联合国 A/76/135

大 会

Distr.: General
14 July 2021
Chinese
Original: English

第七十六届会议

暂定项目表* 项目 96

从国际安全角度看信息和电信领域的发展

从国际安全角度促进网络空间负责任国家行为政府专家组

秘书长的说明

秘书长谨转递从国际安全角度促进网络空间负责任国家行为政府专家组的报告。该专家组系根据大会第 73/266 号决议第 3 段设立。

* A/76/50。

21-04030 (C) 230721 030821

请回收

从国际安全角度促进网络空间负责任国家行为政府专家组的报告

摘要

随着世界对信息和通信技术(信通技术)的依赖程度不断增加，各国在使用信通技术方面的负责任行为对维护国际和平与安全至关重要。

根据大会第 73/266 号决议授权的任务规定，2019-2021 年从国际安全角度促进网络空间负责任国家行为政府专家组继续研究应对信息安全领域现有和潜在威胁的可能合作措施，以增进共同认识和促进有效执行。

本报告载有专家组关于以下主题的结论意见：现有和新出现的威胁；各国负责任行为准则、规则和原则；国际法；建立信任措施；信通技术安全和能力建设方面的国际合作和援助。在每一个议题上，本报告都为往届政府专家组的结论意见和建议提供了更深一层的理解。

目录

秘书长的前言

信息和通信技术(信通技术)仍在迅速改变各国社会，在提供众多机会的同时也带来了巨大的风险。2019 冠状病毒病(COVID-19)大流行进一步加速了我们生活的诸多方面向数字空间的转移和对数字技术的依赖。

与此同时，数字监控和操纵行为正在增加，打造网络世界的方式并不总是符合公众利益。如果任其发展，可能会对社会和个人造成破坏性影响。我们比以往任何时候都更亟需应对这些挑战，利用信通技术带来的惠益，促进各国在国际安全方面的负责任行为。

为履行其任务，2019-2021 年政府专家组在 18 个月的时间里进行了广泛的审议。区域一级的非正式协商和向所有会员国开放的非正式会议，也进一步充实了这方面的工作。该小组的报告与 2021 年 3 月通过共识报告的从国际安全角度看信息和电信领域的发展不限成员名额工作组的工作是相辅相成的。

近年来，各国和其他公共和私营利益攸关方越来越重视联合国促进和平利用信通技术的努力。本着这一精神，本报告是为促成开放、安全、稳定和无障碍的信通技术环境所作的贡献。报告也再次呼吁开展进一步合作，以减少国际和平与安全所面临的网络风险，并确保保护和促进网上和网下的人权和基本自由。

送文函

2021 年 5 月 28 日

我谨转递从国际安全角度促进网络空间负责任国家行为政府专家组的共识报告。该专家组是根据大会第 73/266 号决议执行部分第 3 段于 2018 年设立的。

在该决议中，大会请将于 2019 年成立的基于公平区域分配的政府专家组从政府专家组 2010 年、2013 年和 2015 年共识报告所载评估意见和建议出发，继续开展研究，以增进共同认识，有效执行应对国际信息安全领域现有和潜在威胁的可能合作措施，包括国家负责任行为的准则、规则和原则、建立信任措施、能力建设以及各国使用信息和通信技术时的国际法的适用。大会请秘书长向其第七十六届会议提交一份关于该研究结果的报告。

根据专家组的任务规定，将在联合国裁军事务厅的网站上以收到的原件语文提供关于各国使用信息和通信技术时的国际法的适用这一主题的国家自愿贡献的正式汇编(A/76/136)，但不提供译文。

根据该决议的规定，任命了来自以下 25 个国家的专家：澳大利亚、巴西、中国、爱沙尼亚、法国、德国、印度、印度尼西亚、日本、约旦、哈萨克斯坦、肯尼亚、毛里求斯、墨西哥、摩洛哥、荷兰、挪威、罗马尼亚、俄罗斯联邦、新加坡、南非、瑞士、大不列颠及北爱尔兰联合王国、美利坚合众国和乌拉圭。专家名单附于本报告之后。

专家组举行了四次正式会议：第一次于 2019 年 12 月 9 日至 13 日在联合国总部举行，第二次于 2020 年 2 月 24 日至 28 日在日内瓦举行，第三次于 2021 年 4 月 5 日至 9 日以虚拟形式举行，第四次于 2021 年 5 月 24 日至 28 日以虚拟形式举行。由于 COVID-19 大流行的影响，根据大会第 75/551 号决定，专家组第三次会议被推迟举行。尽管如此，专家组在此期间通过一系列闭会期间非正式磋商继续开展工作。根据其任务规定，专家组还与相关区域组织举行了一系列磋商，并与会员国举行了不限成员名额的磋商会议，以进行互动讨论和交流意见。

专家组对联合国裁军事务厅和联合国裁军研究所联合支助小组的贡献表示感谢。

我还要借此机会对巴西政府指定我担任主席表示感谢，并感谢专家组让我有幸担任主席。我还要感谢我的专家同行、我的巴西同事、联合支助小组成员和联合国秘书处，特别是裁军事务高级代表，感谢他们的支持，感谢他们本着建设性的参与精神分享他们丰富的专业知识。

专家组主席

吉列尔梅·德阿吉亚尔·帕特里奥塔(签名)

一. 导言

1. 本报告反映了政府专家组根据题为“从国际安全角度促进网络空间国家负责任行为”的大会第 73/266 号决议进行的讨论的结果。专家组一个重要的工作组成部分是在 2019 冠状病毒病(COVID-19)大流行期间展开的。疫情突显了数字技术的巨大潜力，同时也加速了世界对数字技术的依赖，从而进一步突出了在国际安全背景下利用信通技术时采取负责任行为的重要性。

2. 本报告借鉴并重申了 2010 年、2013 年和 2015 年联合国政府专家组共识报告中关于现有和新出现的威胁、国际法、负责任国家行为的准则、规则和原则、建立信任以及国际合作和能力建设的评估和建议，这些评估和建议共同构成在使用信通技术领域负责任国家行为不断演变的累积框架。专家组欢迎通过大会第 73/27 号决议所设联合国从国际安全角度看信息和电信领域发展不限成员名额工作组的共识报告，[1] 该报告重申并巩固了这一框架。

3. 专家组根据其任务规定的事项与国际和平与安全的相关性，对这些事项进行了审议。此外，政府专家组还试图为其先前报告中的评估和建议提供更深一层的理解，以为支持实施这些建议提供指导。这种更深一层的理解再次确认了专家组任务规定中不同实质性内容之间的联系，以及在各国执行这些建议的努力中让其他行为体参与进来的重要性，包括酌情让私营部门、民间社会、学术界和技术界参与进来。

