联合国 A/79/81

大 会

Distr.: General
21 May 2024
Chinese
Original: Chinese/English/French/
Russian/Spanish

第七十九届会议

暂定项目表 * 项目 93

从国际安全角度看信息和电信领域的发展

从国际安全角度看信息和电信领域的发展

秘书长的报告

摘要

本报告综述了会员国根据大会第 78/237 号决议提交的答件内容，但不影响会员国各自的立场。报告汇总了各国对信息和通信技术的安全及使用，特别是今后在联合国主持下就这些事项进行定期机构对话的看法。本报告附件全文载列了在通报的截止日期前从会员国收到的观点。报告最后提出了秘书长的意见。

* A/79/50。

目录

一. 导言

1. 根据第 78/237 号决议第 8 段的规定，大会邀请会员国继续向秘书长通报它们对信息和通信技术安全和使用安全的看法和评估意见，特别是对今后在联合国主持下就这些事项进行定期机构对话的看法和评估意见，并请秘书长根据这些意见向大会第七十八届会议提交一份报告，供会员国在 2024 年举行的 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组第八届会议期间进一步讨论。本报告根据这一要求提交。

2. 2024 年 1 月 5 日，裁军事务厅向全体会员国分发普通照会，提请注意第 78/237 号决议第 8 段，并征求它们对此事的意见。截至 2024 年 5 月 1 日收到的意见抄录于本报告附件。在上述日期之后收到的意见已登载在裁军事务厅“Meetings Place”门户网站。[1]

3. 本报告第二节提供了背景资料，说明各国关于就信息和通信技术安全和使用安全进行定期机构对话的讨论情况。第三节综合概述了会员国提交的答复要点，但不影响其各自立场。第四节载有秘书长的意见和结论。

二. 背景

4. 在 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组的主持下，各国继续按照 A/AC.292/2021/1 号文件所载的工作组商定议程，讨论在联合国主持下建立各国广泛参与的关于相关事项的定期机构对话的问题。在 2021 年 12 月至 2024 年 3 月的工作组七次实质性会议期间，各国开展了重点讨论，以进一步讨论关于定期机构对话的建议，包括关于《行动纲领》的建议。

5. 根据 2023 年 7 月以协商一致方式通过的工作组第二次年度进展报告(A/78/265)，各国原则上同意，未来定期机构对话机制将以下列共同要素为基础，并同意继续讨论其他要素：

(a) 这将是一个由国家牵头、由联合国主持的单一轨道的常设机制，向大会第一委员会报告；

(b) 未来机制的目标将是继续促进开放、安全、稳定、无障碍、和平和可互操作的信息和通信技术环境；

(c) 未来机制将以不限成员名额工作组和政府专家组以往报告中就使用信息和通信技术的负责任国家行为框架达成的共识协议作为其工作基础；

(d) 这将是一个开放、包容、透明、可持续和灵活的进程，能够根据各国的需要以及信息和通信技术环境的发展而演进。

[1] https://meetings.unoda.org/ga-c1/general-assembly-first-committee-seventy-ninth-session-2024。

6. 各国还强调协商一致原则对于建立未来机制本身以及该机制的决策进程的重要性。此外，已经鼓励有能力做到的国家考虑设立或支持赞助方案和其他机制，以确保广泛参与相关的联合国进程。

7. 在不限成员名额工作组关于今后就信息和通信技术安全相关事项进行定期机构对话的整个讨论过程中，各国思考了可能的范围和目标、结构、模式，包括决策和执行后续行动。为便于讨论，不限成员名额工作组主席于 2024 年 2 月提供了一份关于信息和通信技术安全常设机制要素草案的讨论文件，后于 2024 年 5 月提供了修订版。还通过第二次年度进展报告要求就定期机构对话专题举行两次专门的闭会期间会议。在上述会议上，各国还将就推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领与不限成员名额工作组之间的关系进行重点讨论。[2]

三. 关于就信息和通信技术安全和使用安全进行定期机构对话的意见

一般性谅解和原则

8. 若干国家在提交的材料中强调了在信息和通信技术使用中的恶意活动的威胁，并指出国际社会日益关切国际安全与稳定面临的潜在威胁。表示关切的是一些国家过度发展信息和通信技术能力，其目的不符合国际法和维护国际稳定与安全的目标。据称，某些行为体涉及信息和通信技术的活动违反国际法。还有国家表示关切恶意活动对个人安全和福祉的影响。

9. 一些国家指出，信息和通信技术可以成为人类进步和发展的催化剂，但也指出，此类技术可能用于违背维护国际安全目标的目的，并对经济和社会发展产生不利影响。

10. 许多国家强调，鉴于目前的安全环境，今后就信息和通信技术安全和使用安全进行的定期机构对话必须侧重于进一步促进开放、安全、稳定、无障碍与和平的信息和通信技术环境。一些国家还着重指出，各国之间必须开展国际合作，以维持上述领域的国际稳定。

11. 许多国家指出，越来越多的国家要求在联合国主持下就相关事项设立一个常设决策机制。此外，许多国家还着重指出，必须借鉴在联合国主持下的以往进程中达成的协定，其中包括政府专家组以及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。[3] 一些国家强调指出，需要借鉴上述“集体成果”，指出这一成果包括各国负责任地使用信息和通信技术的现有规范、国际法对各国使用上述技术的适用性、建立信任措施和能力建设。还有意见认为，

[2] 见 A/78/76。

[3] 见 A/65/201、A/68/98、A/70/174、A/75/816 和 A/76/135。

未来机制应创造空间，以便更深入地讨论此前达成的协定的实际执行工作。在这方面，还有意见认为，政府间联络人名录应成为未来机制的一个组成部分。

12. 若干国家强调，在以往进程中达成的协商一致成果必须保持连续性。同样，若干国家指出，应在目前 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组任务结束后建立新的体制机制或平台。一些国家着重指出，这项工作应不迟于 2026 年完成，以确保连续性。

13. 若干国家强调，必须避免这一领域的国际工作重复，并告诫不要采取平行进程，同时提到各代表团面临的相关能力挑战。许多国家强调，在联合国主持下进行单一轨道、常设和包容性的定期机构对话十分重要。一些国家指出，建立一个单一、包容性的常设机制也有助于提高可预测性和体制稳定性，同时避免需要定期谈判新任务。还有意见指出，资源有限的小国和发展中国家将无法可持续地参与双轨并行进程。此外，另有意见认为，未来机制应成为处理信息和通信技术安全的一站式综合服务点。

14. 一些国家申明，国际法、特别是《联合国宪章》对于维护信息和通信技术环境的和平、安全与稳定是适用和必不可少的。在这方面，有意见认为，可在未来机制中就如何适用国际法进行更深入的讨论。有建议提出设立一个未来机制，探讨关于上述专题的专门工作流程。有意见认为，未来机制可成为讨论国际法的包容性框架，包括交流各国意见、召开专家简报会和探讨上述领域的能力建设活动。

15. 各国讨论了各种基本原则，这些原则应成为就信息和通信技术安全和使用安全进行定期机构对话的未来机制的基础，包括公开性、包容性和透明度，而且认为这一机制应注重行动、单轨和具备民主性。有意见认为，未来机制应由国家主导，并以遵守《宪章》各项原则为基础，这些原则包括各国主权平等、不使用或威胁使用武力以及和平解决争端。还有建议提出，该机制应根据各国不断变化的需求以及确保安全使用信息和通信技术领域出现的新任务，体现适当的灵活性和渐进式发展。

16. 若干国家提及关于推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领的建议。据称，这一建议已载入联合国有关机构的以往报告，包括不限成员名额工作组的协商一致年度报告。还有意见指出，该建议得到了一个跨区域国家组的支持，可成为在本届不限成员名额工作组结束后建立的关于从国际安全角度看信息和通信技术的讨论的常设机构。

17. 若干国家指出，应在任期至 2025 年的当前工作组结束后立即设立一个不限成员名额常设工作组。上述国家指出，目前不限成员名额工作组已证明其效率和相关性，是此类机制以及不限成员名额常设决策工作组的最适当形式，其任务应是注重进一步促进开放、安全、稳定、无障碍及和平的信息和通信技术环境，包括为此制定具有法律约束力的国家负责任行为的规则、规范和原则，以及创建一个有效的执行机制，作为确保国际信息安全的未来普遍性条约的要素。

范围和目标

18. 许多国家强调，今后就信息和通信技术安全和使用安全进行定期机构对话的首要目标是促进这一领域的国际和平与安全。若干国家指出，未来机制应促进一个开放、安全、稳定、无障碍及和平的信息和通信技术环境。一些国家还指出，未来机制应促进各国之间的对话与合作，并有助于防止冲突和误解。

19. 若干国家着重指出，联合国以往进程的协商一致建议形成了使用信息和通信技术的国家负责任行为的综合框架，应继续成为未来体制机制的重点核心。若干国家强调必须支持落实先前商定的成果，另一些国家则指出，未来机制应考虑切实执行不限成员名额工作组达成的协议。有建议提出，未来机制可以制定具体的指导方针，支持各国执行商定的规范性框架，并加强对框架本身的理解。

20. 各国在提交的材料中思考了进一步发展现有框架的必要性。一些国家指出了找出任何差距、制定更多规范或制定新规则和具有法律约束力的义务的备选办法。若干国家支持拟订一项具有法律约束力的文书，其他国家则着重指出，必要时可进一步发展和更新框架，以应对随时间推移而演变的新威胁。若干国家指出，该机制应在两个同样重要的工作方面取得平衡——既有框架的实施及其进一步发展。

21. 有意见认为，未来机制应向前和向后看，注重遵守和执行使用信息和通信技术的负责任国家行为的现有商定框架，特别是加强能力建设，根据最新动态制定新规范，如数据安全规范，以及制定新的能力建设行动计划和具有法律约束力的文书。

22. 许多国家强调，能力建设专题应成为未来机制的核心。一些国家着重指出，必须使现有的努力，包括国际电信联盟和世界银行的相关举措产生协同作用。提及了 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组第二次年度进展报告所附的商定能力建设原则。[4] 若干国家指出，未来机制应促进能力建设工作，包括交流最佳做法信息。若干国家强调了必须采取基于需求和有针对性的努力。有意见认为，机制的能力建设职能必须与各国在国家一级执行负责任国家行为规范框架的努力直接挂钩。

23. 还有意见提出，是否可以借鉴联合国其他论坛现有机制的经验，建立一个专门供资机制，以支持相关的能力建设工作。有建议提出，建立一个自愿的跨区域“伙伴关系制度”，通过这一制度来匹配能力不同的国家，以加强合作和交流良好做法。有建议提出，建立一个多部分的能力建设机制，其中将包括就威胁格局进行交流、自我确定能力需求并匹配需求与资源，以及建立一个交流相关经验的“反馈环路”。

24. 若干国家指出，未来机制可成为信息和通信技术安全领域相关举措和努力的总体体制框架，包括政府间联络人名录。

[4] A/78/265，附件 C。

25. 各国还就其他可能的重点领域提出了建议，包括就国际法如何适用于信息和通信技术的使用以及如何调整现有规范以适应该领域的具体特点达成共识。有意见认为，未来机制可推动关于现有和新出现的威胁以及各国使用信息和通信技术时如何适用包括国际人道法和人权法在内的国际法的讨论。制定和执行国家间建立信任措施和实际合作机制也被确定为待处理项目。

设立、模式和决策

26. 各国对建立未来机制的方式以及建立前的筹备工作进行了各种思考。有意见认为，会员国在目前不限成员名额工作组框架内提交的材料，包括关于行动纲领建议、秘书长根据大会第 77/37 号决议编写的关于这一纲领的报告[5] 以及本报告和不限成员名额工作组报告所载相关建议的材料应成为确定未来机制的范围、结构和模式的基础。

27. 许多国家强调，必须就未来机制的范围、结构和方式达成共识。许多国家表示支持在目前不限成员名额工作组内进一步拟订和发展这一机制。若干国家支持在目前不限成员名额工作组内进一步开展重点突出的专门讨论，以制定该机制，并就其形式和结构寻求共识。关于行动纲领，若干国家支持在 2024 年和 2025 年就上述建议举行专门的闭会期间会议，以进一步制定该机制的各个方面。还建议进一步讨论所涉预算问题。

28. 有意见指出，今后可通过大会协商一致的决议建立定期机构对话。在这方面，有意见认为，应通过一项大会决议设立一个不限成员名额常设工作组。还有意见认为，目前不限成员名额工作组可通过一项随后由大会核可的政治宣言建立未来机制。有建议提出，申明各国承诺遵循负责任国家行为框架可构成这一政治宣言的一个关键要素。

29. 关于行动纲领的具体建议，若干国家表示支持通过一项政治宣言来制定行动纲领。有建议提出，该宣言可得到第一委员会一项决议的补充，说明行动纲领的任务、结构和方式。还有建议提出，应不迟于 2026 年召开一次国际会议，以制定和通过这样一项宣言。有意见认为，如果目前不限成员名额工作组未能就最后报告达成共识，包括就一个机制达成一致意见，则须召开一次更全面的国际会议或通过大会确立其他筹备进程，以确保这些重要的多边讨论的连续性。

后续机制和落实

30. 各国就后续机制提出了各种建议，包括定期会议，如全体会议和审查大会，以及闭会期间会议，包括技术工作组。还建议该机制每年举行正式会议。关于全体会议频率的建议从每两年到每三年举行一次不等。有意见认为，未来机制应召开双年度会议，以落实商定的工作方案。还有意见认为，可能应该定期审查常设机制的运作情况，以确保其做法与不断变化的业务威胁状况相关。

[5] A/78/76。

31. 一些国家支持设立技术工作组，重点处理具体的优先问题，如国际法的适用性、制定新的规范、规则和原则，以及酌情拟订具有法律约束力的义务。有意见认为，技术工作组将构成注重行动的机制的实质部门。有建议提出，应由附属分组审议机制任务的具体方面。有意见认为，应以混合形式举行闭会期间关于具体问题的技术工作组会议，以便各国广泛参与。据称，分组会议不应平行举行，以确保各代表团充分参与。为便利各国广泛参与，有建议提出设立一个研究金方案。

32. 各国建议可能举行的审查会议周期不同，包括每三年、四年或六年举行一次。一些国家指出，此类审查会议应审查负责任国家行为框架，以便在必要时予以更新，并为机制的工作提供战略指导。有意见认为，审查会议应审议是否应在协商一致的基础上制定其他规范、规则、原则或有约束力的义务。

33. 许多国家述及协商一致决策在未来机制中的重要性。一些国家强调，必须以协商一致的方式作出关于实质性问题的决定。若干国家认为，应在建立未来机制的文件中明确规定各国完全遵循协商一致的决策原则。各国建议在未来机制中以各种形式整合各国的决策，例如每两年向大会提交一次进展报告，以及附有相关协商一致决策的年度程序性报告。

34. 一些国家指出，有可能在未来机制的框架内提交国家自愿报告。有建议提出，应报告各国执行规范性框架的情况以及国家做法。有建议提出利用现有工具，如关于各国从国际安全和联合国角度负责任地使用信息和通信技术的联合国建议的国家执行情况调查。[6]

35. 若干国家指出，虽然决策仍将是各国的专属特权，但可能应与区域和次区域组织互动，包括利用协同作用以及借鉴现有的能力建设结构和平台。有建议提出，根据与各国家组和未来机制相关主席的磋商情况，每年与此类组织的代表举行闭会期间会议。还有建议提出，在国际、区域间和区域各级交流最佳做法。

36. 各国对未来机制中与非政府实体的接触进行了不同的思考，并以联合国其他论坛的参与方式为例，如拟订一项关于打击为犯罪目的使用信息和通信技术行为的全面国际公约特设委员会以及老龄问题不限成员名额工作组。许多国家指出，多利益攸关方参与对于机制今后的运作十分重要。据称，未来定期机构对话中的包容性利益攸关方参与将有助于实现维护信息和通信技术领域和平与安全的共同目标，并可带来关于威胁评估和规范执行等事项的宝贵专门知识。一些国家支持非政府实体按照目前不限成员名额工作组商定的方式参与。若干国家支持正式参与和与利益攸关方定期磋商，另一些国家则表示，与非国家行为体的接触应严格以协商和非正式方式进行，例如通过年度闭会期间会议。

37. 一些国家认为裁军事务厅是担任未来机制秘书处的适当实体。

[6] https://nationalcybersurvey.cyberpolicyportal.org。

四. 秘书长的意见和结论

38. 维护信息和通信技术领域的和平与安全仍然是一项紧迫任务。虽然对一系列行为体恶意使用这些技术的担忧有所增加，但国际社会面临日益扩大的数字鸿沟和快速临近的实现可持续发展目标的最后期限。必须采取具体措施，防止冲突向这一领域延伸和进一步升级，包括保护人的生命免受恶意活动的伤害。

39. 虽然国际社会在维护信息和通信技术领域的和平与稳定方面面临巨大挑战，但同样有一个可以利用的坚实基础。二十多年来，各国通过大会主持下的进程在以下方面取得了重大进展：找出现有和新出现的威胁，探讨国际法对各国使用信息和通信技术的适用性，制定使用这些技术方面的负责任国家行为框架，考虑建立信任措施和能力建设举措。这一进展是在协商一致基础上逐步取得的，而且是一贯的。因此，取得进一步进展具备坚实基础。

40. 各国在目前 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组框架内所作的努力证明，可以采取进一步具体行动，实现和平与安全的信息和通信技术环境的共同目标。本论坛的持续进展表明，只要具备足够的政治意愿，不仅可以达成共同协议，还能够采取实际行动。在这方面，我欢迎各国达成协商一致，建立一个全球政府间联络人名录，以加强他们之间的互动与合作。这是促进国际和平与安全并提高透明度和可预测性的一个切实步骤。

41. 在此背景下，各国认识到就这些事项保持定期机构对话至关重要，以便为持续取得进展提供足够的空间。随着这些技术变得越来越普遍，日益进入我们的日常生活，这些问题的相关性预计会提高。

42. 各国普遍认为，此类定期机构对话最适合在联合国主持下进行，因为联合国为此类讨论提供了一个包容各方的平台。还有共识认为，此类对话支持实现在信息和通信技术环境中加强国际和平、稳定和预防冲突的目标。各国还申明了支持此类对话的若干重要原则，如包容性、透明度和注重行动的办法。此外，一致认为需要一个促进各国最广泛参与的单一轨道机制。

43. 根据这些广泛共识和普遍持有的意见，今后就从国际安全角度看信息和通信技术举行定期机构对话似乎是一项可以实现的任务。在已经取得的成功的基础上，各国在目前不限成员名额工作组中有一个巨大的机会，可就联合国主持下以开放、包容和透明方式运作的单一轨道常设机制找到共同点。不限成员名额工作组 2023 年年度进展报告中以协商一致方式商定的未来定期机构对话的共同要素是一个合乎逻辑和有益的出发点。此类事项非常重要，必须抓住这个机会进一步建立信任和信心。在联合国主持下设立一个常设机制是对这些事项进行多边审议的下一个合乎逻辑的阶段，它将借鉴过去的成功，并为今后的进展奠定基础。

附件

从各国政府收到的答复

澳大利亚

[原件：英文]
[2024 年 5 月 1 日]

澳大利亚荣幸应大会第 78/237 号决议的邀请，就国际安全和进一步定期机构对话背景下促进网络空间负责任的国家行为发表意见。

本答件以澳大利亚根据关于从国际安全角度看信息和电信领域的发展的 2023 年第 77/37 号、2022 年第 76/19 号、2021 年第 75/32 号、2020 年第 74/28 号、2016 年第 70/237 号决议、2014 年第 68/243 号和 2011 年第 65/41 号决议提供的答件为依据。

2023-2030 年澳大利亚网络安全战略

2023 年 11 月 22 日，网络安全部长克莱尔·奥尼尔发布了 2023-2030 年澳大利亚网络安全战略，其中阐述了澳大利亚通过全国范围的网络复原力办法实现国内和国际网络安全的愿景。

该战略确定了旨在建立更强大网络防御并在网络事件发生后迅速恢复的六项措施：(a) 强大的企业和公民；(b) 安全技术；(c) 世界级的威胁共享和阻断；(d) 保护重要基础设施；(e) 主权能力；(f) 有韧性的区域和全球领导力。

该战略规定，澳大利亚将继续致力于制定、维护和捍卫国际网络规则、规范和标准，包括维护国际法律和网络空间负责任国家行为规范，并部署一切治国手段，以威慑和应对恶意行为者。

维护国际法律和网络空间负责任国家行为规范

澳大利亚将与现有伙伴协作并建立新的伙伴关系，以维护国际法律和商定的负责任国家行为框架，这是实现网络空间稳定、繁荣、独立和主权的基础。

所有国家都同意在现有国际法律和规范的基础上建立一个基于规则的网络空间。国际法律加上商定的负责任国家行为自愿规范、建立信任措施和能力建设，为网络空间的可预测性和稳定性提供了强有力的框架。在实施和遵守时，该框架提供一整套工具来应对源自国家和国家支持的恶意网络活动所构成的威胁。

澳大利亚将在联合国的讨论中与国际伙伴一道，澄清国际法律如何适用于网络空间，并加强执行网络空间负责任国家行为框架。这些努力将包括通过区域论坛增进合作，包括作为太平洋岛屿论坛的一部分，以及通过与东南亚国家联盟区域论坛的互动接触。

部署一切治国手段，以威慑和应对恶意行为者

澳大利亚将部署一切治国手段，以威慑和应对恶意网络行为者。澳大利亚将与国际伙伴合作采取行动，让那些危及网络空间安全保障的个人和组织付出代价。这包括指出国家破坏或违反国际法律和规范的行为，并对实施或协助实施重大网络事件的人进行制裁，当我们有足够的证据并且这样做符合我们的国家利益时。

澳大利亚将在所有行动中维护现行国际法律和商定的网络空间负责任国家行为自愿规范。

支持一个更具网络韧性的区域

澳大利亚将继续与太平洋和东南亚邻国合作，建设一个更具网络韧性的区域。此类合作与援助将继续由澳大利亚网络事务和关键技术大使协调。

澳大利亚正在调整本国网络合作和能力建设工作的重点，使其更有针对性、更具影响力和更加可持续，也使邻国能够更好地预防网络事件并在事件发生时迅速恢复。我们认识到人们以不同方式接触网络安全问题，我们将继续努力考虑性别平等、残疾状况和社会包容。这包括继续支持联合国妇女与和平和安全议程以及 2021-2031 年澳大利亚妇女、和平与安全国家行动计划。

