联合国 A/70/174

大会

Distr.: General
22 July 2015
Chinese
Original: English

第七十届会议

临时议程* 项目 93

从国际安全角度看信息和电信领域的发展

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

秘书长的说明

秘书长谨随函转递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。专家组是根据大会第 68/243 号决议第 4 段设立的。

* A/70/150。

15-12404 (C) 180815 200815

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

摘要

信息和通信技术(信通技术)提供了广阔的机会，对国际社会的重要性不断增加。然而，同时也出现了对国际和平与安全构成威胁的这一令人不安的趋势。各国必须进行有效合作，才能减少这些风险。

2015 年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审查了各国利用信通技术而产生的现有威胁和潜在威胁，审议了消除这些威胁的行动，包括制定规范、规则、原则和建立信任措施。专家组还审查了国际法如何适用于国家使用信通技术的问题。本专家组在前专家组工作的基础上再接再厉，在这些领域取得了重大进展。

本报告大大扩大了对各项规范的讨论范围。专家组建议各国进行合作，防止有害的信通技术行为，并且不应故意允许他人利用其领土使用信通技术实施国际不法行为。专家组呼吁加强信息交流和提供更多援助，以起诉利用信通技术的恐怖分子和罪犯。为此，专家组强调各国应保证充分尊重人权，包括隐私权和表达自由。

一项重要的建议是，各国不应从事或故意支持蓄意破坏或以其他方式损害关键基础设施的利用和运行的信通技术活动。各国还应采取措施，保护本国关键基础设施不受信通技术的威胁。一国不应危害另一国获授权的应急小组的信息系统，或利用这些小组参与恶意的国际活动。各国应鼓励负责任地报道信通技术的脆弱性，采取合理步骤确保供应链的完整性，并防止恶意的信通技术工具、技术或有害隐藏功能扩散。

建立信任措施可增强合作和透明度，并降低冲突风险。专家组确认了若干用于提高透明度的自愿的建立信任措施，并建议各国考虑采取进一步措施加强合作。专家组呼吁在联合国主持下定期举行广泛参与的对话，并通过双边、区域和多边论坛进行定期对话。虽然国家负有维持一个安全与和平的信通技术环境的首要责任，但如果私营部门、学术界和民间社会能适当参与，将有利于开展国际合作。

能力建设对于合作和建立信任至关重要。专家组 2013 报告(见 A/68/98)呼吁国际社会协助加强关键信通技术基础设施的安全，帮助培养技能，并建议制定适当的立法、战略和规章。本专家组重申这些结论意见，并强调所有国家可以相互学习如何认识和有效应对这些威胁。

专家组强调国际法、《联合国宪章》和主权原则的重要性，它们是加强各国使用信通技术安全性的基础。专家组指出各国拥有采取与国际法相符并得到《宪

章》承认的措施的固有权利，同时有必要进一步研究这一问题。专家组还提到既定国际法原则，包括适用情况下的人道原则、必要性原则、相称原则和区分原则。

专家组在思考今后的工作时，建议大会考虑于 2016 年召集一个新的政府专家组。

专家组请会员国积极审议其建议，并评估如何接受这些建议，以进一步发展和予以落实。

目录

秘书长的前言

很少有技术像信息和通信技术(信通技术)那样对重塑经济、社会和国际关系具有如此大的威力。网络空间触及我们生活的方方面面。好处是巨大的，但也不是没有风险。只有通过国际合作，才能实现网络空间的稳定与安全，而国际法和《联合国宪章》宗旨必须成为这一合作的基石。

本报告所载建议是来自 20 个国家的政府专家提出的，为的是应对由于国家和非国家行为体利用信通技术而存在的和新出现的可能危及国际和平与安全的各种威胁。专家们借鉴了 2010 年和 2013 年的共识报告，提出了制定规范、建立信任、进行能力建设和适用国际法的构想。

在已出现的各种复杂问题中，就存在极端分子、恐怖分子和有组织犯罪集团日益恶意利用信通技术的问题。本报告提出的建议可帮助应对这一令人不安的趋势，并有助于拟定我即将提出的防止暴力极端主义行动计划。

