联合国 A/72/315

大 会

Distr.: General
11 August 2017
Chinese
Original: Arabic/English/French/
Russian/Spanish

第七十二届会议

临时议程* 项目 95

# 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

页次

一. 导言 ..... 3

二. 从各国政府收到的答复 ..... 3

阿富汗 ..... 3

亚美尼亚 ..... 4

白俄罗斯 ..... 5

文莱达鲁萨兰国 ..... 6

加拿大 ..... 7

古巴 ..... 8

厄瓜多尔 ..... 9

萨尔瓦多 ..... 9

爱沙尼亚 ..... 10

芬兰 ..... 10

德国 ..... 11

* A/72/150。

17-13876 (C) 210917 250917

希腊 ..... 12
日本 ..... 14
约旦 ..... 14
马达加斯加 ..... 16
荷兰 ..... 17
挪威 ..... 18
巴拉圭 ..... 19
葡萄牙 ..... 20
卡塔尔 ..... 21
新加坡 ..... 22
土耳其 ..... 22
大不列颠及北爱尔兰联合王国 ..... 23

# 一. 导言

1. 2016 年 12 月 5 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 71/28 号决议。在该决议第 3 段中，大会邀请所有会员国结合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/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 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. 根据这一要求，2017 年 2 月 16 日向所有会员国发出了普通照会，邀请各国就此提供资料。之后，又于 2017 年 6 月 12 日进一步发出了普通照会。截至本报告编写之时收到的回复载于第二节。2017 年 7 月 31 日之后收到的其他回复将以原文张贴在裁军事务厅网站上(www.un.org/disarmament/)。

# 二. 从各国政府收到的答复

## 阿富汗

[原文：英文]
[2017 年 5 月 26 日]

阿富汗伊斯兰共和国信息和通信技术部已就大会关于从国际安全角度看信息和电信领域的发展的第 71/28 号决议执行部分第 3 段报告以下情况。

### 成就

为促进信息技术的国际安全和电子交易的真实性，信息和通信技术部开发了一项重大公共基础设施装置。该部还创建了 NOC 系统，并计划将该系统与各会员国用于识别和核查因特网现有统计和数据流的系统相连接。

该部已起草打击网络犯罪的法律，并将其送交司法部审议。依据这些法律，电子交易将更加安全，网络犯罪可以得到预防，作为根本解决办法。

该部制定了交换安全信息的全国网络战略，为该部即将实施的 NIXA 项目打造了一个信息技术安全框架，同时应对和查明网络犯罪问题。

### 建议

信息和通信技术部请设有网警部门的发达国家合作，协助成立网警队伍。

为应对网络犯罪和严厉打击网络犯罪现象，应当在国际一级建立一个(有利于共享刑事情报的)统一连贯的系统。

确保因特网安全的一个重要解决方案是实行因特网治理。通过因特网治理，可以为负责落实上述网络的所有政府部门和办事处之间交换机密资料和数据奠定基础。在这方面，信息和通信技术部请所有会员国予以合作。

信息和通信技术部还请各会员国提供职业和技术培训方案，支持该部工作人员打击网络犯罪和改善信息安全。

## 亚美尼亚

[原文：英文]
[2017 年 5 月 31 日]

### 对信息安全问题的一般看法

鉴于亚美尼亚共和国电子社会的发展速度很快，有关信息安全的问题重要性与日俱增，对国家安全的各个方面产生了巨大影响。

信息和通信技术(信通技术)领域的趋势带来了全新的威胁和挑战，需要开展系统协调和采取新的办法，以确保安全使用信通技术。考虑到“信息战”技术被运用于不同的冲突环境中，亚美尼亚高度重视确保信息安全以维护国际和平与安全。

### 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

亚美尼亚开展了各类活动，以维护信息安全领域的国家利益和公共利益，遵照国际标准统一相关法律。该领域的一系列规范性法律已生效，包括国家安全战略和信息安全构想以及关于以下领域的法律：打击恐怖主义；国家和官方机密；电子文件和电子签名；个人资料保护；信息自由；大众媒体。

根据政府的有关决定：

(a) 已采取多项实际措施，以确保对政府机构可在因特网上公开查阅的信息进行保护，为其信息系统接入因特网提供可靠的连接；

(b) 通过了关于政府机构的官方因特网网站的最低要求。

亚美尼亚已批准并采用了一套国际标准化组织有关信息安全的标准。2006 年 10 月，欧洲委员会《网络犯罪公约》获得批准，后来又对国家立法作出了适当修正。

亚美尼亚积极参与在独立国家联合体、集体安全条约组织、欧洲联盟和北大西洋公约组织等国际框架内开展的相关方案、培训课程和合作倡议。特别是，亚美尼亚于 2016 年与独立国家联合体成员国举行了分两阶段进行的“网络反恐”联合演习。2017 年初，亚美尼亚提议将《集安组织成员国关于在确保信息安全领域开展合作的协定》提交国内各部门批准。

### 上文第 2 段所述概念的内容

亚美尼亚共和国信息安全构想将“信息安全”这一术语界定为“与个人、社会和国家的整体利益均衡相关联，保护信息领域的国家利益”。

考虑到信息和通信技术的迅猛发展，亚美尼亚共和国于 2017 年底成立了一个机构间工作组，负责起草一项关于确保亚美尼亚的信息安全和信息政策的新构想。

### 国际社会为加强全球一级信息安全可采取的措施

亚美尼亚强调必须就信息安全问题加强和有效开展国际合作，并强调国际电信联盟的作用。

## 白俄罗斯

[原文：俄文]
[2017 年 6 月 5 日]