当区域发生严重网络事件时，澳大利亚将能够更好地响应援助请求。澳大利亚正利用政府、工业和技术界的专门知识，在外交和贸易部建立一个区域网络危机应对小组。针对政府在区域发生重大网络事件后提出的要求，该小组将帮助遏制网络事件的蔓延和影响，并恢复关键的服务和基础设施。

定期机构对话

推进从国际安全角度使用信息和通信技术的负责任国家行为行动纲领

澳大利亚支持在第一委员会主持下建立单一、永久、灵活、包容、透明和注重行动的机制，以讨论、执行和推进大会商定并以协商一致方式重申的网络空间负责任国家行为框架。该框架由国际法律、规范和建立信任措施组成，并由经过协调的能力建设提供支持。行动纲领应提供一个论坛，使所有 193 个会员国能够定期和持续地进行有意义的讨论并采取行动。行动纲领应当能够成长、调整和发展，应有助于执行现有的商定框架，并在出现新的威胁和挑战时，允许以协商一致方式在可能情况下进一步发展该框架。

大会在第 77/37 号决议中欢迎关于制定行动纲领的提议，并请秘书长就行动纲领的范围、结构和内容征求会员国意见。该报告(A/78/76)建议各国继续在 2021-2025 年信息和通信技术安全及使用问题不限成员名额工作组的主持下讨论行动纲领提案的可能范围、结构、原则、内容、职能和后续机制，利用在报告中表达的观点，同时也考虑到裁军事务厅根据大会第 77/37 号决议组织的区域和次区域协商。

不限成员名额工作组在行动纲领的拟订和筹备工作中发挥了关键作用。行动纲领应建立在过去连续六届政府专家组以及首届和本届不限成员名额工作组经过艰苦努力取得的共识和日积月累讨论的基础之上。永久性机制代表着联合国网络架构继往开来的下一个阶段或演变，并保证这些问题在今后得到应有的关注和重视。

大会在第 78/16 号决议中决定在 2021-2025 年不限成员名额工作组完成工作后，至迟于 2026 年建立一个由联合国主持的常设、包容和注重行动的机制，拥有在大会第 77/37 号决议中申明的具体目标，并具备在 2021-2025 年不限成员名额工作组 2023 年度进展报告中以协商一致方式商定的未来定期机构对话的共同要素。

澳大利亚支持关于在 2021-2025 年不限成员名额工作组所做筹备工作的基础上于 2025 年召开一次国际会议以通过行动纲领创始文件的提议。

澳大利亚支持在行动纲领创始文件中阐明各国的承诺，并提供一个可由大会决议核可的机制。创始文件可作为一项政治宣言加以阐述，其中应：

- 核可并重申各国对政府专家组报告[1] 和不限成员名额工作组报告[2] 中商定框架(包括在网络空间适用现有国际法)的政治承诺；
- 在政府专家组和不限成员名额工作组报告所载威胁评估的基础上，回顾与恶意使用信息和通信技术(信通技术)有关的现有和新出现的国际安全威胁；
- 建立一个常设体制机制，推动执行该框架(包括支持各国这样做的能力)和相关模式；
- 如果大会以协商一致方式核可不限成员名额工作组、政府专家小组或其他联合国进程的报告，或在行动纲领审查会议上以协商一致方式达成协议，则允许酌情进一步发展和更新该框架，以纳入协商一致原则、建议和承诺；
- 根据国际社会同意讨论和处理的问题，确定行动纲领的重点工作领域；
- 明确促进和鼓励在相关领域与多利益攸关方群体的相关成员接触。

关于议事规则，澳大利亚重申，行动纲领应要求以协商一致方式就所有问题(包括报告、建议和宣言)达成协议。

为确保行动纲领各项活动以证据为基础并由数据驱动，行动纲领应强调支持执行工作，包括通过具体、有针对性和经过协调的能力建设，还应明确阐述专门能力建设措施。为促进基于需求和证据的有针对性的能力建设，行动纲领

[1] 见 A/65/201、A/68/98、A/70/174 和 A/76/135。

[2] A/75/816。

可鼓励会员国利用标准化报告机制，即联合国关于各国在国际安全背景下负责任使用信通技术的建议执行情况国别调查(可查阅 https://nationalcybersurvey.cyberpolicyportal.org/)，定期调查和自我报告该框架的执行情况(例如，每三年一次或按照审查会议周期)。

澳大利亚认识到包括民间社会、私营部门、学术界和技术界在内的多利益攸关方群体在促进建立自由、开放、安全、稳定、无障碍及和平的网络空间方面至关重要，建议行动纲领允许与相关利益攸关方进行定期和制度化磋商。

综上所述，澳大利亚强调行动纲领应有明确的任务规定，以商定框架为基础并重申该框架；在实质性和程序性两个方面保持灵活，可通过协商一致方式进一步发展该框架；通过自愿报告支持实施工作并通过能力建设实施该框架；具有包容性，因为关于国际安全事项的决定仍然是各国的特权，而讨论和工作组应向多利益攸关方群体开放。

澳大利亚期待继续与秘书长、裁军事务厅和会员国合作，制定一项有效、灵活和包容的行动纲领。

阿塞拜疆

[原件：英文]
[2024 年 5 月 1 日]

近些年来，网络空间发生了重大变化，为改善我们的日常生活提供了从安全保障到通信速度和使用数字技术的前景。网络和关键技术的进步是世界未来繁荣的基础，但也有可能破坏稳定性和可预测性。因此，必须促进能力建设措施、适当保护能力和数字服务，帮助建立一个更安全的网络空间。

国家一级为加强信息安全和促进该领域国际合作所做的努力

阿塞拜疆支持根据大会第 75/240 号决议设立的 2021-2025 年信息和通信技术安全及使用问题不限成员名额工作组的工作。作为大会第 78/237 号决议的共同提案国之一，阿塞拜疆已采取若干步骤，加强信息安全并促进网络安全方面的国际合作。

应当指出的是，阿塞拜疆共和国总统 2023 年 8 月 28 日法令核准的《2023-2027 年阿塞拜疆共和国信息安全和网络安全战略》旨在提高国家信息安全水平，以确保国家、社会和个人安全地使用现代信息和通信技术(信通技术)，为此需要确定和执行确保国家、私人网络和关键信息基础设施安全并保护个人数据的措施，协助为维护《阿塞拜疆共和国宪法》所载的人权和自由创造更有利的条件。作为阿塞拜疆共和国信息安全和网络安全领域的第一项战略，该战略是国家信通技术政策不可分割的组成部分，概述了主要目标、方向、优先任务、相关解决方案以及该领域的综合措施计划。

此外，《战略行动计划》第 8.9.2.3 节提到了“在信息安全实体一级，包括在国家计算机应急响应小组和其他此类小组中组织开展网络安全领域国际合作和

国际经验研究的持续措施”，其主要目标是发展与国际计算机应急响应中心的合作，并确保成为该中心的成员。目前正在开展实际工作，以期扩大相互活动和经验交流。

值得注意的是，《关于确保阿塞拜疆共和国关键信息基础设施安全的规则》和《关于关键信息基础设施物项登记册结构、创建和管理的规则》已于 2023 年由阿塞拜疆共和国内阁相关决定核准。

此外，得益于阿塞拜疆共和国国家安全局和阿塞拜疆网络安全组织协会实施的联合行动，阿塞拜疆在国家网络安全指数国际排名表中的位置已从第八十六位提升至 2023 年的第五十位。

阿塞拜疆共和国国家特别通信和信息安全局制定了确保信息安全准则草案，将提交给政府机构，以确保国家机构的信息安全，包括针对机构信息环境中的潜在威胁确定预防和纠正措施。

网络卫生项目已付诸实施，目的是加强对网络威胁的网络复原力，并提高国家机构雇员以及私营部门和企业主在该领域的认知。

由国家特别通信和信息安全局与国家安全局共同组织的网络节“2023 关键基础设施防御挑战”于 2023 年 10 月 26 日至 27 日举行，旨在增强本地和外国公司以及公共和私营部门机构在网络安全、关键基础设施及金融和电信领域的经验、知识和技能。

2023 年 4 月，由罗马尼亚国家信息学研究发展所组织举办的网络外交国际会议决定，阿塞拜疆将于 2024 年主办下一次会议。

得益于在网络安全领域组建和发展国家生态系统方面开展的实际活动，阿塞拜疆的国际排名显著提高。根据国际电信联盟组织的 2020 年全球网络安全指数，阿塞拜疆提高了 15 分，在 194 个国家中排名第四十，得分为 89.31。

在上述领域的国际协作方面，阿塞拜疆共和国各机构参加了专门为合作打击网络威胁、交流网络安全事件的信息和经验、制定网络安全领域的政策和战略而举办的国际活动，包括拟订打击为犯罪目的使用信息和通信技术行为全面国际公约不限成员名额政府间特设委员会的会议，以及在欧洲联盟和欧洲委员会共同出资的欧洲联盟执法培训机构及打击有组织犯罪培训和行动伙伴关系 CyberEast 项目框架内举行的活动。

加拿大

[原件：英文]
[2024 年 4 月 16 日]

网络空间恶意活动近些年呈增加趋势，加大了高效开展工作的动力，以减轻可能破坏国际安全与稳定的威胁。

加强协作和以行动为导向的努力的必要性必须与相应的联合国网络安全机制相匹配。加拿大强调要在集体成果(现有规范和我们对如何适用国际法的共同理解)的基础上再接再厉，并创造一个空间，按照与我们在全体会议上的讨论有着内在联系的方式，进行更加深入、具体和技术性的讨论。加拿大认为，未来的定期机构对话应在威胁评估、框架执行情况讨论、能力建设和审查任何查明的有待解决的差距之间形成良性循环。研究现实生活中的事项或模拟此类事项的场景，更有可能揭示切实的缓解方案。今后的定期机构对话应注重行动和成果，并显示持续和可衡量的进展。

作为网络空间基础设施的所有者和运营者以及我们在实地的目睹者和倾听者，多利益攸关方群体特别适合以协商方式为我们的工作提供优质和独特的投入。确保利益攸关方有意义地参与未来的定期机构对话，将有助于实现我们维护网络稳定的共同目标。以这种方式让多利益攸关方参与，也是增加和促进将小国和发展中国家纳入我们工作的机会的最有希望的办法。这反过来又最大限度地提高了为所有人实现全球网络复原的潜力。通过真正包容各方，未来的定期机构对话将产生更大的获取支持的潜力，从而能够在网络空间真诚地落实和发展负责任的国家行为。

通过各国在联合国的平等参与，未来的定期机构对话应考虑到所有国家的关切和利益，包括对进一步发展该框架的关切和利益。关于实质性问题的决定应以协商一致方式通过。

加拿大提及并重申其在 2023 年 4 月秘书长根据大会第 77/37 号决议提出的关于行动纲领的报告中就未来定期机构对话所表达的观点。这些观点特别反映出加拿大认可并欢迎迄今为止以协商一致方式通过的报告和建议(例如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和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 2021 年报告)。加拿大认为，不限成员名额工作组履行大会第 75/240 号决议规定任务的最佳行动方针是决定进行一次单轨、长期、注重行动和包容各方的定期机构对话。

加拿大欢迎有机会再次就未来的定期机构对话发表意见。加拿大认为，不限成员名额工作组的现行机制并不理想，也不足以实现我们的集体目标。加拿大不支持重复或永久延长不限成员名额工作组的现行机制。相反，加拿大坚信，在不限成员名额工作组内制定并最好以协商一致方式商定的行动纲领，是确保就网络安全问题开展单轨、长期、注重行动和包容各方的定期机构对话的最佳途径。这一进程将使各方能够更有重点地参与各项规范的执行工作，并就如何适用国际法进行更加深入的讨论，还将确保在关于具体执行成果的讨论以及有针对性的能力建设之间进行更好的、注重行动的协调(不限成员名额工作组内目前没有这种协调)。

加拿大回顾，自 2021 年以来，包括在不限成员名额工作组内分发的工作文件[1] 的背景下，就行动纲领作为未来的定期机构对话进行了实质性讨论。加拿大认可并支持其他会员国关于在联合国开展一个讨论网络安全的单轨进程的呼吁。因此，加拿大告诫不要为定期机构对话建立一个单独的平行进程，与通过大会第 78/16 号决议获得 161 个会员国支持的行动纲领竞争。这将是不适当和不必要的重复，将给会员国带来不必要的人力和财政费用。

行动纲领的结构和运作将通过国际会议决定，国际会议将通过一项政治宣言。设想是由裁军事务厅作为秘书处为行动纲领提供服务。将举行审查会议提供战略方向，类似于目前不限成员名额工作组机制下的开放式全体讨论，并召集技术会议或工作组，以协调与应对特定威胁相关的专题讨论要素(例如确定与实施各项规范最相关的能力建设活动，并将国际法适用于勒索软件)。

行动纲领将利用对能力建设和技术援助的投资，作为促进网络空间负责任国家行为和促进国家间合作的基本要素。将与区域组织合作建立区域参与，以发挥协同作用和协调各项举措。

行动纲领将比发表主席报告更进一步，还将显示持续和可衡量的进展。将通过巩固承诺和参与报告或审查机制，努力填补既有成果与实际做法之间的问责差距，以便能够开展最佳的能力建设活动，增进全世界范围的负责任国家行为。

中国

[原件：中文]
[2024 年 4 月 29 日]

中国关于未来常设机制的观点文件

根据大会题为“从国际安全角度看信息和电信领域的发展”的第 78/237 号决议的要求，中国政府对未来常设机制的立场和观点如下：

未来常设机制是关乎联合国信息安全进程长远发展的重大问题。中方支持在联合国框架下建立唯一的、各方普遍参与的网络安全未来常设机制，在不限成员名额工作组框架下就未来常设机制达成共识是各方的唯一选择。中方不支持任何在工作组外试图建立常设机制的行动，反对“另起炉灶”，这将导致联合国信息安全进程面临分裂，助长地缘政治和阵营对抗势头，不符合所有会员国利益。

关于未来常设机制的结构和功能，应既巩固维护联合国信息安全进程 26 年来达成的重要成果，又面向未来谋求长远发展。在结构上可包括两部分：一是“向后看”，聚焦遵守和履行现有已达成的网络空间负责任国家行为框架，特别是就能力建设充实完善行动方案。二是“向前看”，聚焦与时俱进制定包括数据

[1] 见 https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf。

安全在内的新准则，推动制定有关法律文书，就能力建设等提出新的行动方案。中方提出《全球数据安全倡议》，就数据安全问题提出切实解决方案。《倡议》提出各国不得要求本国企业将境外产生、获取的数据存储在境内，尊重他国主权、司法管辖权和对数据的安全管理权，未经他国法律允许不得直接向企业或个人调取位于他国的数据，并就保护关键基础设施、供应链安全等提出具体主张。《倡议》已作为大会文件正式散发。中方愿与各方一道，以此为蓝本，共同推动制定反映各方意愿、尊重各方利益的网络数字治理国际规则。

未来常设机制应由会员国主导，同时按不限成员名额工作组现有方式确保多利益攸关方参与。可每五年举行一次审议大会，每年举行两到三期全体会议。在审议周期中，前三年应聚焦实质性讨论，并且通过年度程序性报告，如遇会员国广泛关心的重要问题，可以协商一致方式作出有关决定。在审议周期第四年，可启动审议大会筹备进程，并以主席名义起草滚动案文。在审议周期第五年，主要就主席滚动案文进行实质性讨论，总结或谈判达成实质性共识，并对未来五年工作作出规划。

中方愿继续积极参与相关进程，为建立未来常设机制作出贡献。

中方希望上述观点能反映在秘书长相关报告中。

古巴

[原件：西班牙文]
[2024 年 4 月 29 日]

信息和通信技术的发展对社会各个领域产生越来越大的影响。我们必须防止这一发展危及国家安全。

古巴重申，为了人类的共同利益和促进所有国家的可持续发展，应以和平方式使用信息和通信技术，各国应负责任地行事。

我们重申，防止网络空间成为军事行动舞台的唯一途径是所有国家共同合作。

大会必须通过一项具有法律约束力的国际文书，以补充适用的国际法，解决网络安全领域的重大法律空白，并使我们能够有效应对我们面临的越来越多的挑战和威胁。

2021-2025 年信息和通信技术安全及使用问题不限成员名额工作组是实现这一目标的适当论坛。

这个包容、透明的工作组在启动信息和通信技术安全及使用领域定期政府间对话方面发挥的作用应当得到尊重和维护。我们呼吁继续以这种方式开展工作，以便能够产生所有国家都同意的结果。

所有国家都必须尊重这一领域的现有国际标准。访问另一国的信息或电信系统应符合缔结的国际合作协定，并应基于有关国家同意的原则。交换的性质和范围必须遵守授予访问权限的国家的法律。

恶意使用电信，以颠覆国家法律和政治秩序为公开或隐藏目标，违反了这一领域的国际商定规则，是对这一媒介的非法和不负责任使用。

古巴电波一直受到来自国外的攻击，非法电台和电视广播一直在散播意图煽动推翻古巴人民建立的宪法秩序的节目。

2023 年平均每月有超过 7 000 小时针对古巴的节目从美国使用 21 个频率非法传输，违反了《联合国宪章》的宗旨和原则、国际法和国际电信联盟规则。

60 多年来，美国政府对古巴实施的经济、商业和金融封锁给古巴人民造成了严重损失，包括使用和享受信息和通信技术方面。

我们重申，我们明确反对采取违反国际法并阻碍援助、合作和技术转让的单方面胁迫措施。

我们区域认识到信息和通信技术有潜力为发展挑战提供新的解决方案，促进持续、包容和公平的经济增长，并帮助实现 2030 年可持续发展议程。

正如 2024 年在金斯敦举行的拉丁美洲和加勒比国家共同体第八次首脑会议通过的宣言所反映的那样，我们还提请注意促进开放、安全、稳定、无障碍及和平的信息和通信技术环境的必要性。

古巴重申，国际合作对于应对滥用信息和通信技术的危险至关重要。

捷克

[原件：英文]
[2024 年 4 月 30 日]

捷克完全致力于在联合国推动关于网络安全的全球辩论，并感谢不限成员名额工作组和政府专家组迄今取得的进展。

不限成员名额工作组和政府间专家组的主要成就之一是制定并巩固了网络空间负责任国家行为框架。

在这方面，捷克认为，执行网络空间负责任国家行为框架应是未来机构对话的中心主题。此外，捷克支持在不限成员名额工作组于 2025 年结束工作后，在联合国主持下建立一个常设、单轨、包容和注重行动的机制。

与此同时，我们认为，为了在今后建立一种能有效造福于我们所有人的机构对话，必须在当前不限成员名额工作组内继续就其具体形式进行辩论。目前，我们国际社会只有一年多的时间来进行这一辩论。

关于不限成员名额工作组内的辩论，捷克希望提请大家注意，关于未来的机构对话，最成熟、讨论最多、也是最一致的提议是推进在使用信息和通信技术(信通技术)方面负责任国家行为的行动纲领。

与此相反，我们认为，关于从国际安全角度看信息和电信领域的发展的第78/237 号决议并没有以不限成员名额工作组近些年来所达成的渐进办法和共识为基础，而是似乎优先考虑了一小部分国家的利益。

自 2020 年以来，关于行动纲领的辩论一直在持续进行，捷克一直积极参与其中。我们认识到不限成员名额工作组内正在进行的关于行动纲领的讨论对于确定行动纲领的方向和澄清一些可能有争议的问题是有价值的。我们认为，必须继续进行这一辩论，以确定未来机制的内容和方式。鉴于上述，我们建议不限成员名额工作组在 2024 年和 2025 年举行闭会期会议和专门会议，重点讨论行动纲领的特定方面，包括所涉预算问题。

此外，捷克希望提请注意在对行动纲领的讨论中出现的行动纲领的某些方面，捷克认为这些方面是行动纲领最重要的优势：

- 行动纲领将为有关信通技术的国际辩论带来体制稳定，是一个支持联合国内部所有与网络有关的辩论的永久性体制框架，因此将不必就设立一个专门负责信通技术使用问题的新工作组进行定期讨论。
- 行动纲领将支持执行负责任的国家行为框架，并在必要时推动进一步讨论该框架的发展。
- 行动纲领将努力使能力建设原则成为其注重行动的目标之一，并促进在网络能力建设项目中予以落实。行动纲领可利用现有和潜在的能力建设努力，提高其知名度并改善协调。例如，可探讨与国际电信联盟等其他机构开展的网络能力建设活动的协调。
- 行动纲领将促进非政府利益攸关方的切实参与和协作。发动私营部门、学术界和民间社会参与，将带来关于评估威胁和执行准则，包括衡量进展等事项的宝贵专门知识。
- 行动纲领的目标是作为一个全面框架，可涵盖不限成员名额工作组讨论或商定的其他举措。

关于具体方式，捷克赞成在闭会期举行年度全体会议和专门技术工作组会议的想法。

- 某一工作组的设立和终止完全属于各国的职权范围。
- 这些技术讨论的范围和筹备工作将仅限于全体会议确定的专题。例如，讨论将由各国政府的少量专家参加，相关讨论则邀请学术界等其他利益攸关方参加。特别是，这些工作组可侧重讨论保护关键基础设施、应对网络事件以及国际法中关于特定问题的具体规定在网络空间的适用性等专题。

- 如果安排得当，我们认为，设立闭会期技术工作组可大大提高我们的工作效率，并减轻各个代表团的负担。
- 可考虑不将所有闭会期工作组会议都放在纽约举行，而是也可讨论其他地点。

丹麦

[原件：英文]
[2024 年 5 月 1 日]

丹麦认为，执行联合国在使用信息和通信技术(信通技术)方面的负责任国家行为框架对于确保全球开放、稳定和安全的网络空间至关重要。国际社会已确认现行国际法和《联合国宪章》全文适用于信息和通信技术环境，丹麦仍然致力于在网络空间方面执行这一框架。

过去 20 年在制定网络空间负责任国家行为综合框架方面取得了重大进展，包括适用国际法、自愿规范、能力建设和建立信任措施。该框架已多次获得大会一致核可，最近一次是在 2021-2025 年信息和通信技术安全及使用问题不限成员名额工作组的 2023 年度共识进展报告中。