增加网络空间的安全性符合各国的切身利益。我们在这一领域开展工作时必须坚守全球承诺，即促进一个开放、安全与和平的因特网。本着这一精神，我将本报告推荐给大会和全球广大受众，报告为竭尽努力确保信通技术环境的安全作出了重要贡献。

送文函

2015 年 6 月 26 日

谨此提交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。专家组是根据关于从国际安全的角度看信息和电信领域发展的大会第 68/243 号决议第 4 段在 2014 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。

大会在上述决议中要求按公平地域分配于 2014 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、为对付这些威胁可能采取的合作措施，包括国家负责任行为的规范、规则或原则和建立信任措施、在冲突中使用信息和通信技术问题及国际法如何适用于国家使用信息和通信技术问题，以及旨在加强全球信息和电信系统安全的概念，以期促进取得共同的理解。决议还要求该专家组考虑到上一个专家组报告(见 A/68/98)中所载评估和建议，并请秘书长向大会第七十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 20 个国家的专家：白俄罗斯、巴西、中国、哥伦比亚、埃及、爱沙尼亚、法国、德国、加纳、以色列、日本、肯尼亚、马来西亚、墨西哥、巴基斯坦、大韩民国、俄罗斯联邦、西班牙、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。

专家组就从国际安全的角度看信息和电信领域的发展进行了全面深入的意见交流。专家组共举行了四次会议：2014 年 7 月 21 日至 25 日第一次会议在联合国总部举行；2014 年 1 月 12 日至 16 日第二次会议在日内瓦举行；2015 年 4 月 13 日至 17 日第三次会议和 2015 年 6 月 22 日至 26 日第四次会议都在联合国总部举行。

专家组谨对担任报告草稿讨论会主持人的各位专家表示感谢：Florence Mangin (法国)、Katherine Getao(肯尼亚)、Ausaf Ali(巴基斯坦)、Ricardo Mor(西班牙)和 Olivia Preston(联合王国)。

专家组谨对担任专家组顾问并任命 James Lewis 和 Kerstin Vignard 为代表的联合国裁军研究所的投入表示赞赏。专家组还对担任专家组秘书的联合国裁军事务厅的 Ewen Buchanan 和为专家组提供协助的秘书处其他官员表示感谢。

专家组组长

卡洛斯·路易斯·丹塔斯·科蒂尼奥·**佩雷斯**(签名)

一. 导言

1. 根据关于从国际安全的角度看信息和电信领域的发展的大会第 68/243 号决议，秘书长按公平地域分配设立了一个政府专家组，继续研究信息安全领域的现存威胁和潜在威胁、为对付这些威胁可能采取的合作措施，包括国家负责任行为的规范、规则或原则和建立信任措施、在冲突中使用信息和通信技术(信通技术)问题及国际法如何适用于国家使用信通技术的问题，以及旨在加强全球信息和电信系统安全的概念，以期促进取得共同的理解。

2. 一个开放、安全、稳定、无障碍、和平的信通技术环境对于所有人都非常重要，需要各国切实合作，减少国际和平与安全所面临的风险。本报告反映了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建议，并借鉴了前专家组的工作(见 A/65/201 和 A/68/98)。专家组审查了与其任务有关的国际概念和可能的合作措施。专家组重申，推动信通技术用于和平目的，并防止因使用信通技术而出现冲突，符合所有国家的利益。

二. 现有威胁和新出现的威胁

3. 信通技术为社会和经济发展提供了广阔的机会，对国际社会的重要性不断增加。但是，在全球信通技术环境中存在着国家和非国家行为体恶意利用信通技术的事件急剧增加等令人不安的趋势。这一趋势给所有国家带来风险，不当使用信通技术可能危害国际和平与安全。

4. 一些国家正在为军事目的发展信通技术能力。将信通技术用于未来国家间冲突的可能性越来越大。

5. 利用信通技术进行最具破坏性的攻击中包括针对一国的关键基础设施和相关信息系统发动这样的攻击。针对关键基础设施发动破坏性信通技术攻击的风险是真实存在的，并且非常严重。