### 对信息安全问题的一般看法

国际信息安全的现状不能令人满意。有人企图利用信息技术达到政治目的。

白俄罗斯面临着多种独特的信息安全问题：

(a) 在主干网供应商和国内供应商一级乃至托管平台上，对国家部门暴露于分布式拒绝服务的保护不够充分；

(b) 信息安全产品可能具有某些未申报的能力和薄弱环节，却又缺乏及时发现这些问题的能力，这往往有损于保护信息措施的影响；

(c) 入侵者攻击重要基础设施和信息技术基础设施(如电力供应系统和管理生产与运输的自动化系统)的威胁。

### 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

这方面的努力包括：

(a) 跨越整个系统开展工作，以更新关于对限制传播和/或限制提供的信息给予技术保护和密码保护的要求；

(b) 组织和运用涉及信息技术保护和密码保护的技术规范和标准；

(c) 与主要信息安全公司实施信息交流协定；

(d) 与国家机构和组织开展定期合作，以利于迅速应对具体的信息安全事件；

(e) 由各国维护本国的恶意软件侦测软件包；

(f) 通过协调中心进行协商，与集体安全条约组织国家开展合作。

### 审查旨在加强全球信息和电信系统安全的国际构想

白俄罗斯应对国际信息安全问题的一个重要办法，与防止信息和通信技术(信通技术)可能遭到滥用、破坏国家安全、国家稳定和国际安全的必要性有关。

白俄罗斯积极参与包括联合国、集体安全条约组织和欧洲安全与合作组织在内的各个国际组织的各种论坛，探讨国际信息安全问题。

白俄罗斯支持在联合国内通过一项关于国际信息安全的普遍文书的倡议。

### 国际社会为加强全球一级信息安全可采取的措施

在国际一级，必须逐步推进不干涉主权国家内部事务和在信息领域互相放弃侵略行动的原则。应当主要通过支持联合国会员国的信息主权来实现这些措施，其目的在于：

(a) 维护获得、保存和传播完整、可靠和及时的信息的公民权利；

(b) 发展信息社会，让联合国会员国在平等基础上参与全球信息关系；

(c) 确保对防止恐怖主义和极端主义思想扩散的政府间政策进行有效的信息管理；

(d) 确保关键基础设施的业务具有复原力。

### 国际社会为加强全球一级信息安全可采取的措施：

(a) 根据当前和未来的国际法文书的规定，制定国际合作机制；

(b) 在国际社会和控制绝大多数信通技术的多国公司之间建立有效合作，以发现和扼杀信息安全威胁的来源。

## 文莱达鲁萨兰国

[原文：英文]
[2017 年 6 月 29 日]

文莱达鲁萨兰国认为，随着信息和电信领域日益令人瞩目的发展，全球趋势已经出现改变。与此同时，这些进展也带来了新的威胁和挑战，其表现形式为黑客攻击、网络犯罪和网络恐怖主义，危及世界各地的重要基础设施、网络和服务。这些威胁的跨国性和无形性，意味着国际社会必须开展协同努力，建立一个安全和可靠的网络环境。

在国家安全委员会的主持下，文莱达鲁萨兰国在国家一级与多个地方安全机构保持着强有力的合作关系，应对内部的网络安全威胁。文莱国家计算机应急小组成立于 2004 年 5 月，业已成为该国在处理与计算机和互联网有关的安全事件方面的一站式转交处理机构。通过与其他计算机应急小组建立全球范围内的联系，国家工作队能够获得关于信息和通信技术(信通技术)安全威胁的宝贵信息，在国家信通技术基础设施内部分享关于安全风险的调查结果。

文莱达鲁萨兰国致力于与区域和国际伙伴开展合作，不断保持面对重大国际网络威胁时的战备状态。在东南亚国家联盟(东盟)的区域架构内，文莱达鲁萨兰国将参与东盟国防部长扩大会议网络安全问题专家工作组的工作。该工作组将 18 个国家汇集一起，促进实际和有效的合作，加强保护该区域的网络空间和应对网络安全挑战的能力。

文莱达鲁萨兰国政府认识到所有网络平台的威胁，包括云计算和移动系统的威胁，并将其视为文莱安全和防务优先事项的一个重要组成部分。

## 加拿大

[原文：英文]
[2017 年 7 月 17 日]

关于网络问题，加拿大认为：

(a) 一个自由、开放和安全的网络空间对于促进安全、繁荣和人权而言至关重要；

(b) 现有国际法适用于国家对信息和通信技术的使用；

(c) 推广和平时期准则，有助于维护一个用负责任的行为指导国家行动的环境；

(d) 事实证明，实际的建立信任措施能够缓解紧张关系和减少武装冲突风险。

在国家一级，加拿大政府于 2010 年推出网络安全战略，把重点放在确保加拿大网络系统的安全和为加拿大人民提供在线保护。政府最近完成了一项对现有网络安全措施的审查。在此基础上，加拿大将于 2017 年底公布处理网络安全问题的新办法。

2017 年防务政策纳入了新的投资和政策指导方针，以更好地利用网络能力来为军事行动提供支持。加拿大军队的现有网络实力将与其他军事工具一样面临严格的监管，包括适用的国内法和国际法及接战规则。

在国际一级，加拿大通过多种方式积极处理网络问题：

(a) 加拿大继续促进制订和平时期网络空间国家行为准则，包括推广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 2012-2013 年和 2014-2015 年的成果；

