联合国 A/75/816

大 会

Distr.: General
18 March 2021
Chinese
Original: English

第七十五届会议

议程项目 98

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

秘书长的说明

根据大会第 73/27 号决议和第 75/550 号决定，秘书长谨向大会成员转递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报告。

21-03673 (C) 120421 140421

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报告

一. 导言

1. 大会第 73/27 号决议决定，从 2019 年开始召集一个不限成员名额工作组，在协商一致的基础上采取行动，作为优先事项，继续进一步制定国家负责任行为的规则、规范和原则及其实施方式；如有必要，对其进行修改或制定额外的行为规则；研究在联合国主持下建立有广泛参与的定期机构对话的可能性；并继续研究信息安全领域的现有威胁和潜在威胁及为消除这些威胁可以采取的合作措施，国际法如何适用于国家使用信息和通信技术问题，建立信任措施和能力建设，以期促进取得共同的理解，并向大会第七十五届会议提交关于这一研究结果的报告，并提供利用自愿捐款与有关各方，即商界、非政府组织和学术界举行闭会期间协商会议的可能性，就工作组任务范围内的问题交流意见。大会又决定该工作组应于 2019 年 6 月举行组织会议，以便商定与工作组有关的组织安排。

2. 大会第 75/550 号决定注意到，由于 2019 冠状病毒病(COVID-19)大流行，原定于 2020 年 7 月 6 日至 10 日举行的第三届也是最后一届实质性会议被取消，决定不限成员名额工作组在继续根据大会第 73/27 号决议规定的任务开展工作的同时，于 2021 年 3 月 8 日至 12 日召开第三届也是最后一届实质性会议。

二. 组织事项

A. 会议开幕和会期

3. 工作组于 2019 年 6 月 3 日举行了组织会议，于 2019 年 9 月 9 日至 13 日举行了第一届实质性会议，于 2020 年 2 月 10 日至 14 日举行了第二届实质性会议，并于 2021 年 3 月 8 日至 12 日举行了第三届实质性会议，均在总部举行。

4. 裁军事务厅和联合国裁军研究所为工作组提供了实质性支持。大会和会议管理部提供了秘书处服务。

B. 出席情况

5. 实质性会议的与会者名单载于 A/AC.290/2019/INF/1、A/AC.290/2020/INF/1 和 A/AC.290/2021/INF/1 号文件。

C. 主席团成员

6. 在 2019 年 6 月 3 日的组织会议上，工作组以鼓掌方式选举 Juerg Lauber(瑞士)为主席。

D. 通过议程

7. 在同一会议上，工作组通过了 A/AC.290/2019/1 号文件所载的其所有会议的议程。议程如下：

1. 选举主席团成员。
2. 通过议程。
3. 工作安排。
4. 一般性意见交流。
5. 关于大会第 73/27 号决议第 5 段所载实质性问题的讨论：
   (a) 进一步制定大会第 73/27 号决议第 1 段所列国家负责任行为的规则、规范和原则及其实施方式；如有必要，对其进行修改或制定额外的行为规则；
   (b) 研究在联合国主持下建立有广泛参与的定期机构对话的可能性；
   (c) 继续研究信息安全领域的现有威胁和潜在威胁及为消除这些威胁可以采取的合作措施，以期促进取得共同的理解；
   (d) 国际法如何适用于国家使用信息和通信技术问题；
   (e) 建立信任措施；
   (f) 能力建设，以及大会第 73/27 号决议第 3 段提及的概念。
6. 其他事项。
7. 通过最后报告。

8. 还在同一会议上，工作组还决定按照大会各主要委员会的议事规则开展工作，同时根据大会第 73/27 号决议以协商一致的方式采取行动。工作组又决定，根据大会议事规则和惯例，所有会员国都有权派代表参加工作组。获得大会观察员地位的非成员国、政府间组织和实体可长期应邀作为观察员出席工作组的届会和参与工作组的工作。联合国系统的有关实体也将受邀参加，但仅为技术资料的目的。此外，根据第 1996/31 号决议，具有经济及社会理事会咨商地位的有关非政府组织应知会工作组秘书处，表示有兴趣参加工作组的工作。工作和职责与工作组的范围和宗旨相符的其他有关非政府组织亦应知会工作组秘书处表明兴趣，并可在无异议的基础上应邀以观察员身份参加工作。

