[2016 年 5 月 27 日]

关于网络问题，加拿大认为：

- 一个自由、开放和安全的网络空间对于全球安全、经济繁荣以及促进人权、民主和包容至关重要。
- 任何应对网络威胁的办法都必须同时尊重人权和基本自由。
- 现有国际法适用于国家对信息和通信技术的使用。
- 推广和平时期准则，有助于维护一个通过负责任的行为指导国家行动、维持伙伴关系和支持网络空间稳定的环境。
- 实用建立信任措施已被证明能够缓解紧张关系和减少武装冲突风险。

在国家一级，加拿大政府自 2010 年推出网络安全战略以来，一直致力于帮助确保加拿大网络系统的安全，为加拿大人民上网提供保护。自那以来，加拿大还发起了“确保网络安全”公共认知运动。政府近期还承诺对现有措施进行审查，以保护加拿大人民和我们的关键基础设施免受网络威胁。

在国际一级，加拿大通过多种方式积极处理网络问题：

- 加拿大将继续促进制订和平时期网络空间国家行为准则，包括推广 2012-2013 年和 2014-2015 年联合国政府专家组的成果。加拿大已获选参加 2015-2016 年专家组的工作。
- 加拿大于 2015 年 7 月批准了《布达佩斯公约》。加拿大鼓励各国成为该公约缔约国，或以该公约为示范，执行本国有关网络犯罪问题的法律。
- 自 2007 年以来，加拿大已承诺提供 825 万美元用于支持美洲和东南亚地区的网络安全能力建设项目。
- 加拿大是全球网络专才论坛的创始伙伴。
- 加拿大与美国通过“停止/思考/连接”联盟，统一了两国的网络安全公共认知运动倡议。
- 加拿大还与美国一道，实施旨在加强两国网络基础设施复原能力的网络安全行动计划。
- 加拿大一贯致力于在各种论坛制订建立信任措施，包括欧洲安全与合作组织和东南亚国家联盟地区论坛。
- 加拿大支持北大西洋公约组织(北约)努力加强北约和各个盟国的网络防御能力。加拿大已向北约卓越合作网络防御中心捐赠 100 万美元。

- 加拿大支持使用信息和通信技术作为发展工具，包括帮助社区组织提供冲突时紧急援助等基本服务。

- 加拿大国际发展研究中心帮助在世界各地推动发展，通过信息和通信技术促进发展研究和能力建设。

哥伦比亚

[原件：西班牙文]
[2016 年 6 月 13 日]

哥伦比亚通过“数字生活”计划(2010-2014 年)和新的“数字生活为人民”计划(2014-2018 年)完成了数字革命，仅用五年时间就将因特网连接总数从 220 万增加到超过 1 220 万。哥伦比亚将成为第一个所有城市都有高速因特网连接的拉丁美洲国家。在同一时期，各教育实体获得了 200 多万台终端机；微型和中小型企业目前已有 74%与因特网相连(相比 2010 年只有 7%)；上网家庭数增长了 90%；我们还通过 7 621 个数字生活小站(设在居民人数超过 100 人的农村中心)，将因特网送到最偏远的农村地区。除其他许多成就外，我们还拥有拉丁美洲最大的数字创业者群体，人数超过 10 万。

国家政府认识到，如果得不到公民或企业的信任，也就是说，如果在数字环境中感受不到安全，那么，就不可能最大限度地利用信息和通信技术。数字安全事件不断增加，对这种感受的影响也越来越大。

(a) 国家一级为加强信息安全和促进该领域国际合作所作的努力：

哥伦比亚不久前刚刚推出了新的国家数字安全战略，载于 2016 年 CONPES 3854 号文件，其中设法确保哥伦比亚政府、公共和私营组织、执法人员、学术界和广大个人有能力在一个可靠且安全的数字环境中最大限度地获取经济和社会效益，同时大幅提高所有经济部门的竞争力和生产力。该政策由众多利益攸关方参与制订，哥伦比亚也因此成为世界上最早将 2015 年 9 月经济合作与发展组织发布的数字安全风险管理建议纳入国家政策的国家之一，在本区域更是第一个这样做的国家。

该政策首先规定制订清晰的数字安全体制框架。为此目的，将在政府最高级别建立协调和咨询机构，并在国家行政部门的所有机构中设立跨部门联络单位。其次，将创造适当条件，使众多利益攸关方能够在社会经济活动中管理数字安全风险，并在使用数字环境的过程中建立信任，包括为此建立积极持续参与的机制，确保制订适当的法律和监管框架，以及提供关于数字环境中负责任行为的培训。第三，将采取风险管理办法，在国家一级和跨国一级加强数字环境中的国防和安全。最后，同样重要的是建立具有战略重点的常设机制，促进国家和国际各级在数字安全领域的合作、协作和协助。