(b) 加拿大于 2015 年 7 月批准了欧洲委员会《网络犯罪公约》(《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，设计本国有关网络犯罪问题的法律；

(c) 自 2007 年以来，加拿大已投入 1 100 万美元用于支持网络安全能力建设项目；

(d) 加拿大还与美国一道，实施旨在加强其网络基础设施应对能力的网络安全行动计划；

(e) 加拿大一贯致力于在各种论坛推行建立信任措施，包括欧洲安全与合作组织和东南亚国家联盟地区论坛；

(f) 加拿大支持北大西洋公约组织和各盟国为加强网络防御所做的努力。

## 古巴

[原文：西班牙文]
[2017 年 4 月 5 日]

大会第 71/28 号决议指出，科技进展有民用和军事两种用途，必须防止这些进展影响到国际安全。

必须在多边一级采取措施，推动审议信息安全领域的现有威胁和潜在威胁，以及防止和应对这些威胁的可能战略。

所有国家开展合作，是避免网络空间变成军事战场的唯一途径。

古巴支持根据第 58/32 号决议设立的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工作，一名古巴专家还参与了该专家组的工作。

我们认为，有必要设立一个具有法律约束力的国际监管框架，对现行国际法构成补充，且适用于信息和通信技术。

信息和电信系统如果被设计或被用于给一个国家的基础设施造成破坏，就可以转化为武器。所有国家都必须尊重该领域现有的国际标准。接入另一国的信息或电信系统应符合缔结的国际合作协定，并以征得所涉国家的同意这一原则为基础。交流的性质和范围必须遵守准许接入的国家法律。

出于破坏缔约国法律和政治制度的公开或秘密意图，将电信用于敌对目的的做法，违反了这一领域国际公认的准则，构成了非法和不负责任地使用这些手段的罪行。这种做法可能导致不利于国际和平与安全的紧张关系和局势，并可能对缔约国基础设施的健全产生不利影响，损害其民事和军事领域的安全。

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的做法感到极为关切，因为这可能引发国际冲突。

美国一直通过非法电台和电视广播不断攻击古巴的空中电波，传播专门用于煽动推翻古巴人民建立的宪法秩序的节目。2016 年，美国从其领土上平均每周使用 25 个频率播放 1 875 小时针对古巴的非法广播。美国针对古巴不断传送的无线电和电视广播，违反了《联合国宪章》的宗旨和原则、国际法以及国际电信联盟的规定。

古巴再次要求立即停止这些侵犯古巴主权的侵略性政策，而且这也不符合各国之间在相互尊重和合作的基础上发展关系的原则。

古巴还希望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。

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 月在多米尼加共和国基多举行的拉共体第五次首脑会议再次强调了通过包括因特网在内的信息和通信技术来促进和平、人类福祉、发展、知识、社会包容和经济增长的重要性。

古巴重申，为应对滥用信息和通信技术所带来的危险，国际合作是不可或缺的。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可以发挥重要作用。

## 厄瓜多尔

[原文：西班牙文]
[2017 年 7 月 28 日]

厄瓜多尔认为，国际关系中的安全必须建立在各国之间的互信和互相尊重基础上。有关大规模开展不加区分的间谍活动监控世界各国公民通信的丑闻不断曝光，这和利用信息和通信技术违反国际法的行为一样，都违反了尊重主权和不干涉国家内部事务的原则。此外，这些行为给国家间关系造成了严重的不稳定因素，进而影响到国际安全。这些间谍活动也侵犯了各项基本人权。

因此，厄瓜多尔支持努力继续研究信息安全领域的现有威胁和潜在威胁、应对此类威胁的可能合作措施、如何将国际法适用于各国对信息和通信技术的使用，以及这一领域负责任的国家行为的规范、规则和原则。

## 萨尔瓦多

[原文：西班牙文]
[2017 年 5 月 24 日]

为履行对联合国的义务，萨尔瓦多谨报告：根据大会关于“从国际安全角度看信息和电信领域的发展”的第 71/28 号决议，萨尔瓦多武装部队在 2016 年采购了加密机关文件的系统，以加强信息安全。这一制度目前正在执行中。

## 爱沙尼亚

[原文：英文]
[2017 年 5 月 31 日]

爱沙尼亚认识到，网络世界的安全已成为更广泛的国际安全领域内一个非常重要的问题。因此，联合国的作用和参与日益重要。

因特网安全一直是爱沙尼亚政府高度重视的优先事项之一。有关这一问题的主要指导文件是国家网络安全战略(2014-2017 年)。爱沙尼亚政府安全委员会网络安全理事会支持战略层面的机构间合作，并监督落实网络安全战略的各项目标。北大西洋公约组织网络合作防御英才中心设在塔林，截至 2017 年 5 月 30 日，共有 20 个出资会员国。

爱沙尼亚坚信，数字服务的广泛使用，需要高水平的网络安全。爱沙尼亚认为，网络安全的社会经济和政治-军事方面之间有着相互联系。爱沙尼亚认为，各国不能对国家重要基础设施发起袭击。爱沙尼亚还呼吁采取负责任的行为，打造全球化通信基础设施，促进信息获取权与对信息和通信技术(信通技术)的信任。爱沙尼亚认为，每个国家都有责任起草并实施国家法律，协助控制非国家行为体恶意使用信通技术的行为，并设法更好地编制、传播和推广积极、负责的网络政策、说明和论证。