E. 工作安排

9. 在分别于 2019 年 9 月 9 日、2020 年 2 月 10 日和 2021 年 3 月 8 日举行的每届实质性会议第一次会议上，工作组商定了 A/AC.290/2019/2、A/AC.290/2020/1 和 A/AC.290/2021/1 号文件所载的工作安排。

F. 文件

10. 工作组收到的所有正式文件、工作文件、技术文件和其他文件的完整清单，可查阅以下专门网站：www.un.org/disarmament/open-ended-working-group/。

G. 工作小组的审议工作

11. 工作组第一届实质性会议在其 9 次全体会议上审议了议程项目 3 至 5。

12. 工作组第二届实质性会议继续在其 9 次全体会议上审议议程项目 5。

13. 工作组第三届实质性会议审议了议程项目 5 至 7。

14. 为在 2019 冠状病毒病(COVID-19)大流行期间继续工作，工作组于 2020 年 6 月 15 日、17 日和 19 日、7 月 2 日、2020 年 9 月 29 日至 10 月 1 日、2020 年 11 月 17 日至 19 日、2020 年 12 月 1 日至 3 日以及 2021 年 2 月 18 日、19 日和 22 日举行了非正式虚拟会议。

15. 工作组于 2019 年 12 月 2 日至 4 日举行了非正式闭会期间多方利益攸关方协商会议。应工作组主席的要求，会议由新加坡网络安全局首席执行官 David Koh 主持，会议纪要已提交并分发给工作组成员。[1]

三. 通过报告

16. 在 2021 年 3 月 12 日举行的第三届实质性会议上，工作组审议了题为“通过报告”的议程项目 7，并通过了经口头订正的文件 A/AC.290/2021/L.1 和 A/AC.290/2021/CRP.2 所载的报告。

17. 鉴于联合国总部实施的 COVID-19 限制措施，工作组第三届实质性会议的会议次数受限，解释立场的发言汇编将作为 A/AC.290/2021/INF.2 号文件印发。

[1] 可查阅 www.un.org/disarmament/open-ended-working-group/。

附件一*

最后实务报告

A. 导言

1. 75 年前，联合国成立。尽管此后世界经历了巨大变革，但联合国的宗旨和永恒的理想仍然具有根本的现实意义。在重申其对基本人权的信念，承诺促进各国人民的经济和社会进步，并为正义和尊重国际法创造条件的同时，各国决心齐心协力，维护国际和平与安全。[2]

2. 信息和通信技术(信通技术)的发展对联合国工作的所有三大支柱，即和平与安全、人权、可持续发展，都有影响。信通技术和全球互联互通一直在推动人类进步和发展，改变社会和经济，并扩大合作机会。

3. 建立并维护国际和平、安全、合作和对信通技术环境的信任，其迫切性从未如此明确。数字领域出现的不良趋势会破坏国际安全与稳定，拖累经济增长和可持续发展，阻碍充分享有人权和基本自由。这些趋势包括越来越多地利用信通技术作恶。

4. 全球当前的健康危机彰显信通技术的重要惠益和我们对它们的依赖，包括提供必不可少的政府服务、传达重要的公共安全信息、开发创新解决方案以确保业务连续性、加速研究、通过虚拟手段帮助确保教育延续性和社会凝聚力。在此充满不确定性的时刻，国家以及私营部门、科学家和其他行为体利用数字技术使个人和社会保持联系和健康。与此同时，COVID-19 大流行表明，利用社会面临巨大压力的时机企图浑水摸鱼的恶意活动，会带来怎样的风险和后果。疫情也凸显了消除数字鸿沟、在每个社会和部门建立复原力以及坚持以人为本的做法的必要性。

5. 由于信通技术可能会被用于不符合维护国际和平、稳定与安全的宗旨，大会认识到，信通技术的传播和利用事关整个国际社会的利益，广泛的国际合作将最终产生最有效的对策。[3]