丹麦与欧洲联盟一样，认为大会 2023 年 12 月 22 日通过的关于从国际安全角度看信息和电信领域的发展的第 78/237 号决议的部分内容是基于非协商一致的案文。更具体而言，序言部分第 16 段和执行部分第 5 段所依据的提案仅得到有限几个国家的支持。丹麦感到关切的是，这可能导致重新解释现有的协商一致文件。因此，丹麦不能支持第 78/237 号决议。

关于根据该决议执行部分第 8 段提出的要求

联合国一再呼吁在国际安全背景下建立一个永久性的联合国网络问题机制。随着大会于 2023 年 10 月决定制定一项行动纲领，以推进在国际安全背景下使用信息和通信技术方面的负责任国家行为，我们已经落实了上述呼吁。

关于未来机制的讨论已取得显著进展，丹麦愿就未来定期机构对话发表以下补充意见。

正如 2019-2021 年从国际安全角度看信息和通信领域发展不限成员名额工作组所明确指出的那样，这一机构对话应侧重于支持实施规范性框架，该工作组得出的结论是，未来机构对话应“是一个拥有具体目标、注重行动的进程，建立在以往成果之上，包容，透明，由共识驱动，以成果为基础”。[2]

行动纲领应提供永久性的体制机制，以跟踪商定准则的执行情况，支持和促进能力建设，提供建议并定期更新。与此同时，行动纲领应具有灵活性，允许以履行现有承诺过程中吸取的经验教训为基础，进一步发展该框架。

[2] A/75/816，第 74 段。

丹麦认为，必须承认所有利益攸关方在塑造网络安全的未来方面都可以发挥有意义的作用。为确保包容对话，必须允许企业、非政府组织和学术界等相关利益攸关方正式参与磋商，并不断交流意见，以表明对不同视角集思广益的承诺。这种包容对于建立有效和全面对话以应对网络安全的多方面挑战至关重要。

行动纲领可举行年度正式会议，并允许举行技术会议，重点讨论相关方面的工作组可全年举行会议。未来的机制应定期召开审查会议，以审查负责任国家行为框架，必要时更新该框架，并为该机制的工作提供战略指导。

在本届不限成员名额工作组的剩余任期里，应专门拿出时间和精力，进一步阐述行动纲领的各个方面。为了确保向行动纲领顺利过渡，有必要讨论常设机制所涉预算问题，并确定联合国今后履行这些职能的相关行为体。

埃及

[原件：英文]
[2024 年 2 月 26 日]

一. 导言

1. 会员国与国际社会一样，日益关切恶意使用信息和通信技术(信通技术)现象泛滥，以及一些国家过度发展信通技术能力，其目的与国际法和维护国际稳定与安全的目标不符，而且可能对其他国家基础设施的完整性产生不利影响，损害其他国家在民用和军事领域的安全。

2. 联合国通过 2010 年、2013 年、2015 年和 2021 年政府专家组以及 2021 年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评估和建议，[1] 已在解决这些关切方面取得了进展，从而建立起一个日积月累不断发展的框架，促进这些进程所阐述的在使用信通技术方面的负责任国家行为。

3. 政府专家组 2010 年、2013 年、2015 年和 2021 年报告、不限成员名额工作组 2021 年报告以及当前从国际安全角度看信息和通信领域发展不限成员名额工作组的第一次和第二次年度进展报告都呼吁成员国在使用信通技术方面接受指导。此外，这一商定框架还强调，国际法，特别是《联合国宪章》，对于维护和平与稳定以及促进开放、安全、稳定、无障碍及和平的信通技术环境是适用的，也是必不可少的。

4. 针对使用信通技术方面负责任国家行为的现有规范、规则和原则框架可以减少国际和平、安全和稳定面临的风险，同时不限制或禁止在其他方面符合国际法的行动。

5. 2020 年，埃及和法国发起了关于推进在国际安全背景下使用信通技术方面负责任国家行为的联合国行动纲领的提案，该提案随后由一个跨区域国家组制

[1] 见 A/65/201、A/68/98、A/70/174、A/75/816 和 A/76/135。

定，并反映在政府专家组最后报告、不限成员名额工作组 2021 年报告以及当前不限成员名额工作组的第一次和第二次年度进展报告中。

6. 秘书长发表了一份报告(A/78/76)，综合了各国关于行动纲领范围、结构、原则、内容、筹备工作和制定方式的意见。

7. 未来任何关于定期机构对话的机制都必须建立在既有成果和大会以协商一致方式核可的现有商定框架的基础之上。

8. 新的机制或平台应在 2025 年之后，在当前不限成员名额工作组的任务结束后建立。这意味着将不会有任何重复努力或建立平行轨道的机会。该机制应是联合国主持下的“一站式”全面平台，从国际安全角度处理与信息和电信领域发展有关的问题，并推进在使用信息和通信技术方面的负责任国家行为。

9. 会员国原则上同意，定期机构对话机制将具有单轨、由国家主导、永久、包容、透明和灵活的特点。[2]

二. 未来联合国定期机构对话机制的目标和范围

10. 作为一个定期机构对话平台，使所有会员国都能够参与一个建立在现有框架基础上的单轨、永久、包容、透明、灵活、注重行动、基于成果、由共识驱动的进程。

11. 促进开放、安全、稳定、无障碍、和平和可互操作的信通技术环境。

12. 防止因使用信通技术而产生冲突，并寻求通过和平手段解决相关争端。

13. 巩固既有网络工具(联络点目录和将由不限成员名额工作组通过的所有其他建议)，以保持其有效运作并酌情进行审查。

14. 制定具体指导方针，支持会员国执行商定的规范、规则和原则，包括通过促进国际合作和援助。

15. 其范围应侧重于以下三个支柱：

(a) **落实现有商定成果**。通过审查会员国按照商定的标准化报告模板自愿提交的国家执行情况报告，定期评估会员国执行商定框架的情况；

(b) **发展现有框架**。确定会员国在实施框架方面的差距和面临的各种挑战，推动提出应对这些挑战的相关可行建议，并恢复对概念问题的审议，例如国际法的适用性或在这一领域制定新规则和具有法律约束力的义务的必要性；

(c) **促进能力建设**。采取切实步骤促进国际合作，并定期评估是否需要采取额外行动以应对当前和新出现的挑战，同时考虑到快速变化的环境，交流可在国家、区域和国际各级实施的最佳做法(包括立法和行政框架以及为保护关键基础设施而采取的措施)，并根据受援国自身的需求评估，按照 A/76/135 号文件所载的能力建设原则，为能力建设提供具体支持。应设想为相关活动建立一个

[2] A/78/265，第 55 段。

专门的供资机制，包括依靠现有工具和新工具的可能性，例如世界银行网络安全多捐助方信托基金。

三. 建立未来的定期机构对话机制

16. 会员国在当前不限成员名额工作组关于行动纲领提案的框架内提交的意见和建议、秘书长根据大会第 77/380 号和第 78/237 号决议提交的报告以及 2021-2025 年不限成员名额工作组报告所载的相关可能建议，应作为建立该机制的基础，特别是就其范围、结构和模式而言。

17. 会员国应继续积极参与当前根据大会第 75/240 号决议设立的不限成员名额工作组，以期达成协商一致的报告，包括建立未来定期机构对话机制的建议。

18. 该机制应在当前不限成员名额工作组内进一步阐述和发展，避免任何重复努力或制造竞争，并在联合国内部处理信通技术的国际安全方面保持协商一致的精神。

19. 该机制应在当前不限成员名额工作组于 2025 年结束任务后，通过该工作组最后报告的建议建立，同时可考虑通过一项基于包容和透明协商和筹备进程的协商一致的大会决议建立未来定期机构对话的可能性。会员国可在当前不限成员名额工作组内商定通过一项政治宣言建立这一机制，该宣言可由大会决议核可，其中包括建议的机制模式。未来峰会的成果可提及就这一事项达成初步协议。

四. 结构和可能的模式

定期会议

20. 该机制可采取行动纲领的形式，每六年召开一次审查会议，重点讨论以下问题：

(a) 研究和审查该机制的执行情况，确定今后几年的主要优先行动，然后为以后的会议通过一项工作方案；

(b) 考虑是否应在协商一致基础上制定新的规范、规则、原则或具有约束力的义务，以更新该框架。

21. 该机制应定期召开两年期会议，以执行审查会议通过的工作方案，并通过审查会员国定期提交的国家执行情况报告，跟踪会员国执行商定规范、规则和原则的情况。

22. 每届会议主席应在每次审查会议和后续两年期会议前召开筹备协商会议。

23. 商定机制可通过协商一致方式决定举行闭会期会议或设立非正式工作组，重点讨论具体的相关问题，包括国际法的适用性和拟订新的规范、规则和原则，以及酌情拟订具有法律约束力的义务或文书。

报告

24. 在商定机制下将鼓励会员国自愿轮流每两年提交一次国家执行情况报告，至少每三个周期(每六年)提交一次报告。这一进程可以联合国关于国际安全背景下国家负责任使用信通技术的建议执行情况全国调查模型为指导。会员国还不妨在其国家执行情况报告中列入一节，阐述本国在能力建设领域的优先事项和需求。

25. 每次两年期会议和审查会议都应以协商一致方式通过一份最后报告，包括一份成果文件，并提交第一委员会下届会议审议和核可。

决策

26. 行动纲领应以协商一致方式通过关于实质性问题的决定。

秘书处

27. 裁军事务厅为该机制提供秘书处服务。

利益攸关方的参与

28. 该机制是一个政府间进程，谈判和决策是会员国的专属特权。

29. 该机制将致力于以系统、持续和实质性的方式与相关利益攸关方接触。

30. 根据第 1996/31 号决议具有经济及社会理事会咨商地位的相关非政府组织可通知秘书处它们有兴趣参加该机制的工作。

31. 与该机制的范围和宗旨相关并有能力的其他感兴趣的非政府组织也可通过提交关于该组织宗旨、方案以及在与该机制范围相关领域开展的活动的资料，通知秘书处它们有兴趣参加。相应地，这些组织将在无异议基础上受邀作为观察员参加该机制的正式会议。

32. 经认证的利益攸关方将能够出席行动纲领的正式会议，在专门的利益攸关方会议上作口头发言，并提交书面意见。应鼓励会员国善用无异议机制，同时铭记包容精神。

33. 如果对非政府组织提出反对意见，提出意见的会员国将向机制主席表明其反对意见，并在自愿基础上向主席说明其反对意见的一般依据。主席将应任何会员国的要求与其分享收到的任何信息。

34. 主席将在闭会期组织与利益攸关方的非正式磋商会议。

35. 该机制可促进与相关区域和次区域举措的协调，包括通过其可能的参与和贡献。

爱沙尼亚

[原件：英文]
[2024 年 4 月 30 日]

根据大会第 78/237 号决议的要求，爱沙尼亚谨提交关于信息和通信技术(信通技术)安全及使用问题未来定期机构对话的国家立场。

近些年来，在当前充满挑战的地缘政治环境中，国际安全背景下使用信通技术面临的威胁继续加剧并显著演变。使用信通技术的威胁越来越大，导致与对经济和社会发展的负面影响有关的挑战越来越多，对国家和国际稳定也产生了影响。正如政府专家组和不限成员名额工作组的工作所表明的那样，这些影响仍然是多边讨论的重点。

在一个跨区域国家组广泛支持制定一项行动纲领之后，我们支持将行动纲领作为第一委员会下的一个常设体制机制，重点是执行商定的网络空间负责任国家行为框架，同时也允许酌情进一步发展该框架。我们认为，这种定期机构对话将有助于缓和紧张局势、预防冲突和促进和平利用这些资源。

这一国家立场是对秘书长关于行动纲领的报告(A/78/76)中所载爱沙尼亚国家贡献的更新，其中除其他外，借鉴了在大会第 78/16 号决议中反映的进展和在 2021-2025 年不限成员名额工作组内的讨论情况。

1. **行动纲领应以现有成果和负责任国家行为框架为基础，侧重于国家在国际和平与安全背景下使用信通技术**。爱沙尼亚认为，使用信通技术必须符合维护国际稳定与安全的目标，并遵从商定成果和负责任国家行为框架。我们强调，会员国使用信通技术应以政府专家组 2010 年、2013 年、2015 年和 2021 年报告以及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 2021 年报告为指导。行动纲领机制应建立在这些前提之上，并以维护一个开放、稳定、安全、无障碍及和平的信通技术环境为目标。爱沙尼亚认为，一些现有或拟议举措，例如全球联络点名录，将为行动纲领模式的有效运作提供有益的支持。

2. **行动纲领应采取中立形式，提供体制稳定性**。从小国的角度看，讨论国家使用信通技术的进一步进程必须具有明确性和体制稳定性。因此，爱沙尼亚主张在当前 2021-2025 年信息和通信技术安全及使用问题不限成员名额工作组于 2025 年结束任务后建立一个单一的常设结构，以推进该工作组的讨论。我们支持进一步讨论将行动纲领确立为促进使用信通技术方面负责任国家行为机制的结构、模式和时间轴，同时考虑到所有会员国的意见。爱沙尼亚支持按照在大会第 77/37 号决议中的商定，至迟于 2026 年通过国际会议建立这一机制。爱沙尼亚认为，拟议的行动纲领模式将使大会不必每两年、三年或四年就建立新的网络进程进行辩论。我们希望会员国将行动纲领框架视为一个有用和中立的框架，不需要有平行的进程。

3. **行动纲领应提供一个整体框架，以包容的方式推进不限成员名额工作组期间提出的各项议题**。我们欢迎会员国越来越有兴趣对不限成员名额工作组会议

正在进行的辩论中重点讨论的各种专题作出贡献。不限成员名额工作组目前的讨论是实质性的，不同会员国提出了各种各样的想法。我们认为，行动纲领框架可以为会员国提出与信通技术及国际和平与安全有关的问题提供一个“求助”场所。因此，行动纲领可以为提出和更详细地分析这些想法提供一个整体框架。

4. **行动纲领还应包括明确和透明的方式，让多利益攸关方群体实质性参与，并进一步受益于他们的专长和知识**。让多利益攸关方群体参与有助于会员国实施负责任国家行为框架，并设计和提供由需求驱动的能力建设工作，以提高全球网络复原力。同样，行动纲领还可以通过与区域和专题组织合作，利用和发展现有相关举措来加强区域参与。

5. **行动纲领应允许采取更加灵活但重点突出的形式，继续讨论负责任国家行为框架**。爱沙尼亚希望强调，行动纲领框架的设计还应考虑到小国因能力有限而面临的挑战，从而建立在对预计工作量的合理期望之上：

(a) 我们建议，行动纲领机制的内容可包括每年举行全体会议，讨论负责任国家行为框架主要支柱下的专题；

(b) 我们还支持以向所有感兴趣的参与者开放的工作组形式进行重点讨论，包括但不限于威胁、能力建设、建立信任、规范以及国际法。另一种选择是将这些工作组的重点放在保护关键基础设施等更多专题上。参加工作组应当是自愿的，工作流程的创建将由各国在年度全体会议上决定。

(c) 我们还支持组织审查会议(例如，每四年一次)，以便与会者评估进展情况，审议对任务授权以及工作安排或行动纲领的任何进一步可能的修正。

6. **除其他专题外，行动纲领应为讨论国际法提供一个包容性框架**。爱沙尼亚欢迎就国际法及其如何适用于国家使用信通技术问题开展越来越积极和实质性的讨论。会员国将受益于对如何适用现有规则的深入理解和共同看法，以及对任何可能的差距的更详细分析。行动纲领将为继续进行这些讨论提供一个包容各方的场所。具体而言，行动纲领可以为讨论国际法的下列要素提供一个平台：(a) 继续讨论国际法如何适用于网络空间；(b) 分享国家观点；(c) 就国际法如何适用于信通技术使用问题举行专门会议，重点讨论具体专题以便进行更详细的阐述；(d) 专家简报；(e) 基于场景的讨论；(f) 国际法能力建设。

7. **行动纲领应面向行动，并大力注重能力建设**。未来讨论的一项内容应当是执行商定的负责任国家行为框架。行动纲领还可鼓励自愿报告国家执行工作，这将有助于实现许多目标，例如建立信任、透明度以及能力和需求摸底。行动纲领应以协调和互补的方式评估现有的能力建设举措。例如，在设计行动纲领时应注意到现有的摸底调查工作和资源，如 Cybil 门户网站和欧洲联盟 CyberNet 对欧洲联盟成员国网络能力建设项目的摸底调查。

法国

[原件：法文]
[2024 年 4 月 30 日]

一. 导言

20 多年来，各国都认识到，信息和通信技术(信通技术)推动人类进步和发展，但它也可能被用于违背维护国际稳定与安全目标的目的。

自 2003 年以来，大会第一委员会设立了一系列工作组，这些工作组致力于在数字环境中维护国际和平、安全与稳定。为此，这些工作组整合了在使用信通技术方面的负责任国家行为框架，大会多项决议以协商一致方式核可了该框架。[1]

各工作组还讨论了建立定期机构对话的问题，以解决与在国际安全背景下使用信通技术有关的问题。

工作组强调，此类对话应尤其注重支持框架执行工作。特别是，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(2019-2021 年)得出结论认为，今后的定期机构对话“应是一个有具体目标而且注重行动的进程，建立在以往成果的基础上、包容各方、透明、以达成共识为导向、以成果为基础”。[2]各国还强调“探索专门用于对商定规范和规则的执行情况采取后续行动的机制的效用”。[3]

各国指出，该框架具有累积性和演变性，可以随着时间的推移制定更多规范。各国还指出了今后酌情制定更多具有约束力的义务的可能性。[4]今后的定期机构对话必须支持执行现有的商定框架，但也要允许今后可能的进一步发展，特别是针对新出现的挑战和威胁。

在这方面，一个跨区域国家集团自 2020 年提出的制定一项行动纲领的提议将为第一委员会提供一个常设体制机制，以监测商定框架的执行情况，并在必要时进一步发展该框架。

秘书长在其关于推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领的报告(A/78/76)中，建议各国在 2021-2025 年信息和通信技术安全及使用安全问题不限成员名额工作组的主持下，继续讨论行动纲领提案的可能范围、结构、原则、内容、职能和后续机制，同时借鉴在报告中表达的意见，并考虑到裁军事务厅根据大会第 77/37 号决议组织的区域和次区域协商。

---

[1] 见大会第 70/237 和 76/19 号决议。

[2] A/75/816，附件一，第 74 段。

[3] A/75/816，附件一，第 73 段。

[4] 大会第 76/19 号决议，序言部分第十段。

本文更新了法国为 A/78/76 号文件提交的国家材料，反映了在通过大会第 78/16 号决议后取得的进展和 2021-2025 年不限成员名额工作组正在进行的讨论情况。

二. 范围和目标

作为第一委员会的一项机制，行动纲领将处理与在国际安全背景下使用信通技术有关的问题。其总体目标是通过维护一个开放、安全、稳定、无障碍及和平的数字环境，为维护国际和平与安全作出贡献。

为此，行动纲领的目标应当是：

- 合作：通过合作应对网络威胁，以及在各国之间和与利益攸关方开展包容性对话，缓减紧张局势，预防冲突，促进和平利用信通技术。
- 稳定：通过支持执行并酌情进一步发展基于国际法(包括国际人道法和人权法)、负责任国家行为规范、建立信任措施和能力建设的负责任国家行为框架，促进网络空间的稳定。
- 韧性：通过执行负责任国家行为框架，促进弥合数字鸿沟，加强全球韧性。

三. 结构和内容

组织结构

行动纲领可基于一份政策文件，该政策文件除其他外将：

(a) 重申各国对相关决议和报告中确认的负责任国家行为框架的政治承诺。[5] 这一创始承诺将考虑到 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组通过的共识成果，例如建立一个全球政府间联络点目录，可能建立一个全球合作门户网站或建立威胁登记册的想法。未来的行动纲领必须以这些共识成果为基础；[6]

(b) 建立一个常设体制机制，旨在：㈠ 促进执行框架，包括为各国开展相关的能力建设；㈡ 酌情进一步发展框架；㈢ 鼓励多利益攸关方在相关领域开展合作。

作为一项常设机制，行动纲领可基于以下组织结构：

- 定期全体会议，可每年或半年举行一次(法国愿意在考虑到各国能力以及行动纲领紧跟数字领域发展需要的情况下，进一步讨论此类会议的最佳周期)。在这些会议上可以：(a) 讨论现有的和新出现的威胁；(b) 审议规范、规则和原则的执行情况；(c) 继续讨论国际法如何适用于信通

[5] 包括大会第 76/19 号决议、政府专家组 2010 年、2013 年、2015 年和 2021 年共识报告、不限成员名额工作组(2019-2021 年)2021 年报告和 2021-2025 年不限成员名额工作组第一次进度报告。应当铭记，本届工作组今后的共识成果将丰富这一不断累积和演变的框架。

[6] 见大会第 77/37 号决议序言部分第二段和大会第 78/16 号决议序言部分第二段。

技术使用问题，确定潜在的差距；(d) 讨论建立信任措施的实施情况；(e) 确定能力建设优先事项，包括在自愿报告的基础上予以确定；(f) 确定今后要采取的行动，确定闭会期间会议的工作方案。可在年度会议上就建立技术工作流程作出协商一致决定，这些工作流程将向所有国家和利益攸关方开放，旨在解决具体问题(见下文)。技术和法律专家的参与将受到鼓励。

- 闭会期间会议，其将推进年度会议上商定的工作方案。这些会议可根据年度会议确定的优先事项和工作领域，采取侧重于具体工作流程的不限成员名额的技术会议或工作组的形式。

- 审查大会，例如可以每四年举行一次，审议是否应更新框架，并酌情进一步发展框架(见下文)。可以建立一个专门的工作流程，以深入讨论国际法如何适用于信通技术使用问题，并评估框架中是否存在可能需要进一步发展框架的差距。

内容

(a) **促进执行框架**

在行动纲领下，将鼓励自愿报告为执行框架而采取的国家措施，办法是建立专门的报告制度或促进现有机制(如联合国裁军研究所的国家执行情况示范调查或提交秘书长的国家报告)。这种报告将有助于确定框架执行方面的优先事项，评估能力建设需求。

可在行动纲领年度会议上通过和定期更新关于国家执行工作的可执行建议。根据上述组织结构，可在行动纲领年度会议上建立不限成员名额的技术会议或工作组，以推动对框架执行方面的具体问题的讨论。