爱沙尼亚连续第四次担任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成员。该专家组已成为一个富有成效的论坛。今后，专家组可以成为一项有用的工具，不仅有助于研究网络威胁和可能的补救办法，而且也有助于了解不同国家如何执行现有的国际法和国际规范、规则和原则。爱沙尼亚认为，工作组应继续工作，促进会员国之间开展对话，推动交流信息和最佳做法。此外，专家组还应讨论实际合作的措施和机制，以推动会员国的能力建设，其最终目标是使会员国具备应对因特网所有方面挑战的能力。

必须继续推进政府专家组在 2014-2015 年会议上取得的进展，进一步促进在网络空间支持开放、问责和其他民主价值的国家行为规范。爱沙尼亚期待着专家组 2017 年 6 月完成的另一份共识报告。

## 芬兰

[原文：英文]
[2017 年 7 月 21 日]

芬兰很荣幸有机会就大会第 71/28 号决议的执行情况提交报告。

在国家一级，芬兰作出了以下方面的努力：

(a) 国家网络安全战略(2013 年)及其最新执行方案(2017 年)确定了加强网络安全和复原能力的关键准则和行动；

(b) 芬兰设立了国家网络安全中心和网络犯罪预防中心，并在外交部任命了一位主管网络事务的大使。国家信息安全战略于 2016 年获得通过；

(c) 芬兰积极促进在欧洲联盟范围内的网络空间事务合作；

(d) 芬兰支持各种形式的促进发展的信息和通信技术及与网络相关的能力建设项目。芬兰是全球网络专才论坛的创始伙伴。2016 年，芬兰加入了世界银行数字发展伙伴关系信托基金。芬兰支持基于多利益攸关方模式的互联网治理。芬兰一直积极参与信息社会世界首脑会议及其后续进程，包括参与因特网治理论坛的工作和并为其提供资金。2017 年 4 月，第八届芬兰因特网论坛在赫尔辛基举行；

(e) 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。

(f) 芬兰赞同关于从国际安全角度看信息和电信领域发展政府专家组 2015 年的报告，并积极参与专家组的工作。芬兰积极参与讨论网络空间国际法问题，例如就《塔林手册 2.0》进行协商和参加联合国裁军研究所开办的讲习班；

(g) 芬兰于 2012 年加入了“自由在线联盟”，并为“数字捍卫者伙伴关系”作出了贡献。芬兰还在赫尔辛基举办了 2016 年世界新闻自由日会议；

(h) 芬兰加入了欧洲委员会《网络犯罪公约》。新出台的战略警务计划(2015 年)旨在预防计算机犯罪和发展有关网络安全的专门知识。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包括：

(a) 芬兰非常重视政府专家组的工作，并已准备为其成功作出贡献，包括进一步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应对能力和安全；

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

## 德国

[原文：英文]
[2017 年 5 月 30 日]

信息和通信技术(信通技术)的发展提供了经济、社会和科学领域的诸多机会。确保网络空间的访问权并维持网络空间数据的完整性、真实性和保密性，已成为二十一世纪的重大问题。

在一个日益相互关联的世界中，各个国家、重要基础设施、企业和个人都有赖于信息和通信技术的可靠运作。滥用信通技术的影响并不局限于网络空间，而

是可能导致社会、经济、政治和其他方面的损失。例如，对国家机构或民主和政治进程发起的袭击，能够对公共秩序和安全造成影响。

德国应对这些挑战的办法，是通过在以下三个层次上促进国家在利用信通技术的过程中遵守国际法、遵从规范和建立互信：

(a) 在全球范围内，德国支持努力就如何将国际法适用于国家使用信通技术的过程、制定自愿的非约束性规范、规则或原则塑造负责任的国家行为达成一致，以期打造一个开放、安全、稳定、无障碍、和平的信通技术环境。在这方面，历届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工作尤为重要。德国专家积极参加了这些工作组的工作，并致力于推动执行其建议。现在应当扩大辩论的范围，让更多的联合国会员国加入到辩论中来，以期普及国际安全领域的信通技术工作。德国支持联合国发挥主导作用和加强联合国在这一领域的能力。有很多议题值得进一步探讨，包括在打击网络攻击领域内的国际信息共享与合作。应当制定得到普遍尊重的明确规则，遏制恶意使用网络能力的行为和出于经济目的的在线间谍活动；

(b) 在区域一级，建立信任措施有助于化解信通技术事件的风险，防止其升级为政治乃至军事危机。在欧洲安全与合作组织(欧安组织)内，德国多年来一直积极参与制定和执行各种建立信任措施，以期加强国家使用信通技术的安全。2016 年德国担任欧安组织轮值主席期间，参加国同意采取更多的此类措施。2016 年欧安组织部长理事会汉堡会议核准了这些措施，并颁布了执行这些措施和开展进一步工作的指令。今后需要超越政治-军事方面，扩展至安全的多个层面。在欧安组织之外，德国还支持其他大陆的区域组织开展类似努力。

(c) 在双边一级，德国与多个合作伙伴保持着网络对话，并开展定期的网络磋商。在既有的伙伴关系基础上，德国还支持其他国家开展网络安全能力建设。2016 年 11 月，德国政府在更新其网络安全战略时决定有意设立一个德国国际网络安全研究所，以加强这方面的努力并使之系统化。