6. 将信通技术用于除招募、资助、训练和煽动以外的恐怖主义目的，包括对信通技术或离不开信通技术的基础设施发动恐怖袭击，这种可能性已越来越大。如果放任不管，可能威胁到国际和平与安全。

7. 邪恶的非国家行为体(包括犯罪集团和恐怖分子)五花八门，揣着不同的动机，可以极快的速度发生恶意的信通技术行动，并且在出现信通技术事件后很难找到事件的源头，所有这些都增加了风险。国家有理由担心可能存在不利于稳定的误解，有可能发生冲突，并有可能危害本国国民、财产和经济。

8. 国家间确保信通技术安全的能力处于不同水平，将增加一个相互关联世界的脆弱性。

三. 国家负责任行为的规范、规则和原则

9. 信通技术环境对于国际社会确定如何将规范、规则和原则适用于国家开展与信通技术有关的活动，既是机遇，又是挑战。目标之一就是为负责任的国家行为确定更多自愿的非约束性规范，并加强对增强信通技术环境的稳定性与安全的共同理解。

10. 对负责任的国家行为进行自愿的非约束性规范，可降低国际和平、安全与稳定所面临的风险。因此，作出规范并无意要限制或禁止符合国际法的行动。制定规范反映了国际社会的愿望，确立了负责任的国家行为标准，使国际社会能够评估国家的活动和意图。规范有助于防止信通技术环境中的冲突，促进和平利用信通技术，以便充分实现将信通技术用于加强全球社会和经济发展。

11. 专家组以往的报告反映了根据现有国际规范和承诺就国家在信通技术安全性和使用方面负责任行为达成的新的共识。本专家组的任务是继续研究国家负责任行为规范，决定拟定哪方面的现有规范适用于信通技术环境，鼓励更大程度地接受各项规范，并确定需要在哪方面制定考虑到信通技术复杂性和独特属性的更多规范，以期促进达成共同理解。

12. 专家组注意到中国、哈萨克斯坦、吉尔吉斯斯坦、俄罗斯联邦、塔吉克斯坦和乌兹别克斯坦提出的关于信息安全国际行为准则的建议(见 A/69/723)。

13. 考虑到现有的和新出现的威胁、风险和脆弱性，并借鉴前专家组 2010 年 7 月和 2013 年 6 月报告中的评估和建议，本专家组为促进一个开放、稳定、安全、无障碍、和平的信通技术环境，提出关于自愿的非约束性国家负责任行为规范、规则或原则建议如下，供各国审议：

(a) 各国应遵循联合国宗旨，包括维持国际和平与安全的宗旨，合作制定和采用各项措施，加强信通技术使用的稳定性与安全性，并防止发生被公认有害于或可能威胁到国际和平与安全的信通技术行为；

(b) 一旦发生信通技术事件，各国应考虑所有相关信息，包括所发生事件的更大背景，信通技术环境中归属方面的困难，以及后果的性质和范围；

(c) 各国不应蓄意允许他人利用其领土使用信通技术实施国际不法行为；

(d) 各国应考虑如何以最佳方式开展合作，交流信息，互相帮助，起诉利用信通技术的恐怖分子和犯罪者，并采取其他合作措施对付这种威胁。各国也许需要考虑是否有必要在这方面制定新的措施；

(e) 各国在确保安全使用信通技术方面，应遵守关于促进、保护和享有因特网人权的人权理事会第 20/8 和 26/13 号决议，以及关于数字时代的隐私权的大会第 68/167 和 69/166 号决议，保证充分尊重人权，包括表达自由；

(f) 各国不应违反国际法规定的义务，从事或故意支持蓄意破坏关键基础设施或以其他方式损害为公众提供服务的关键基础设施的利用和运行的信通技术活动；

(g) 各国应考虑到关于创建全球网络安全文化及保护重要的信息基础设施的大会第 58/199 号决议和其他相关决议，采取措施，保护本国关键基础设施免受信通技术的威胁；