例如，可在年度会议上确定框架执行方面的专题优先事项(实施某项特定规范或建立信任措施、数字产品和服务安全、保护关键基础设施等)。为了推动讨论此种优先事项、分享技术专门知识并讨论最佳做法和挑战，可在年度会议上设立一个专门的工作流程。该工作流程下的工作将向所有国家开放，并在行动纲领闭会期间会议上进行。不限成员名额技术会议或工作组的结论和建议将提交下次全体会议。

行动纲领将支持与执行框架有关的能力建设举措，并将有助于加强这一领域的多利益攸关方合作以及与其他相关举措的协调。

- 各国不妨考虑在今后的行动纲领下设立一个自愿基金，为旨在促进负责任国家行为框架的某些活动提供资金。该基金可仿效联合国支持军备管制合作信托基金。[7] 该工具所资助的举措或项目应符合职权范围，这些职权范围可在行动纲领的第一次会议上确定(促进遵守框架，遵守

[7] 联合国支持军备管制合作信托基金，见 https://disarmament.unoda.org/unscar/。

不限成员名额工作组(2019-2021 年)最后报告中商定的能力建设指导原则等)。

- 行动纲领还将用于发挥现有努力和举措的效力。行动纲领会议和能力建设技术工作组闭会期间会议将使各国能够讨论能力建设的优先事项(考虑到根据自愿报告所确定的需求)，并使利益攸关方能够提出相关倡议。不妨在行动纲领下建立“核证”制度，以便核可和促进符合行动纲领目标的活动。

- 其他组织(如国际电信联盟或世界银行网络安全多捐助方信托基金)的代表可在行动纲领会议上通报情况，以确保不同实体采取的能力建设措施(各自在任务规定和职权范围内行事)互为协调和补充。

(b) **发展框架**

为了应对新的挑战，可在定期会议或审查会议上，在协商一致的基础上对框架进行必要的更新(通过促进关于进一步发展该框架的讨论，包括通过加深对规范以及在使用信通技术方面如何适用现有国际法的共同理解，找出这些理解中的差距，并酌情考虑是否需要额外的自愿、不具约束力的规范或额外的具有法律约束力的义务)。[8]

(c) **多利益攸关方参与**

考虑到“各国对维护国际和平与安全负有首要责任”，[9] 而且各国必须在第一委员会的所有进程中保持其核心作用(包括专属决策权)，法国支持在未来行动纲领的范围内加强与利益攸关方的对话与合作。

- 对成果文件的决策和谈判仍将是各国的专属特权。

- 但在这方面，第一委员会各相关工作组一再强调酌情进一步加强与民间社会、私营部门、学术界和技术界合作的宝贵价值。[10] 与这些行为体的合作对于各国履行其在负责任行为框架下的承诺至关重要。此外，这些利益攸关方本身“有责任以不危及和平与安全的方式使用信通技术”。[11] 私营行为体还可以为讨论带来宝贵的专门知识，并为能力建设工作作出贡献。

- 因此，行动纲领会议的组织安排应使利益攸关方能够参加正式会议、发言和提供投入，正如第一委员会其他进程的情况一样，在这些进程中，它们的专门知识是有用的，例如在根据《禁止或限制使用某些可被认为具有过分伤害力或滥杀滥伤作用的常规武器公约》召集的致命

[8] 见大会第 78/16 号决议，第 3(b)段。

[9] A/75/816，附件一，第 10 段。

[10] A/75/816，附件一，第 22 段。

[11] A/75/816，附件一，第 10 段。

自主武器系统领域新兴技术问题政府专家组。[12] 这种安排允许多利益攸关方在正式场合进行对话，从而有利于提高进程的透明度。

- 为确保这些会议的包容性，应鼓励和支持各区域集团的利益攸关方参与，包括为此实施具体的赞助方案。

四. 制定行动纲领的方式和筹备工作

筹备工作

法国支持 2021-2025 年不限成员名额工作组继续进行有重点的专门讨论，以进一步发展行动纲领，并就制定工作寻求共识。

不限成员名额工作组(2019-2021 年)和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(2019-2021 年)在其最后报告中建议进一步发展行动纲领，包括通过 2021-2025 年不限成员名额工作组。2021-2025 年不限成员名额工作组在其 2022 年进度报告中也呼吁重点讨论行动纲领。

通过 2023 年举行的区域磋商和秘书长的报告(A/78/76)，有可能收集到大量各国家组的意见。秘书长在报告中强调，坚定地在之前共识协议和大会所取得进展的基础上，以包容各方和透明的方式审议行动纲领提案，是一项值得努力的工作。2021-2025 年不限成员名额工作组在其第二次年度进展报告中着手这项工作，原则上并以协商一致方式商定了“共同要素”，以期以建设性方式就未来定期机构对话机制形成共识。[13]

大会第 77/37 号决议规定，秘书长关于行动纲领的报告将提交给大会，并将作为 2021-2025 年不限成员名额工作组开展进一步讨论的基础。大会第 78/16 号决议强调，2021-2025 年不限成员名额工作组应在关于行动纲领的进一步工作中发挥关键作用，以期在不限成员名额工作组结束后至迟于 2026 年确立行动纲领。

因此，2021-2025 年不限成员名额工作组的闭会期间会议和专门会议应于 2024 年和 2025 年举行，以进一步发展行动纲领的各个方面，起草创始文件。

设立

法国赞成继续讨论设立未来机制的确切方式。

大会第 77/37 号决议提到召开一次“国际会议”，作为制定行动纲领的一个备选办法(正如《从各个方面防止、打击和消除小武器和轻武器非法贸易的行动纲领》所采用的做法)。大会第 78/16 号决议决定在 2021-2025 年不限成员名额工作组会议结束后，至迟于 2026 年设立一个联合国主持下的机制，该机制将是常设的、包容性的、面向行动的，拥有大会第 77/37 号决议中申明的具体目标，具备 2021-2025 年不限成员名额工作组第二次年度进展报告中以协商一致方式商定

[12] 《禁止或限制使用某些可被认为具有过分伤害力或滥杀滥伤作用的常规武器公约》议事规则(2016 年在公约缔约国第五次审议大会的框架内通过)第 49 条。

[13] A/78/265，第 55 段。

的未来定期机构对话的共同要素。如果各国作出决定，可在 2021-2025 年不限成员名额工作组所做筹备工作的基础上，于 2025 年召开一次国际会议，通过该机制的创始文件。

该国际会议应在协商一致的基础上作出决定，至少在实质性问题上。应允许相关利益攸关方参加(可对它们进行认证，方式类似于大会第 75/282 号决议规定的拟订一项关于打击为犯罪目的使用信息和通信技术行为的全面国际公约特设委员会参会者的认证方式)。

之后大会可以通过一项欢迎会议成果的决议，并就召开新设立的机制的首次会议作出决定。

格鲁吉亚

[原件：英文]
[2024 年 3 月 20 日]

关于今后在联合国主持下定期就信息和通信技术使用问题进行机构对话，格鲁吉亚认为，推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领可最佳推动联合国关于网络安全和网络空间负责任国家行为倡议。

在当前地缘政治事态发展快速且不可预测的安全环境下，某些行为体结合使用常规和非常规战争手段，威胁到基于规则的国际秩序。令人遗憾的是，一些行为体通过网络行动违反国际法情况时有发生。

国际社会必须坚持不懈地追究这些行为体在网络空间的非法和不可接受行为的责任，确保这些行为有法律后果。

在本届 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组于 2025 年结束工作后，《行动纲领》可以作为一个适当平台，就国际法在网络空间适用问题开展有针对性的对话。

我们主张将《行动纲领》作为第一委员会中的一个统一框架，专门探讨网络安全问题，并提供一个有利于采取着重行动的举措和取得切实进展的可靠结构。

在国家、区域和全球层级缺乏能力是一个重大挑战。因此，《行动纲领》应协助各国努力制定规范性框架，并提供能力建设援助，缩小数字鸿沟。

格鲁吉亚欢迎建立全球政府间联络点名录。这一举措标志着联合国在加强网络安全领域的国际合作与协调方面迈出了重要一步。

鉴于信息和通信技术发展迅速，未来国际框架必须具有充分的灵活性，确保其今后可以适用。这一国际论坛应纳入一个机制，以便通过定期全体会议或审查会议促成的共识，定期修订框架。这些会议可以重新评估现有框架，并酌情决定进一步加强或发展框架。

格鲁吉亚坚决支持透明和包容各方的多利益攸关方做法，强调国家和非国家行为体均应积极参与关于这些事项的机构对话框架。

德国

[原件：英文
[2024 年 4 月 30 日]

A. 行动纲领的基本原则

德国倡导制定一项行动纲领，作为注重行动、包容各方、透明灵活的常设论坛，以便在第一委员会内就信息和通信技术的安全与使用安全问题定期进行机构对话。该行动纲领应作为当前 2021-2025 年信息和通信技术安全与使用问题不限成员名额工作组的单轨后续机制。该机制应不迟于 2026 年开始运作，以便在工作组完成任务后落实工作组的成果，并重申大会第 78/16 号决议所载关于在联合国主持下建立一个机制的决定，具体目标在第 78/37 号决议中予以重申，并在 2021-2025 年不限成员名额工作组第二次年度进展共识报告(A/78/265)中商定了共同要素。

平行进程或双重结构要避免，不要让各国切实参与和确保务实讨论的能力负担过重。为了做好平稳过渡的准备，各国之间需要在当前不限成员名额工作组内继续讨论行动纲领的范围、结构和内容，以期就行动纲领的实质内容和方式达成共识。目标应该是，所有会员国在工作组 2025 年最后一届会议后紧接着举行的专门会议上核可这一行动纲领。

行动纲领的总目的是促进各国就执行在使用信息和通信技术(信通技术)方面的负责任国家行为的现行国际框架开展对话与合作，从而为网络空间的国际和平与安全作出贡献。为此需要：

- 根据从国际安全的角度看信息和电信领域的发展不限成员名额工作组 2021 年最后报告中商定的准则，以及第二次年度进展报告附件 C 中确认的能力建设商定原则，开展网络能力建设。利用与其他论坛所载机制的协同作用将有助于避免结构重叠和资源稀释。
- 建立信任措施，包括有效执行在第二次年度进展报告(A/78/265，附件 B)中商定的建立信任措施的不完全初步清单，特别是全球联络点名录。
- 在国际、区域间和区域各级交流最佳做法。
- 相关利益攸关方切实参与。

此外，行动纲领应成为常设平台，推动讨论现有和新出现的威胁以及国际法(包括国际人道法和人权)如何适用于各国使用信通技术问题。在行动纲领内应有可能进一步讨论并酌情发展网络空间负责任国家行为的国际框架，以适应和应对随时间演变的新威胁。

行动纲领应为工作组目前正在拟订的其他网络安全机制，如印度建议的网络门户和肯尼亚建议的网络储存库，提供总体体制框架。

行动纲领的总目标、具体目标和基本原则应以大会商定的政治宣言的形式确定。宣言应得到第一委员会决议的补充，说明行动纲领的任务、结构和方式。政治宣言和第一委员会决议都应基于上述将于 2025 年举行的专门会议的成果。

B. 行动纲领的任务、结构和方式

在吸取以往和现有文书的经验教训的基础上，行动纲领的任务设计应确保各国包容和透明地有效参与，并允许衡量负责任国家行为框架的执行进展情况，包括通过自愿报告机制，如联合国裁军研究所(裁研所)关于联合国从国际安全角度就各国负责任地使用信通技术的建议执行情况国别调查。国家之间以及与区域组织和非国家行为体的能力建设与合作，对于应对国家执行工作滞后领域至关重要。

根据在第二次年度进展共识报告中商定的共同要素，行动纲领的结构和方式应包括：

(a) 将在纽约总部举行的年度会议：

㈠ 审查和衡量框架和规定任务的执行进展情况；

㈡ 讨论框架的潜在演变，包括进一步增进对国际法在网络空间的适用的共同理解；

㈢ 通过关于具体专题的决定；

㈣ 就信通技术的使用对国际和平与安全造成的当前和新出现的威胁交流信息；

㈤ 进一步拟订网络能力建设措施；

㈥ 考虑到威胁形势的变化并认识到行动纲领是一项灵活机制，根据会员国的需要，考虑可能以渐进方式进一步发展行动纲领；

(b) 根据本届不限成员名额工作组建立的全球联络点名录，实施和进一步拟订建立信任措施。除了本身是一项建立信任措施外，该名录还应为执行第二次年度进展报告商定的不完全的全球建立信任措施清单提供基础，总体目标是减少网络空间中误解和冲突的风险。它还应用来讨论、通过和实施其他全球建立信任措施。通过促进制定和执行专门的建立信任措施，该名录将成为《行动纲领》的核心支柱，并侧重于实施现有框架；

(c) 每四至六年举行审查大会，以便根据网络空间的动态演变以及国际和平与安全面临的相关风险，对行动纲领进行可能的调整；

(d) 裁军事务厅担任行动纲领秘书处。除了筹备年度会议和审查大会外，该厅还将负责管理全球联络点名录和其他建立信任措施；

(e) 裁研所向各国提供相关的监测和审查工具(如第二次年度进展共识报告商定的规范执行情况核对表)，并开展与实施框架有关的研究活动；

(f) 在闭会期间举行更多技术工作流程会议的可能性。专门的技术工作流程除其他外，可侧重于推进网络能力建设、建立信任措施、国际法、包括国际人道法的适用以及当前和新出现的威胁等专题。对工作流程的参与应当是自愿的，向所有国家开放，并保持区域平衡。工作流程的数量和设置，包括利益攸关方的参与和会议频率以及可能的混合工作模式，应考虑到各国切实参与的能力，并应在年度会议上以协商一致方式决定。

各国应保留在行动纲领范围内就成果开展谈判并作出决定的专属权利。与此同时，纲领应有机制与非政府利益攸关方(多边和区域组织、民间社会、私营部门和学术界)接触。行动纲领应提供机会，让利益攸关方以类似于“拟订一项关于打击为犯罪目的使用信息和通信技术行为的全面国际公约特设委员会”的方式进行包容性和有意义的参与(特别是，会员国否决利益攸关方参与时应公开说明理由；排除利益攸关方应通过投票决定)。这包括有权在会议、审查大会和闭会期间另外召开的技术工作流程会议上发言和提交书面意见。此外，应为大多数形式的参与提供混合选项，以增加审议的包容性。

特别是在建立信任措施和能力建设方面，应利用区域和次区域两级或其他论坛的现有举措和结构，实现协同增效(例如与区域组织、世界银行网络安全多捐助方信托基金和全球网络专门知识论坛)。

联合国其他论坛的现有供资机制，如军控领域的拯救生命实体基金或联合国支持军备管制合作信托基金，可以为建立一个以培训和分享最佳做法的形式支持网络能力建设工作的机制提供有益指导。此外，可以设想实施一个研究金方案，促进发展中国家代表团的广泛资本代表性。

可以建立一个自愿的跨区域“伙伴关系制度”，将网络空间负责任国家行为框架执行能力强的国家与能力较弱的一个或多个国家配对。这种机制将加强各国之间的合作，促进对话和最佳做法交流，提高各国全面执行规范的能力。在这方面，欧洲安全与合作组织“采取建立信任措施”的做法可作为参考模型。

爱尔兰

[原件：英文
[2024 年 5 月 1 日]

爱尔兰是一个开放的社会，拥有高度互联的数字化经济，爱尔兰敏锐地意识到国际安全环境在恶化，特别是恶意网络活动增加。认识到这一点，我们已在国内采取行动，并与欧洲联盟伙伴一道提高应对能力，建设我们识别、预防和遏制威胁的能力，并促进以国际法和人权为核心的、开放、安全的全球网络空间。

然而，这一挑战的全球性要求国际采取全面对策，我们就该立场一直清晰明确。爱尔兰支持以协商一致方式制定联合国《关于在使用信息和通信技术(信通技术)方面负责任国家行为的规范框架》，并受此鼓舞。该框架是政府专家组(2010 年、2013 年、2015 年和 2021 年)和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(2021 年)提出的多项共识建议的重要产物。2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组两份最新年度进展共识报告也核可了该框架。

去年，爱尔兰公布了支持在网络空间适用国际法的国家立场，这是《规范框架》的四大支柱之一。爱尔兰致力于与欧洲联盟其他成员国和国际伙伴合作，根据《规范框架》采取行动，并通过在全球实施该框架促进和平与稳定。

爱尔兰认为，实施和加强《规范框架》对于维护网络空间的国际安全至关重要，因此应成为机构定期对话机制的核心。按照《行动纲领》提案中的具体设想，在本届不限成员名额工作组之后可能提出的机构定期对话未来框架确认，《规范框架》至关重要，并可让定期审查会议来审查框架。

爱尔兰一贯全力支持特殊对待《行动纲领》倡导的关于信通技术安全的机构定期对话，其为今后长期对话提出了一个注重行动的包容性机制。《行动纲领》做法将提供一个由联合国主持的、多利益攸关方参与的、包容区域的透明常设对话机制。如大会第一委员会各项决议所述，《行动纲领》得到了广泛支持，无论是在不限成员名额工作组的审议期间，还是在大会上广泛的各区域性国家组的投票上，一直如此。

确保所有国家都能利用信通技术的好处，同时通过能力建设措施降低风险，是《规范框架》的一个关键支柱，也是爱尔兰的一个优先事项。各国有责任缩小数字鸿沟，建设抵御恶意网络活动的应对能力。

第一委员会题为“从国际安全角度看信息和电信领域的发展”的第 78/237 号决议没有反映《规范框架》的重要性，也没有反映许多会员国表达的广泛观点，因此爱尔兰无法支持该决议。爱尔兰认为，该决议所提做法无法满足大多数会员国的需要。事实上，爱尔兰的结论是，该决议可能会破坏不限成员名额工作组过去几年来得以取得进展的基于共识的渐进方法。

爱尔兰仍然希望在本届不限成员名额工作组结束之前，以协商一致方式建立一个今后定期进行机构对话的机制，并将与所有国家合作，倡导一个反映《规范框架》的、着重行动的包容性方式。

关于如何开展特别是《行动纲领》做法的讨论包括提议举行年度正式会议，全年就具体政策问题进行不限成员名额的详细讨论并召开技术会议。技术小组可以讨论性别、数字鸿沟和非政府实体在实施准则性框架中的作用等问题。技术小组可以处理诸如性别、数字鸿沟和非政府实体在执行《规范框架》方面的作用等问题。技术工作流应是自愿的，对所有国家开放，而且，最后产生的业务结论要植根于实施《规范框架》的经验教训。

第一委员会各项决议倡导采用《行动纲领》做法，基于对一委这些决议的跨区域支持，这一特殊机制可加强同区域组织的区域互动和合作，以支持基于需求的能力建设。

令人鼓舞的是，拟议的《行动纲领》还将允许包括私营部门、学术界和民间社会在内的相关利益攸关方正式参与并与之定期磋商，以便就相关问题提供投入。爱尔兰大力赞成多利益攸关方参与机构定期对话，坚信这将更好地集中努力支持各国执行负责任的国家行为框架和受需求驱动的能力建设，以提高网络复原力。

为了在不限成员名额工作组任期结束前全面开展机构定期对话，爱尔兰支持在 2024 年和 2025 年组织闭会期间会议和不限成员名额工作组专门会议，包括讨论所涉预算问题。

日本

[原件：英文]
[2024 年 4 月 30 日]

1. 导言

日本支持制定一项推进网络空间负责任国家行为的行动纲领作为未来机制。日本认为，行动纲领是我们继续讨论网络空间负责任国家行为的适当论坛。行动纲领是一个注重行动的框架，应作为一个平台，支持各国努力执行商定的负责任国家行为规范和原则，为此鼓励分享最佳做法和查明各国面临的具体挑战。

《行动纲领》应是本届 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组的唯一后续机制，并在不限成员名额工作组完成任务后开始运作，以落实工作组的成果。行动纲领将在本届不限成员名额工作组任期结束后制定，不会实行双轨制。

日本愿为讨论尽可能作出最佳贡献，同时铭记行动纲领很有希望作为实际执行国际商定规范和原则的程式。

本文更新了 A/78/76 号报告所载日本国家贡献，考虑到大会第 78/16 号决议促成的进展以及在 2021-2025 年不限成员名额工作组内继续讨论情况。

2. 范围/目标

行动纲领的目的是推动维护和平与稳定以及促进一个开放、安全、稳定、无障碍及和平的信息和通信技术环境。

为此，行动纲领尤其应力求实现下列目标：

(a) 提出建议，指导各国努力执行负责任国家行为规范和原则；

(b) 鼓励自愿报告国家做法，以确定每个会员国的需求和挑战；

(c) 应受援国的请求，协助开展针对需求和挑战的能力建设；

(d) 具有包容性，并确保会员国和多利益攸关方广泛参与。

此外，行动纲领应成为推进经常性项目的常设平台，促进讨论现有和新出现的威胁、建立信任措施拟订事宜以及现行国际法如何适用于网络空间的问题。

3. 结构和内容

(a) 推动实施框架的结构

在明确《行动纲领》的范围、结构和内容时，《从各个方面防止、打击和消除小武器和轻武器非法贸易的行动纲领》的工作可作为参考。《小武器行动纲领》规定了国家、区域和国际各级的具体措施。然后，各国可就其法律和体制发展及其他做法提交自愿报告，并举行年度审查会议。

就网络行动纲领而言，自愿报告应包括一份核对表，列明每个国家执行规范的情况，例如每个国家或区域制定保护关键基础设施的政策、法律和准则的情况，以及事件应对情况。各会员国若还能具体说明并列出需要何种能力建设，会有意义。这项工作应有助于提供一个支持在各国执行规范的国家做法的框架。

行动纲领的结构和方式应包括每年或每年两次在联合国定期举行全体会议。行动纲领全体会议将能够通过并定期更新关于国家执行工作的可执行建议。例如，全体会议可确定框架执行方面的专题优先事项，如执行特定规范、现有和新出现的威胁、保护关键基础设施等。

为了支持进一步就此议题进行交流，全体会议可决定设立一个专门的工作流程，或不限成员名额的技术会议或工作组，在《行动纲领》全体会议闭会期间举行，并将其结论提交给下一次全体会议。

为补充关于框架今后发展的讨论，将在行动纲领框架内召开审查会议，会议频率待定，以期考虑到技术的快速发展，特别是不给发展中国家代表团造成负担。

本届不限成员名额工作组建立的全球联络点名录将成为《行动纲领》的一个组成部分，以落实和进一步制定建立信任措施。

(b) 能力建设

行动纲领将支持与执行框架有关的能力建设工作，确保多利益攸关方参与。

行动纲领有必要查明会员国在执行框架方面的能力差距，并利用现有的能力建设举措来弥补这些差距。

在行动纲领会议期间，可由其他组织(如东南亚国家联盟和日本网络安全能力建设中心、国际电信联盟和世界银行网络安全多捐助方信托基金)的代表通报情况，确保各机构开展的能力建设活动互为协调和补充。