德国结合国际安全开展的信息和通信技术工作是促进信通技术安全的整体工作的一个组成部分。最近采取的国家监管措施，例如 2015 年的《信息技术安全法》和 2016 年对国家网络安全战略的重大修改，目的都在于改善德国信通技术的总体安全。

## 希腊

[原文：英文]
[2017 年 5 月 26 日]

在欧洲委员会框架内，希腊已通过第 4411/2016 号法令(2016 年 8 月 3 日 A´ 142 号政府公报)批准了《欧洲委员会网络犯罪公约》(2001 年 11 月 23 日，布达佩斯)和《网络犯罪公约关于宣告利用计算机系统犯下的种族主义或仇外行为为犯罪行为的附加议定书》(2003 年 1 月 28 日，斯特拉斯堡)。

值得一提的是，将欧洲联盟关于网络和信息系统安全的指令纳入国家法律的进程业已启动。这一指令对于加强国家一级抵御网络攻击的应对能力而言至关重要，该指令还为欧洲联盟所有成员国规定了与此目的相关的多项义务，包括通过了一项关于网络和信息系统安全的国家战略。

根据希腊国防部提供的资料，希腊的网络安全愿景是发展全方位的能力，捍卫国家的基础设施和网络，抵御最新的网络犯罪和网络威胁。这包括在希腊的国防相关组织最高战略层面处理网络防御问题，将网络防御进一步纳入国防行动，并将覆盖面扩大至可部署的网络。希腊在国家一级为加强信息安全和促进国际合作所作的努力有：

(a) 目前正在制订国家网络防御战略框架，即将成为法律的国家网络安全战略制定了网络安全总体框架，并规定了维持网络安全最低要求的必要行动；

(b) 网络防御已成为国防行动计划的一部分，国家紧急警报系统已被纳入涉及信息系统的大多数政策文件，并已被纳入全国所有的重大演习中。网络安全已被列入所有公共组织的危机时期行动计划中；

(c) 希腊一直在发展并不断改善军队计算机事件应对中心的事件应对/应急能力。快速反应小组可以在短时间内部署，协助应对军队或公共网络的网络事件并从中复原。出现故障或网络攻击后的恢复指令已经纳入计算机信息安全政策文件；

(d) 目前正在为所有国家军事防御网络系统建造网络安全行动中心。在国家一级，有 4 个负责公共部门和私营部门的计算机应急小组。

为了实现更高程度的信息安全，国际社会可采取以下措施：

(a) 通过全面运作的国家网络安全行动中心，提高事件应对能力、网络监测能力和可操作的网络威胁防御能力；

(b) 将网络防御充分融入到业务活动中；

(c) 制定国家网络安全和网络防御战略；

(d) 加强网络防御从业人员的网络意识，提高现有的技术能力；

(e) 持续培训网络防御组织从业人员；

(f) 实现国家法律与全球网络安全法律和指令之间的统一。

根据希腊警方提供的资料，第 178/2014 号总统令第 30 条规定希腊警察网络犯罪司的任务包括预防、调查和起诉通过因特网或其他电子传播媒体实施的犯罪。网络犯罪司是一个独立的中央机构，直接对希腊警察总长负责。

该司设有多个部门，其中之一负责电子和电话通信安全及软件和版权保护。具体来说，该部门负责调查希腊境内非法渗透计算机系统和盗窃、破坏或贩运软件、数字数据和视听作品的犯罪行为。

希腊警察网络犯罪司与国家情报局的下属机构——国家反电子攻击局密切合作。该局的任务是负责防止并消极和积极地打击针对通信网络、数据存储设施及信息和通信技术系统的电子攻击。此外，该局还负责处理数据和通知主管当局。

## 日本

[原文：英文]
[2017 年 7 月 27 日]

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、不会无端拒绝或排斥有意访问网络的所有行为体的空间。日本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。

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。

日本的努力分为以下三个部分：促进网络空间的法治、建立信任措施和能力建设。

在促进法治方面，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自愿准则。这是确保国际社会的稳定性和可预测性的基础。鉴于信息和通信技术的独有特征，我们需要进一步明确个别规则和原则的适用办法。

在推动建立信任措施的过程中，必须确保透明度和共享信息；然而，各国采取的措施力度各不相同，因为每个国家都有权自主决定其力度。日本通过双边对话和东南亚国家联盟地区论坛等多边框架，积极促进建立信任。有必要研究开展实际合作的途径。

在能力建设方面，日本一直努力促进制订网络安全法律、法规和政策框架，并一直致力于保证政府机构和关键信息基础设施运营者的网络安全；采取措施打击网络犯罪；开发人力资源，培养网络安全专家；研究和开发网络安全技术。在这些经验和积累的知识基础上，日本将进一步就能力建设问题开展积极合作。

## 约旦

[原文：阿拉伯文]
[2017 年 3 月 23 日]

信息和通信技术对我们日常生活而言已经不可或缺。信息和通信技术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，而且对个人与地方社区和更广泛的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。必须通过技术和法律手段来应对这些风险，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。约旦利用这些网络来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-阿拉伯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) 在不依赖供应商帮助的情况下，培训并验证了所有通信系统用户及维护和支助人员，以确保任何时候都具有最优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，以改善国家及区域安保协调与合作；

(f) 积极参加国际会议并了解最新成果，以增强友军之间的互补性，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。

应始终重视让公民认识无处不在的网络威胁，以及如何通过网络安全措施最大限度地减少和抗击使用电子系统时所面临的此类威胁。在处理任何类型的信息时，都必须加强安全意识——如果此种行动不会有碍于妥善利用该技术的话。