(h) 一个国家应适当回应另一国因其关键基础设施受到恶意信通技术行为的攻击而提出的援助请求。一个国家还应回应另一国的适当请求，减少从其领土发动的针对该国关键基础设施的恶意信通技术活动，同时考虑到适当尊重主权；

(i) 各国应采取合理步骤，确保供应链的完整性，使终端用户可以对信通技术产品的安全性有信心。各国应设法防止恶意信通技术工具和技术的扩散以及使用有害的隐蔽功能；

(j) 各国应鼓励负责任的报道信通技术的脆弱性，分享有关这种脆弱性的现有补救办法的相关资料，以限制并可能消除信通技术和依赖信通技术的基础设施所面临的潜在威胁；

(k) 一个国家不应进行或故意支持开展活动，危害另一国授权的应急小组(有时称为计算机应急小组或网络安全事件应对小组)的信息系统。各国不应利用经授权的应急小组从事恶意的国际活动。

14. 专家组指出，虽然这些措施对于促进一个开放、安全、稳定、无障碍、和平的信通技术环境可能是至关重要的，然而，特别是对发展中国家而言，在他们获得适足能力之前，也许不能立即付诸实施。

15. 鉴于信通技术的独特属性，可能需要在一段时间后制定更多规范。

四. 建立信任措施

16. 建立信任措施可加强国际和平与安全。它们能够加强国家间合作、透明度、可预测性和稳定性。各国在建立信任和确保一个和平的信通技术环境的工作中，应考虑到裁军审议委员会 1988 年通过的并经大会第 43/78(H)号决议核可的建立信任措施的指导方针。为加强信任与合作，减少冲突风险，专家组建议各国考虑采取以下各项自愿的建立信任措施：

(a) 在政策和技术层面确定对付严重的信通技术事件的联络点，并建立联络点目录；

(b) 酌情建立和支持双边、区域、次区域和多边协商机制和程序，以加强国家间的建立信任措施，减少可能因信通技术事件而产生的误解、事件升级和冲突风险；

(c) 鼓励酌情在自愿基础上在双边、次区域、区域和多边层面建立透明度，以增强信心，为今后的工作提供指导。这可包括自愿分享下列方面的国家意见和信息：信通技术及其使用所面临的国家和跨国威胁的各个方面；信通技术产品的脆弱性和已发现的有害隐藏功能；确保信通技术安全的最佳做法；区域和多边论坛制定的建立信任措施；与信通技术安全有关的国家组织、战略、政策和方案；

(d) 各国就本国自认为关键的基础设施类别及国家为保护这些基础设施所作的努力自愿提供看法，包括提供信息说明关于保护数据和靠信通技术带动的基础设施的国家法律和政策。各国应力求促进跨界合作，解决关键基础设施存在的超国界脆弱性问题。这些措施可包括：

㈠ 建立保护数据和靠信通技术带动的基础设施的国家法律和政策信息库，出版被认为适合发行的关于这类国家法律和政策的材料；

㈡ 建立关于保护靠信通技术带动的关键基础设施的双边、次区域、区域和多边协商机制和程序；

㈢ 在双边、次区域、区域和多边基础上，建立处理与信通技术有关的请求的技术、法律和外交机制；

㈣ 通过国家自愿作出的安排，视事件的规模和严重程度对信通技术事件进行分类，为交流有关事件的信息提供便利。

17. 各国应考虑采取更多的建立信任措施，在双边、次区域、区域和多边基础上加强合作。这可包括国家自愿达成的协议，以便：

(a) 加强相关机构之间处理信通技术安全事件的合作机制，建立更多的技术、法律和外交机制，以处理与信通技术基础设施有关的请求，包括酌情考虑进行应对事故和执法领域人员的交流，并鼓励研究机构和学术机构之间进行交流；

(b) 加强合作，包括建立协调中心交流关于恶意使用信通技术的信息，并为调查提供协助；

(c) 建立国际计算机应急小组和(或)网络安全应急小组或官方指定履行这一职能的组织。国家不妨考虑在其关键基础设施定义内设立这类机构。各国应支持和协助这些国家应急小组和其他获授权机构的运作与相互间合作；