4. 在推进政府专家组报告中的评估和建议、开发针对本区域的机制、加强能力建设工作以支持实施这些评估和建议方面，区域和次区域机构发挥着重要作用，专家组对这一作用表示认可。根据专家组的任务规定，在专家组与会员国在纽约举行的非正式磋商会议期间，以及通过与区域组织协作举行的一系列磋商，各方与专家组分享了这些和其他相关的见解和经验。[2]

5. 专家组重申，一个开放、安全、稳定、无障碍、和平的信通技术环境对所有国家都至关重要，需要各国开展有效合作，以降低对国际和平与安全的风险。促进将信通技术用于和平目的，符合所有行为体的利益，对共同利益至关重要。在这些努力中，对主权、人权和基本自由的尊重以及可持续数字发展仍然居于核心位置。

二. 现有和新出现的威胁

6. 信通技术以及日益数字化和相互联通的世界，为全球各地的社会提供了巨大的机遇。但专家组确认，以往报告中指出的严重的信通技术威胁依然存在。涉及国家和非国家行为体恶意使用信通技术的事件，在范围、规模、严重性和复杂性

[1] A/75/816。

[2] 各次磋商的报告可在以下网址查阅：https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf 和 https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf。

上都有增加。虽然信通技术威胁在不同区域的表现形式各不相同，但其影响也可能是全球性的。

7. 专家组强调 2015 年报告的评估意见，即一些国家正在发展用于军事目的的信通技术能力；在未来的国家间冲突中使用信通技术的可能性越来越大。

8. 包括国家和其他行为体在内的持续威胁行为体开展的恶意信通技术活动，对国际安全与稳定、经济和社会发展以及个人的安全和福祉构成重大威胁。

9. 此外，各国和其他行为体正在积极利用更复杂、更尖端的信通技术能力，用于政治和其他目的。另外，专家组还注意到，各国恶意利用信通技术促成的秘密宣传运动来影响另一国的进程、体制和整体稳定的情况有所增加，令人担忧。这些做法破坏信任，有可能造成升级，并可能威胁到国际和平与安全，并可能对个人造成直接和间接的伤害。

10. 在前几份专家组报告中，专家组讨论了针对在国内、区域或全球提供服务的关键基础设施实施的有害信通技术活动，这种攻击的可能性日趋严重。特别令人关切的是，恶意信通技术活动影响到关键的信息基础设施、向公众提供基本服务的基础设施、对互联网的普遍可用性或完整性至关重要的技术基础设施，以及卫生部门实体。COVID-19 大流行表明，利用我们的社会面临巨大压力的时机企图浑水摸鱼的恶意信通技术活动，会带来怎样的风险和后果。

11. 新兴技术增加了促进发展的机遇，但其不断演变的属性和特征也扩大了攻击面，创造了新的载体和漏洞，可被恶意信通技术活动利用。确保经营性技术和构成物联网的互联计算设备、平台、机器或对象中的漏洞不被恶意利用，已经成为一项严峻的挑战。

12. 世界各国保障信息系统安全的能力仍然各不相同，发展应对能力、保护关键信息基础设施、识别威胁和及时应对威胁的能力也各不相同。这些能力和资源方面的差异，与利用信通技术有关的国家法律、规范和实践的差别，以及对可用于减轻、调查此类事件或从此类事件中恢复的现有区域和全球合作措施的认识和利用机会的不平等，增加了脆弱性和对所有国家的风险。

13. 专家组重申，除了把信通技术用于招募、筹资、培训和煽动等恐怖主义目的，还用于对信通技术或依赖这一技术的基础设施发动恐怖袭击等其他目的，正变得越来越有可能，如果置之不理，可能会威胁到国际和平与安全。

14. 专家组还重申，恶意的非国家行为体(包括犯罪集团和恐怖分子)多种多样，动机也各不相同，另外恶意信通技术行动的发生速度快，追踪信通技术事件源头的难度大，这些因素都增加了风险。

三 准则、规则和原则

15. 专家组重申，关于各国对信通技术的利用，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。规范和现有的国际

法是相辅相成的。规范无意限制或禁止在其他方面符合国际法的行动。规范反映了国际社会的期望，确立了负责任的国家行为标准。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。

16. 专家组还强调规范与建立信任措施、国际合作和能力建设之间的相互关系。鉴于信通技术的独特属性，专家组重申 2015 年报告中的意见，即今后可以制定额外的准则，并另行指出，今后有可能酌情拟订具有约束力的补充义务。

17. 除了在联合国系统内开展的工作外，专家组还认可在区域一级执行规范所积累的宝贵经验，包括在纽约与会员国举行的非正式磋商期间以及根据其任务规定通过与区域组织合作分享的经验。专家组指出，今后在国际安全背景下开展的信通技术工作应考虑到这些努力。专家组还注意到中国、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)。

18. 协商一致通过的大会第 70/237 号决议促请会员国将政府专家组 2015 年报告作为使用信通技术的指南。该报告包括 11 条自愿、不具约束力的国家负责任行为规范。根据其促进负责任行为的任务规定，专家组对这些规范又增加了一层理解，强调这些规范对各国在国际和平与安全背景下使用信通技术的预期行为很有价值，并举例说明了各国可在国家和区域两级为支持执行规范所作出的各种体制安排。专家组提醒各国，应根据《联合国宪章》和其他国际法规定的义务开展这些努力，以维护一个开放、安全、稳定、无障碍和和平的信通技术环境。呼吁各国避免和不得以不符合负责任国家行为准则的方式利用信通技术。

规范 13(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，合作制定和采取各项措施，加强信通技术使用的稳定性与安全性，并防止发生公认对国际和平与安全有害或可能对其构成威胁的信通技术做法。

19. 维护国际和平与安全、开展国际合作是联合国的创始宗旨之一。这一规范提醒人们，开展合作携手推动信通技术用于和平目的，并防止因滥用信通技术而出现冲突，是所有国家的共同愿望，符合所有国家的利益。

20. 在这方面，为了促进这一准则，专家组鼓励各国避免利用信通技术和信通技术网络开展可能威胁到维护国际和平与安全的活动。

21. 前几届政府专家组和不限成员名额工作组建议的措施，是利用信通技术的负责任国家行为的初步框架。为促进这种合作，并提供进一步的指导，专家组建议各国在国家一级建立或加强现有的机制、结构和程序，如相关政策、立法和相应的审查程序；危机和事件管理机制；整体政府合作和伙伴关系安排；以及与私营部门、学术界、民间社会和技术界的合作与对话安排。同时，鼓励各国汇编和精简其提交的关于规范执行情况的资料，包括自愿考察本国的努力和分享本国的经验。