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(内联网)；

(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. 网络犯罪法；

2. 电子交易法；

3. 已拟订国家网络安全和保护战略；

4. 已拟订国家网络安全和保护政策；

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连接网络；

(g) 在某些网络中使用闭合内联网，尽量避免使用万维网；

(h) 加强联合国内联网，使其与公共网络分离。应通过加密、安全防护和存取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) 2003 年组建的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应包含一名来自约旦的代表。

(c) 加强安全理事会成员之间的科研合作与培训交流。

## 马达加斯加

[原文：法文]
[2017 年 6 月 20 日]

联合国的建议建立在国际安全的基础上，其设想的行动包括：

- 旨在加强全球信息和电信系统安全的研究；

- 评价信息安全领域所有的现有威胁和潜在威胁，并通过适当战略应对这些威胁；
- 国家官员参与加强信息安全，以期在全球一级建立对安全问题的共同理解；

第 71/28 号决议专门处理信息和电信问题，这是一个在马达加斯加迅速扩展的领域。我们对这一决议的回复需要该领域的实地专家的投入。

## 荷兰

[原文：英文]
[2017 年 5 月 31 日]

荷兰很荣幸有机会就大会第 71/28 号决议的执行情况作出回复。

网络空间(特别是因特网)是经济和社会发展的关键资源。网络空间的重要性与日俱增，为国际社会带来了新的挑战。各国社会之间的相互关联程度很高，又高度依赖因特网及信息和通信技术，越来越容易受到滥用这些技术的影响。地缘政治紧张局势映射到网络空间，各国及其他行为体越来越多地利用网络行动谋求其战略利益。然而，这些网络行动有可能造成国际关系不稳定，有可能对国际和平与安全构成风险。

显而易见，必须开展国际合作，才能减少这些风险。鉴于以上几点，荷兰根据其国际网络战略“建设数字桥梁”的要求，正在加紧参与维持网络空间和平与稳定的网络外交，促进国际法律秩序，培养安全合作文化。

国际社会正在采取措施化解这些风险。在这方面，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编写的报告十分重要。荷兰还对本国能够为政府专家组 2017 年的工作作出贡献表示感谢。

荷兰继续促进就网络空间的负责任国家行为开展包容各方的对话，通过各种活动捍卫网上人权和促进能力建设。荷兰开展了多方面努力，其中最值得注意的是：

(a) 本着支持国际法律秩序发展的优良传统，荷兰组织各国法律顾问就《网络活动适用国际法塔林手册 2.0》举行磋商；

(b) 荷兰支持联合国裁军研究所组织了 3 次关于网络准则、国际法和打击恶意工具与技术传播的系列讲习班，将外交官和技术界成功地聚集一堂；

(c) 最后，荷兰发起了多项倡议来促进出台指导准则，包括倡议设立网络空间稳定性问题全球委员会，负责提出建议制定规范和政策，以加强国际安全和稳定。

所有这些努力的目的都在于使数字化时代的国际关系和网络空间本身更加稳定、更加安全。荷兰认为，为减少冲突风险和维持一个开放、自由和安全的网络空间，这些努力是不可或缺的。

## 挪威

[原文：英文]
[2017 年 7 月 27 日]

挪威是世界上数字化程度最高的国家之一，越来越多地依赖于一个运作良好和安全的网络空间。挪威坚定致力于建立一个自由、开放、和平和安全的网络空间，保护其经济和社会效益，并使之惠及所有人。网络空间不分国界，只有通过各国与私营部门之间的密切合作，国际一级的网络空间安全才能得到保证。

### 为加强信息安全所作的努力

国家举措

政府发布了一份题为“信通技术安全：共同的责任”(2016-2017 年)的白皮书，其内容包括改善国家一级相关行为体之间协调的国家框架计划，以及建立一个技术平台，以便公共和私营机构之间更好地分享信息。

2017 年 3 月 31 日，安全和情报部门联合网络协调中心成立。

国际举措

政府发布了一份关于挪威外交政策所面临的全球安全挑战的白皮书(2014-2015 年)，其中网络威胁问题占据了重要位置。

挪威即将推出一项网络空间国际战略。

挪威参与了若干与网络议题有关的区域合作倡议，例如：

(a) 在欧洲安全与合作组织(欧安组织)内部开展工作制定规范和建立信任措施，以减少因使用信息和通信技术(信通技术)而产生的冲突风险；

(b) 与设在塔林的北大西洋公约组织合作网络防御英才中心密切合作，包括关于国际法在网络领域的适用和理论发展；

(c) 欧洲委员会《网络犯罪公约》。

挪威支持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工作。

挪威参与关于网络问题的双边和区域对话，特别是在北欧国家的框架内。

### 国际社会为加强全球一级信息安全可采取的措施

挪威认为，在各国使用信通技术的过程中，适用于网络空间的国际法和各国遵守国际法的义务(特别是根据《联合国宪章》应承担的义务)是指导其行为的基本框架。国际社会需要进一步探讨国际法在网络领域的适用问题，以及在网络空间中的负责任行为规范。

一个可持续的全球因特网取决于在开放、安全、稳健和自由之间实现恰当的平衡。而这只能通过国际合作与全球和区域层面的对话才能得到保证。诸如联合

国、欧洲联盟、经济合作与发展组织和欧洲安全与合作组织等论坛正在开展的工作应当继续下去。

普遍人权也适用于网络领域。个人在线下享有的各项权利在线上也必须得到保护，特别是表达自由，包括搜寻、接收和传递信息的自由以及隐私权。

## 巴拉圭

[原文：西班牙文]
[2017 年 7 月 31 日]