(b) 第 70/237 号决议第 3 段所述概念的内容：

哥伦比亚作为最近成立的政府专家组(2014-2015 年)的成员，完全同意需要进一步审视与信息和全球电信系统安全有关的概念，以及与网络空间适用国际法有关的事项。

(c) 国际社会为加强全球一级信息安全可采取的措施：

综上所述，我们完全赞同政府专家组成员专家一致发布的建议，包括各国为促进和平使用信息和通信技术自愿采取措施和良好做法以及开展能力建设与合作的建议，让这些技术继续作为经济和社会发展工具，服务于各国，特别是技术欠发达国家。

古巴

[原件：西班牙文]
[2016 年 5 月 6 日]

古巴与第 70/237 号决议有着同样的关切，即信息技术和手段可能会被用于破坏国际稳定和安全，还可能对各国基础设施的完整性造成不利影响，损害各国民事和军事安全。

第 70/237 号决议还适时地强调，需要防止信息资源或技术被用于犯罪或恐怖主义目的。

在这方面，古巴重申对某些个人、组织和国家暗中非法使用其他国家的计算机系统来攻击第三国感到极为关切，因为这可能引发国际冲突。

所有国家开展合作，是防止和应对这些威胁、避免网络空间变成军事战场的唯一途径。

通过使用电信，明里暗里破坏各国法律和政治秩序，这种行为违反该领域的国际公认准则，会导致紧张关系和状况，也可能损害国际和平与安全。

拉丁美洲和加勒比国家元首和政府首脑在 2014 年 1 月于哈瓦那举行的拉丁美洲和加勒比国家共同体(拉共体)第二次首脑会议上宣布拉丁美洲和加勒比区域为和平区，以便除其他目标外，促进国家之间以及与其他国家的合作和友好关系，不论各国在政治、经济和社会制度或发展水平上有何差异，同时实现宽容及睦邻和平共处。

2016 年 1 月在基多举行的拉共体第四次首脑会议再次强调了通过信息和通信技术包括因特网来促进和平、人类福祉、发展、知识、社会包容和经济增长的重要性。会议还重申，和平使用信息和通信技术必须符合《联合国宪章》的宗旨和原则以及国际法。会议着重指出，决不能将此类技术用于扰乱社会或制造可能助长国家间冲突的局势。

不过，由于美国政府违反《联合国宪章》的宗旨和原则以及国际电信联盟的各种规章，不断发送反对古巴的电台和电视广播，侵犯古巴主权，上述努力继续受到威胁。

这些非法电台和电视广播持续攻击古巴的空中电波，散布专门为煽动推翻古巴人民建立的宪政秩序而设计的节目。举个例子，仅 2016 年第一季度，就使用 23 个频道，平均每周发送了 1 880 个小时反对古巴的非法广播。

古巴希望能立即终止这些挑衅政策，因为这些政策也不符合古巴和美国两国政府在恢复外交关系时的商定，在相互尊重与合作的基础上发展关系。

古巴还希望取消给古巴人民造成严重损害的经济、商业和金融封锁，因为这些封锁对古巴人民日常生活的各个领域，包括信息和通信领域带来了有害影响。

国际合作对于应对滥用信息和通信技术带来的危险不可或缺。国际电信联盟在政府间辩论网络安全问题时可以发挥重要作用。

古巴支持第 70/237 号决议，将继续为全球和平发展信息和电信技术并使其造福于全人类作出贡献。

萨尔瓦多

[原件：西班牙文]
[2016 年 4 月 26 日]

萨尔瓦多武装部队已升级周边安保计算机设备，并实施了针对计算机网络资源的安保政策(定期更换用户密码，限制使用 USB 接口及 DVD 和 CD 读取器，以及禁止使用 C 类设备)。

芬兰

[原件：英文]
[2016 年 5 月 31 日]

芬兰很荣幸有机会就大会第 70/237 号决议提供资料。在国家一级，芬兰已作出下列努力：

(a) 芬兰国家网络安全战略(2013 年)及其执行方案(2014 年)确定了加强网络安全和复原能力的关键准则和行动。执行方案目前正通过一个多利益攸关方协商进程进行更新，目标是在 2016 年完成。

(b) 自国家网络安全战略通过以来，芬兰设立了国家网络安全中心和网络犯罪预防中心，并任命了一名网络事务大使。国家信息安全战略于 2016 年 2 月获得通过。

(c) 作为芬兰发展合作的组成部分，芬兰支持各种信息和通信技术促进发展及网络能力建设项目。芬兰是全球网络专才论坛的创始伙伴，并已加入美国牵头

的到 2020 年让 15 亿人上网的“全球连接倡议”。芬兰打算加入新设立的世界银行数字发展伙伴关系信托基金，并支持以多利益攸关方模式进行互联网治理。

(d) 芬兰在多边和区域论坛上以及在双边接触中，都积极就网络问题开展国际对话。在欧洲安全与合作组织(欧安组织)框架内，芬兰致力于加强网络空间的信任、安全和稳定，并执行商定的网络建立信任措施和安保措施。