行动纲领应发挥其作为联合国主持下的平台的作用，以便协同和利用其他区域组织当前正在开展的努力，而不是独自开展能力建设方案。

(c) 国际法和规范

2021 年 5 月，日本提交并公布了《日本政府关于适用于网络活动的国际法的基本立场》，重申包括《联合国宪章》全文在内的现行国际法适用于网络活动。日本就现行国际法如何适用于网络活动阐述了当前立场，重点阐述了日本对最

重要、最基本事项的看法。日本依然希望，各国政府宣布对适用于网络活动的国际法的基本立场，以及在国际和国内法院和法庭适用国际法，将加深国际社会对国际法如何适用于行动纲领所述网络活动的共识。

《行动纲领》还将通过建立自己的报告制度或倡导现有机制(如联合国裁军研究所关于联合国从国际安全角度就各国负责任使用信通技术的建议执行情况国别调查或提交秘书长的国家报告)，鼓励自愿报告国家执行工作。这种报告将为确定框架执行方面的优先事项提供依据，并摸清能力建设方面的需求。

行动纲领全体会议可以讨论如何深化将国际法用于网络空间的认识。还可以创建一个专门的工作流程，推动就现行国际法如何适用于网络活动进行交流。可以根据会员国的授权，利用专门工作流来交流国家意见，并开展情景讨论。这种专门工作流程可侧重于一般问题、国际法的具体概念或专题议题，如针对关键基础设施的网络行动，同时也涵盖国际法的相关原则。

(d) 多利益攸关方参与

无论是作为基础设施要素的所有者和运营者，还是作为社区代言，利益攸关方均是网络空间的核心。鉴于网络空间的相互关联性，让多利益攸关方社区参与联合国的讨论至关重要。

《行动纲领》将促进与多利益攸关方社区接触与协作，包括可以开展尽可能最佳的能力建设活动。

4. 制定今后机制的筹备工作和方式

日本支持在 2021-2025 年不限成员名额工作组内进一步进行有重点的讨论，以便进一步阐述今后机制。

拉脱维亚

[原件：英文]
[2024 年 4 月 30 日]

自 2003 年以来很长一段时间，使用信息和通信技术(信通技术)负责任国家行为框架一直列在大会第一委员会的议程上，并在数个政府专家组和不限成员名额工作组进行了讨论，这强调了负责任使用信通技术在维护国际稳定与安全方面日益重要。各国之间的合作对于有效应对网络空间日益增长的威胁和建立各国之间的信任至关重要。出于这些原因，现在是时候决定在联合国内建立一个常设机制来长远处理网络安全问题了。

在现代互联世界中，网络攻击变得比以往任何时候都更加复杂、更具破坏性和更加频繁。网络环境在不断发展。针对关键基础设施的网络攻击、出于政治动机的攻击、勒索软件攻击和恶意使用人工智能情况不断增加。因此，网络安全在国际安全辩论中的重要性毋庸置疑。

为了应对网络空间前所未有的恶意活动，拉脱维亚正在加强本国网络安全和应对能力。除其他外，拉脱维亚在国内和欧洲联盟内组织和开展网络威胁狩

猎行动，而且，我国政府机构与公民和公私实体分享知识和经验。2023 年和 2024 年，拉脱维亚与欧洲联盟其他成员国一道，多次公开谴责恶意网络活动，包括针对民主进程和机构的网络攻击。

关于在联合国主持下建立“机构定期对话”的提议此前在第一委员会讨论过，并记入 2019-2021 年不限成员名额工作组的最后报告。[1] 2019-2021 年不限成员名额工作组得出结论认为，今后进行机构定期对话的机制应是“一个有具体目标而且注重行动的进程，建立在以往成果的基础上、包容各方、透明、以达成共识为导向并以成果为基础”。[2] 在 2021-2025 年不限成员名额工作组 2023 年年度进展报告中，各国商定了共同要素，尤其是商定了国家主导的单轨常设机制。[3]

日益增长的网络威胁要求集中国家精力和资源，从长远加强各国之间的合作与信任，而不是讨论每几年产生新机制的方式，并冒着今后进展支离破碎的风险。拉脱维亚作为一个小国，支持促进有效利用有限资源的单轨办法。

针对建立一个常设机制以便采用连贯一致的长期做法促进各国使用信通技术负责任行为的呼吁，提出了一项行动纲领。[4] 大会 2022 年关于《行动纲领》的第 77/37 号决议[5] 和 2023 年关于《行动纲领》的第 78/16 号决议[6] 在大会上得到了各国广泛支持，这一倡议是以透明、包容和渐进的方式制定的。

《行动纲领》作为联合国常设机制

拉脱维亚认为，大会第 77/37 号和第 78/16 号决议大力授权着手制定《行动纲领》。《行动纲领》应成为第一委员会内一个包容、着重行动、由国家主导的常设机制，并成为所有国家参与的平台。其总体目标是促进加强国际和平与安全，防止国家间的冲突和误解。《行动纲领》涵盖事项应涉及按照国际法使用信通技术以及执行联合国网络空间负责任国家行为框架。如大会第 77/37 号决议所述，《行动纲领》将“考虑到”2021-2025 年不限成员名额工作组“通过的协商一致成果”。[7]

网络空间的稳定与安全将通过支持实施和酌情进一步发展[8] 基于国际法、包括《联合国宪章》全文在内的负责任国家行为框架予以推进。如政府专家组

[1] 2019-2021 年不限成员名额工作组的最后报告，第 68-74 段。

[2] 同上，第 74 段。

[3] 2021-2025 年不限成员名额工作组第二次年度进展报告(A/78/265)，第 55(a)段。

[4] https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber- PoA.pdf.

[5] 大会第 77/37 号决议，推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领。

[6] 大会第 78/16 号决议，推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领。

[7] 大会第 77/37 号决议，第 2 段。

[8] 大会第 76/19 号决议，序言部分第十段。

2013 年、2015 年和 2021 年报告以及不限成员名额工作组 2021 年和 2022 年报告所商定，国际法、包括国际人道法适用于在网络空间维护和平、安全与稳定，而且必不可少。

为推动执行负责任国家行为框架，行动纲领将支持基于需求的相关能力建设活动。重要的是，要推动能力建设方面的集体工作，并分享我们的经验和最佳做法，以提高国家和全球抵御网络威胁的能力。

年度正式会议可在《行动纲领》框架内举行。在正式会议之间，《行动纲领》的工作可在专事具体问题的技术工作组内安排。例如，一个技术工作组可致力于进一步增进对国际法如何适用于使用信通技术的认识。在正式会议上将通过技术工作组编写的建议。审查会议期间应定期审查《行动纲领》的其他优先事项。

技术小组可根据正式会议的决定予以设立和终止。技术工作组必须具有包容性，对所有国家开放，确保各国专家能够线下或线上(混合形式)参与。作出关于技术小组及其工作方式的决定应考虑到小国的能力和资源。

与利益攸关方——民间社会、私营部门、学术界——定期进行全面对话至关重要，应通过《行动纲领》加以促进。他们在不断发展的网络领域的专业知识非常宝贵，因此，他们的意见对推动落实负责任国家行为有重要意义。利益攸关方本身也“有责任以不危及和平与安全的方式使用信通技术”，[9] 因为是他们在推动发展新技术。

2024 年和 2025 年，应在 2021-2025 年不限成员名额工作组的其余届会和闭会期间会议上组织有重点的进一步讨论，以继续阐述《行动纲领》的不同方面，包括其制定方式。《行动纲领》应在 2021-2025 年不限成员名额工作组结束后投入运作。

荷兰王国

[原件：英文]
[2024 年 5 月 1 日]

导言

荷兰继续深为关切国家和非国家行为体恶意使用信息和通信技术(信通技术)对国际安全与稳定、经济和社会发展以及个人安全与福祉造成的风险日增。另据指出，世界日益互联互通，而各国在信通技术安全方面能力水平不同，可能增加脆弱性。

为了应对这些挑战，各国通过一系列政府间进程开展工作，制定了关于从国际安全角度使用信通技术负责任国家行为的不断演变的累积框架。大会通过各协商一致决议一再核可了这一框架。

[9] 2019-2021 年不限成员名额工作组的最后报告，第 10 段。

为了在这些成就的基础上进一步取得进展，荷兰强调有必要在根据大会第75/240号决议所设2021-2025年信息和通信技术安全和使用安全不限成员名额工作组结束本届任期工作后，建立定期机构对话。为此，荷兰支持关于制定推进从国际安全角度使用信通技术负责任国家行为的未来行动纲领的倡议，大会第77/37和78/16号决议对这项倡议表示欢迎。

根据题为“从国际安全角度看信息和电信领域的发展”的第78/237号决议执行部分第8段，荷兰谨此提交其对信息和通信技术安全和使用安全的看法和评估意见，特别是对今后在联合国主持下就这些事项定期进行机构对话的看法和评估意见。下述意见进一步借鉴了荷兰根据第77/37号决议为秘书长报告(A/78/76)提交的材料。

在2021-2025年不限成员名额工作组内，在就国际信通技术安全定期进行机构对话的未来机制寻找共同点方面取得了相当大的进展。在这方面，荷兰欢迎不限成员名额工作组《2023年年度进展报告》所载关于机构定期对话的“共同要素”。荷兰仍致力于在2021-2025年不限成员名额工作组内就此事项取得进一步进展。

范围和目标

荷兰重申大会第78/16号决议执行部分第4段，认为应在2021-2025年不限成员名额工作组结束后，不迟于2026年在联合国主持下建立一个包容各方和注重行动的常设机制，该机制具有大会第77/37号决议所述具体目标，以及2021-2025年不限成员名额工作组2023年年度进展报告中以协商一致方式商定的今后定期进行机构对话的共同要素。

荷兰支持在联合国主持下制定《行动纲领》的倡议，以促进在国际安全背景下网络空间负责任国家行为。《行动纲领》应基于不限成员名额工作组2023年年度进展报告中以协商一致方式商定的今后定期举行机构对话的共同要素，并以2021-2025年不限成员名额工作组的协商一致成果为基础，就范围、结构、内容和方式作出决定。

结构和方式

荷兰同意，行动纲领应当是一个包容各方、以达成共识为导向、以成果为基础的透明进程。行动纲领的任务可以源自一份创始文件，这份文件申明各国以网络空间负责任国家行为框架为指导的政治承诺，并制定一项机制进一步落实框架所定目标。

行动纲领应开放供所有联合国会员国、常驻观察员、政府间组织和其他组织以及专门机构参加。尽管各国对维护国际和平与安全负有首要责任，但行动纲领还应允许私营部门、学术界和民间社会等相关非政府利益攸关方切实参与，包括在正式场合参与。

《行动纲领》的结构可包括：

(a) 定期召开审查会议，评估不断变化的网络威胁形势和《行动纲领》举措，必要时更新框架，并提供战略指导；

(b) 举行不限成员名额全体讨论会，讨论当前和新出现的威胁，进一步讨论如何适用国际法，讨论建立信任措施的执行情况，确定能力建设的优先事项，审议规范、规则和原则执行情况，并为不限成员名额技术会议和实际举措提供指导；

(c) 举行不限成员名额技术会议和/或工作组，开展着重行动的讨论，向相关利益攸关方开放，并专门讨论具体问题。

制定行动纲领的筹备工作和方式

第 78/16 号决议、第 77/37 号决议和秘书长的报告(A/78/76)为制定《行动纲领》提供了初步路线图。2025-2026 年，在不限成员名额工作组结束工作后，荷兰设想举行一次向非政府利益攸关方开放的国际会议，在包括 2021-2025 年不限成员名额工作组等开展的筹备工作的基础上通过创始文件和(或)政治宣言。

未来机制中的能力建设

在不影响不限成员名额工作组的成果和大会关于建立未来机制的决定的情况下，荷兰提出以下要素，以促进网络能力建设，推动执行不断演变的累积框架，并加强这方面的国际合作。该提议围绕一个四步周期展开：

(a) 交流威胁情况，为此交流有关威胁的专门技术知识，并考虑如何从网络空间负责任国家行为共识框架的视角应对这些威胁；

(b) 自我确定能力需求，为此对照不断演变的负责任国家行为累积框架进行自愿报告。可以利用现有的自愿报告方法，例如裁研所(墨西哥-澳大利亚倡议)关于联合国从国际安全角度就各国负责任使用信通技术的建议执行情况国别调查；

(c) 按需匹配资源。未来机制可作为一个召集平台。此外，鉴于联合国的普遍性和公认性，联合国秘书处可在促进协调各组织和机构的网络能力建设工作方面发挥作用。未来机制可建立在现有工具基础上，如全球网络专门知识论坛 Cybil 门户网站，可能还有 2021-2025 年不限成员名额工作组目前正在审议的提案，如会员国提出的能力建设目录和全球网络安全合作门户网站；

(d) 建立一个反馈回路，各国可借此交流执行工作和网络能力建设活动方面的经验，这可为进一步讨论各国在国际安全背景下使用信通技术提供信息。

作为未来机制一部分的能力建设工作应根据不限成员名额工作组《2023 年年度进展报告》中商定的能力建设原则进行。

新西兰

[原件：英文]
[2024 年 4 月 30 日]

1. 20 多年来，网络安全一直是各国在联合国主持下讨论的一个议题。相继成立的工作组——政府专家组和不限成员名额工作组——得以就从国际安全角度看网络安全相关问题进行了定期交流。

2. 这些工作组取得了重要的奠基式成果，这些成果通过建立一个网络空间负责任国家行为框架，共同促进了国际安全与稳定，该框架已得到大会认可，并以四大支柱为基础：

- 国际法——所有联合国会员国都同意，国际法适用于国家在网络空间的行为
- 和平时期国家负责任在线行为规范
- 支持透明度、可预测性和稳定性的建立信任措施
- 旨在确保所有国家都能降低互联互通增加带来的风险、同时仍能从中受益的能力建设措施。

3. 新西兰完全赞同大会第 78/237 号决议决定在 2021-2025 年不限成员名额工作组会议结束后，至迟于 2026 年设立一个联合国主持下的、包容各方、注重行动的常设机制，其具有大会第 77/37 号决议申明的具体目标，具备 2021-2025 年不限成员名额工作组 2023 年年度进展报告中以协商一致方式商定的未来定期机构对话的共同要素。

4. 我们设想，在本届 2021-2025 年不限成员名额工作组结束时，以联合国第 77/37 号和第 78/237 号决议通过的提议为基础，将这一机制作为联合国在国际安全背景下讨论网络安全的“永久场所”。我们欢迎并支持法国代表一个跨区域集团提出的决议，该决议提供了一个明确、透明的途径，让所有国家以补充本届不限成员名额工作组的方式审议未来机制的范围、结构、内容和方式。在这方面，我们支持制定具备以下特点的行动纲领：

(a) 充当 2025 年后联合国网络安全讨论的单一常设机制，确保可预测性和机构稳定性。开展谈判商定常设机制的方式，从长远来看也可提高效率。目前各届工作组重新审议和商定工作方式需要进行冗长、反复的谈判，占用了重要的实质性讨论时间；

(b) 立足于经商定的、包括与国际法和国际人权法义务保持一致的网络空间负责任国家行为框架，确保行动纲领依托历届政府专家组和不限成员名额工作组的奠基式工作并在此基础上进一步推进，从而促进网络负责任国家行为；

(c) 包容多利益攸关方参与，其中包括(对网络空间的国际和平与安全负有责任的)政府、企业、民间社会、技术专家、学术界和其他组织，推动建设自由、

开放、安全和可互操作的互联网。新西兰对纳入非政府利益攸关方(以发言和提交书面报告等形式)参与讨论的方式表示支持，这些讨论包括任何正式和非正式会议以及审查会议；

(d) 注重行动，包括注重推动负责任国家行为框架的切实行动，并注重推动支持各国执行框架以及执行问责和监测机制的能力建设措施；

(e) 可灵活并作出调整，以应对新兴威胁。

俄罗斯联邦

[原件：俄文]
[2024 年 4 月 9 日]

关于设立一个就信息和通信技术安全和使用安全有决策职能的不限成员名额常设工作组的概念文件

共同起草者：白俄罗斯共和国、布基纳法索、布隆迪共和国、古巴共和国、朝鲜民主主义人民共和国、马里共和国、缅甸联邦共和国、尼加拉瓜共和国、俄罗斯联邦、苏丹共和国、阿拉伯叙利亚共和国、厄立特里亚国、委内瑞拉玻利瓦尔共和国、津巴布韦共和国

联合国 2021-2025 年信息和通信技术(信通技术)安全和使用安全不限成员名额工作组的讨论表明，国际社会要求在联合国主持下就此问题建立一个单一的常设决策机制。我们认为，这种机制的最佳形式是不限成员名额工作组，此种工作组已在实践中证明了自己的效力和意义。

具有决策职能的未来不限成员名额常设工作组的任务应侧重于通过切实执行 2021-2025 年不限成员名额工作组达成的协议，进一步促进开放、安全、稳定、无障碍及和平的信通技术环境。属于任务范围的问题包括：

- 继续制定关于国家负责任行为的具有法律约束力的规则、规范和原则，并建立有效的执行机制，作为确保国际信息安全的未来普遍条约的要素；
- 就国际法如何适用于信通技术的使用以及现有规范如何适应信息空间的特性(其跨界层面、匿名和有无可能采用隐藏功能)形成共识；
- 制定和实施建立信任措施和国家间切实合作机制，包括通过被授权实体/机构之间的既定联络渠道和全球政府间联络点名录，应对与信通技术及其使用相关的信息安全威胁，并防止全球信息空间中的国家间冲突；
- 建立机制和方案，协助各国提高保护本国信息资源的能力，同时考虑到具体需要。

未来的不限成员名额常设工作组应遵循下列原则：

- 开放、包容、民主和透明；

- 在联合国大会第一委员会的主持下，各国在促进关于各国使用信通技术安全问题对话方面发挥主导作用；
- 遵守《联合国宪章》各项原则(国家主权平等、不使用武力和不以武力相威胁及和平解决国际争端)；
- 任何决定均以协商一致方式且仅由各国做出；
- 不应在联合国几个谈判平台上重复进行确保信通技术安全和使用安全的国际努力；
- 与以往不限成员名额工作组和政府专家组的共识成果和建议的连续性；
- 灵活性并能随着各国需求的变化和新的信通技术安全挑战的出现而不断发展。

程序问题：

- 在不限成员名额常设工作组内作出的任何决定都应由各国以协商一致方式核准(这一参数应在设立不限成员名额常设工作组的大会决议中明确说明)；
- 时间线：不限成员名额常设工作组应在本届不限成员名额工作组结束时开始工作，每年在纽约联合国总部举行两届正式会议(所有会员国都应无一例外地派代表参加)；
- 报告形式：向联合国大会提交进度报告，每两年以协商一致方式予以通过；
- 结构：联合国会员国可视需要决定设立附属分组，以更详细、更深入的方式处理具体方面任务。然而，此种分组的会议不应同时举行，以确保所有代表团都能充分参与；
- 治理：不限成员名额常设工作组的工作应由一个主席团进行，主席团由一名主席、两名副主席、一名报告员和(如有需要)分组主席(也具有副主席的地位)组成。主席团的组成应由各国在公平地域分配的基础上，每两年以协商一致方式核准，并从每个区域组轮流产生。

最好为不限成员名额常设工作组提供一个机制，在商定决定后迅速予以正式确认(根据默许程序，随后在下届会议上核准)。应采取实际步骤，通过适当的电子门户网站，让各国之间继续交流信息。

不限成员名额常设工作组与有关区域组织和协会合作将是有益的，为此，工作组主席可与各国家组磋商，而且每年可与其代表举行一次闭会期间会议。

非国家行为体(非政府组织、企业界及科学与学术界)对不限成员名额常设工作组工作的参与应纯属磋商的、非正式性的；例如，通过每年举行一次闭会期间会议。只有经核可的(各国协商一致同意的)非国家行为体才有权作为观察员出席正式活动。

新加坡

[原件：英文]
[2024 年 5 月 1 日]

新加坡仍然致力于就网络安全问题进行包容性的全球公开对话，在这方面，我们认为，所有国家承诺今后进行单轨定期机构对话至关重要。今后的单轨定期机构对话对于促进普遍接受和认可 1998 年以来所有会员国在联合国商定的不断演变的使用信息和通信技术(信通技术)负责任国家行为累积框架以及为进一步发展和实施这一框架提供一个共同的全球平台至关重要。在这方面，所有国家都要能够集中精力于单一进程，确保讨论仍有实质性，而不是支离破碎。资源有限的小国和发展中国家也会无法可持续地参与双轨并行进程。

新加坡认为，我们应继续依托 2021-2025 年信通技术安全和使用安全不限成员名额工作组第二次年度进展报告(A/78/265，第 55 段)中商定的定期机构对话的四个共同要素，建立我们就单轨常设机制达成共识所需的信任和信心。

各国须利用剩余的有限时间和空间，努力在本届不限成员名额工作组内就定期机构对话的前进方向达成共同愿景。当务之急是建立共识。在这方面，新加坡支持巴西在不限成员名额工作组第七届实质性会议上所作提议，即在本届不限成员名额工作组于 2025 年结束工作之前，暂停在大会第一委员会提出有关信通技术安全的决议。我们支持不限成员名额工作组主席继续就定期机构对话的前进方向开展讨论，以期进一步发展和完善关于这种对话的共识提案。

下一步，我们认为，本届不限成员名额工作组在未来机制内就会议范围、结构、目标和频率达成一致意见会富有成效。回答这些实际问题是在所有国家已经商定的共同要素基础上更进一步的合乎逻辑的方式。这样做还会让各代表团、特别是资源有限的小代表团早日明确其 2025 年后的工作，让它们可以开始进行必要的规划，以充分利用其有意义的参与。为了确保为普遍的单轨常设机制奠定可持续基础，新加坡还强调，未来机制的设计必须足够广泛和包容，以便利今后继续讨论所有代表团的提议和优先事项。特别是，定期审查常设机制的运作情况会有益，以确保我们的做法切合不断变化的威胁形势。在这方面，新加坡支持主席 2024 年 2 月 20 日关于常设机制要素草案的讨论文件中所述做法和结构。新加坡期待着与所有代表团进行建设性合作，进一步完善这些要素草案，以期在本届不限成员名额工作组第三次年度进展报告中以协商一致方式予以通过。

土耳其

[原件：英文]
[2024 年 5 月 1 日]

信息和通信技术已成为社会和经济不可或缺的一部分，影响到生活的方方面面。这些技术被个人和国家用于许多领域。如今，国家开发和利用技术的技

能在发展和增长中发挥着重要作用。从交通运输到通信，从国防工业到医学科学，从生产到教育和贸易，信息技术已成为几乎每个领域发展的主要因素。

研究表明，未来几年技术发展趋势将加快。其中，能够带来新的技术标准和新的业务领域，并对现有领域进行重大变革的企业将脱颖而出。物联网、5G、大数据、区块链、人工智能、无人驾驶汽车和智能机器人被视为将照亮我们现在和未来的技术。

另一方面，这些技术在为我们提供诸多机遇的同时，也带来了网络安全风险。网络威胁的结构正变得越来越复杂，数量也与日俱增，据研究，2022 年全球将有超过 4.93 亿次勒索软件尝试。[1]

在这方面，网络安全是技术健康发展和融合的每个阶段都需要解决的问题。信息和通信系统的安全漏洞可能会导致这些系统无法使用或被滥用，或造成生命损失、大规模经济损失、扰乱公共秩序和(或)侵犯国家安全。

确保网络安全不仅是在技术密集的领域应对威胁的必要条件，而且也是影响各国福利和国家安全的重要因素，因为它给社会和经济生活带来了风险。有鉴于此，各国在网络安全领域投入了大量资金，开发网络安全技术，努力确保其在网络环境中的安全，提高抵御攻击的能力。

在我国，应对网络威胁被视为一项国家政策。在这方面，交通运输和基础设施部在战略层面上开展了确保国家网络安全的研究，信息和通信技术局在技术层面上开展了研究。此外，其他机构和组织也为这些研究作出贡献。

作为自 2012 年以来开展的研究的一部分，已制定并实施了《国家网络安全战略和行动计划》。最近，根据《2020-2023 年国家网络安全战略和行动计划》开展了以下方面的研究：全天候保护关键基础设施的网络安全；提高网络事件应对小组的能力；社会各阶层安全使用网络空间；保持高度的网络安全意识；与国家利益攸关方和国际利益攸关方共享信息和开展合作；制定确保保护、最大限度地减少网络犯罪和提高威慑力的机制。

此外，交通运输和基础设施部已开始研究制定新的网络安全战略和行动计划，涵盖 2024-2028 年。在此背景下，正在继续开展研究，以确保所有利益攸关方之间的有效合作，增加网络安全威胁情报的获取、制作和共享，提高国家应对网络事件的准备水平，开发专家人力资源，开发快速检测和早期响应机会，并对关键部门和基础设施进行风险分析。

土耳其网络应急小组(隶属于信息和通信技术局的土耳其国家网络应急小组)自 2013 年以来负责协调土耳其的网络事件应对工作。除了网络威胁检测和网络事件应对(包括事前、事中和事后)外，土耳其网络应急小组确保实施针对网络威胁的预防措施，并确保网络威慑。

[1] www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide.