6. 有鉴于此，根据大会第 73/27 号决议设立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(不限成员名额工作组)是推动审议这一重要问题的良机。该工作组提供了一个民主、透明和包容各方的平台，使所有国家都能参与信通技术的国际安全层面工作、表达观点并扩大合作。联合国会员国的积极参与和各种其他相关利益攸关方投入其中表明国际社会对人人享有和平、安全的信通技术环境有着共同的愿望和集体利益，而且决心合作实现这一目标。

---

* 未经正式编辑发布。

[2] 《联合国宪章》序言。

[3] 例如见 A/RES/53/70，序言部分第 6 段。

7. 不限成员名额工作组是为营造开放、安全、稳定、无障碍、和平的信通技术环境而开展国际合作的一座重大里程碑。2003 年以来，已六次成立政府专家组，研究信息安全领域的现有和潜在威胁以及合作应对这些威胁的可能措施。[4] 这些小组通过其三份具有累积性质的共识报告(2010 年、2013 年和 2015 年)，提出了 11 项关于负责任国家行为的自愿的、不具约束力的规范，并认识到随着时间的推移可以制定更多的规范。[5] 此外，专家组建议了建立信任、建设能力和开展合作的具体措施。他们还重申，国际法，特别是《联合国宪章》，对于维护信息和通信技术环境中的和平、安全和稳定是适用的，也是必不可少的。在大会第 70/237 号决议中，会员国一致同意将政府专家组 2015 年报告作为使用信通技术的指南，从而巩固信通技术使用方面的负责任国家行为初步框架。在这方面，不限成员名额工作组还注意到大会第 73/27 号和第 73/266 号决议。

8. 在此基础上，工作组重申这一框架，并就这一具有全球意义的主题寻求联合国所有会员国的共识和互谅。工作组按照其任务规定，讨论了以下问题：信息安全领域的现有和潜在威胁以及合作应对这些威胁的可能措施；进一步制定国家负责任行为的规则、规范和原则；国际法如何适用于国家使用信通技术的问题；建立信任措施；能力建设；在联合国主持下定期开展广泛参与的机构对话的可能性。在努力建立共识和促进国际和平、安全、合作和信任的过程中，不限成员名额工作组的讨论遵循包容性和透明度的原则。

9. 联合国应继续在促进各国使用信息和通信技术的对话方面发挥主导作用。工作组认识到，联合国其他机构和论坛对数字技术各方面进行的专门讨论既重要又互补。

10. 各国负有维护国际和平与安全的主要责任，但所有利益攸关方都有责任以不危及和平与安全的方式使用信通技术。由于信通技术的国际安全层面横跨多个领域和学科，因此来自政府间组织、区域组织、民间社会、私营部门、学术界和技术界的代表使工作组得益于各人所具备的专长、知识和经验。2019 年 12 月，工作组举行了为期三天的非正式协商会议。与会国与众多其他利益攸关方之间进行了内容丰富的讨论。[6] 此外，这些利益攸关方通过书面材料和与工作组开展非正式交流的方式，提出具体提议和良好做法范例。一些代表团还主动开展多利益攸关方协商，以有助于向工作组建言献策。

11. 铭记各国和各区域的不同情况、能力和优先事项，工作组承认，数字技术的惠益分布不均；缩小数字鸿沟，包括通过普遍、包容和非歧视性地获取信通技术和实现连通，依然是国际社会的当务之急。

12. 工作组欢迎众多女代表参加会议，并欢迎在讨论中突出反映性别观点。工作组强调缩小“性别数字鸿沟”的重要性，并强调在从国际安全角度对使用信通技

[4] A/RES/58/32、A/RES/60/45、A/RES/66/24、A/RES/68/243、A/RES/70/237、A/RES/73/266。

[5] A/65/201、A/68/98 和 A/70/174。

[6] 见“从国际安全角度看信息和电信领域的发展问题不限成员名额工作组闭会期间非正式协商会议主席摘要”，可查阅 https://www.un.org/disarmament/open-ended-working-group/。