规范 13(b)：一旦发生信通技术事件，各国应考虑所有相关信息，包括所发生事件的大背景，信通技术环境中归责方面的困难，以及后果的性质和范围。

22. 这项规范承认，归责是一项复杂的工作，在确定信通技术事件的源头前，应考虑一系列因素。在这方面，本报告第 71(g)段及专家组以往报告中呼吁采取的审慎态度，有助于避免国家之间发生误解和紧张局势升级。

23. 鼓励受到恶意信通技术活动影响的国家，以及此类恶意信通技术活动涉嫌源自其领土的国家，由有关主管当局进行相互协商。

24. 恶意信通技术事件的受害国在评估事件时应考虑所有方面。在确凿的事实证据支持下，这些方面可以包括事件的技术属性；事件的范围、规模和影响；更为宏观的背景，包括事件对国际和平与安全造成的影响；有关国家之间的协商结果。

25. 受影响国在应对可归于另一国的恶意信通技术活动时，应遵循《联合国宪章》和其他国际法规定的义务，包括与通过和平手段解决争端和国际不法行为有关的义务。各国还可以利用可供采用的各种外交、法律和其他协商备选方案，以及自愿机制和其他政治承诺，通过协商和其他和平手段解决分歧和争端。

26. 为了在国家一级落实这一规范、便利调查和解决涉及他国的信通技术事件，各国可建立或加强相关的国家结构、与信通技术有关的政策、程序、立法框架、协调机制以及与相关利益攸关方建立的伙伴关系和其他形式的接触形式，评估信通技术事件的严重性和可复制性。

27. 区域和国际层面的合作，包括国家计算机事件应急响应小组/计算机安全事件响应小组、各国信通技术主管部门和外交界之间的合作，可以加强各国发现和调查恶意信通技术事件以及在就事件得出结论之前证实本国关切和调查结果的能力。

28. 各国还可以利用多边、区域、双边和多利益攸关方平台，就各国处理归责问题的办法(包括如何区分不同类型的归责)以及信通技术威胁和事件交流做法、分享信息。专家组还建议，联合国在今后的工作中还可以考虑如何促进对归责问题的共同理解和实践交流。

规范 13(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。

29. 这项规范反映了如下期望，即一国若秉持善意得知或被告知，利用信通技术实施的国际不法行为源自其领土或从其领土过境，则该国将采取一切适当、合理可用和可行的步骤侦查、调查和处理这种情况。这项规范所蕴涵的理解是，一个国家不得允许另一个国家或非国家行为体利用其境内的信通技术实施国际不法行为。

30. 各国在考虑如何实现这项规范的目标时，应牢记以下几点：

(a) 这项规范期望一个国家在其能力范围之内采取合理措施，以相称、适当和有效的手段以及符合国际法和国内法的方式制止本国领土上正在进行的活动。尽管如此，并不能指望各国能够或应该监测本国领土上的所有信通技术活动。

(b) 一国若知晓他方利用信通技术在其境内从事国际不法行为，但却缺乏处理能力，可考虑以符合国际法和国内法的方式寻求他国或私营部门援助。建立相应的结构和机制来拟定和回应援助请求，可能有助于落实这一规范。各国在提供援助时应秉持善意并遵从国际法行事，不得乘机对寻求援助的国家或对第三国实施恶意活动。

(c) 受影响国可通知不法活动的来源国。被通知国应确认收到通知，以促进合作和信任，并尽一切合理努力协助确定国际不法行为是否已经实施。确认收到这一通知，并不表示同意通知中所载的信息。

(d) 源自第三国领土或基础设施的信通技术事件本身并不意味着该国对该事件负有责任。此外，通知一国其领土正被用于实施不法行为，本身并不意味着该国要对该行为本身负责。

规范 13(d)：各国应考虑如何最好地合作交流信息，相互协助，起诉使用信通技术从事的恐怖主义和犯罪行为，并采取其他合作措施应对此类威胁。各国可能需要考虑是否需要在这方面制定新的措施。

31. 这项规范提醒各国，必须开展国际合作，以应对犯罪分子和恐怖分子利用互联网和信通技术构成的跨界威胁，包括用于招募、资助、培训和煽动目的，策划和协调袭击，宣传其思想和行动，以及本报告中强调的其他此类目的。这项规范确认，通过现有措施和其他措施，在应对涉及恐怖主义和犯罪集团和个人的这类威胁和其他此类威胁方面取得进展，有助于促进国际和平与稳定。

32. 遵守这一规范意味着需要具备相应的国家政策、立法、结构和机制，促成就相关的技术、执法、法律和外交事项开展跨境合作，打击利用信通技术从事犯罪和恐怖主义活动的行为。

33. 专家组鼓励各国加强和进一步发展可促进相关国家、区域和国际组织交流信息、开展援助的机制，目的是提高各国的信通技术安全意识，减少网络恐怖主义和犯罪活动的运作空间。此类机制可加强相关组织和机构的能力，同时在国家之间建立信任，强化负责任的国家行为。专家组还鼓励各国制定适当的规程和程序，收集、处理和储存利用信通技术从事犯罪和恐怖主义行为的相关网络证据，并及时协助调查，确保根据国际法所规定的国家义务采取此类行动。

34. 在联合国内部，一些专门的论坛、进程和决议专门探讨利用信通技术从事恐怖主义和犯罪行为所带来的威胁，以及应对这种威胁所需的合作办法。相关大会决议包括关于第十二届联合国预防犯罪和刑事司法大会的第 65/230 号决议，该决议决定设立一个不限成员名额政府间专家组，全面研究网络犯罪问题；关于促进技术援助和能力建设以加强打击为犯罪目的使用信通技术的国家措施和国际合作，包括信息共享的第 74/173 号决议；关于打击为犯罪目的使用信通技术的第 74/247 号决议。

35. 各国还可以利用现有的进程、举措和法律文书，并考虑增加程序或沟通渠道，促进信息交流和援助，打击利用信通技术从事犯罪和恐怖主义活动的行为。在这

方面，专家组鼓励各国继续加强联合国和区域一级正在进行的努力，应对利用互联网和信通技术实施犯罪和从事恐怖主义的行为；鼓励各国为此目的与国际组织、行业行为体、学术界和民间社会发展合作伙伴关系。