(e) 芬兰赞同国际安全背景下信息和通信技术领域联合国政府专家组 2015 年的报告。芬兰积极参与讨论网络空间国际法问题，包括就《塔林手册 2.0》进行协商以及参加联合国裁军研究所讲习班。芬兰于 2012 年加入了“自由在线联盟”，并为“数码卫士伙伴关系”作出了贡献。

(f) 芬兰于 2007 年成为《布达佩斯公约》缔约国，并于 2015 年推出了新的战略政策计划，将资源用於预防计算机犯罪和开发网络安全知识。此外，芬兰还制订了全面预防网络犯罪计划。

国际社会开展进一步工作的优先领域：

(a) 芬兰非常重视新成立的政府专家组的工作，并已准备为其成功作出贡献，包括推动确定网络空间负责任国家行为准则，尤其强调和平时期活动；

(b) 在欧安组织框架内进一步制订和执行区域建立信任措施；

(c) 继续支持网络能力建设，以期加强网络空间的复原力和安全；

(d) 芬兰将继续支持和鼓励多利益攸关方对话，并优先加强国家及国际公私伙伴关系。

印度

[原件：英文]
[2016 年 6 月 9 日]

信息技术有助于经济增长和社会连通，但也有需要应对的严峻挑战。在信息和通信技术部门发展壮大的同时，网络威胁也与日俱增，包括网络攻击、网络犯罪、网络恐怖主义、间谍和洗钱。有证据显示，恐怖主义团体(如伊黎伊斯兰国)使用互联网和社交媒体平台开展邪恶的活动，包括招募、集资、宣扬和鼓吹激进。滥用社交媒体是一个重大关切。社交媒体虽然带来巨大的连通性，但也可能会被滥用于加剧族裔和社会分歧。

对国际社会而言，重要的是对网络空间国家行为有一个共同的理解，并按照联合国政府专家组 2015 年报告的建议，采取建立信任和能力建设措施。对因特网治理问题的讨论不能因为语义上有分歧而陷入停滞。虽然不同利益攸关方在各自领域有着不同的作用，但在涉及国家安全的网络安全问题上，各国政府要发挥首要作用。对于网络威胁、网络犯罪和网络恐怖主义，要建立适当的信息分享机

制。政府机构之间还要开展实时合作，处理网络犯罪问题。此外，网络战争和网络理论及其对国际安全的影响问题，也应在所有国际论坛上进行讨论。虽然网络空间负责任国家行为原则仍然有待商定，但联合国政府专家组 2015 年报告所列对建立信任措施的共同理解可用于在网络安全领域采取适当的能力建设措施。在这方面，全球网络专才论坛制订的框架提供了有益的指导。

印度是信息和通信技术的重要利益攸关方，支持在因特网治理中推行多利益攸关方主义，并主动参加了各类国际论坛，包括政府专家组、信息社会世界首脑会议成果文件执行情况全面审查公开协商进程和互联网名称与数字地址分配机构。印度在与所有利益攸关方协商后采取了统筹办法，通过一系列政策、法律、技术和行政步骤应对网络安全关切，并促进该领域的国际合作。印度的法律框架已经与世界上的其他法律框架保持一致。国家网络安全政策(2013 年)已经推出，目标是为公民、企业和政府建立安全且复原力强的网络空间，其中强调了网络安全领域的能力建设、技能拓展和公私伙伴关系。

日本

[原件：英文]
[2016 年 5 月 27 日]

对信息安全问题的一般看法

日本认为，网络空间应当是一个能够保证自由、没有不必要限制、所有想要访问者都不会被无端拒绝或排斥的空间。我们的努力遵循以下五项原则：信息自由流动、法治、开放、自治和多利益攸关方办法。

国家一级为加强信息安全和促进该领域国际合作所作的努力

1. 国家一级为加强信息安全所作的努力

根据 2015 年 9 月制订的网络安全战略，日本致力于加强信息安全。

2. 国家一级为促进国际合作所作的努力

日本的努力分为以下三个部分：(1) 网络空间的法治；(2) 建立信任措施；(3) 能力建设。关于促进法治，日本主动为国际讨论作出贡献，以促进对现有国际法适用于网络空间的共同理解，并制订不具约束力的负责任国家行为自愿准则。关于建立信任措施，日本通过双边对话和东南亚国家联盟(东盟)地区论坛等多边框架，积极促进建立信任。关于能力建设，日本以东盟地区为重点，积极参与人力资源开发援助和技术合作。