术的有关问题作出决策的过程中，务必促进妇女的有效和切实参与，发挥她们的领导作用。

13. 工作组强调，其任务构成的各个要素相互关联，相辅相成，共同促进一个开放、安全、稳定、无障碍、和平的信通技术环境。

B. 结论和建议

14. 与会国审议了不限成员名额工作组任务的实质性方面，回顾大会第 73/27 号决议欢迎 2010 年、2013 年和 2015 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有效工作以及秘书长转交的相关成果报告，[7] 得出以下结论和建议，包括应对信通技术威胁以及促进开放、安全、稳定、无障碍及和平的信通技术环境的具体行动和合作措施。

现有和潜在威胁

15. 与会国在结论中表示越来越关切恶意利用信通技术对维护国际和平与安全、进而对人权和发展造成的影响。特别是，与会国对为破坏国际和平与安全的目的发展信通技术能力表示关切。信通技术方面的有害事件越来越频繁和巧妙，而且不断演变和多样化。如果不采取相应措施确保信通技术的安全，连通的增加和对信通技术的依赖会带来意想不到的风险，使社会更容易遭受恶意信通技术活动的影响。尽管信通技术给人类带来宝贵的惠益，但恶意利用会产生重大而且深远的负面影响。

16. 与会国回顾说，一些国家正在发展用于军事目的的信息和通信技术能力，而且在未来的国家间冲突中使用信息和通信技术的可能性越来越大。国家和非国家行为体包括恐怖主义分子和犯罪集团恶意使用信通技术的事件持续增加。一些非国家行为体展示出以往只有国家才具备的信通技术能力。

17. 与会国还得出结论认为，国家利用信通技术的方式如不符合其根据框架应承担的义务，包括自愿规范、国际法和建立信任措施等，会给国际和平与安全、国家间的信任和稳定造成破坏，并可能增加国家之间未来发生冲突的可能性。

18. 与会国得出结论认为，对于支持向公众提供基本服务的关键基础设施和关键信息基础设施而言，恶意的信通技术活动有可能会造成毁灭性的安全、经济、社会和人道主义后果。此类基础设施可能包括医疗设施、金融服务、能源、水、交通和卫生设施，不过，将哪些基础设施指定为关键基础设施由每个国家自行决定。针对关键基础设施和关键信息基础设施的信通技术恶意活动破坏了人们对政治和选举进程及对公共机构的信任和信心，或影响到互联网的普遍可用性或完整性，此类活动亦是一个真实存在且日益严重的问题。这类基础设施或许由私营部门拥有、管理或运营，或许与另一个国家共享或联网，或许跨国运营。因此，为了保护这类基础设施的健全完整、正常运作和可供使用，国家之间或公私之间抑或必须开展合作。

[7] A/65/201、A/68/98 和 A/70/174。

19. 与会国还得出结论认为，开展违反国际法义务的信通技术活动，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，不仅可能对安全构成威胁，而且可能对国家主权、经济发展和生计构成威胁，并最终威胁到个人的安全和福祉。

20. 由于所有国家对数字技术的依赖程度都在日益加深，与会国得出结论认为，缺乏有关恶意信通技术活动的意识和充足的侦测、防御或应对能力，可能会加剧国家的脆弱性。正如当前全球卫生紧急情况期间有目共睹的：既有的脆弱性在危机之时会进一步放大。

21. 与会国得出结论认为，各国的数字化程度、能力、信通技术的安全性和复原力、基础设施和发展程度不一，所经受的威胁也可能各异。这种威胁对不同的群体和实体也可能产生不同的影响，包括对青年人、老年人、妇女和男子、弱势群体、特定职业、中小型企业和其他人的影响。

22. 鉴于数字威胁情况日益令人担忧，同时认识到没有哪个国家能够免遭这些威胁的影响，与会国强调迫切需要落实并进一步制定合作措施，应对这种威胁。与会者申明，尽可能共同行动并以相互包容的方式采取行动将取得更有效、更深远的成果。在这方面，与会国还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。

23. 与会国强调信通技术可带来的积极的经济和社会机会，并得出结论认为，令人关切的是对这些技术的滥用，而不是技术本身。

负责任国家行为的规则、规范和原则

24. 自愿、不具约束力的负责任国家行为规范能够减少国际和平、安全与稳定所面临的风险，在提高可预测性和降低错觉风险方面发挥重要作用，因此有助于预防冲突。与会国强调，这些规范反映了国际社会对各国使用信通技术行为的期望和标准，使国际社会能够评估各国的活动。根据大会第 70/237 号决议，并确认大会第 73/27 号决议，会议呼吁各国避免和不使用不符合负责任国家行为准则的信通技术。