土耳其网络应急小组网络安全的主要重点领域是：

- 网络能力建设
- 技术措施
- 收集和传播威胁情报
- 保护关键基础设施

在改善国家网络安全的背景下，2013 年以来还成立了 14 个关键部门/基础设施(如能源、医疗卫生、银行和金融、水管理、电子通信和关键公共服务)的部门网络应急小组和 2 200 多个机构网络应急小组。所有网络应急小组在土耳其网络应急小组的协调下全天候工作，以减轻网络风险并应对网络威胁。土耳其网络应急小组使用检测和预防工具进行监测，并使用报告工具与相关方分享信息。土耳其网络应急小组为土耳其境内的所有网络应急小组开发了信息共享平台，以便发布警报、警告和安全通知。该平台提供了一个高效安全的通信渠道。

网络安全演习是合作和防范的另一项重要活动。这种在国家和国际层面进行的演习有助于加强网络空间和测试针对潜在网络威胁采取的措施。自 2011 年以来，交通运输和基础设施部组织了 7 次国家网络安全演习和 2 次国际网络安全演习。最近，在国家一级，举行了“网络盾牌 2022”演习。继“网络盾牌 2022”之后，在我国交通运输和基础设施部以及信息和通信技术局的合作下，“金融部门网络盾牌 2022”演习于 2022 年 10 月 20 日至 21 日举行，公共机构和组织参加了演习。在这些演习中，通过土耳其网络应急小组内部开发的技术基础设施和场景，参与者获得了实际的网络安全体验，并分享了在潜在网络攻击情况下应采取的步骤。计划在今后一段时间内组织一次国际网络安全演习。

网络安全是一个摆在全世界议程上的问题，需要在国际层面作出努力。区域和全球层面的合作以及网络安全领域的信息和情报共享在帮助各国应对网络风险和威胁方面发挥着重要作用。在此背景下，土耳其正在开展这一领域的双边、区域和国际合作；参与联合国、北大西洋公约组织(北约)、欧洲安全与合作组织(欧安组织)、二十国集团、经济合作与发展组织、经济合作组织、发展中八国组织、区域军控协助中心–安全合作中心、突厥语国家组织等国际组织的政策和战略制定活动，并做出贡献。此外，土耳其网络应急小组通过其在事件应对和安全小组论坛、可信引导者、国际电联、网络安全共同进步联盟、北约恶意软件信息共享项目和伊斯兰合作组织计算机应急小组等国际平台的成员资格，继续开展网络威胁情报共享活动。我国还作为赞助国参加了北约合作网络防御卓越中心，并且是北约虚拟网络事件支持能力机制的成员。此外，还与许多国家签署了关于网络安全的谅解备忘录和双边合作协定。

土耳其网络应急小组已被 MITRE 公共漏洞和暴露方案接纳，在这方面，它为第三方软件、硬件或产品的漏洞指定公共漏洞和暴露号码，在漏洞管理方面提供流程协调。

土耳其加入了若干多边网络安全协定。土耳其批准了欧洲委员会《网络犯罪公约》(《欧洲条约汇编》第 185 号)。土耳其还为拟订一项关于打击为犯罪目的使用信息和通信技术行为的全面国际公约特设委员会开展的研究做出了贡献。此外，土耳其是《推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领》的共同提案国之一，并坚决支持联合国大会第 77/37 号决议，支持进一步努力将《行动纲领》建成一个永久性、包容性和以行动为导向的机制。

1. 土耳其全国网络安全组织

在信息和通信安全领域，特别是土耳其的网络安全领域，值得注意的是，该领域的进展可追溯到 1991 年。1991 年，网络犯罪被加进《土耳其刑法》(第 765 号)，[2] 土耳其在网络安全领域的征程由此开始。从那时起，土耳其在网络安全的各个领域取得了里程碑式的重要成就，网络安全是国家安全的重要组成部分。以下是截至 2012 年实施的各项举措的非详尽清单：

- 1999 年，土耳其制定国家信息基础设施总体规划。[3]
- 2002 年，启动电子土耳其倡议行动计划。[4]
- 2003 年，提出土耳其电子转型项目与 2003-2004 年短期行动计划。[5]
- 2004 年，颁布《电子签名法》(第 5070 号)[6] 和《土耳其刑法》(第 5237 号)。[7]
- 2006 年，发布《2006-2010 年信息社会战略和行动计划》。[8]
- 2007 年，成立土耳其计算机事件应对小组协调中心。
- 2007 年，颁布《关于互联网出版物和打击利用此类出版物实施犯罪的法律》(第 5651 号)。[9]
- 2008 年，《电子通信法》(第 5809 号)[10] 与第一次国家网络安全演习同时实施。

[2] https://www.mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf.

[3] http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/991000_TuenaRapor.pdf.

[4] http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/020800_E-TurkiyeEylemPlani.pdf.

[5] https://webdosya.csb.gov.tr/db/cbs/icerikler/2005-20180522115122.pdf.

[6] https://kamusm.bilgem.tubitak.gov.tr/dosyalar/mevzuat/kanunlar/kanun.pdf.

[7] www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm#1.

[8] http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf.

[9] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf.

[10] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf.

- 2010 年发布的《国家安全委员会宣言》承认网络威胁的全球影响及其对国家安全的影响。
- 同年，土耳其实现与《欧洲委员会网络犯罪公约》(《布达佩斯公约》)(《欧洲条约汇编》第 185 号)接轨。
- 根据部长会议关于管理和协调国家网络安全工作的决定，2012 年成立了网络安全委员会，[11] 同年还成立了土耳其科技研究委员会信息学和信息安全研究中心网络安全研究所。[12]

这些里程碑标志着该领域的重大进展。如上所述，在土耳其的议会制政体时代，部长会议于 2012 年 6 月 11 日批准了一项关于执行、管理和协调国家网络安全研究的决定。[13] 根据这一决定，设立了网络安全委员会，[14] 并责成当时的交通运输、海洋事务和通信部(现交通运输和基础设施部)履行委员会秘书处的职责，并与有关机构协调网络安全活动。[15]

在过去十年中，土耳其网络安全领域的发展步伐明显加快。主要的里程碑包括：启动该国第一个《2013-2014 年国家网络安全战略和行动计划》，[16] 建立国家网络事件应对中心[17] (设在信息和通信技术局内)[18] 以及发布概述网络事件应对小组创建、作用和工作原则的宣言。[19] 此外，在《2013-2014 年国家网络安全战略和行动计划》的框架内，在公共机构和组织内设立了网络事件应对小组(机构网络事件应对小组、部门网络事件应对小组)。网络事件应对小组是机构和部门组织，旨在快速识别网络环境中的威胁和潜在攻击，并制定和共享解决这些攻击所造成问题的措施。因此，这些小组的目标是向机构和组织提供网络应对技能。目前，有 14 个部门网络事件应对小组在国家网络事件应对中心的协调下开展工作，2 100 多个机构网络事件应对小组正在努力保护土耳其的网络环境。

2012 年在土耳其武装部队内设立的网络防御中心后来发展成为网络防御司令部。同样，2011 年在安全总局内设立的打击网络犯罪司后来于 2013 年改组。

2014 年颁布的第 6518 号法律[20] 在网络安全领域引入了一些规定——在 2008 年颁布的规范电子通信部门的第 5809 号法律中增加条款。根据第 5809 号法律的

[11] https://www.btk.gov.tr/siber-guvenlik-kurulu.

[12] https://bilgem.tubitak.gov.tr/en/sge/.

[13] https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf.

[14] www.btk.gov.tr/siber-guvenlik-kurulu.

[15] www.uab.gov.tr/.

[16] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf.

[17] www.usom.gov.tr/.

[18] www.btk.gov.tr/.

[19] www.usom.gov.tr/hakkimizda.

[20] www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm.

新增条款，成立了由公共机构高级管理人员组成的网络安全委员会，由交通运输、海洋事务和通信部部长担任主席。上述法律第 5 条增加了(h)项，规定交通运输、海洋事务和通信部的职责是“确定确保国家网络安全的政策、战略和目标，制定行动计划，开展网络安全教育和提高认识活动”。

根据该法规，网络安全委员会被指定为负责最终批准和有效执行交通运输、海洋事务和通信部确定的国家政策、战略和行动计划的主要机构。该委员会还负责就与确定关键基础设施有关的提案作出决定，并确定哪些机构和组织可免受与网络安全有关的全部或部分规定的约束。

2016 年，颁布了关于个人数据保护的第 6698 号法律[21] 和《2016-2019 年国家网络安全战略和行动计划》。[22] 此外，信息和通信技术局获得根据这一时期的需要制定的第 671 号法令[23] 的授权——该法令规定“信息和通信技术局应采取或需要采取各种措施，保护公共机构和组织以及自然人和法人免受网络攻击，并对这些攻击提供威慑”。随后，在国防工业主席团(现为国防工业秘书处[24])的协调下，于 2017 年启动建立土耳其网络安全集群，并完成了个人数据保护委员会的任命，该委员会开始开展活动。

2018 年，随着第 703 号法令的颁布，网络安全委员会被废除。[25] 该法令宣布，该委员会的职责和任务将移交给“总统指定的一个委员会或当局”。然而，尽管任命了一些与这些职责有关的部分人员，但迄今为止，这些职责尚未正式移交给任何委员会或机构。随着向总统制政体过渡，决策过程也发生了变化。制定政策的权力已移交给共和国总统。政策委员会的任务是制定和发展这些政策(第 1 号总统令，[26] 第 20-22 条)，而各部委则负责执行这些政策。

自 2018 年 7 月 10 日起，随着总统制政体下第 1 号总统令的实施，“制定与网络安全有关的政策和战略建议”的职责被分配给在总统领导下运作的安全和外交政策委员会(第 1 号总统令，第 36/1/ğ 条)。根据第 1 号总统令，“制定加强信息安全和网络安全的项目”的职责分配给了土耳其共和国总统府[27] 数字化转型办公室，特别是数字化转型办公室下属的网络安全司。[28] 该司的职责包括：

- 根据总统制定的政策，为公共机构和关键基础设施制定网络安全战略。
- 监测进展情况，以有效实施全国网络安全政策、战略和行动计划。

---

[21] https://kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law.

[22] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf.

[23] www.resmigazete.gov.tr/eskiler/2016/08/20160817-18..htm.

[24] www.ssb.gov.tr/Default.aspx?LangID=2.

[25] https://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3-1.pdf.

[26] https://www.mevzuat.gov.tr/mevzuatmetin/19.5.1.pdf.

[27] https://cbddo.gov.tr/en/.

[28] https://cbddo.gov.tr/en/department-of-cyber-security/.

- 开展研究以确定关键基础设施。
- 促进公共部门、私营部门和大学之间的合作，促进国家网络安全生态系统的发展。
- 开展研究，以在各部门(特别是关键基础设施)开发国内和本国网络安全产品，并在公共部门推广使用。
- 执行预防和保护活动，以保护关键技术和信息资产。
- 研究如何在运营关键基础设施的公共机构和组织中建立和管理信息安全系统，这包括制定技术标准和程序，以及监测和指导应用的原则。

此外，根据 2018 年 7 月 10 日官方公报发布的第 1 号总统令成立了国家技术局，[29] 设在工业和技术部[30] 下。该局在网络安全方面的职责如下：

- 提高信息技术和先进技术产品与系统的网络和信息安全成熟度；
- 开发国内和本国网络安全产品；
- 在全国范围内扩大国内和本国产品的使用；
- 增强数据中心和数据处理基础设施；
- 通过各种激励计划支持网络安全生态系统。

总之，各种法律、法规和其他立法指定了若干机构来监督国家网络安全。这些机构的网络安全相关职责来自这些不同的立法。与大多数其他国家类似，土耳其的网络安全被认为是多个政府实体的共同责任。数字化转型办公室同交通运输和基础设施部开展了与制定网络安全战略和政策有关的研究。每个组织在其各自的领域内都有自己的一系列角色和责任。

2. 数字化转型办公室在网络安全方面的角色和责任

在 2018 年过渡到总统制政体后，根据第 1 号总统令成立了土耳其共和国总统府数字化转型办公室，该总统令于 2018 年 7 月 10 日在官方公报上发布后生效。随后，2019 年 10 月 24 日发布的第 48 号总统令扩大了数字化转型办公室的任务。[31]

数字化转型办公室的成立标志着土耳其数字化工作的新时代和思维方式的转变。自其成立以来，公共部门的数字化转型开始采用一种更加一致和全面的机构间方法。因此，除了实现更快、更透明和更有效的行政管理外，该办公室还旨在集中协调、管理和运营不同机构根据公共部门的技术发展、社会需求和改革趋势分别开展的数字化转型活动。此外，该办公室旨在从战略和实践上统

[29] https://www.sanayi.gov.tr/merkez-birimi/c03f1f3bae27/hakkimizda.

[30] https://www.sanayi.gov.tr/anasayfa.

[31] https://cbddo.gov.tr/en/governance-and-responsibilities.

一协调与网络安全、国家技术、大数据和人工智能有关的活动，并有效实施高级别战略。因此，在数字化转型办公室的协调下，为保护土耳其的数字基础设施并使其成为具有威慑力的网络强国，制定了宏观层面的目标并实施了相关举措。

数字化转型办公室在网络安全领域有以下职责，包括制定政策法规，建立网络安全生态系统，提高公众意识，能力建设，加强公共基础设施和制定标准：

- 根据总统确定的政策，为公共机构和关键基础设施制定网络安全战略。
- 制定支持国家网络安全和信息安全的项目。
- 跟踪在全国范围内有效实施网络安全政策、战略和行动计划的进展情况。
- 致力于确定关键基础设施。
- 向有关部门提出对哪些机构和组织免于适用全部或部分网络安全规定的建议。
- 通过加强公共部门、私营部门和大学之间的合作，为创建国家网络安全生态系统做出贡献。
- 确定网络安全的优先领域，将私营部门的能力引导到关键领域，防止重复投资。
- 致力于在各个领域(主要包括关键基础设施)开发地方和国家网络安全产品，并在公共部门扩大此类解决方案的使用。
- 开展预防和保护活动，保护关键技术和信息资产。
- 在公共机构和运营关键基础设施的组织中建立和运行信息安全管理系统，确定技术标准、程序和原则，监测和指导实施工作。

目前，数字化转型办公室是管理我国公共机构和关键部门网络安全问题的主要机构。除了履行网络安全委员会的职责外，该办公室还与所有机构合作，在全国范围内协调战略和行动计划的制定和有效执行。

3. 数字化转型办公室在政策制定方面的活动和项目

尽管对网络安全的概念有不同定义，但其简单而包容的定义可以表述为：一门应用于网络空间各个点的安全学科，涵盖信息技术的各个组成部分。鉴于第四次工业革命被认为是一场旨在汇集信息技术和所有重要机制的革命，预计网络安全学科将作为这场革命中在安全方面的调整融入我们的生活学科。

如果执行安全纪律时不按照安全纪律行事，就会出现安全和隐私问题。从全国范围考虑，突出的战略目标是保护关键基础设施、确保各机构和组织之间的安全数据共享以及将来源和目的地为国内的数据流量保持在国内。其目的是

通过基于风险的分析和规划方法，提高机构、部门和国家对网络事件的防备水平。

为了确保数字世界的安全，各国政府制定和公布网络安全战略，并指定相关机构负责确保其实现和进行监督。我国在这方面也履行了自己的义务。由于我国在交通运输和基础设施部的协调下就这一问题开展了工作，分别公布了以下战略：

- 2013-2014 年国家网络安全战略和行动计划[32]
- 2016-2019 年国家网络安全战略和行动计划[33]
- 2020-2023 年国家网络安全战略和行动计划[34]

上述国家网络安全战略和行动计划正在取得进展，以整体的方式确保连续性，其中包括确保已进入我们生活的新技术安全的措施。

在数字化转型办公室的支持下，最新的《2020-2023 年国家网络安全战略和行动计划》[35] 已于 2020 年 12 月 28 日发布。该战略和行动计划旨在支持我国经济发展，保障社会生活和国家安全，并将我国定位为网络安全领域的国际品牌。在这方面，该战略侧重于与土耳其网络安全愿景和使命相一致的四年期相关政策，并旨在进一步推进以往战略所取得的成绩。《2020-2023 年国家网络安全战略和行动计划》确定的战略目标分为八大支柱：

- 保护关键基础设施并增强韧性
- 国家能力建设
- 有机的网络安全网络
- 新一代技术的安全性
- 打击网络犯罪
- 发展和培养国家和国内技术
- 将网络安全融入国家安全
- 加强国际合作

[32] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf.

[33] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf.

[34] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf.

[35] https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/national-cyber-security-strategy-2020-2023.pdf.

3.1 战略和行动计划监测系统

开发了战略和行动计划监测系统，以有效管理和监测总统府编制的战略和行动计划，以及土耳其网络安全集群在数字化转型办公室内开展的活动。该系统跟踪各项行动的进展情况，并根据预定目标评估其绩效和成绩。

此外，数字化转型办公室还负责支持科学、技术和创新政策委员会协调的政策制定活动，包括：

- 网络安全和通信基础设施技术国家政策提案
- 关于 5G 及以后的下一代通信技术的国家政策建议
- 国家网络安全技术路线图

3.2 2023 年总统年度计划中的措施

根据《2020-2023 年国家网络安全战略和行动计划》，数字化转型办公室直接负责或与之直接相关的 2023 年总统年度计划[36] 中的措施如下：

- 将更新国家网络安全战略，加强网络安全法规和技术基础设施，并建立强有力的协调结构。
  - 将制定网络安全框架立法。
  - 将制定《2024-2027 年国家网络安全战略和行动计划》。
- 将确定并实施在关键基础设施中建立信息安全管理系统的程序和原则。
  - 将更新《信息和通信安全指南》。
- 为了使网络安全生态系统受益，并开发该领域附加值更高的产品和解决方案，将开发由公共研究机构和大学参与的网络安全产品和技术项目，并以开放源码的形式与网络安全生态系统共享这些项目的成果。
- 将努力加强国家网络安全生态系统，提高其国际竞争力。
  - 将举办国际网络安全商业论坛。
  - 将启动国内网络安全产品推广平台，以建立一个生态系统，使所需的国内网络安全产品得以成熟和出口。
- 为培养网络安全领域的合格劳动力，将开发职业院校的网络安全课程并制定职业标准。
  - 将完善开设网络安全课程的职业学校的现有网络安全课程。

[36] https://www.sbb.gov.tr/wp-content/uploads/2022/11/2023-Yili-Cumhurbaskanligi-Yillik-Programi.pdf.