决议第 3 段所述概念的内容

确认国际法的可适用性并制订不具约束力的网络空间负责任国家行为自愿准则，是确保国际社会稳定和可预测的基础。

国际社会为加强全球一级信息安全可采取的措施

关于促进法治，日本认为需要进一步阐述对和平时期国际法规则、与自卫权有关的法律和国际人道主义法的审议情况，并在下一期政府专家组中制订自愿准则。对于建立信任措施和能力建设，关键是推动每一个国家和区域执行政府专家组报告载列的建议。有必要研究开展实际合作的途径。

约旦

[原件：阿拉伯文]
[2016 年 5 月 2 日]

信息和通信技术已成为我们日常生活的必要组成部分，不仅以各种方式促进社会、文化和经济增长及地方社区发展，对个人与地方社区和广大世界开展互动也有诸多影响。

信息和通信技术的飞速进步使其面临风险和挑战。这些风险必须通过技术和法律手段予以应对，以期找到有效且实际的办法来减少风险和防止可能的灾难性后果。

约旦军队通过技术开发，在促进国家、区域及全球各级的安全与和平方面发挥了积极作用，包括使用这些技术来确保信息及有线和无线通信的安全，具体情况如下：

(a) 更新了通信和信息系统，为此使用加密 IP 技术，在约旦全境包括边界地带安装了有保护的网络，用于加强国家和区域安全；

(b) 参加与国际社会的安保合作，为此采用了与北大西洋公约组织和美国军队相互兼容、而且符合 1 类国际加密标准的通信系统；

(c) 提高了技术能力，为此添置了不依赖基础设施的通信系统，用于维护冲突区、难民营和偏远地区的国家安全。约旦军队还使用这一技术，支持在世界各地冲突地区的维持和平行动；

(d) 培训并验证了所有通信系统用户及维护和支助人员，没有找供应商帮助，以确保任何时候都具有最高层次的可靠性和可依赖性；

(e) 对军方使用的所有系统适用最高指挥和控制标准，以提高国家及区域安保协调与合作的水平；

(f) 积极参加国际会议并了解会议成果，以增强友好军队之间的互补性，避免干预区域邻国所使用的通信系统，并确保对国际边界进行有协调的控制和监视。

重点始终应当是让公民认识无处不在的网络威胁，以及如果能够使用电子系统，通过网络安全措施最大限度地减少和抗击这些威胁。在处理各类信息的同时加强安全认知，不应妨碍技术带来的效益。

为保护国家命脉信息网络，目前已采取下列措施：

(a) 对所有语音、数据和视频通信系统进行加密；

(b) 使用闭合网络(内网)；

(c) 通过自成一体的外围设备，建立与其他安全机构的联系；

(d) 采用信息和通信安全措施以及“需要知道”原则。不间断地检查访问权限和用户身份。

(e) 使用虚拟网络，根据信息访问权限，让用户与联网屏幕互动。访问或连接不能通过闪存驱动器等其他设备进行；

(f) 约旦已颁布下列网络安全立法：

(1) 关于网络犯罪问题的法律已经颁布；

(2) 关于电子交易问题的法律已经颁布；

(3) 国家网络安全和保护战略已经拟订；

(4) 国家网络安全和保护政策已经拟订；

(5) 国家网络安全和保护战略已于 2012 年获得内阁核准。

我们提议采取下列全球措施：

(a) 按照重要程度对通信网络和信息进行分类；

(b) 执行网络安全和保护措施；

(c) 适用“需要知道”原则；

(d) 使用加密和跳频等技术措施；

(e) 核查用户和网络服务权限并进行归类；

(f) 通过自成一体的外围设备将网络相连接；

(g) 在某些网络中使用闭合内网，尽量避免使用万维网；

(h) 加强联合国内网，使其与公共网络分离，并通过加密、安全防护和服务权限核查等技术和安全措施，对其进行保护；

(i) 促进计算机应急小组之间的合作，跟踪违规行为，安装防护设施，并弥补不足之处；

(j) 散发安全措施和处理违规行为的程序。

我们强调，信息和通信技术可通过以下方式，在推动可持续发展方面发挥潜力，特别是在比较贫穷和偏远的地区：

(a) 信息和通信技术可加速消除贫穷，例如，通过流动银行服务，将直接和实际效益带给世界各地从未有过银行体验的数百万人；

(b) 现代技术和新通信媒体向农民提供关键的作物耕种信息，可缓解饥荒带来的影响。

建议：

(a) 组建国际响应和恢复小组，应对网络安全事件、危机和灾难；

(b) 定于 2016 年组建的从国际安全角度看信息和通信领域的发展联合国政府专家组应包含约旦的代表；

(c) 加强安全理事会成员之间的科学和研究合作及培训交流。

黎巴嫩

[原件：阿拉伯文]
[2016 年 5 月 24 日]