25. 与会国重申，规范并不取代或改变国家根据国际法承担的约束性义务或权利，而是提供额外的具体指导，说明什么是国家在使用信通技术方面的负责任行为。准则不寻求限制或禁止在其他方面符合国际法的行动。

26. 与会国同意有必要保护所有支持向公众提供基本服务的关键基础设施和关键信息基础设施，并努力确保互联网的普遍可用性和完整性，同时，与会国进一步得出结论认为，COVID-19 大流行凸显了通过实施针对关键基础设施的规范(如联合国大会第 70/237 号决议以协商一致方式确认的规范)来保护包括医疗服务和设施在内的医疗保健基础设施的重要性。

27. 与会国申明，必须支持和进一步努力执行各国承诺在全球、区域和国家各级接受指导的规范。

28. 与会国重申大会第 70/237 号决议并确认大会第 73/27 号决议，认为各国应：采取合理的步骤，包括通过制定客观的合作措施，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；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；并鼓励负责任地报告信通技术的脆弱性。

29. 鉴于信通技术的独特属性，与会国重申，考虑到工作组会上的规范提议，今后可以继续制定更多规范。与会国还得出结论认为，进一步制定规范和落实现有规范彼此并不排斥，而可同时进行。

工作组建议

30. 各国自愿调查本国为执行规范所做的努力，积累和分享执行规范的经验和良好做法，并继续向秘书长通报本国在这方面的看法和评估意见。

31. 各国不应违反国际法规定的义务，从事或故意支持蓄意破坏关键基础设施或以其他方式损害为公众提供服务的关键基础设施的利用和运行的信通技术活动。此外，各国应继续加强措施，保护所有关键基础设施免受信通技术威胁，并就关键基础设施保护方面的最佳做法加强交流。

32. 各国与有关组织包括联合国合作，进一步支持所有国家执行和制定负责任国家行为规范。鼓励有能力提供专门知识或资源的国家这样做。

33. 各国回顾大会第 70/237 号决议，肯定大会第 73/27 号决议，注意到各国关于在联合国今后有关信通技术的讨论中制定国家负责任行为的规则、规范和原则的建议，并注意到第 75/240 号决议设立了 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。

国际法

34. 认识到大会第 70/237 号决议，并肯定设立工作组的大会第 73/27 号决议，与会国重申，国际法，尤其是《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。在这方面，促请各国避免和不采取任何不符合国际法、特别是《联合国宪章》的措施。与会国还得出结论认为，需要就国际法如何适用于国家使用信通技术的问题进一步达成共识。

35. 与会国还重申，各国应通过谈判、调查、调解、和解、仲裁、司法解决以及诉诸区域机构或安排，或由其自行选择的其他和平手段，寻求和平解决争端。

36. 与会国得出结论认为，考虑到信通技术环境的独特属性，为了深化在国际法如何适用于国家使用信通技术这一问题上的共识，各国之间可就此问题交流看法，并确定需要在联合国内进一步深入讨论的国际法具体专题。

37. 为了让所有国家深入了解国际法如何适用于各国使用信通技术问题，并推动国际社会内部建立共识和共同理解，与会国得出结论认为，需要以客观中立的方式作出更大努力，建设国际法、国家立法和政策方面的能力。

工作组建议

38. 各国继续自愿向秘书长通报本国在从国际安全角度看国际法如何适用于国家使用信通技术问题上的看法和评估意见，并继续酌情通过其他渠道自愿分享本国观点和做法。

39. 凡有能力做到的国家继续按照本报告第 56 段所载原则，支持以客观中立的方式作出更大努力，建设国际法、国家立法和政策方面的能力，使所有国家都能在国际法如何适用于各国使用信通技术的问题上推动建立共同理解，并促使国际社会内部建立共识。