- 将确定从开设网络安全课程的职业学校毕业的学生的职业名称，并制定相关标准。

3.3. 2024 年总统年度计划中的措施

根据《2020-2023 年国家网络安全战略和行动计划》，数字化转型办公室直接负责或与之直接相关的 2024 年总统年度计划[37] 中的措施如下：

- 将提高网络应对能力和安全成熟度水平，以应对金融市场面临的网络安全威胁。
  - 将公布一项关于确保国家网络安全和加强网络威慑的法规，以涵盖金融部门。
- 将支持与网络安全领域的国际标准保持一致，并支持土耳其参与国际联合项目。
  - 考虑到国际标准和欧洲联盟立法，将完成关于物联网安全的二级立法。
- 考虑到欧洲联盟的网络和信息安全指令(NIS2)及其在网络安全领域的新努力和国际最佳做法，将发布确保国家网络安全的法规。
  - 将公布一项关于确保国家网络安全和加强网络威慑的法规。
  - 将开展对物联网安全性进行监管的研究。
  - 将对物联网设备进行网络安全检查。
  - 将确定国家网络安全框架立法所需的二级法规，相关准备工作正在进行中。
  - 将就第 5070 号《电子签名法》和其他相关立法开展工作，为远程签名服务提供法律依据。
  - 将开展宣传活动，扩大远程签名服务在公共机构和私营部门的使用。
- 将确保国家网络安全活动的最高级别协调，并建立有效的协调和管理结构，以促进机构间合作。
  - 将公布专门的网络安全立法，规范国家网络安全组织的职能、职责和责任。
  - 将协调编制《2024-2028 年国家网络安全战略和行动计划》的准备工作，并将建立数字环境下行动和活动的监督机制。

[37] https://www.sbb.gov.tr/wp-content/uploads/2023/10/2024-Yili-Cumhurbaskanligi-Yillik-Programi.pdf.

- 将努力制定国家网络安全应急和危机管理计划。
- 将加强网络威胁情报共享网络。

- 将通过增加资源的多样性和开发人工智能和大数据分析应用，加强网络威胁情报的获取和共享过程，并努力及早发现和预防对国家网络安全的威胁。
  - 将对网络威胁情报资源进行需求分析。
  - 将加强事件应对和协调能力。
  - 将启动由人工智能和大数据分析支持的网络安全项目，以检测网络钓鱼域、恶意软件命令和控制中心以及僵尸网络。
- 将确定并实施在关键基础设施中建立信息安全管理系统的程序和原则。
  - 将对在关键基础设施中建立信息安全管理系统进行流程分析。
  - 将为在关键基础设施中建立信息安全管理系统开展监管工作。
- 将在关切领域建立网络安全标准。
  - 将对《欧洲联盟网络安全法》建立的认证框架进行研究，并确定网络安全产品、服务和流程所需的标准。
  - 与行业信息和通信安全准则有关的条款将纳入《信息和通信安全指南》。
  - 将开发一个模型，以确定根据《信息和通信安全指南》应接受审计的关键企业。
  - 将根据《信息和通信安全指南》为审计进程做准备。
  - 将开展有关《信息和通信安全指南》的宣传活动。
- 将开发网络安全测试基础设施。
  - 将对网络安全应用和研究中心、网络安全试验台和大学集成实验室的现状进行分析。
- 将增加国内网络安全产品的使用，特别是公共机构的使用。
  - 将为网络安全部门的发展及其参与全球市场制定路线图。
- 将制定培训合格劳动力的计划，增加网络安全领域的就业机会。
  - 将为合格青年雇员组织网络安全竞赛。
  - 将开展合作与协调活动，以确定网络安全领域工作人员的职业标准。

- 将改进培训内容、质量和环境，以便根据网络安全部门的需求培训劳动力。
  - 将开展在线和基于实验室的网络安全培训。
  - 将通过信息和通信技术局学院继续开展在线网络安全培训。
  - 应用网络安全培训将在费蒂赫网络培训中心举行。
- 将开展研究，以提高公众对网络安全的认识。
  - 将开展研究，以开发中小学网络安全课程内容。
  - 将制定《信息和通信安全指南》合规和审计程序以及关于信息安全意识的培训计划。
  - 将举办研讨会、培训及比赛等活动以提高网络安全意识。
- 将加强公共机构实施信息和通信安全措施、建立、运行和审计信息安全管理系统的机制。
  - 将为确保信息和通信安全的程序和原则制定二级法规。
  - 将对属于公共机构和组织的域名的使用和监测进行立法和基础设施研究。

4. 数字化转型办公室关于法规和网络安全指南的活动和项目

数字化转型办公室开展了重要活动，通过采取措施保护公共部门和私营部门免受网络威胁，提高国家应对能力。这些工作的主要目标包括改进网络安全法规和政策、建立审计机制、防止关键基础设施被供应商锁定、确保安全的技术改造和保护国家数据。一些正在进行的研究总结如下：

- 已经制定了一项法规草案，以确定有关公共机构和组织托管的网站安全以及“gov.tr”子域名分配的程序和原则。
- 已编写了确保信息和通信安全的法规草案，以规定实施信息和通信安全措施的技术要求。此外，法规草案还包括建立、实施、维护、审计和持续改进信息安全管理系统的规定，以防止或减轻信息安全风险。该法规草案规定的要求适用于所有公共机构。
- 正在制定国家网络安全法。该法旨在通过独特的“网络安全治理框架”处理国家网络安全治理和组织问题，该框架与技术发展相适应，并将提高国家对当前网络威胁的应对能力。

本节的其余部分总结了已经实施或完成的计划。

4.1 关于信息安全措施的第 2019/12 号总统通告

信息的日益数字化、直接获取信息的便捷性、基础设施的数字化以及信息管理系统的激增带来了严重的安全风险。在此背景下，发布了《关于信息安全

措施的第 2019/12 号总统通告》，[38] 以降低所遇到的安全风险，并确保可能威胁国家安全或扰乱公共秩序的重要类型数据的安全。该通告包括提供关键基础设施服务的公共机构和私营部门应遵守的 21 项基本信息和通信安全措施。[39] 为确保数据得到保护，总统通告旨在确保一个国家拥有的数据留在该国境内。此外，报告强调，制定和使用国家网络安全解决方案是土耳其的主要优先事项之一。最后，报告还指出，“应在数字化转型办公室的协调下编写《信息和通信安全指南》，以减轻和消除安全风险，特别是确保关键数据的安全”。

4.2 《信息和通信安全指南》

除了上述关于信息安全措施的第2019/12号总统通告，2020年发布了《信息和通信安全指南》文件。[40] 该指南的主要目的是确定详细的网络安全措施，以确保可能导致扰乱公共秩序或可能威胁国家安全的关键信息/数据和基础设施的安全。该指南是在这一领域发布的第一份国家参考文件，强调有必要制定一项涵盖信息和通信安全所有方面的全面安全战略。该指南在加强公共机构和关键基础设施服务提供商的网络防御能力方面发挥着重要作用。此外，《关于信息安全措施的第 2019/12 号总统通告》和《信息和通信安全指南》都要求产品供应商声明其产品没有任何后门。

4.3 《信息和通信安全审计指南》

为实现《信息和通信安全指南》所订目标并确保成果的持续性，数字化转型办公室编制了《信息和通信安全审计指南》，[41] 并于 2021 年 10 月公布，其中确认信息和通信安全可通过有效的审计及监督活动实现。

提供关键基础设施服务的公共机构、组织和企业应在《信息和通信安全指南》规定的期限内完成其合规活动，并至少每年进行一次审计研究，以确保其所开展的活动和采取的措施符合规定。

范围内的各组织不仅要遵守《信息和通信安全指南》的要求，还要对安全措施的有效实施情况以及实施过程是否符合相关要求进行定期审计和评估。因此，至少每年一次的定期审计应由内部审计部门或经认可的第三方审计公司进行。范围内的各组织必须进行的审计政策和程序记录在数字化转型办公室于2021年发布的《信息和通信安全审计指南》中。

4.4 信息和通信安全审计员/公司认证计划

信息和通信安全审计员/公司认证计划旨在提供确定将根据《信息和通信安全指南》执行合规性审计的公司和审计员的资格和能力所需的技能。该计划正

[38] https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf.

[39] https://cbddo.gov.tr/en/presidential-circular-no-2019-12-on-information-security-measures.

[40] cbddo.gov.tr/en/icsguide/.

[41] https://cbddo.gov.tr/en/icsaguide/.

在与土耳其标准研究所和土耳其科学技术研究委员会合作实施。自 2021 年以来，共有 163 名审计员和 23 家公司根据认证计划获得认证和授权。

4.5 信息和通信安全合规和审计监测系统

信息和通信安全合规和审计监测系统[42] 已开发，并于 2023 年 1 月 4 日投入使用。该系统可监测《信息和通信安全指南》所涵盖的所有组织的审计结果。自那时以来，已有 2 945 名用户和 1 191 个组织在该系统注册。各组织可提供有关其遵守《信息和通信安全指南》情况和审计活动的进展信息。各组织信息安全管理系统的当前合规水平也可通过该数字平台进行跟踪。

4.6 国家网络安全治理模型分析和报告项目

国家网络安全治理模式分析和报告项目旨在审查土耳其的网络安全治理模式，该项目已经完成。通过对不同国家的案例进行比较分析，提出了改进建议。因此，制定了土耳其“网络安全治理框架”。

项目完成后，于 2022 年 12 月 13 日举办了国家网络安全讲习班，分享国家网络安全治理模式分析和报告项目的成果。40 多家公共机构和 100 多名与会者在讲习班上交流了意见和建议。根据讲习班的结果，确定有必要制定国家网络安全法。该法的定稿工作正在进行中。

5. 数字化转型办公室在网络安全生态系统方面的活动和项目

5.1 土耳其网络安全集群

2017 年 10 月，公共部门机构，学术界和私营部门的主要网络安全公司受邀讨论这些机构之间可能的合作，从而建立了土耳其网络安全集群。[43] 如今，该集群在数字化转型办公室和国防工业秘书处的协调下运作，拥有 200 多个成员，提供 400 多种产品和服务。自 2018 年起，土耳其网络安全集群也是“合作创新和网络安全全球生态系统”的成员。

土耳其网络安全集群追求几个目标，包括：

- 增加网络安全公司的数量
- 支持成员公司发展技术、行政和财务能力
- 改进产品和服务的品牌建设
- 提高网络安全生态系统的标准
- 提高成员公司在国内和全球市场的竞争力
- 提高网络安全领域的人力资本

[42] cbddo.gov.tr/en/bigdes/.

[43] https://siberkume.org.tr/.

- 提高全社会对网络安全的认识

虽然私营部门没有参与这种合作的法律义务，但公共部门与私营机构之间的互信与合作一直是重点。这一努力背后的主要动机是加强买方与供应商的关系、共同的分销渠道、联合社交机会以及大学与公司开展的研发活动，这些活动可以为双方创造更好的机会和利益。由于共同的经济利益，集群中的公司变得比单独经营的公司更有生产力，更有创新性，因此更具竞争力。

如果没有最高级别公共当局的支持，通常不可能在网络安全领域取得成功。土耳其拥有在海外扩张的公司，也有合格、独特的网络安全产品在海外销售。其中一些产品也包含在加特纳报告中。入侵和攻击模拟类别就是其中之一。

5.2 对外经济关系委员会 - 数字技术商业委员会 - 网络安全委员会

为提高国内和本国公司在海外的效率，在数字化转型办公室的支持下，在对外经济关系委员会的协调下，数字技术商业委员会[44] 于 2022 年 6 月成立。数字技术商业委员会致力于开展以下项目：

- 土耳其数字技术生态系统的全球化
- 适应新趋势
- 获得国际融资、数字化转型和监管

数字技术商业委员会的目标是：

- 增加《财富》500 强中土耳其公司的数量和土耳其独角兽公司的数量
- 使土耳其成为技术中心，并与其他国家建立数字走廊
- 加强土耳其高科技产品出口
- 通过对外经济关系委员会的 144 个双边商业委员会促进科技公司的国际化
- 通过与初创企业合作，支持工业企业的数字化转型
- 通过创建平台，汇集全球风险资本、国内风险资本、规模企业和初创企业，增加该行业风险资本的规模和数量
- 找出该行业面临的问题，并向相关政府机构通报这些问题

数字技术商业委员会下设以下小组委员会：云技术、金融技术、移动技术、游戏、网络安全、软件技术、创新技术、风险投资、医疗卫生技术、Web 3 区块链。可以看出，在这个结构中有部门视角，网络安全也是一个小组委员会。

在土耳其，开发网络安全领域的国内技术具有重要战略意义，并被视为国家安全问题。因此，重点在于创造可与国外同类产品和服务相媲美的强大、大

[44] https://www.deik.org.tr/sectoral-business-councils-digital-technologies-business-council?pm=65.

规模产品和服务。随着人们对数据风险和威胁的认识不断提高，全球网络安全市场最近出现了显著增长。网络安全产品和服务的市场份额预计将继续增加。

土耳其是这一不断扩大的经济的一部分，与私营部门和政府机构合作，在全球范围内开发其解决方案。因此，数字化转型办公室正在努力加强国内网络安全技术。这项工作是第1号总统令规定任务的一部分。该总统令规定：开展研究，以在各领域(特别是关键基础设施)开发国内和本国网络安全产品，并在公共部门推广使用。

为了鼓励“国内网络安全生态系统”的发展，在数字化转型办公室的协调下启动了一项系统性方法。该方法旨在将激励制度与公共采购相结合，评估国内网络安全产品的成熟度，并逐步加强和扩大这些产品。

“国内网络协调小组”于 2021 年在数字化转型办公室的协调下成立，由国防工业秘书处、工业和技术部、国家供应办公室、公共采购局和战略和预算主席团领导。财政和金融部、土耳其科学技术研究委员会、土耳其标准研究所、土耳其卫星通信公司、交通运输和基础设施部以及信息和通信技术局后来也加入了该小组。小组的主要目标是鼓励在国内外所有部门使用国内和本国的网络安全产品，主要侧重于公共部门。该小组的活动分为五大支柱：政策、立法、标准化/成熟度、激励/支持/融资和国际化。

6. 数字化转型办公室提高网络安全意识的活动和项目

6.1 “技术节”网络安全竞赛

数字化转型办公室意识到，鉴于信息和通信技术(信通技术)的重要性，对网络安全意识和技能的需求日益迫切。在这方面，数字化转型办公室也举办竞赛，以提高网络安全意识。其中一个优秀项目是“非法侵入伊斯坦布尔”。它被公认为是一项全球性的非凡竞赛，自 2018 年以来一直作为“技术节”(航空、航天和技术节)[45] 的一部分举办。这些竞赛向世界各地的所有黑客敞开大门，让他们在伊斯坦布尔展示自己的才华，竞赛名为“非法侵入伊斯坦布尔”。只有 2020 年的竞赛在加济安泰普举行，名为“非法侵入措伊格码”。2022 年 8 月，数字化转型办公室在宗古尔达克举办“2022 年非法侵入黑海”竞赛。

“2023 年非法侵入大师”竞赛于 2023 年 4 月 23 日举行，报名于 2023 年 3 月截止。最终入围者是在网上赚取赏金阶段确定的。在 4 月 28 日举行的决赛阶段，选手们要面对一个以智能设备网络安全为主题的情景。黑客们试图通过寻找智能家居设备、管理这些设备的移动应用程序以及接收这些设备数据的云基础设施中的漏洞来入侵系统，并试图接管系统。

每年的竞赛内容都会涉及不同的概念，如操作技术系统安全、漏洞赏金或“夺旗”网络安全挑战。这些竞赛旨在提高人们的网络安全意识，并为该行业

[45] www.teknofest.org/en/.

输送新人才。另一方面，该项目的一个间接好处是在全球范围内宣传土耳其的网络安全。

“2024年非法侵入大师”竞赛[46]的申请截止日期为2024年5月31日，决赛阶段将于2024年8月作为“技术节”的一部分在伊斯坦布尔举行。[47]

6.2 网络情报竞赛

此外，数字化转型办公室还与国家教育部、青年和体育部等相关公共机构、私营部门和非政府组织合作，组织了几个网络安全营和培训项目以及“夺旗赛”。这些训练营和培训项目确保激励足够多的年轻人在网络安全领域发挥自己的才能。还必须指出，参加这些活动的学生人数超过100万。

此外，另一个优秀活动是网络情报竞赛。[48]网络情报竞赛是培训和加强意识活动的一部分，旨在让更多人具有网络安全意识，在这方面，这些竞赛非常有效。共有150万名小学、初中和高中学生参加了竞赛。

该竞赛是一项在线活动，针对小学、中学和高中分别举办。试题由数字化转型办公室准备，并在国家教育部的支持下根据现行课程最终确定。通过数字化转型办公室、国家教育部和教育信息网络平台的社交媒体账户发布公告。在竞赛中，在最短时间内给出最多正确答案的学生将获得惊喜礼物和奖励，以提高他们在这一领域的积极性。

第四届网络情报知识竞赛于2023年举行。该竞赛于2020年10月首次举办，由总统府和国家教育部合作组织，分别针对小学、初中和高中。小学生组的竞赛于2023年12月27日举行，中学生组于2023年12月28日举行，高中生组于2023年12月29日举行。本次竞赛共有16 915名小学生、15 955名初中生和4 528名高中生报名。

6.3 《数字队员》卡通

数字化转型办公室在全国范围内开展了许多关于提高网络安全意识的研究，并认识到即使儿童不上网也需要提高数字素养。这不仅仅是技术知识，而指的是使儿童在数字世界中既安全又有能力的知识、技能和态度。为此开发的一个针对儿童的重要项目是一部名为《数字队员》[49]的流行卡通片。该系列卡通片自2020年起在土耳其广播电视台儿童频道播出。该项目的主要目标是提高儿童的数字认知、素养和意识。《数字队员》系列包括10集，内容是与数字化转型办公室合作编写的。各集内容涉及广泛的主题，从儿童安全上网到网络欺凌，从网络成瘾到人工智能，从物联网到数字化对生活和国家技术的影响。

---

[46] https://hackmasters.com.tr/.

[47] www.teknofest.org/en/competitions/hack-masters/.

[48] https://cbddo.gov.tr/en/projects/cyberintelligencecontest/.

[49] https://www.youtube.com/watch?v=YnuLs6GAogM&ab_channel=CBDijitalD%C3%B6n%C3%BC%C5%9F%C3%BCmOfisi.

7. 数字化转型办公室在网络安全教育方面的活动和项目

毫无疑问，确保国家网络安全的最重要组成部分之一是具有足够能力和专门知识的人力资源。为了满足我国在这一领域的需要，数字化转型办公室开展了提高现有人力资源能力水平的活动。其中一些举措详述如下。

7.1 与土耳其共和国国家教育部合作开办网络安全职业高中

已采取具体步骤，在正规教育中发展网络安全领域的技能和能力，因此，2020 年开始为中等教育阶段编制课程。

伊斯坦布尔技术园职业技术安纳托利亚高中是土耳其的第一所网络安全高中，由国家教育部在土耳其网络安全集群、国防工业秘书处、数字化转型办公室和伊斯坦布尔技术园的协助下建立。该学校位于伊斯坦布尔技术园，提供信息技术、网络管理和网络安全领域的教育。

网络安全职业高中自开办之日起就一直是首选学校。

7.2 与土耳其共和国高等教育委员会合作建立网络安全职业学院

数字化转型办公室启动了一个新项目，通过进一步发展上述网络安全职业高中应用的模式，培养网络安全领域的合格人才。随着数字化转型办公室与高等教育委员会于 2022 年签署合作议定书，[50] 网络安全职业学院迈出了第一步。

仅提供网络安全领域教育课程的网络安全职业学院于 2023 年开办。这些学校开设的第一门课程是“网络安全分析师和操作员”。[51] 该课程已在土耳其的 4 所主要大学启动：安卡拉大学、埃格大学、盖布泽技术大学和伊斯坦布尔技术大学。

8. 全球指数中的土耳其

由于数字技术在地方和国家层面的应用，网络安全已成为与国家实体安全同等重要的问题。鉴于威胁日益严重，公共部门和私营部门已在网络安全领域进行了充分投资。在公共、私营和军事领域开展了许多协调项目；重要的国防工业组织进行了大量投资；在学术领域建立了专门的网络安全研究所；依靠国家力量开发了新产品和新技术。由于这些努力，土耳其近来已成为网络安全领域最成功的国家之一。

由于政府和公共部门行为体为实现这些目标所做的努力，土耳其在全球网络安全指数中的排名受到了积极影响。

土耳其在全球网络安全指数中排名靠前，反映了该国迄今为止所取得的成就。

[50] https://cbddo.gov.tr/projeler/siber-myo/.

[51] cbddo.gov.tr/sss/siber-myo/.