(d) 酌情扩大和支持计算机应急小组和网络安全应急小组的做法，如交流关于脆弱性、袭击规律和减少攻击的最佳做法，包括协调反应、组织演习、协助处理信通技术相关事件和加强区域及部门合作等方面的信息；

(e) 针对其他国家的请求，以符合国家和国际法的方式合作调查涉及信通技术的犯罪或将信通技术用于恐怖主义目的，或减轻从本国领土发起的恶意信通技术活动的影响。

18. 专家组重申，鉴于信通技术的发展速度和威胁程度，有必要加强共同理解和增强合作。在这方面，专家组建议在联合国主持下定期举行广泛参与的对话，并通过双边、区域和多边论坛及其他国际组织进行定期对话。

五. 信通技术安全和能力建设方面的国际合作和援助

19. 各国负有维护国家安全、保障公民安全，包括信通技术环境安全的首要责任，但有些国家可能缺乏足够的能力来保护本国的信通技术网络。国家若缺乏能力可能使公民和关键基础设施容易受到恶意行为体的攻击，或使其无意间成为恶意行为者的避风港。国际合作与援助可发挥重要作用，使各国能够保证信通技术的安全性，确保将其用于和平用途。通过加强国家开展合作与集体行动的能力，为信通技术安全领域的能力建设提供援助，对于国际安全也至关重要。专家组一致认为，能力建设措施应设法促进将信通技术用于和平目的。

20. 专家组赞同 2010 年和 2013 年报告中关于能力建设的建议。2010 年报告建议各国确认支持欠发达国家能力建设的措施。2013 年报告呼吁国际社会共同努力提供援助，以便加强关键信通技术基础设施的安全性；开发技能并拟订适当立法、战略和监管框架，以履行职责；弥合信通技术安全及其使用方面的鸿沟。本专家组还强调指出，能力建设不仅仅关系到发达国家对发展中国家的知识和技能转让，而是所有国家都可以相互学习，认识他们所面临的威胁及如何有效应对这些威胁。

21. 各国应在通过以往的联合国决议和报告(包括题为“创建全球网络安全文化以及评估各国保护关键信息基础设施的努力”的大会第 64/211 号决议)开始的工作的基础上再接再厉、考虑自愿采取下列措施，为确保需要援助和提出援助请求的国家的信通技术安全提供能力建设方面的技术和其他援助：

(a) 协助加强与计算机应急小组和其他获授权机构的合作机制；

(b) 向发展中国家提供援助和培训，以加强使用信通技术(包括关键基础设施)的安全性，以及交流法律和行政最佳做法；

(c) 协助获取被视为对信通技术安全至关重要的技术；

(d) 建立应对网络安全事件和解决这方面短期问题的互助程序，包括快捷援助程序；

(e) 促进跨界合作，解决关键基础设施的超国界脆弱性问题；

(f) 制定信通技术安全能力建设工作的可持续性战略；

(g) 将信通技术安全意识和能力建设作为国家计划和预算的优先重点，并使其在发展和援助规划中获得适当位置。这可包括为教育和指导各机构和每个公民而设计的信通技术安全意识方案。可以与国际组织，包括联合国及其机构、私营部门、学术界和民间社会组织共同努力实施这样的方案；

(h) 鼓励进一步开展关于法证或合作措施等方面的能力建设工作，严防犯罪分子或恐怖分子使用信通技术。

22. 发展区域性的能力建设做法是有益的，因为这种做法能够考虑到具体的文化、地理、政治、经济或社会层面，还可以因地制宜。

23. 为了信通技术安全能力建设，各国可以考虑在既有伙伴关系的基础上制订双边和多边合作举措。这些举措将有助于改善国家之间应对信通技术事件的有效互助环境，有关国际组织，包括联合国及其机构、私营部门、学术界和民间社会组织可进一步发展这类举措。