规范 13(e)：各国应在确保安全使用信通技术方面遵守人权理事会关于在互联网上增进、保护和享有人权的第 20/8 和 26/13 号决议，以及大会关于数字时代的隐私权的第 68/167 和 69/166 号决议，保证充分尊重人权，包括表达自由权。

36. 这项规范提醒各国根据各自的义务，尊重和保护网上和网下的人权和基本自由。在这方面，需要特别重视以下权利：表达自由权，包括不分国界寻求、接收和传递任何媒介形式信息的自由，以及《公民权利和政治权利国际公约》、《经济、社会、文化权利国际公约》和《世界人权宣言》中的其他相关条款。遵守这项规范还有助于促进不歧视和缩小数字鸿沟，包括性别平等方面的数字鸿沟。

37. 通过该规范所述决议和此后的其他决议，既是对在国家使用信通技术问题上出现的新挑战与新困境的承认，也是对相应解决这些困境的必要性的承认。任意或非法的大规模监控等国家行为可能对行使和享有人权(特别是隐私权)产生特别不利的影响。

38. 各国在落实这项规范时，应考虑上述决议所载的具体指导意见。各国还应该注意到自 2015 年政府专家组报告以来通过的各项新决议，并对可能需要根据当前事态发展推进的新决议作出贡献。

39. 各国促进尊重人权和遵守人权准则、确保负责与安全使用信通技术的努力应相互补充、相互促进、相互依存。这种办法能够促成一个开放、安全、稳定、无障碍、和平的信通技术环境，也有助于实现可持续发展目标。

40. 专家组承认技术创新对所有国家至关重要，但新兴技术也可能对人权和信通技术安全产生重要影响。为解决这一问题，各国可考虑以更加包容、更加无障碍且不致负面影响单个社区或群体的方式，投资和推动指导信通技术发展和利用的技术措施和法律措施。

41. 专家组指出，联合国内部设有多个论坛专门处理人权问题。此外，专家组肯定了各类利益攸关方以不同方式推动保护和促进网上和网下人权和基本自由的做法。让这些群体参与有关信通技术安全的决策进程，可以推动促进、保护和享有网上人权的努力，并有助于阐明和最大限度地减少各项政策对民众(包括对弱势群体)的潜在负面影响。

规范 13(f)：一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。

42. 关于这项规范，实施信通技术活动蓄意破坏关键基础设施，或以其他方式损害向公众提供服务的关键基础设施的使用和运营，可能产生国内、区域和全球的连带影响，给民众带来更大的伤害风险，并且可能会升级，可能引发冲突。

43. 这项规范还指出了关键基础设施作为国家资产的根本重要性，因为这些基础设施构成社会重要功能、服务和活动的支柱。倘若这些设施遭到严重损害或破坏，无论是人力代价，还是对一国经济、发展、政治与社会运作和国家安全的影响，都会是巨大的。

44. 正如规范 13(g)指出，各国应采取适当措施保护本国关键基础设施。在这方面，每个国家根据本国的优先事项和关键基础设施分类方法，确定归本国管辖的哪些基础设施或部门应视为关键设施或部门。

45. 2019 冠状病毒病(COVID-19)大流行促使人们更深认识到，通过实施涉及关键基础设施的规范(如本规范及规范(g)和(h))等方式，保护卫生保健和医疗基础设施和公共设施，具有极端的重要性。向公众提供基本服务的关键基础设施部门的其他实例还包括能源、发电、水和环境卫生、教育、商业金融服务、交通、电信等部门和选举进程。关键基础设施也可以指那些跨越多个国家提供服务的基础设施，例如对互联网的普遍可用性或完整性至关重要的技术基础设施。这类基础设施对国际贸易、金融市场、全球运输、通信、卫生或人道主义行动可能至关重要。强调这类基础设施作为例子，并不妨碍各国将其他基础设施指定为关键基础设施，也绝非纵容针对上文未提及的基础设施类别所实施的恶意活动。

46. 为支持落实这项规范，专家组鼓励各国除考虑上述因素外，还应在国家层面制定并依照其国际法律义务采用相关政策和立法措施，确保一国开展或支持的可能影响另一国关键基础设施或影响另一国提供基本公共服务的信通技术活动符合这项规范，并接受全面审查和监督。

规范 13(g)：各国应考虑到大会第 58/199 号决议，采取适当措施，保护本国关键基础设施免受信通技术的威胁。

47. 这项规范重申了所有国家保护其管辖范围内的关键基础设施免受信通技术威胁的承诺，以及这方面开展国际合作的重要性。

48. 一个国家将某一基础设施或部门指定为关键基础设施或部门，可能有助于保护该设施或部门。各国除确定其认为关键的基础设施或基础设施部门外，还确定需要采取哪些必要的结构、技术、组织、立法和监管措施保护本国关键基础设施，并在发生事故时恢复功能。大会关于“创造全球网络安全文化及保护重要的信息基础设施”的第 58/199 号决议及其附件[3] 强调了各国为此可在国家一级采取的行动。

49. 一些国家是提供区域或全球服务的基础设施的东道国。对此类基础设施的信通技术威胁可能会产生破坏稳定的影响。参与此类安排的国家可提倡与相关基础设施的所有者和运营者开展跨境合作，以加强针对此类基础设施的信通技术安全措施，并加强现有流程和程序或制定补充流程和程序，以发现影响此类基础设施的信通技术事件并减轻其影响。

[3] A/RES/58/199，该决议是包括大会 A/RES/57/239 和 A/RES/64/211 号决议在内的一揽子三项决议之一。

50. 鼓励采取措施确保信通技术产品在其整个生命周期内的安全和保障，或根据其规模和严重程度对信通技术事件进行分类，也将有助于实现本规范的目标。

规范 13(h)：各国应对关键基础设施遭到恶意使用信通技术行为破坏的另一国提出的适当援助请求作出回应。各国还应回应另一国的适当请求，减轻源自其领土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。

51. 这项规范提醒各国，在回应关键基础设施受到恶意信通技术行为影响的另一国的援助请求时，国际合作、对话以及对所有国家主权的应有尊重至关重要。在处理那些有可能威胁到国际和平与安全的行为时，这项规范尤为重要。

52. 在收到援助请求后，各国应在其能力和资源范围内提供在当时情况下合理可用和切实可行的一切援助。一国可选择寻求双边援助，或通过区域或国际安排寻求援助。各国还可以请私营部门提供服务，协助回应援助请求。

53. 建立必要的国家结构和机制，发现可能威胁国际和平与安全的信通技术事件并减轻其影响，有助于切实落实这一规范。此类机制是对现有的日常信通技术事件管理和解决机制的补充。例如，希望请求他国援助的国家若能知晓应与谁联系、应使用何种适当的沟通渠道，会很有帮助。收到援助请求的国家需要顾及请求的紧迫性和敏感性，尽可能透明及时地确定本国是否有能力、人力和资源提供所请求的援助。不应期望收到请求援助的国家保证实现特定的结果或成果。