40. 各国继续在今后的联合国进程中就国际法如何适用于各国使用信通技术问题进行研究和开展讨论，以此作为澄清问题和进一步就此形成共识的关键一步。

建立信任措施

41. 建立信任措施包含透明、合作和稳定措施，有助于预防冲突，避免错觉和误解，并且有助于缓解紧张局势。这类措施是国际合作的一种具体体现。建立信任措施如果有必要的资源、能力以及各方的参与，可以加强信通技术的整体安全、复原力及和平使用。建立信任机制还能够支持落实负责任的国家行为规范，因为这些措施可以增进信任，并确保各国在使用信通技术时更有清晰度、可预测性和稳定性。建立信任措施还能与负责任国家行为框架的其他支柱一起，推进在各国之间形成共识，从而有助于更和平的国际环境。

42. 由于建立信任措施是循序渐进自愿采用的，因此可以就涉及共同利益的共同目标建立沟通、构筑桥梁并启动合作，从而成为克服误解导致的国家间不信任的第一步。因此，建立信任措施可能为今后扩大和建立更多的安排和协议奠定基础。

43. 与会国得出结论认为，不限成员名额工作组内的对话本身就是一种建立信任措施，因为对话促进就威胁和脆弱性方面的看法、国家和其他行为体的负责任行为及良好做法公开透明地交流意见，从而最终支持集体制定和实施国家使用信通技术负责任行为框架。

44. 此外，与会国得出结论认为，联合国在制定和支持实施全球建立信任措施方面具有至关重要的作用。每一份政府专家组协商一致报告都建议了切实的建立信任措施。除了针对信通技术的这些建议外，大会在第 43/78(H)号协商一致决议中核可了联合国裁军审议委员会制定的建立信任措施指导方针，其中概述了建立信任措施的宝贵原则、目标和特点，可供制定针对信通技术的新措施时考虑。

45. 与会国依据各自在信任和既有关系方面的重要资产，得出结论认为，区域和次区域组织已作出重大努力，制定建立信任措施，使之适应具体情况和优先事项，提高认识，并在成员之间交流信息。此外，进行区域、跨区域和组织间交流能够构建新的协作、合作和相互学习的渠道。由于并非所有国家都是区域组织的成员，而且并非所有区域组织都已具备建立信任措施，因此与会国指出，这种措施只是补充联合国和其他组织促进建立信任措施的工作。

46. 与会国依据在工作组会上分享的经验教训和做法，得出结论认为，为了确保建立信任措施达到预期目标，必须预先建立国家和区域机制和结构，并建设诸如国家计算机应急小组等适当的资源和能力。

47. 作为一项具体措施，与会国得出结论认为，建立国家联络点这一具体措施本身就是建立信任措施，而且也是落实其他许多建立信任措施的一个有益措施，在危机时刻具有宝贵价值。与会国可能会发现，设立联络点对外交、政策、法律和技术交流以及报告和处理事件等诸多方面也很有助益。

工作组建议

48. 各国继续自愿向秘书长通报其看法和评估意见，并补充说明双边、区域或多边各级相关建立信任措施方面的经验教训和良好做法。

49. 各国自愿确定并考虑适合其具体情况的建立信任措施，同时与其他国家合作执行这些措施。

50. 各国自愿实施透明度措施，酌情以自我选定的形式和论坛分享相关信息和经验教训，包括通过联合国裁军研究所的网络政策门户网站分享。

51. 尚未采取相关行动的国家考虑各自不同的能力，除其他外指定技术、政策和外交层面的国家联络点。还鼓励各国继续考虑在全球一级建立此类联络点名录的模式。

52. 各国考虑各区域具体情况和相关组织结构上的差异，探讨定期就建立信任措施跨区域交流经验教训和良好做法的机制。

53. 各国继续考虑双边、区域和多边层面的建立信任措施，并鼓励提供开展建立信任措施的合作机会。

能力建设

54. 国际社会能否预防或减轻恶意信通技术活动影响取决于每个国家作好准备和进行应对的能力。这对发展中国家而言尤其具有现实意义，以便促进其真正参与国际安全角度的信通技术讨论，并促进其消除关键基础设施脆弱性的能力。能力建设有助于发展技能、开发人力资源、制定政策和建设机构，从而提高各国的复原力和安全程度，使之能够充分享受数字技术的惠益。能力建设对促进遵守国际法和执行负责任的国家行为规范、支持落实建立信任措施发挥着重要的支持作用。在一个数字上相互依存的世界里，能力建设的惠益不仅限于初始受惠国，而且有助于为所有各方建立一个更安全、更稳定的信通技术环境。