六. 国际法如何适用于信通技术的使用

24. 2013 年报告指出，国际法，尤其是《联合国宪章》，对维护国际和平与稳定以及促进一个开放、安全、稳定、无障碍、和平的信通技术环境是适用的和不可或缺的。根据其任务规定，本专家组审议了国际法如何适用于国家使用信通技术的问题。

25. 各国遵守国际法，特别是《宪章》规定的义务，是它们使用信通技术以及促进一个开放、安全、稳定、无障碍、和平的信通技术环境的重要行动框架。履行这方面的义务是关于国际法适用于国家使用信通技术的审查工作的核心。

26. 在审议国际法适用于国家使用信通技术问题时，专家组确认至关重要的是各国承诺下列《宪章》宗旨和国际法原则：主权平等；以不危及国际和平与安全和正义的方式，通过和平手段解决国际争端；在国际关系中不对任何国家的领土完整或政治独立进行武力威胁或使用武力，或采用不符合联合国宗旨的任何其他方式；尊重人权和基本自由；不干涉他国内政。

27. 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。

28. 在前专家组工作的基础上，以及在《宪章》和大会第 68/243 号决议规定的任务指导下，本专家组就国际法如何适用于国家使用信通技术的问题提供了如下非详尽无遗的意见：

(a) 各国对其领土内的信通技术基础设施拥有管辖权；

(b) 各国在使用信通技术时，除其他国际法原则外，还必须遵守国家主权、主权平等、以和平手段解决争端和不干涉其他国家内政的原则。国际法规定的现有义务适用于国家使用信通技术。各国必须遵守国际法规定的义务，尊重和保护人权及基本自由；

(c) 专家组强调了国际社会对和平利用信通技术促进人类共同利益的愿望，回顾《宪章》全部内容的适用性，指出各国拥有采取符合国际法和得到《宪章》承认的措施的固有权利。专家组认识到需要进一步研究这一事项；

(d) 专家组提到既定的国际法律原则，包括适用情况下的人道原则、必要性原则、相称原则和区分原则；

(e) 各国不得使用代理人利用信通技术犯下国际不法行为，并应力求不让非国家行为体利用其领土实施这类行为；

(f) 各国必须就按照国际法归咎于它们的国际不法行为履行国际义务。但是，如果迹象表明信通技术活动由某国发起或源自其领土或信通技术基础设施，可能这件事本身并不足以将此活动归咎于该国。专家组指出，须经证实后才能对国家组织和实施不法行为提出指控。

29. 专家组指出，取得对国际法如何适用于国家使用信通技术问题的共同理解对于促进一个开放、安全、稳定、无障碍、和平的信通技术环境，具有重大意义。

七. 结论和今后工作建议

30. 对于恶意使用信通技术对国际和平与安全造成风险的认识已有显著提高。专家组认识到信通技术可以加速驱动发展，并且符合保持全球连通性和信息自由安全流动的需求，认为确定今后工作的可能措施很有助益，其中包括但不限于以下内容：

(a) 各国在法律、技术和政策层面共同和单独地进一步发展使用信通技术促进国际和平与稳定的概念；

(b) 在区域和多边两级加强合作，提高对恶意使用信通技术对国际和平与稳定构成的潜在威胁和靠信通技术带动的关键基础设施安全性的共同理解。

31. 虽然各国对维持一个安全、和平的信通技术环境负有首要责任，但是，确定私营部门、学术界和民间社会组织适当参与的机制将有利于开展有效合作。

32. 可能有用的进一步学习和研究领域包括与国家利用信通技术有关的概念。为所有会员国提供服务的联合国裁军研究所正是这样一个可以请来进行相关研究的实体，也可以请其他相关智囊团和研究组织进行研究。

33. 联合国可以发挥主导作用，促进各国就使用信通技术的安全性问题开展对话，并对将国际法、规范、准则和原则适用于负责任的国家行为达成共同理解。在进一步工作中，可以考虑就信通技术安全问题的国际对话与交流采取举措。这些工作不应重复其他国际组织和论坛正在开展的工作，即处理罪犯和恐怖分子利用信通技术的问题以及人权和因特网治理等问题。