当今时代，网络安全影响到一系列经济、社会、政治、军事和人道主义问题。网络恐怖主义将是今后最重大的威胁之一，对超级大国和发展中国家都是如此。

网络战争发生于多个层面，包括：招募和动员网站；心理战；因特网信息交换和传播；针对网站、数据和信息系统的电子黑客；以及网络恐怖主义。

网络恐怖主义威胁在所有国家都有增加。黎巴嫩遭受网络攻击的主要是银行业(Gauss 病毒)和通信业。大多数电子服务都经常遭受攻击。

黎巴嫩促进网络安全与国际合作的努力包括：

- 1999 年颁布了关于电信保密的第 140 号法律和关于知识产权的第 75 号法律。两项法律都在某种程度上述及软件盗版问题。
- 2006 年，国内安全部队总局刑事调查司设立了打击网络犯罪和保护知识产权办公室。
- 2007 年设立了通信监管局，该局已成为国际打击网络威胁多边伙伴关系的积极成员。
- 2009 年，陆军司令部在情报总局内设立了电子取证司。
- 国防部目前正与本国及全球相关机构协作，致力于设立黎巴嫩计算机突发事件响应小组。国防部参加了所有相关举措，并举办了会议和培训班。
- 2012 年，内阁发布了关于设立国家安全委员会管理政府网站的决定。该委员会包含国防部的一名代表。

- 2013 年，内阁组建了负责研究朝向黎巴嫩领土的以色列敌军通信塔所致威胁的委员会。该委员会由国防部担任主席，成员包括其他相关部委。
- 2015 年，黎巴嫩军队设立了专职的网络安全司。
- 议会目前正在审议电子交易法草案。

国际社会为加强全球一级信息安全可采取的措施包括：

- 遵守联合国和信息社会世界首脑会议通过的旨在传播信息文化的决议，并与相关国际机构建立合作框架，确保分享信息和最佳做法。
- 国家打击信息犯罪的法律和规章应与全球规则统一，以防止出现数字天堂。
- 建立全球信息危机管理系统，并通过强有力的国际立法，加强本国法律应对全球和国际网络犯罪行为的能力。

波兰

[原件：英文]
[2016 年 7 月 18 日]

1. 一般看法

网络安全对于保持经济增长和维持民间社会运作至关重要。网络攻击不仅会影响私营部门和公共行政当局，还会影响关键基础设施中的工业自动化系统。

考虑到这些威胁的性质以及工商企业、行政部门和社会对信息技术的日益依赖，有必要确保信息和电信安全系统的连贯一致。所有利益攸关方，包括国家、企业和非政府组织，都必须参与其中，为确保网络安全作出贡献。

遵守国际法和国际准则，是国家之间维持网络空间和平与安全的必要条件。

提高国家能力，是加强国际网络空间安全的关键要素。

扩大网络空间的信任，将对国家之间在其他领域的关系产生积极影响。

网络空间和现实世界的人权和基本自由应得到同样的保护。尊重因特网上的基本自由，对于民主社会、可持续增长和繁荣不可或缺。

2. 本国加强网络安全和国际合作的举措

波兰的网络安全系统以各机构网络为基础，各实体在民事和军事层面以及与网络犯罪有关的领域开展合作。

波兰政府正在加紧努力制订国家网络安全战略和国家网络安全法。波兰网络安全系统的关键要素将包括程序、人员和技术。

去年，波兰主办了多项重要国际活动，为促进国际合作作出了贡献，包括 2015 年电信和信息安全会议(SECURE 2015)、欧洲网络安全论坛(cybersecforum.eu)以及关于境外安全保障问题的国际网络安全会议。

3. 全球一级为加强网络安全可采取的措施

有必要进一步制订网络空间建立信任措施，在全球、区域和国家各级执行。

国际社会应鼓励在网络安全领域开展国家能力建设。

必须深化双边及区域合作。由波兰、捷克共和国、斯洛伐克、匈牙利和奥地利组成的中欧网络安全平台是区域努力的一个极佳例子。

通过网络安全领域的国际演习，可以更好地理解威胁的性质和应对手段。“网络欧洲”或北大西洋公约组织的“锁盾”演习，就属于这种情况。

不应低估让代表非政府组织、工商企业和学术界的利益攸关方参与国际对话的作用。

葡萄牙

[原件：英文]
[2016 年 5 月 31 日]