巴拉圭认为，随着各国政府对信息和通信技术及网络空间的依赖程度日益加深，信息安全已成为全球范围内一个日益重要的领域。必须采取协调一致的、强有力的和成比例的措施，应对网络攻击事件的增长。如果没有一项全球一级的战略对策，一国在网络安全领域的努力将是零散、重复、效率低下和不可持续的。

为加强国家一级的信息安全，2017 年 4 月，巴拉圭政府批准了一项国家网络安全计划，在网络空间中发挥作用和利益相关的所有部门的代表直接参与了这项计划的起草工作。该计划为这一领域的政府和国家政策奠定了基础，并确定了巴拉圭为加强其关键资产的安全、实现一个安全、可靠和应对能力强的网络空间而将采取的行动。巴拉圭刑法界定了网络犯罪。在过去五年中，巴拉圭主办了伊比利亚-美洲信息安全会议暨交易会，以交流经验，了解进展情况，评估因增加使用信息和通信技术而产生的挑战的解决方案。

在次区域一级，南方共同市场(南共市)的常设机构“南共市信息安全、隐私权和技术基础设施主管当局会议”提出与网络安全有关的共同政策和举措建议。此外，美洲区域还有一项美洲网络安全综合战略，该战略确认信息系统和网络的所有参与者都必须了解其在安全方面的作用和责任，以打造网络安全文化。

建立一个有效的框架，以保护全球范围内的信息网络和系统(包括因特网)，并对事故作出应对和恢复努力，有赖于国际社会采取下列措施：

- 向用户提供信息，使他们能够保护自己的信息系统免遭威胁和杜绝安全漏洞
- 促进公共和私营部门之间的伙伴关系，推动教育和提高认识
- 确定和评估技术标准和最佳做法，以确保通过通信网络传递的信息安全，并力推其获得通过
- 促成有关网络犯罪问题的政策和立法，以保护用户，防止和阻止不当和非法使用计算机设备，同时尊重用户的隐私权。

## 葡萄牙

[原文：英文]
[2017 年 7 月 27 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 71/28 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。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；但是另一方面，葡萄牙认为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完整性造成负面影响。

第 71/28 号决议要求会员国在以下四个领域提供资料：

(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。

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在 2013 年的报告(A/68/98)中就以下领域提出了一些建议：国家负责任行为的规范、规则和原则；建立信任措施和信息交流；能力建设措施。

针对这些建议，葡萄牙发表以下看法：

### 体现负责任国家行为的准则、规则和原则

葡萄牙认为，网络信息安全相当重要，而且越来越重要。

我们必须强调在努力执行关于网络安全和健全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完整性受损事件。

在概念方面，必须强化“相关法规应主要源自国际规则”的观点。

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。

### 加强信任和信息分享措施

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)之间的信息共享至关重要。

在国家一级，葡萄牙把努力的重点放在完成有公共和私营实体参加的联合演习；促进技术标准化；并举办会议和研讨会，其中一些有国际演讲者参加。

### 能力建设措施

制订能力建设措施十分重要。然而，在培训和维持有关活动的人力资源方面，面临着诸多困难。

有必要促进知识的获取权，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。

## 卡塔尔

[原文：英文]
[2017 年 5 月 4 日]

卡塔尔国早已认识到，信息安全和网络安全不仅是一个技术问题，而且还是关乎国家政策的事项。为此，卡塔尔于 2005 年成立了计算机应急小组(见 www.Qcert.org)，以促进变革，加快步伐广泛采用有效的网络安全做法和政策，现在还承担着障卡塔尔国数字资产的国家任务。

2013 年，首相设立了国家网络安全委员会。委员会制定了一项国家网络安全战略，以改善卡塔尔的安全态势，并通过五个支柱确保国家继续走向成功和增长的道路。这五个支柱确定了卡塔尔将在哪些方面采取行动：

- 保护国家重要信息基础设施
- 通过及时分享信息、协作和行动应对和解决网络事件和网络攻击，并从中恢复
- 建立法律和监管框架，以使网络空间安全无虞、充满活力
- 培育网络安全文化，促进对网络空间的安全和适当利用
- 发展和培养国家网络安全能力。

计算机应急小组成功地提供了各种信息安全服务，以满足卡塔尔国的选民、企业和组织的需要，特别是在对事件应对、情报、抗灾能力、培训和提高认识、危机管理、重要公共基础设施许可证办理和标识以及建立国家信息安全合规框架等领域。

卡塔尔认为，目前各国掌握和分享区域和国际一级网络态势感知的能力还存在差距，不足以为有效的决策提供支持。必须在合作预防方面开展更多的工作，以确保所有的网络基础设施和服务机构都能够加强网络安全和确保应对能力，特别在涉及政府、服务机构、企业、消费者和公民日常生活的正常运作方面。

在持续开展信息交流的情况下，如今的网络安全比以往任何时候都更有效率。通过说明国家核查和合规方法的协作框架，有关信息共享协定的工作将成为各国的重要资产。

网络攻击迟早会发生，各国政府、各组织和企业必须携手协作，有备无患。

## 新加坡

[原文：英文]
[2017 年 7 月 31 日]