根据国际电信联盟(国际电联)于 2021 年发布的全球网络安全指数，[52] 土耳其在全球排名第 11 位，较上一年上升 9 位，在欧洲排名第 6 位。

在当今的全球格局中，信通技术发挥着不可或缺的作用。信通技术是我们社会的筋骨，将全球各地的经济、政府和个人错综复杂地联系在一起。想象一个没有即时通信、无法无缝获取信息或无法以电子方式开展业务的世界，那将是一个截然不同的现实。信通技术已明显影响到人类生活的方方面面，从知识传播、医疗保健提供到娱乐和社交领域。信通技术赋予公民权力，促进突破性创新，并以前所未有的速度推动经济增长。此外，政府可以利用信通技术的力量，以更高的效率、透明度和包容性提供服务，促进更具参与性和更强大的民主框架。

然而，这种互联模式在带来巨大好处的同时，也有一个重要的隐患，那就是安全问题。随着我们对信通技术的依赖不断扩大，我们面临的脆弱性也随之增加。恶意行为体，从谋求个人利益的网络罪犯到怀有地缘政治目的的国家支持的实体，都会利用这些漏洞，将关键基础设施、存放敏感数据的政府系统以及公民的个人信息作为目标。信通技术基础设施的全球互联性质形成了一个相互依存的复杂网络，世界某个偏远角落的一次安全漏洞可能会在其他地方产生连锁反应，可能会扰乱基本服务，造成经济困难，并削弱公众信心。人工智能和物联网等新技术的出现带来了全新的安全挑战，需要立即关注并开发创新解决方案，因为这些技术通常会在保护庞大的互联设备网络方面引入新的攻击载体和复杂性。

因此，当务之急是在利用信通技术的巨大潜力与减少相关风险之间保持明智的平衡。各国必须优先重视信息和通信技术的安全，并将其视为国家安全的当务之急。这需要采取多方面的办法。最重要的是制定强有力的国家网络安全战略，并辅之以强有力的公私伙伴关系，充分利用政府和行业的专业知识和资源。

政府与企业合作，投资于对公民和政府官员的网络安全教育和认识，同样至关重要。这种教育不仅应包括识别和减轻网络威胁的技术技能，还应促进公民的网络安防文化。

此外，促进信通技术安全方面的国际合作至关重要。在这方面，在联合国框架下定期进行机构对话非常重要。会员国必须共同努力，建立一个促进网络空间负责任行为的国际规范、标准和法律框架。这一框架应包括促进对网络威胁作出快速反应的信息共享协议、更有效打击网络犯罪的合作执法努力，以及制定确立网络空间可接受行为规范的国际条约。归根结底，目标不仅仅是采取单纯的防御性措施，而是要建设一个有韧性的信通技术基础设施。这包括设计的系统不仅要有抵御网络攻击的能力，还要有快速恢复、尽量减少中断和保持数据完整性的能力。此外，促进以合乎道德的方式开发和使用信通技术也很重要。会员国可以通过优先考虑用户隐私，倡导负责任的研究做法，最大限度地

[52] www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

减少滥用的可能性，以及确保信通技术系统开发和部署的透明度，确保这一强大的技术为人类价值观的更大利益服务。

通过在促进创新的同时优先考虑安全问题，会员国可以确保信通技术在塑造我们的世界中继续发挥变革性的积极作用。这种合作方式，加上持续的警惕和适应，对于确保人人享有安全和繁荣的数字未来至关重要。

美利坚合众国

[原件：英文]
[2024 年 5 月 1 日]

导言

联合国会员国承认，信通技术有可能被用于有违维护国际和平与稳定目标的目的。多年来，各国在联合国主持下齐聚一堂，讨论并处理这一问题。各国经协商一致，肯定了从国际安全角度看信息和电信领域的发展政府专家组和 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组的报告，从而围绕关于信通技术使用问题负责任国家行为的框架凝聚了共识。这个旨在加强国际稳定的框架由以下内容构成：接受相关国际法包括《联合国宪章》； 一套不具约束力的规范；建立信任措施。

虽然这个框架在全球得到支持，但框架要取得成功，取决于各国遵守并执行框架内容。正如 2015 年政府专家组的共识报告所述，各国申明，有必要在联合国主持下建立有广泛参与的定期机构对话。[1] 不限成员名额工作组在这项努力的基础上继续推进，不断重申各国有必要为今后的机构对话建立一项机制。[2]

此外，在不限成员名额工作组最近协商一致的年度进展报告中，各国商定了定期机构对话的一套初步共同要素，并商定继续讨论今后的《行动纲领》。重要的是，各国商定，今后定期的机构对话应将“关于《负责任的国家行为框架》的协商一致协议作为其工作的基础”。[3] 各国还同意，今后的对话应是单一轨道、国家主导和常设的。[4] 各国还得出结论，该机制将是开放、包容、透明、可持续的和灵活的，[5] 以便能够根据需要适应快速演变的网络威胁形势。秘书长于 2023 年 4 月发布了一份报告(A/78/76)，其中强调了制定《行动纲领》的紧迫性，并着重指出不限成员名额工作组 2023 年年度进展报告中确定的共同要素所涉及的许多相同问题，包括该框架“必须作为”《行动纲领》的“基线”。[6]在报告中，秘书长还得出结论认为，许多国家重视非政府利益攸关方的包容性和有意义的

[1] A/70/174，第 18 段。

[2] A/75/816，第 70-74 段；A/78/265，第 52 段。

[3] A/78/265，第 55(c)段。

[4] 同上，第 55 (a)段。

[5] 同上，第 55 (d)段。

[6] A/78/76，第 42 段。

参与。[7] 各国继续呼吁多利益攸关方切实参与不限成员名额工作组的正式会议和闭会期间会议。

在过去两年中，各国已围绕《行动纲领》形成合力，将其作为联合国第一委员会讨论网络问题的未来常设机制。最近，几乎所有联合国会员国都投票赞成第 78/16 号决议，大会在该决议中决定在当前信息和通信技术安全和使用安全不限成员名额工作组结束工作后，在联合国主持下建立该机制。

如该决议所述，《行动纲领》将作为联合国的一个常设但灵活的机制，推动该框架的工作，以加强网络空间的和平与安全，包括通过与多利益攸关方群体进行有意义的接触，以及通过联合国作为信息共享平台的作用促进能力建设。

《行动纲领》的范围

大会第 77/37 号决议对《行动纲领》的范围和任务规定如下：

> “一个常设、包容各方、注重行动的机制，讨论现有和潜在的威胁；支持各国的能力和努力，以负责任国家行为框架为指导，履行和推进各项承诺，其中包括关于国家在使用信息和通信技术时适用国际法的自愿、不具约束力的规范，以及建立信任和能力建设措施，如大会第 76/19 号决议、政府专家组 2010 年、2013 年、2015 年和 2021 年报告、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 2021 年报告以及 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组第一次年度进展报告所申明；讨论并酌情进一步发展这一框架；促进与相关利益攸关方的接触与合作；并定期审查在执行行动纲领方面取得的进展以及行动纲领今后的工作”。[8]

大会在第 78/16 号决议中重申了第 77/37 号决议所阐述的《行动纲领》的目标，并决定该机制将具有不限成员名额工作组 2023 年进展报告中概述的共同要素。此外，大会还决定，《行动纲领》的范围、结构、内容及方式将基于不限成员名额工作组的协商一致成果。

在确认政府专家组和不限成员名额工作组报告的《行动纲领》决议和协商一致决议中，各国一再申明，期望各国在行动中以 2010 年、2013 年、2015 年和 2021 年政府专家组及 2021 年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评估和建议以及目前不限成员名额工作组的协商一致产品（如第一次年度进展报告和第二次年度进展报告）、特别是“通过这些进程拟订并以协商一致方式通过的关于在使用信息和通信技术方面负责任国家行为不断演变的累积框架”为指引。[9] 这一共识框架由政府专家组和不限成员名额工作组协商一致的报告阐述，并一再得到所有会员国的赞同，是《行动纲领》的基础。

---

[7] A/78/76，第 40 段。

[8] 大会第 77/37 号决议，第 1 段。

[9] 大会第 78/16 号决议，序言部分第 8 段。

会员国将确定《行动纲领》的方向，并随时间推移修订纲领，同时始终优先注重框架的实际执行工作以及专门用于执行框架的能力建设工作。《行动纲领》具有常设性质，这将使其成为各国在开展这些工作时的一项持久资源。

《行动纲领》作为常设机制，还应能灵活调整应对未来威胁，并可敏捷评估各国不断变化的需求以及应对这些威胁的最佳做法。在《行动纲领》中，各国还可以考虑共识框架是否以及如何随着时间的推移而演变。

非国家利益攸关方将是《行动纲领》进程的组成部分。几乎所有国际或国内的能力建设工作都涉及私营部门、民间社会、学术界和其他非国家利益攸关方的活动和专门知识。《行动纲领》的参与方式必须尽可能包容各利益攸关方，以便充分利用这些利益攸关方的专门知识。

《行动纲领》的设立

成员国必须争取在 2021-2025 年不限成员名额工作组结束后，于 2025 年顺利过渡到《行动纲领》。这种过渡必须通过不限成员名额工作组的最后报告来推动，该报告应重申大会第 77/37 号决议以共识框架为基础确定的《行动纲领》的任务，阐明其面向行动的架构和工作方法，确定优先工作领域，确认对利益攸关方的参与采取最大程度的包容性办法，并确定到 2026 年正式启动《行动纲领》的下一步措施和详细时间安排。

为全面确定《行动纲领》的模式，可能需要多召开一次筹备会议或再开展一个进程。此外，如果不限成员名额工作组未能就最后报告达成共识，则需要通过联合国大会召开一次更全面的“国际会议”[10] 或通过大会建立其他筹备进程，以履行第 78/16 号决议中概述的在 2026 年之前启动《行动纲领》的指示。《行动纲领》会议必须在 2026 年开始，以确保这些重要的多边讨论的连续性。

鉴于《行动纲领》的任务是处理信通技术使用的和平与安全层面，自然将在联合国第一委员会下设立。裁军事务厅应顺理成章成为这一未来机制的秘书处。《行动纲领》应尽可能在现有预算资源范围内运作。

结构

《行动纲领》的结构应包括每年举行三至四次会议的各技术工作组、年度全体会议和定期审查会议。《行动纲领》将由联合国裁军事务厅内的一个秘书处办公室提供支持。

为使这些工作组尽可能具有包容性，将邀请所有有关国家组成重点小组，共同制定支持执行《框架》的具体建议。这些建议将纳入报告，供全体会议审议，并最终供大会审议。

[10] 大会第 77/37 号决议，第 3 段。

这些工作组必须由跨区域人员组成，并采取跨领域办法来实施框架，就下列问题提出建议、进行评估和采取最佳做法：

- 保护关键基础设施；
- 在发生严重网络事件后促进国家之间的合作；
- 加强对网络空间不负责任的国家行为的问责的方法；
- 分享有关不断变化的网络威胁形势的信息；
- 提高各国遏制和瓦解信通技术威胁的能力。

以问题为基础的讨论将有助于就框架的实施开展跨领域的实质性讨论，打破威胁、规范、国际法和能力建设等传统的各自为政的局面。在不限成员名额工作组会议上，各国反复强调，这些议题相互交织，需要通盘考虑。各国还一致认为，能力建设尤其贯穿所有议题。在各实施工作组内优先讨论能力建设需求，将提出现实可行的建议，并加快实施速度。

应授权年度全体会议评估各技术工作组的进展情况，推进这些工作组提出的任何建议，讨论当前和新出现的威胁，并审议建立信任措施等实际举措的状况。全体会议可根据需要为技术工作组和实际举措提供指导。

定期审查会议应每三年或四年举行一次（取代会议当年的年度全体会议），供所有会员国评估不断变化的网络威胁状况、《行动纲领》倡议和工作组的成果，必要时更新《框架》，并为《行动纲领》未来的全体会议、工作组和其他倡议提供战略方向和任务授权。对《行动纲领》的这种定期审查将使各国能够根据情况的变化灵活调整《行动纲领》。

2026 年《行动纲领》启动后，第一委员会每年都将通过决议或决定确认《行动纲领》年度会议的协商一致成果。第一委员会还将确认定期审查会议的成果。

《行动纲领》秘书处由裁军事务厅运作，其任务是支持《行动纲领》各次会议的行政管理工作；维护信息共享平台、通信机制和档案；管理实际举措和项目，如联络点名录、威胁储存库和信息共享门户网站。

能力建设

鉴于各国在发展网络知识和技能方面出于各个不同阶段，联合国已认识到“能力建设对于各国在信息和通信技术安全领域开展合作和建立信任至关重要”。[11] 联合国可发挥关键作用，召集并协调积极参与相关网络问题能力建设的多利益攸关方行为体，突出介绍这一系列行为体，并按照会员国指示执行具体能力建设方案。

[11] 同上，序言部分第 20 段。

《行动纲领》的主要能力建设职能必须与各国在国家一级执行框架的工作直接挂钩。《行动纲领》还应促进专门讨论各国为执行框架需要何种能力建设，从而确保行动框架的工作契合各国不同的具体需求。换言之，《行动纲领》应旨在提高国际社会对网络能力建设重要性的认识，以支持该框架，促进与其他利益攸关方就现有网络能力建设项目进行协调和信息共享，同时还提供指导和最佳做法，供各国在地方/国家一级实施该框架时使用。

美国认识到，许多国家仍然缺乏对该框架及其重要性的深入了解。许多国家还缺乏着手实施该框架所需的国家一级网络安全能力，包括与支持性规范和建立信任措施有关的国内当局和能力。目前有一系列联合国和非联合国实体在国家网络安全政策和战略、网络事件管理和关键基础设施保护、国内网络犯罪立法、网络安全文化和网络安全标准以及国际网络安全援助的捐助方协调和匹配等领域拥有专门知识。《行动纲领》不应重复或取代现有的此类努力。所有这些项目——主要是多利益相关方性质的项目——都能加强各国的国家安全态势，并最终使框架得以实施，尽管它们不属于《行动纲领》的任务范围。

多利益攸关方的参与

各国必须保留在《行动纲领》范围内的专属决策权。然而，包括民间社会、学术界、区域和国际机构以及私营部门在内的非政府利益攸关方在多边论坛中发挥积极作用，为正式讨论带来专门知识，并为能力建设工作作出贡献。相关的非国家利益攸关方必须有机会作为观察员积极参与《行动纲领》并作出贡献，但无表决权。非政府利益攸关方的专门知识在技术组或工作组内将特别重要。这些技术工作组将促进与一系列非国家利益攸关方进行更深入、更务实的接触。利益相关方还可以定期提交报告，介绍他们为实施以《框架》为重点的举措所做的努力，包括能力建设。

为使《行动纲领》(包括在其附属技术工作组内)尽可能包容相关利益攸关方，其模式应建立在利益攸关方参与的现有黄金标准基础上，包括对各国反对意见具有透明度和评估可能排除参与的程序。例如，各国可以参考借鉴老龄问题不限成员名额工作组。老龄问题工作组的模式为会员国提供了反对某个组织参与的机会，但要求公开提出反对意见，让会员国了解，并随后进行表决，以确定是否应将遭到反对的组织排除在外。在第一轮中没有会员国反对的组织自动获准参加正式会议。[12]

除了考虑如何认可利益攸关方出席《行动纲领》会议之外，模式还应就经认可的利益攸关方如何在实践中为《行动纲领》的讨论做出贡献提供指导。在这方面，拟订一项关于打击为犯罪目的使用信息和通信技术行为的全面国际公约特设委员会可作为一个模式。特设委员会模式允许多利益攸关方参与，包括：

- 出席任何公开正式会议。

[12] 如 A/AC.278/2011/2 号文件 F 节所述。

- 视可用时间情况，在会员国讨论结束时就每个实质性议程项目作口头发言。鉴于会议可用时间有限，多利益攸关方可考虑以平衡和透明的方式，结合公平地域代表性、性别均等和多利益攸关方多样性，在他们自己当中挑选发言人“。

- 提交有字数限制的书面材料。将这些提交材料的原文发布在特设委员会网站上。[13]

《行动纲领》还应利用区域一级现有的专门知识和正在开展的工作。允许这些实体作为利益攸关方参与《行动纲领》的讨论，将有助于联合国层面的工作更好地与区域工作相结合，并顾及具体的区域挑战和情况。

委内瑞拉玻利瓦尔共和国

[原件：西班牙文]
[2024 年 4 月 26 日]

2023 年 12 月 22 日通过的大会第 78/237 号决议第 8 段邀请所有会员国继续向秘书长通报它们对信息和通信技术的安全及使用方面的看法和评估意见，特别是对今后在联合国主持下就这些事项进行定期机构对话的看法和评估意见，并请秘书长根据这些意见向大会第七十八届会议提交一份报告，供会员国在 2024 年不限成员名额工作组第八届会议期间进一步讨论。

在这方面，委内瑞拉玻利瓦尔共和国认为，有必要强调不限成员名额工作组及其工作方式对于完成大会第 75/240 号决议所规定任务的重要性。近年来取得的成绩，例如建立全球政府间联络点名录，表明不限成员名额工作组目前的形式相当成功，特别是因为它在决策和批准年度报告方面依赖协商一致。

委内瑞拉玻利瓦尔共和国认为，联合国应继续在促进各国就使用信息和通信技术问题进行对话方面发挥核心和关键作用。信息和通信技术的独特性意味着需要制定新的原则和规则，最好是具有法律约束力的原则和规则，以填补现有国际法与虚拟领域现实之间的差距。

鉴于上述情况，迫切需要在 2025 年之后设立一个新的常设不限成员名额工作组，以保持 2021-2025 年不限成员名额工作组工作的连续性，这将有助于加强新一届不限成员名额工作组的能力，以制定和调整具有法律约束力的新规则，帮助加强信息和通信技术使用方面的国际安全。

此外，将于 2025 年后成立的下一个不限成员名额工作组必须有能力应对会员国之间巨大的数字鸿沟所带来的挑战，这种鸿沟使得难以制定旨在加强信息和通信技术使用方面的国际安全的全球战略。

[13] A/AC.291/6，第 3 段。

最后，不限成员名额工作组主席为在工作组所有活动中达成共识所做的广泛努力得到广泛支持，委内瑞拉玻利瓦尔共和国重申愿意继续参与并支持这一进程。

从政府间组织收到的答复

欧洲联盟

[原件：英文]
[2024 年 4 月 29 日]

网络空间，特别是全球、开放的互联网，已经成为我们社会的支柱之一。它提供了一个推动互联互通和经济增长的平台。欧洲联盟及其成员国支持基于法治、人权、基本自由和民主价值观的开放、稳定和安全的全球性网络空间，从而实现全球社会、经济和政治发展。

国际社会认识到，包括《联合国宪章》全文在内的现行国际法适用于网络空间的国家行为，对于维护和平与稳定，促进开放、安全、和平和无障碍的信通技术环境至关重要。

2010 年、2013 年、2015 年和 2021 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协商一致建议、2021 年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协商一致建议，以及 2021-2025 年信息和通信技术安全和使用安全不限成员名额工作组 2022 年和 2023 年协商一致年度进展报告，制定并巩固了国家在网络空间负责任行为的框架。该框架包括国际法在网络空间的适用情况、负责任国家行为自愿规范、建立信任措施和能力建设。

欧洲联盟及其成员国重申，我们承诺根据这些现有协定采取行动，并承诺根据国际法，包括《联合国宪章》全文，以及网络空间负责任国家行为准则采取行动。我们致力于通过讨论和论坛，如目前的不限成员名额工作组，促进和推动网络和平与稳定。

在此背景下，并根据我们对不限成员名额工作组工作的支持，欧洲联盟无法支持大会于 2023 年 12 月 22 日通过的题为“从国际安全角度看信息和电信领域的发展”的第 78/237 号决议。

欧洲联盟认为，该决议本可以更好地体现不限成员名额工作组、其先前的进程和以往协商一致的决议中达成的脆弱共识。

主要是该决议没有提及在使用信通技术方面负责任国家行为的累积和演变的框架。这一框架是二十多年谈判的结果，并一再得到大会的一致赞同。

相反，该决议，特别是序言部分第 16 段和执行部分第 5 段，强调了得到少数国家支持的某些实质性提议，欧盟担心这些提议可能会阻碍过去几年来不限成员名额工作组得以取得进展的渐进和基于共识的方法。

欧洲联盟及其成员国认为，执行联合国在使用信通技术方面负责任的国家行为框架，对于确保开放、安全、稳定、无障碍及和平的信通技术环境至关重要，我们关切地看到，该决议依赖于非协商一致的案文，这可能导致重新解释不限成员名额工作组的工作和现有的协商一致文件。

欧洲联盟仍然充分致力于在目前的不限成员名额工作组中找到推进共识的共同点，以及在目前的不限成员名额工作组结束后集体努力设计一个包容、常设和面向行动的定期机构对话机制。

关于根据该决议第 8 段提出的要求：

关于 2021-2025 年不限成员名额工作组结束后未来机制的讨论已取得很大进展。大会第 77/37 号决议授权的秘书长报告(A/78/76)载有关于制定《推进从国际安全角度使用信息和通信技术的负责任国家行为的行动纲领》的范围、结构、原则、内容、筹备工作和方式的意见和结论。此外，2021-2025 年不限成员名额工作组在 2023 年年度进展报告中商定了未来定期机构对话机制的共同要素。最后，2021-2025 年不限成员名额工作组主席在一份讨论文件中提出了更多共同要素，其中借鉴了各代表团的建议和不限成员名额工作组第六届实质性会议的讨论情况。

考虑到在确定未来机制的共同要素方面取得的进展，欧洲联盟将进一步表达其对未来定期机构对话机制的看法。

推进网络空间的国际安全与稳定，加强对联合国网络空间负责任国家行为框架的理解和执行，应继续是联合国主持下关于这些事项的定期机构对话的优先事项。

响应 2021 年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和政府专家组报告中提出的在联合国主持下建立常设、包容、透明和广泛参与的机构对话的呼吁，《行动纲领》是一个跨区域国家集团发起的建议，[1] 为提出设立在联合国层面进行定期机构对话的常设结构提供了机会，从而使国际社会能够将讨论重点放在实质性问题上，而不是就未来进程反复进行辩论。在这方面，《行动纲领》可成为今后在第一委员会内开展合作的不断发展的机制。

为此，集体的重点应当是寻求在我们工作的两个同样重要的方面——从国际安全角度使用信通技术方面负责任国家行为的既定框架的实施和该框架的进一步发展——之间取得平衡。该框架的发展，除其他外，源于在履行现有承诺过程中汲取的经验教训。

该机制应具有包容性，以行动为导向，为详细的讨论和交流提供一个平台，促进能力建设，并允许进一步发展规范性框架，并在协商一致的基础上根据信通技术环境的不断发展更新该框架。

[1] 见 https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber- PoA.pdf。

该框架还应允许私营部门、学术界和民间社会等相关利益攸关方正式参与定期磋商，以审议相关问题并提供其独特的观点和专门知识。这将进一步侧重于支持各国促进实施负责任的国家行为框架和以需求为导向的能力建设，以提高国家和全球的网络韧性。

《行动纲领》应基于联合国政府专家组和不限成员名额工作组历次共识报告所载的规范性框架以及由此产生的承诺和行动。未来的机制应每隔几年(例如每三年或四年)召开一次定期审查会议，审查负责任的国家行为框架，必要时更新框架，并为机制的工作提供战略方向。

《行动纲领》可举行年度正式会议，对全年举行的不限成员名额的详细讨论的工作进行整理。年度正式会议可决定设立不限成员名额的技术会议、工作组或工作流，以通过《行动纲领》重点推进具体的优先问题。

技术工作流的参与应当是自愿的，并向所有国家开放。工作流的设置，包括利益攸关方的参与，以及会议的频率，应在年度会议或审查会议上决定。这些会议应着眼于制定一份成果文件，其中包含在实施负责任国家行为框架过程中吸取的经验教训基础上得出的行动结论，并不断加以改进。

《行动纲领》还可以通过与区域组织合作，利用现有的相关举措，并在现有的能力建设结构和平台的基础上，加强区域参与。这些集体努力将有助于各国阐明和接受基于需求的能力建设。在强调各国对维护国际和平与安全负有首要责任以及各国在《行动纲领》中的核心作用的同时，应通过提供包容性和有意义的参与场所，加强与利益攸关方的交流与合作。

关于《行动纲领》的筹备工作和建立问题，不限成员名额工作组应在 2024 年和 2025 年举行闭会期间会议和专门会议，继续拟订《行动纲领》的不同方面，包括常设机制所涉预算问题，并确定联合国内部履行这些职能的相关行为体。这些会议的成果应反映在不限成员名额工作组相应的年度进展报告中。《行动纲领》应在 2021-2025 年不限成员名额工作组结束后开始实施。