大会关于从国际安全角度看信息和电信领域的发展的第 70/237 号决议回顾了科学和技术在这一背景下的重要性，确认这些领域的发展会带来民事和军事应用。如果说，信息和电信领域的进步意味着有更多机会拓展知识、开展国家间合作、促进人类创造力以及在整个社区传送信息，另一方面我们却发现，这些技术和手段可能会被用来破坏国际稳定和安全，还可能对各国的国家诚信造成负面影响。

第 70/237 号决议回顾 2015 年政府专家组的报告，要求会员国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该领域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概念所含内容；

(d) 国际社会为加强全球一级信息安全可采取的措施。

A/68/98 号文件所载报告就下列领域提出了一些建议：关于负责任国家行为的准则、规则和原则的建议；关于建立信任措施和信息交换的建议；关于能力建设措施的建议。

针对这些建议，葡萄牙发表以下看法：

一. 体现负责任国家行为的准则、规则和原则

1. 葡萄牙认为，网络信息安全相当重要，而且越来越重要。

2. 我们必须强调在努力执行关于网络安全和诚信的立法方面取得的进展，包括为此采取风险评估办法，要求在技术上和组织上采取适当的合作安全措施，并报告对服务部门的运作有重大影响的安全违规或诚信缺失现象。

3. 在概念方面，重要的是强化关于相关法规应主要源自国际法的观点。

4. 在国际一级，重要的是加强信息分享以及在边界地区开展实地训练演习。

二. 加强信任和信息分享措施

1. 至关重要的是结合全球化的广泛背景，促进在所有(公共和私营)利益攸关方之间分享信息。

2. 在国家一级，我们致力于完成有公共和私营实体参加的联合演习，推动技术标准化，并举办会议和研讨会，其中一些有国际演讲者参加。.

三. 能力建设措施

1. 制订能力建设措施相当重要。不过，在培训和保持与这些活动有关的人力资源方面困难不少。

2. 有必要为获取知识提供便利，并推动在所有主要利益攸关方之间就安全等多个领域进行集体培训。

塞尔维亚

[原件：英文]
[2016 年 5 月 31 日]

考虑到确保和发展信息安全的重要性，塞尔维亚共和国已将这一领域视为信息社会的一个战略优先事项。

塞尔维亚共和国国民议会于 2016 年 1 月通过了信息安全法，确定了信息安全的主管当局，负责依照国家和国际标准拟订法规，与其他国家主管当局合作，并开展执法检查。这项法律还界定了对塞尔维亚特别重要的信息和通信技术(信通技术)系统，运营方必须为确保信息安全采取适当的技术和组织措施。这些系统是：(a) 公共机构的信通技术系统；(b) 处理敏感个人信息的信通技术系统；(c) 公共利益领域(能源、运输、燃气、银行、保健等领域)的信通技术系统。

主管当局开展国际合作，尤其就具有下列特征之一的风险和事件发出警报：(a) 发展迅速，可能成为高风险；(b) 超出国家能力；(c) 可能影响到不止一个国家。

该法律在电子通信和邮政服务管理局内设立了国家计算机应急小组，除其他外，将与其他国家的类似机构开展合作。

该法律还规定了针对电磁泄露发射的密码安全和保护。

各国应合作加强全球信息和电信系统的安全，特别是维持有效和有针对性的网络安全事件信息交换、警报和通告机制。为此目的，各国应任命协调人，并将联系方式公之于众。应特别重视对关键基础设施的保护，在相关事件影响到不止一个国家的情况下尤其如此。各国还应就该领域的知识交流和教育开展合作。

考虑到在相互连通的世界里，网络攻击的风险增加，特征也更为明显，国际社会应鼓励各国开展合作和对话，促进建立相互网络安全能力，并向旨在促进信息安全领域合作的国际组织提供支持。共同和有效合作将有助于建立更加安全且有所保护的全球信通技术环境，让国家和公民远离网络世界的各种风险。

西班牙

[原件：西班牙文]
[2016 年 5 月 26 日]

西班牙认为，信息和通信技术(信通技术)为国际社会提供了巨大机遇，而且重要性不断提高。不过，也有一些令人不安的趋势给国际和平与安全带来了风险。因此，各国应开展有效合作，防止网络空间的有害做法，在知情情况下决不允许本国领土被用于实施使用此类技术的国际不法行为。

2015 年 7 月，国家网络安全委员会核准了源自国家网络安全计划的九项具体计划，以执行 2013 年国家网络安全战略提出的措施。

西班牙积极参加欧洲联盟、欧洲安全与合作组织、北大西洋公约组织、欧洲委员会和经济合作与发展组织所有涉及网络安全的战略举措。

2015 年，西班牙加入了“自由在线联盟”和全球网络专才论坛。

西班牙支持 2015 年 12 月通过的关于全面审查信息社会世界首脑会议各项成果执行情况的大会高级别会议的成果文件。

加强连通性、创新和获取信通技术，对于推动千年发展目标取得进展起了重要作用。西班牙认为，信息社会世界首脑会议进程应与 2030 年可持续发展议程保持密切一致，因为获取信通技术已成为一项发展指标，其本身也是一种愿景。