54. 在请求另一国提供援助和回应援助请求方面建立共同、透明的流程和程序，能够为该规范所述的合作提供便利。在这方面，制定提出援助请求和回应援助请求的通用模板，可确保援助请求国向其寻求援助的国家提供尽可能完整、准确的信息，为开展合作和及时作出回应提供便利。此类模板可由双边、多边或区域一级自愿制定。回应援助请求的通用模板可包含以下内容：确认收到请求；若可以提供援助，应说明可提供的援助的时间框架、性质、范围和条件。

55. 若恶意活动源自某一特定国家的领土，则该国主动提供所请求的援助并开展此类援助，会有助于最大限度地减少破坏、避免误解、降低升级风险、帮助恢复信任。参与合作性机制，确定危机沟通的手段和模式以及管控和解决事件的手段和模式，有助于促进遵守该规范。

规范 13(i)：各国应采取合理步骤，确保供应链的完整性，以便最终用户能够对信通技术产品的安全抱有信心。各国应设法防止恶意信通技术工具及技术的扩散以及有害隐蔽功能的使用。

56. 这项规范确认有必要促进最终用户对开放、安全、稳定、无障碍和和平的信通技术环境的信心和信任。确保信通技术供应链的完整性和信通技术产品的安全性，防止恶意信通技术工具及技术的扩散以及有害隐蔽功能的使用，对于这方面以及国际安全、数字经济发展和更广义的经济发展越来越重要。

57. 全球信通技术供应链分布广泛，日益复杂，相互依存，并且涉及多方。可采取以下合理步骤促进开放性，确保供应链的完整性、稳定性和安全性：

(a) 在符合一国国际义务的前提下，建立全面、透明、客观、公正的国家一级供应链风险管理框架与机制。此类框架可包括风险评估，其中应考虑到各种因素，包括新技术的裨益和风险。

(b) 制定政策和方案，以便客观促进采购信通技术设备和系统的供应商和供货商采用良好做法，以便在国际上建立对信通技术产品和服务的完整性和安全性的信心，提高质量，促进选择。

(c) 在国家政策中，以及在与各国和相关行为体在联合国和其他场合的对话中，更加关注如何确保所有国家能够平等开展竞争和创新，以便充分实现将信通技术用于加强全球社会和经济发展，促进维护国际和平与安全，同时保障国家安全和公共利益。

(d) 采取合作措施，如在双边、区域和多边层面交流供应链风险管理方面的良好做法；制定和实施全球可互操作的供应链安全共同规则和标准；制定其他旨在减少供应链脆弱性的方法。

58. 为防止恶意信通技术工具及技术的开发和扩散以及有害隐蔽功能(包括后门程序)的使用，各国可考虑在国家一级：

(a) 采取措施加强供应链的完整性，包括要求信通技术供应商将安全和保障纳入信通技术产品的设计、开发和整个生命周期。为此，各国还可考虑建立独立、公正的认证程序。

(b) 采取旨在加强数据保护和隐私的立法和其他保障措施。

(c) 采取措施，禁止在信通技术产品中植入有害隐蔽功能，禁止利用可能损害系统和网络(包括关键基础设施)保密性、完整性和可用性的漏洞。

59. 除上述步骤和措施外，各国还应继续鼓励私营部门和民间社会发挥适当作用，改善信通技术及其使用的安全性，包括改善信通技术产品的供应链安全，从而促进实现这项规范的目标。

规范 13(j)：各国应鼓励负责任地报告信通技术的漏洞，分享关于这些漏洞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。

60. 这一规范提醒各国，必须确保信通技术漏洞得到迅速解决，以减少恶意行为体利用信通技术的可能性。及时发现和负责任地披露和报告信通技术漏洞，可以防止有害或威胁性做法，增强信任和信心，减少对国际安全与稳定的相关威胁。

61. 漏洞披露政策和计划及相关的国际合作旨在为此类披露工作的常态化提供一个可靠和一致的程序。协调一致的漏洞披露程序可以最大限度地减少脆弱产品对社会造成的危害，并促使国家和应急小组之间报告信通技术漏洞和请求援助的工作实现系统化。此类程序应与国内立法保持一致。

62. 在国家、区域和国际一级，各国可以考虑出台公正的法律框架、政策和方案，为处理信通技术漏洞的决策提供指导，并遏制其商业传播，以防止任何滥用技术漏洞的做法可能对国际和平与安全或人权和基本自由构成风险。各国还可以考虑为研究人员和渗透测试者提供法律保护。

63. 此外，各国还可与相关行业和其他信通技术安全行为体协商，根据相关国际技术标准，制定有关以下问题的指导和激励措施：负责任地报告和管理漏洞以及不同利益攸关方在报告过程中各自的作用和责任；待披露或公开分享的技术信息的类型，包括分享关于严重信通技术事故的技术信息；以及如何处理敏感数据，确保信息的安全性和机密性。

64. 往届政府专家组关于建立信任与国际合作、援助和能力建设的建议，特别有助于就各国可以出台哪些机制和程序促进负责任地披露漏洞达成共识。各国可以考虑利用现有的多边、区域和次区域机构以及涉及不同利益攸关方的其他相关渠道和平台来实现这一目标。

规范 13(k)：各国不应开展或蓄意支持损害另一国授权应急小组(有时称为计算机应急小组或网络安全事件应急小组)信息系统的活动。一国不应利用授权的应急小组从事恶意的国际活动。

65. 这项规范反映了这样一个事实，即计算机应急小组/计算机安全事件响应小组或其他经授权的应急机构在管控和解决信通技术事件方面负有独特的责任和职能，因而在促进维护国际和平与安全方面发挥着重要作用。它们对于有效发现和缓解信通技术事件的直接和长期负面影响至关重要。损害应急小组的做法可能会破坏信任，妨碍它们履行职能的能力，并可能产生更广泛的、往往是不可预见的跨部门后果，并可能对国际和平与安全造成影响。专家组强调必须避免将计算机应急小组/计算机安全事件响应小组政治化，必须尊重其职能的独立性。

66. 许多国家认识到，计算机应急小组/计算机安全事件响应小组在保护国家安全、保护公众和防止信通技术相关事件造成经济损失方面发挥着关键作用，因此将其归入本国关键基础设施的一部分。