作为一个高度互联的小国，新加坡支持一个安全和有应对能力的网络空间，其基础为国际法、明确界定的负责任国家行为准则和旨在遵从这些准则的、协调一致的能力建设努力。为应对网络威胁所构成的新挑战，必须开展强有力的国际合作。新加坡将为此贡献自己的力量。

2015 年，新加坡成立了网络安全局，对国家网络安全职能实行统一监管。2016 年 10 月，新加坡推出了网络安全战略，概述了其保护基本服务免受网络威胁和打造一个安全的网络空间的整体方法。该战略以四大支柱为基础：建设有应对能力的基础设施；打造一个更安全的网络空间；发展充满活力的网络安全生态系统；加强国际伙伴关系。

在区域一级，新加坡正致力于建立和深化与邻国的共同能力。新加坡与东南亚国家联盟(东盟)合作启动了一个 1 000 万新元的网络能力方案，为区域能力建设努力作出补充。根据这一方案，新加坡于 2017 年 5 月举办了一次东盟网络准则讲习班，并将于 2017 年 8 月举办一次东盟网络安全能力建设讲习班。新加坡还主办了一年一度的新加坡国际网络周，包括东盟网络安全问题部长级会议和国际网络领袖专题讨论会，供政府、产业界和学术界的全球领袖参与区域事务，讨论新出现的问题和交叉问题。

在多边合作方面，新加坡支持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工作，包括专家组在其 2015 年报告中列出的 11 条准则。必须界定和执行享有广泛共识的准则，特别是实际作业准则。这些准则包括：不支持蓄意破坏关键基础设施的在线活动；不支持对计算机安全事件响应小组应对网络事件构成阻碍的活动；不利用计算机安全事件响应小组从事恶意的国际活动。

## 土耳其

[原文：英文]
[2017 年 7 月 31 日]

信息和通信技术(信通技术)已成为当今社会和经济生活的重要组成部分。信通技术为社会财富和发展及个人的日常生活作出了贡献；其使用范围广泛，包括公共部门和私营部门、重要基础设施部门和个人。尽管存在网络安全风险，信通技术在土耳其和全世界得到广泛应用。

在这一背景下，土耳其参加了许多倡议，促进有关网络安全问题的合作努力，其目的在于确保网络安全。在这方面，通过运输、海洋事务和通信部的协调，土耳其举行了国家网络安全演习；第一次国际网盾演习是在伊斯坦布尔完成的。同时，土耳其每年还定期参与并促进与网络安全有关的国际演习，即北大西洋公约组织(北约)网络联盟、北约锁盾和北约危机管理演习。

土耳其加强了与联合国、北约、欧洲联盟、欧洲安全与合作组织及其他国际组织和非政府组织、学术界和舆论领袖的对话和合作。目前正在通过举办大型会议、培训班、研讨会、会议、研究生教育和其他支助性方案来巩固这一方法。土耳其与多个国家缔结了双边协定，在区域网络安全努力中发挥着牵头作用。

北约网络防务委员会核准了说明北约及其盟国之间合作的谅解备忘录，签署备忘录的相关工作目前正在进行中。土耳其是北约卓越合作网络防御中心的出资国。土耳其参与北约民间应急规划委员会的工作以及区域军备控制核查和执行援助中心-安全合作中心的各次会议，正在稳步发展就各类事项开展的合作。土耳其是全球网络专才论坛的创始国之一，并加入了框架文件和《全球论坛海牙宣言》。

2015 年 11 月 15 日和 16 日，在土耳其举行的 20 国集团首脑会议作出了一项关于网络安全的决定，强调重视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工作。

2010 年，土耳其在斯特拉斯堡签署了《欧洲委员会网络犯罪公约》，并通过 2014 年第 6533 号法令核准了《公约》，后来又完成了将其纳入国家立法的程序。

通过收集、审查和评估在各次会议和常识性平台上生成的信息，土耳其制定了 2016-2019 年国家网络安全战略和行动计划。

加强全球一级的信息安全并培育国际社会的安全文化，对于每个人而言都是至关重要的。与此同时，每个国家为维护国家安全都有权采取措施保护本国免遭恶意利用信通技术的恐怖分子、极端分子、有组织犯罪集团和自由职业黑客的破坏。在这方面，加强国际法和巩固双边国际协定也具有十分重要的意义。

## 大不列颠及北爱尔兰联合王国

[原文：英文]
[2017 年 7 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 71/28 号决议作出回复，这些回复以 2016 年对第 70/237 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或缺的基础。网络空间活动所造成的实际威胁和潜在威胁仍然值得严重关注。2016 年 10 月公布的新国家网络安全战略，将为联合王国在今后五年中保卫本国资产、威慑对手和发展网络安全部门的努力奠定基调。

联合王国继续在关于网络安全问题的国际讨论中发挥牵头作用。联合王国为所有 5 期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。尽管 2017 年的政府专家组尚未达成协商一致意见，联合王国仍致力于在运用现有国际法、商定的负责任国家行为自愿准则和建立信任措施的基础上促进网络空间的国际稳定框架，并辅之以协调一致的能力建设方案。联合王国还欢迎欧洲安

全与合作组织和其他区域论坛提出实施建立信任措施的建议，并将努力在采取此类措施方面继续以身作则。

本回复概述了联合王国关于支持和改善网络安全以及分享国内和世界各国最佳做法的努力，包括与国际合作伙伴共同应对网络犯罪、重大事件和开展能力建设的努力。联合王国期待着取得进一步进展，并很高兴能够积极参与处理这些问题。联合王国将继续全面参与加强网络安全领域的能力和国际合作。