西班牙支持就网络安全问题达成国际共识，认为各国应继续思考如何在网络空间解释和适用国际法的原则和准则，特别是与使用或威胁使用武力、人道主义法以及保护个人的基本权利和自由有关的原则和准则。

西班牙支持国际社会关于和平使用信通技术为全人类造福的愿景。西班牙认为，《宪章》在这方面完全适用。依照国际法采取措施，及时、合理和恰当地应对可能影响国家安全的威胁或攻击，是各国的固有权利。

瑞士

[原件：英文]
[2016 年 6 月 7 日]

1. 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、经济及政治活动一个不可缺少的驱动因素。瑞士致力于抓住使用信通技术带来的机遇。不过，信通技术的使用也使得信息和通信基础设施的功能缺陷很容易被犯罪、情报、政治军事或恐怖分子滥用。经由电子网络实施的干扰、操纵和具体攻击，是信息社会必然要面对的风险。

2. 国家一级为加强信息安全和促进该领域国际合作所作的努力

2012 年，瑞士联邦政府通过了防止瑞士遭受网络风险的国家战略，为采取全面应对办法奠定了基础。该战略寻求改进对网络风险和新现威胁的早期侦测，使瑞士的基础设施作为一个整体，更有能力抵抗网络攻击，并从总体上减少网络风险。该战略还提到需要建立网络安全文化，让所有参与者共同承担责任，以及基于风险的应对办法。还提倡在政府一级进行协调，并开展国家(即公私伙伴关系)及国际合作。该战略包含 16 项措施。瑞士联邦政府已于 2013 年通过了关于执行该战略的详细计划。

3. 决议第 3 段所述概念的内容

必须通过加强国际合作，应对网络风险(上述战略确定的第 5 项行动)。瑞士在网络安全领域的对外政策侧重于制订负责任国家行为准则、建立信任措施和能力建设。因此，瑞士参加了各种国际进程。欧洲安全与合作组织(欧安组织)已通过了网络安全领域的建立信任措施。瑞士认为这一进程至关重要。此外，伦敦进程是瑞士参加的另一个重要进程。瑞士还支持一系列旨在开展能力建设的项目。

4. 国际社会为加强全球一级网络安全可采取的措施

国际社会采取的所有措施都必须在安全和人权考虑因素之间达成平衡。民众在线下享有的权利，在线上也必须得到同样的保障。需要进一步制订用于建立信任和信心的措施。欧安组织通过的一整套建立信任措施对于加强安全极为重要。开展切合实际的联合活动，通过交换信息和增强合作提高透明度，有助于实现网络空间的全面稳定。

多哥

[原件：法文]
[2016 年 6 月 2 日]

信息和电信的进步虽然是国家发展的巨大资产，但也给国家及国际安全带来威胁。这是一个经常被犯罪分子或恐怖分子利用的虚拟空间。

多哥未能幸免于这一威胁，而且也已经发现与信息和通信技术有关的犯罪活动，从网络诈骗和其他类型的欺诈，到儿童色情和侵犯他人的自由和诚信，不一而足。

在恐怖主义泛滥的时代，网络和社交媒体成为恐怖组织的宣扬和招募平台。此外，大多数国家正在向电子行政过渡，我们的政府面临重大挑战，行政部门的运转以及民事和军事安全很可能会因为网络攻击而遭到损害。

面对这一情况，重要的是在本国和国际上采取措施，对信息和电信部门进行监管，确保它们不被用于犯罪目的。

多哥为此已采取多项措施，包括：

- 通过 2011 年 7 月 6 日关于系统和强制识别电信服务订购者身份的第 2011-120/PR 号法令；
- 通过关于电子通信的第 2012-018 号法律和关于修订第 2012-018 号法律的第 2013-003 号法律；
- 拟订关于网络犯罪、加密技术、网络安全、个人数据保护和电子交易问题的立法草案。

这些法规的目的是确保所有信息和电信活动有迹可查，并建立一个防止信息和电信网络被欺诈性入侵的安全机制。

多哥还认为，有必要建立一个机构监督框架，例如计算机应急小组，负责确保国家一级的网络安全，作为邮政和电信管理当局的补充。

还需要加强人员能力，使参与确保网络安全的执法机构及公共和私营实体能够采取有效行动，应对任何形式的威胁。

此外，在国际电信联盟和联合国框架内开展国际合作，也有助于加强信息和电信安全。

土库曼斯坦

[原件：俄文]
[2016 年 3 月 28 日]