67. 在考虑其涉及应急小组的行动如何有助于实现国际和平与安全方面，各国可以公开宣布或采取措施，申明不会利用获授权的应急小组从事恶意的国际活动，并认可和尊重获授权的应急小组工作的行动领域和指导性道德原则。专家组注意到这方面新出现的举措。

68. 各国还可以考虑制定其他措施，例如建立国家信通技术安全事件管控框架，并指定相关部门的角色和责任，包括计算机应急小组/计算机安全事件响应小组的角色和责任，以促进计算机应急小组/计算机安全事件响应小组与其他相关安全和技术机构在国家、区域和国际各级的合作与协调。此种框架可以包括各种政策、监管措施或程序，明确规定计算机应急小组/计算机安全事件响应小组的地位、权限和任务，并将计算机应急小组/计算机安全事件响应小组的独特职能与政府的其他职能区分开来。

四. 国际法

69. 国际法是各国共同致力于预防冲突和维护国际和平与安全的基础，也是增强国家间信任的关键。在审议国际法如何适用于各国使用信通技术的问题时，专家组重申前几届政府专家组在其报告中提出的关于国际法的评估和建议，特别是：国际法，尤其是整个《联合国宪章》，对维护和平与稳定以及促进开放、安全、稳定、无障碍、和平的信通技术环境是适用和不可或缺的。这些评估和建议与以往报告的其他实质性内容都强调，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的重要行动框架。

70. 在这方面，专家组还重申各国承诺遵守下列《宪章》宗旨和国际法原则：主权平等；通过和平手段以不危及国际和平与安全和正义的方式解决国际争端；在国际关系中不对任何国家的领土完整或政治独立使用武力或以武力相威胁，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。

71. 在往届专家组工作的基础上，以及在《宪章》和大会第 73/266 号决议规定的任务指导下，本届专家组对 2015 年政府专家组报告中关于国际法如何适用于各国使用信通技术的评估和建议提出了更深一层的理解，具体如下：

(a) 专家组指出，根据《联合国宪章》第二条第三款和第六章规定的义务，对于任何国际争端，包括涉及使用信通技术并且继续使用可能危及维护国际和平与安全的国际争端，当事方应首先寻求以《联合国宪章》第三十三条所述以下途径解决争端：谈判、调查、调停、和解、公断、司法解决、区域机关或区域办法之利用、或各国自行选择之其他和平方法。专家组还指出，《联合国宪章》中与和平解决争端有关的其他条款也很重要。

(b) 专家组重申，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。国际法规定的现有义务适用于国家的信通技术相关活动。根据这些义务，各国可以通过制定政策和法律，建立必要的机制，保护其境内的信通技术基础设施免受与信通技术有关的威胁，籍此对其境内的信通技术基础设施行使管辖权。

(c) 根据不干涉他国内政原则，任何国家都无权直接或间接干涉另一国的内部事务，包括通过信通技术进行干涉。

(d) 根据《联合国宪章》，各国在使用信通技术时，在国际关系中应避免以武力相威胁或使用武力，或以与联合国宗旨不符的任何其他方式侵害任何国家的领土完整或政治独立。

(e) 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《联合国宪章》全部内容的适用性，再次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，并指出需要继续研究该事项。

(f) 专家组指出，国际人道法仅适用于武装冲突局势。专家组回顾 2015 年报告中注意到既定的国际法律原则，包括在适用情况下的人道原则、必要性原则、

相称性原则和区分原则。专家组认识到，需要进一步研究这些原则如何以及何时适用于各国对信通技术的利用，并强调回顾这些原则绝不是要给冲突披上合法外衣或鼓励冲突。

(g) 专家组重申，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。专家组还重申，各国不得利用代理人利用信通技术实施国际不法行为，并应努力确保非国家行为体不利用其领土实施此类行为。同时，专家组回顾说，如果有迹象表明一项信通技术活动是从一国领土或信通技术基础设施发起或以其他方式产生的，这本身可能不足以将该活动归于该国；专家组指出，对国家提出的组织和实施不法行为的指控应得到证实。援引国家对国际不法行为的责任涉及复杂的技术、法律和政治考量。

72. 在不妨碍现有国际法和国际法今后进一步发展的情况下，专家组认识到，各国在联合国就国际法的具体规则和原则如何适用于各国使用信通技术的问题继续进行集体讨论和交换意见，对于加深共同理解、避免误解、提高可预测性和稳定性而言是不可或缺的。各国之间的区域和双边意见交流，可以为此类讨论提供参考和支持。

73. 根据专家组的任务规定，将在联合国裁军事务厅的网站上提供关于各国使用信通技术时的国际法的适用这一主题的国家自愿贡献的正式汇编(A/76/136)。专家组鼓励所有国家继续通过联合国秘书长并酌情通过其他渠道自愿分享其国家观点和评估意见。

五. 建立信任措施

74. 专家组指出，通过促进信任、合作、透明度和可预测性，建立信任措施可以促进稳定，有助于减少误解、升级和冲突的风险。建立信任是一项长期和渐进的承诺，需要各国持续参与。联合国、区域和次区域机构以及其他利益攸关方的支持有助于建立信任措施的有效运作和巩固。

75. 为支持各国努力建立信任和确保和平的信通技术环境，专家组鼓励各国公开重申其对第 2 段所述负责任国家行为框架的承诺，并依照该框架行事。专家组还鼓励各国考虑到联合国裁军审议委员会 1988 年通过并经大会第 43/78(H)号决议一致核可的建立信任措施准则，并考虑区域和次区域一级与建立信任措施及其运作相关的新做法。

合作措施

联络人

76. 在政策和技术层面确定适当的联络人有助于各国之间直接进行安全的沟通，帮助预防和处理严重的信通技术事件，缓解危机情况中的紧张局势。联络人之间的沟通有助于缓解紧张局势，防止因信通技术事件而可能产生的误解和错误认知，包括那些影响关键基础设施和造成国家、区域或全球影响的事件。沟通还可以增加信息共享，使各国能够更有效地管控和解决信通技术事件。

77. 在建立联络人或参与联络人网络时，各国不妨考虑：

(a) 在政策、外交和技术层面指定专门的联络人，并就联络人的具体属性提供指导，包括预期的角色和职责、协调职能和就绪要求。

(b) 制定政府间和政府内部程序，以确保危机期间联络人之间的有效沟通。标准化模板可以注明所需信息的类型，包括技术数据和请求的性质，但要有足够的灵活性，以便在无法获得某些信息的情况下也能进行沟通。

(c) 借鉴区域联络人网络的经验教训和良好做法，包括讨论、制定和实施在国家、区域和国际范围内利用联络人网络的实际方法，包括及早测知严重信通技术事件的方法，以期加强指定联络人网络之间的协调和信息共享。