34. 专家组指出大会考虑在 2016 年召集一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，具有重要意义，以便继续研究信息安全领域的现存威胁和潜在威胁、为对付这些威胁可能采取的合作措施，以及国际法如何适用于国家使用信通技术的问题，包括国家负责任行为的规范、规则和原则、建立信任措施和能力建设，以期促进取得共同理解。

35. 专家组赞扬各国际组织和区域集团为信通技术安全做出了宝贵的努力。各国就使用信通技术的安全问题开展的工作，应考虑到这些努力。会员国应酌情鼓励建立新的双边、区域和多边对话、协商和能力建设平台。

36. 专家组建议会员国积极审议本报告所载建议，即如何帮助创建一个开放、安全、稳定、无障碍、和平的信通技术环境，并评估如何接受这些建议，以进一步发展和加以落实。

附件

从国际安全角度看信息和电信领域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副司长
Aliaksandr Chasnouski (第三和第四届会议)

外交部国际安全和军控司司长
Vladimir N. Gerasimovich 大使(第一届会议)

白俄罗斯常驻日内瓦联合国代表团参赞
Ivan Grinevich(第二届会议)

巴西

公使、对外关系部主管政治事务副部长办公室主任
Carlos Luís Dantas Coutinho Perez

中国

外交部网络事务协调员
吴海涛(第三和第四届会议)

外交部网络事务协调员
傅聪(第一和第二届会议)

哥伦比亚

信息技术和通讯部信息技术标准和架构司司长
Jorge Fernando Bejarno

埃及

大使、外交部主管裁军、国家安全与和平利用核能副助理外交部长
Sameh Aboul-Enein

埃及常驻联合国代表团公使
Amr Aljowaily(第三届会员)

爱沙尼亚

外交部副部长兼法律顾问
Marina Kaljurand

法国

大使、外交部网络安全协调员
Florence Mangin

外交部战略事务、安全与裁军司
Leonard Rolland(第一届会议)

德国

联邦外交部网络政策协调人员主管
Karsten Geier

加纳

国家通讯管理局董事会成员
Mark-Oliver Kevor

以色列

外交部网络安全协调员
Iddo Moed

日本

外务省负责联合国事务大使、负责网络政策大使兼外交政策局副总干事
Takashi Okada(第三和第四届会议)

外务省负责联合国事务大使、负责网络政策大使兼外交政策局副总干事
Akira Kono(第二届会议)

外务省外交政策局国际安全事务高级谈判员，Takao Imafuku(第一届会议)

肯尼亚

信息、通讯与技术部信通技术秘书
Katherine Getao

马来西亚

国家安全理事会网络和空间安全司首席助理秘书
Nur Hayuna Abd Karim(第四届会议)

国家安全理事会网络和空间安全司次官
Md Shah Nuri bin Md Zain(第一、第二和第三届会员)

墨西哥

墨西哥国家安全委员会-联邦警察派驻美利坚合众国和加拿大专员
Edgar Zurita

巴基斯坦

联合参谋总部战略计划司技术处总干事
Ausaf Ali(第一、第二和第四届会议)

巴基斯坦常驻联合国代表团公使
Khalil Hashmi(第三届会员)

大韩民国

外交部国际安全司司长
Chul Lee(第二和第四届会议)

大韩民国驻比利时王国和欧洲联盟大使馆参赞
Hyuncheol Jang (第一和第三届会员)

俄罗斯联邦

俄罗斯联邦总统负责信息安全国际合作事务特别代表、无任所大使
Andrey V. Krutskikh

西班牙

外交与合作部网络安全无任所大使
Ricardo Mor(第四届会议)

外交与合作部网络安全无任所大使
Alicia Moral(第一、第二和第三届会员)

大不列颠及北爱尔兰联合王国

内阁办公厅网络安全和信息保障办公室助理主任
Olivia Preston

美利坚合众国

美国国务院国务卿办公室网络事务协调员办公室网络问题副协调员
Michele G. Markoff