中立是土库曼斯坦国内政策和外交政策的基础，以国家利益、全球安全和共同进步之间的密切关系为依托。对于土库曼斯坦，一个源于中立地位和国际义务的关

键因素是其外交政策的爱好和平性质。因此，所有问题都无一例外地通过政治和外交途径、主要是联合国和其他国际组织得到解决。土库曼斯坦完全支持国际上为制止大规模毁灭性武器及其运载工具和相关技术扩散所作的努力，并主张将裁军作为全球安全的一个先决条件。在立法中，土库曼斯坦宣布放弃拥有、制造、储存或运输核生化及其他类型的大规模毁灭性武器，包括这类武器的新品种及其生产技术。

土库曼斯坦已加入多项以鼓励缔约国保持全球和平、和谐与安全为主要目的的国际裁军文书。

土库曼斯坦特别重视加强国际和平与安全，呼吁减少武器数量，认为世界上武器越少，世界发展就越稳定和平静，各国和各国人民之间的信任和了解也越深。土库曼斯坦 2013 年至 2017 年外交政策框架文件强调指出，土库曼斯坦将继续积极促进裁军进程和削减武器库，主要是减少大规模毁灭性武器。

土库曼斯坦总统在 2015 年 6 月 5 日的部长内阁会议上讲话，其中特别提到我国对全球社会的国际义务。他强调指出，中立意味着不依附政治、经济或军事联盟和集团；拥有军力足够强大的军队来保护我国的和平与自由；摒弃大规模毁灭性武器，禁止这类武器进入我国领土和领空；坚决秉持普遍人权价值观和民主原则，在国内保障公民的和谐与和平；与联合国及国际人道主义组织密切合作推行国内政策和外交政策。

2015 年 6 月 3 日，在大会第六十九届会议期间，关于土库曼斯坦永久中立地位的第 69/285 号决议得到 193 个国家的一致通过。这清晰表明，我国保障区域及国际和平、安全和可持续发展的有效政策得到了普遍承认。决议强调了土库曼斯坦永久中立地位对加强区域和平与安全的重要贡献，以及对我国与世界各国发展友好和互利关系的重要贡献。

作为联合国中亚地区预防性外交中心的东道国，土库曼斯坦呼吁该机构在联合国会员国和其他组织，包括欧洲安全与合作组织、欧洲联盟和独立国家联合体的帮助下，更多地参与区域问题的各个方面。

2015 年在阿什哈巴德成功举办了关于维护中亚地区和平、稳定与安全的国际论坛。作为裁军领域国际条约、联合国公约和多边文书的缔约国，土库曼斯坦打算继续尽最大努力，首先在区域一级推动这些进程，并争取由土库曼斯坦定期举办中亚区域裁军会议。

大不列颠及北爱尔兰联合王国

[原件：英文]
[2016 年 5 月 31 日]

联合王国很荣幸有机会就大会题为“从国际安全角度看信息和电信领域的发展”的第 70/237 号决议作出回复，这些回复以 2015 年对第 69/28 号决议的回复

为基础。联合王国在回复中倾向于使用“网络安全”一词，以避免因为在这一背景下对“信息安全”一词的不同解释而出现混淆。

联合王国确认网络空间是国家及国际关键基础设施的基本组成部分，是网上经济及社会活动不可缺少的基础。联合王国回顾2015年国家安全风险评估报告，其中确认网络仍然是国家安全的一级威胁。联合王国继在上一份国家网络安全战略(2011-2016 年)实施期间拨出 8.6 亿英镑专款之后，今后五年还将为此拨出 19 亿英镑。新的国家网络安全战略将于 2016 年发布，包括设立一个新的国家网络安全中心。

联合王国确认，国际协作是成功实现网络安全的核心。我们继续促进建立一个自由、开放、和平和安全的网络空间，让经济和社会效益得到保护，并惠及所有人。联合王国通过全球制止网上儿童性剥削行为联盟(WePROTECT)等倡议，牵头应对跨界网络安全挑战。我们还致力于在国际上分享最佳做法，确保全球社会在拓展网络安全能力方面获得援助。

联合王国继续积极和建设性地参加关于网络安全问题的国际讨论。我们为所有四期联合国政府专家组提供了专家，并认为最近一期专家组的共识报告在重申国际法适用于网络空间方面取得了宝贵进展，各国遵守国际法、特别是《联合国宪章》规定的义务，是各国使用信息和通信技术的基本行动框架。

联合王国还欢迎继续在欧洲安全与合作组织讨论今后可采取的网络空间建立信任措施，并在其他区域组织开展类似工作。

联合王国很高兴能够积极参与讨论这些重大议题，并期待进一步参与加强网络安全领域的能力和国际合作。