78. 由于应对全球信通技术安全威胁还需要具有包容性和普遍性的全球办法，各国可以请联合国秘书长促成所有会员国之间就区域和次区域一级业已存在的与联络人网络相关的经验教训、良好做法和指导意见进行自愿交流。此类工作可能有助于促进在全球一级建立此类中央联络人名录的相关讨论。

对话和协商

79. 通过双边、次区域、区域和多边协商和接触进行对话可以增进国家之间的理解，鼓励增进信任，并有助于各国在缓解信通技术事件影响方面开展更密切的合作，同时降低误解和升级的风险。私营部门、学术界、民间社会和技术界等其他利益攸关方可以为促进此类协商和参与作出重大贡献。

80. 区域机构在制定和实施建立信任措施方面采取了重要步骤，这些步骤可以减少信通技术事件可能引发的错误认知、升级和冲突等风险。参与这些区域集团有助于重点突出本区域的特点和关切，而区域间的交流则有助于这些组织之间相互学习。专家组鼓励各国继续这项工作，并与目前尚不是相关区域或次区域组织成员的国家积极接触。

81. 为继续加强与国家计算机应急小组和其他授权机构有关的合作措施，各国可鼓励通过现有的区域和全球应急组织和网络，分享和传播关于建立和维持计算机应急小组/计算机安全事件响应小组以及关于事件管控的信息和良好做法。给予计算机应急小组/计算机安全事件响应小组的此类鼓励和支持，还将有助于提高各国对其根据规范 13(k)就计算机应急小组/计算机安全事件响应小组和其他相关机构作出的承诺的认识。

透明度措施

82. 通过交流各国对信通技术安全事件和其他相关威胁的看法和做法，并公开提供信通技术安全咨询、指导、证据基础和决策支持数据，这些提高透明度的自愿措施，对于建立信任、打造可预测性、减少误解和升级的可能性以及帮助各组织和机构做出良好的风险管理决策非常重要。

83. 为进一步提高国家行为的透明度和可预测性，提供获得更广泛的意见和经验的机会，加强国家准备状态，及早意识到日益严重的威胁，各国可考虑利用双边、

次区域、区域和多边论坛和非正式协商，自愿分享关于现有和新出现的与信通技术安全有关的威胁和事件、信通技术产品脆弱性分析的国家战略和标准、关于风险管理和预防冲突的国家和区域办法的信息和良好做法、经验教训或白皮书，包括分享根据信通技术事件的规模和严重性对事件进行分类的国家做法。

84. 各国还可以利用这些现有论坛阐明立场，并自愿就以下问题交流信息：有关信通技术安全的国家办法；数据保护；对信通技术支持的关键基础设施的保护；信通技术安全机构的任务和职能，以及国家或组织层面的信通技术战略及其运作所依据的法律和监督制度。

85. 政府专家组以往报告中关于建立信任措施的建议，为应对关键基础设施面临的日益增长的威胁和执行相关规范提供了合作基础。专家组鼓励各国继续提高对关键基础设施保护重要性的认识，促进关键基础设施利益攸关方之间的信息共享，分享良好做法和指导意见。在适当情况下，各国可以利用现有平台和报告方式(见下文第 86 段)自愿分享如何对关键国家基础设施和在区域或国际上提供基本服务的关键基础设施进行分类、相关国家政策和立法、风险评估框架以及如何对影响关键基础设施的信通技术事件进行识别、分类和管理的本国观点。

86. 各国还可以利用联合国资源，如向秘书长自愿报告、联合国裁军研究所(裁研所)的网络政策门户网站，以及其他相关国际和区域组织的资源，以整合各国自愿提供的关于解决涉及国际安全和稳定的信通技术安全问题的国家战略、政策、立法和方案的信息和良好做法。

六. 信通技术安全和能力建设方面的国际合作和援助

87. 专家组强调在信通技术安全和能力建设领域开展合作和提供援助的重要性，并强调这对于专家组任务全部内容而言十分重要。加大合作力度，同时在涉及私营部门、学术界、民间社会和技术界等其他利益攸关方的信通技术安全领域提高援助和能力建设的有效性，有助于各国运用负责任使用信通技术的国家行为框架。这些建议对于弥合国家内部和国家之间在与信通技术安全有关的政策、法律和技术问题上的现有分歧至关重要。这些建议可能还有助于实现国际社会的其他目标，如可持续发展目标。

88. 信通技术安全和能力建设方面的国际合作和援助可以提高各国发现、调查和应对威胁的能力，并确保所有国家都有能力负责任地使用信通技术。这些合作和援助还有助于确保所有国家实现关键基础设施的必要保护水平和必要安全水平，具备足够的事件管控能力，并能够在发生源自其领土或影响其领土的恶意信通技术活动时请求援助或回应援助请求。

89. 专家组建议进一步加强信通技术安全和能力建设方面的国际合作和援助，为各国在以下领域的努力提供支持：

(a) 制定和实施国家信通技术政策、战略和方案。

(b) 建立和加强计算机应急小组/计算机安全事件响应小组的能力，并加强计算机应急小组/计算机安全事件响应小组之间的合作安排。

(c) 提高关键基础设施的安全性和复原力，并改进对关键基础设施的保护。

(d) 建设或加强各国发现、调查和解决信通技术事件的技术、法律和政策能力，包括通过投资开发人力资源、机构以及具有复原力的技术和教育方案。

(e) 加深对国际法如何适用于各国使用信通技术的共识，并促进各国在这方面的交流，包括通过在联合国举行的讨论。

(f) 加强所有国家的技术和法律能力，以调查和解决严重的信通技术事件。

(g) 落实商定的自愿、非约束性负责任国家行为规范。

(h) 为此目的，并作为评估本国优先事项、需求和资源的一种手段，鼓励各国使用联合国不限成员名额工作组建议的国家执行情况自愿调查。[4]

90. 为了弥合数字鸿沟，并确保所有国家从此类及其他援助和能力建设领域受益，专家组鼓励各国尽可能承诺提供财政资源及技术和政策专门知识，以支持请求援助的国家努力加强信通技术安全。

91. 在推进信通技术安全和能力建设方面的国际合作和援助方面，专家组强调能力建设的自愿、政治中立、互利和互惠性质。在这方面，本集团欢迎不限成员名额工作组建议的关于进程、目的、伙伴关系和人员的能力建设原则，并鼓励所有国家在努力推进合作和援助时遵循这些原则。[5]

92. 促进共识和相互学习也可以加强信通技术安全和能力建设领域的国际合作和援助。各国应考虑以多学科、多利益攸关方、模块化和可衡量的方式开展信通技术安全和能力建设方面的合作。通过与联合国和其他全球、区域和次区域机构以及其他相关利益攸关方合作推动有效协调和实施能力建设方案，通过鼓励提高透明度，分享有关能力建设方案有效性的信息，这一点是可以做到的。

七. 结论和对今后工作的建议

93. 随着各国对信通技术的依赖性与日俱增，在国际安全背景下利用信通技术时遵守负责任国家行为的共同框架，对于所有国家从这些技术中获益、保护这些技术免遭滥用和应对滥用行为至关重要。

94. 专家组将重点放在促进共识和有效执行上，并在以往报告建议的基础上，确定和进一步明确了各国可以采用的方法并就其提供指导，以确保合作措施能够有效应对信通技术安全领域现有和潜在的威胁。这些方法在报告以下章节中有明确的概述：负责任国家行为的规则、规范和原则；国际法；建立信任；国际合作和

[4] 不限成员名额工作组最后实务报告，第 65 段。

[5] 不限成员名额工作组最后实务报告，第 56 段。

能力建设，其中每一章节都体现了政府专家组以往报告中提出的负责任国家行为的基本要素。

95. 专家组还确定了未来工作的可能领域，包括但不限于：

(a) 加强双边、区域和多边层面的合作，以促进就恶意使用信通技术构成的现有威胁和新威胁、对国际和平与安全构成的潜在风险以及信通技术支持的基础设施的安全问题达成共识。

(b) 进一步分享和交流关于以下内容的意见：负责任国家行为的规范、规则和原则；执行规范和建立信任措施的国家和区域做法；国际法如何适用于国家对信通技术的使用，包括确定具体的国际法专题以供进一步深入讨论。

(c) 在考虑到上文第 90 段的情况下，围绕本报告中的评估和建议进一步加强国际合作和能力建设，以确保所有国家都能为维护国际和平与安全作出贡献。

(d) 酌情确定能够促进其他重要利益攸关方，包括私营部门、学术界、民间社会和技术界参与实施负责任行为框架的机制。

(e) 要求为所有会员国服务的裁研所并鼓励其他适当的智囊团和研究机构就本报告讨论的议题开展相关研究。

96. 专家组鼓励继续推进在联合国主持下从国际安全角度看信通技术问题的包容各方和透明的谈判进程，其中包括根据大会第 75/240 号决议设立的 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组并对工作组加以肯定。专家组建议今后的工作以政府专家组和不限成员名额工作组的累积工作为基础。

97. 专家组鼓励各国继续努力，在联合国及其他区域和多边论坛内推进负责任国家行为框架，以包容各方、协商一致、务实和透明的方式支持定期对话、协商和能力建设。在这方面，根据不限成员名额工作组的成果，专家组注意到关于推进信通技术中负责任国家行为的各种建议，这些建议除其他外将支持各国履行其在信通技术使用方面的承诺(尤其是《行动纲领》)的能力。在审议这些建议时，应通过各国在联合国的平等参与来考虑所有国家的关切和利益。在这方面，应进一步制定《行动纲领》，包括在根据大会第 75/240 号决议设立的不限成员名额工作组进程中。

98. 专家组建议会员国以本报告和往届政府专家组的评估和建议以及不限成员名额工作组最后报告(A/75/816)中的结论和建议为指导，并考虑如何进一步发展和实施这些结论和建议。

附件

从国际安全角度促进网络空间负责任国家行为政府专家组成员名单

澳大利亚
Johanna Weaver
澳大利亚外交贸易部网络事务大使特别顾问

巴西
Guilherme de Aguiar Patriota
大使，巴西驻孟买总领事

中国
王磊
外交部网络事务协调员

爱沙尼亚
Heli Tiirmaa-Klaar
网络外交无任所大使，外交部网络外交司司长

法国
Henri Verdier
欧洲与外交部数字事务大使

德国
Regine Grienberger(第三和第四次会议)
联邦外交部网络外交政策大使

Wolfram von Heynitz(第一和第二次会议)
联邦外交部国际网络政策协调参谋

印度
S. Janakiraman
外交部电子政务、信息技术和网络外交司司长兼联合秘书

印度尼西亚
Rolliansyah Soemirat(第三和第四次会议)
外交部国际安全和裁军司司长

Harditya Suryawto(第二次会议)
外交部国际安全和裁军司负责网络技术和网络问题参赞

Grata Endah Werdaningtyas(第一次会议)
外交部国际安全与裁军司国际安全与裁军问题主任

日本
赤堀毅
外务省联合国事务和网络政策大使

约旦
Feras Mohammad Abdallah Alzoubi
约旦武装部队国家网络安全计划部主任

哈萨克斯坦
Asset Nussupov
哈萨克斯坦共和国总统办公厅部门负责人

肯尼亚
Katherine Getao
信通技术管理局首席执行官

毛里求斯
Kaleem Ahmed Usmani
毛里求斯计算机应急小组负责人

墨西哥
Gerardo Isaac Morales Tenorio
外交部多层面安全协调员

摩洛哥
Abdellah Boutrig
上校，国防部信息系统安全总局援助、培训、控制和专门知识主任

荷兰
Carmen Gonsalves
外交部国际网络政策负责人

挪威
Simen Ekblom (第三和第四次会议)
外交部网络政策协调员

Anniken Krutnes(第一和第二次会议)
外交部安全政策和高北纬地区司副司长

罗马尼亚
Mihaela-Ionelia Popescu
外交部网络政策协调员

俄罗斯联邦

Andrey Krutskikh
俄罗斯联邦总统信息安全领域国际合作特别代表，外交部国际信息安全司司长

Vladimir Shin(第三和第四次会议)
外交部国际信息安全司副司长

新加坡

David Koh
新加坡网络安全局首席执行官兼网络安全专员

南非

Doc Mashabane
司法和宪法发展部总干事

Moliehi Makumane(第三和第四次会议)
南非政府专家组代表特别顾问

瑞士

Nadine Olivieri Lozano
大使，联邦外交部国际安全司司长

联合王国

Kathryn Jones
外交、联邦和发展事务部国家安全局国际网络治理负责人

Alexander Evans(第一次会议)
外交、联邦和发展事务部前网络事务主任

美国

Michele Markoff
美国国务院网络问题代理协调员

乌拉圭

Noelia Martínez Franchi(第三和第四次会议)
外交部多边事务主任

Alejandra Erramuspe(第一和第二次会议)
总统办公厅电子政务和信息社会机构高级干事