55. 确保开放、安全、稳定、无障碍、和平的信通技术环境，要求各国开展有效合作，以降低对国际和平与安全的风险。能力建设是国际合作的一个重要方面，也是捐助国和受援国的自愿行为。

56. 与会国在考虑并进一步探讨被广泛接受的原则后得出结论认为，从国际安全角度看国家使用信通技术方面的能力建设应遵循以下原则：

进程和目的

- 能力建设应是一个可持续的进程，由不同行为体开展和为不同行为体开展的具体活动组成。

- 具体活动应该有明确的目的并注重成果，同时有利于实现开放、安全、稳定、无障碍、和平的信通技术环境这一共同目标。

- 能力建设活动应该是以证据为依据、政治上中立、透明、问责、不设条件。

- 能力建设应以充分尊重国家主权原则的方式进行。

- 可能需要为获取相关技术提供便利。

伙伴关系

- 能力建设应该以相互信任为基础，以需求为导向，符合各国认定的需求和优先事项，并在充分承认国家自主权的情况下开展。能力建设的合作伙伴应自愿参与这项工作。

- 由于能力建设活动应根据具体需要和具体情况量身定做，因此所有各方都是积极合作伙伴，负有共同但有区别的责任，包括在能力建设活动的设计、执行、监测和评价方面进行协作。

- 所有合作伙伴都应保护和尊重国家政策和计划的保密性。

人民

- 能力建设工作应尊重人权和基本自由，对性别问题有敏感认识，是性别包容的，具有普遍性、非歧视。

- 应确保敏感信息的机密性。

57. 与会国得出结论认为，能力建设是一项对等互惠的工作，即所谓的“双向通道”，期间参与者相互学习，所有各方都因全球信通技术安全的普遍改善而受益。此外，与会国回顾南南合作、南北合作、三边合作和以区域为重点的合作所具有的价值。

58. 与会国得出结论认为，能力建设应有助于将数字鸿沟转化为数字机会。特别是，能力建设目的应该是促进发展中国家真正参与相关讨论和论坛，并加强发展中国家在信通技术环境中的复原力。

59. 与会国得出结论认为，能力建设可有助于各方进一步理解并处理由于缺乏信通技术安全、国家层面技术能力和政策能力之间协调不力加之不平等和数字鸿沟等相关挑战而产生的系统性风险和其他风险。与会国认为，旨在使各国能够认定和保护国家关键基础设施并合作保护关键信息基础设施的能力建设工作特别重要。能力建设还可能有助于各国加深对国际法如何适用的理解。国家、区域和国际各级的信息共享和协调可使能力建设活动更有效、更具战略性，更符合国家的优先事项。

60. 除技术技能、机构建设与合作机制外，与会国得出结论认为，迫切需要在外交、法律、政策、立法和监管等一系列领域积累专门知识。在这方面，与会国强调发展外交能力参与国际和政府间进程的重要性。

61. 与会国回顾需要对能力建设采取具体、注重行动的方式。与会国得出结论认为，此类具体措施可包括在政策和技术两个层面提供支持，如制定国家网络安全战略，提供取得相关技术的机会，支持计算机应急小组或计算机安全事件响应小组以及设立专门的培训和针对特定需要的课程，包括“培训员培训”方案和专业认证。与会国还确认，建立交流法律和行政方面的良好做法等信息的平台可带来惠益，其他相关利益攸关方对能力建设活动的宝贵贡献也是如此。

62. 与会国得出结论认为，盘点各国就本报告中的结论和建议所作努力以及会员国商定以协商一致的第 70/237 号决议为指导的评估意见和建议，是一项有价值的工作，以便确定进展情况并确定哪些方面需要进一步开展能力建设。

工作组建议

63. 各国在国际安全领域开展信通技术方面的能力建设工作时遵循第 56 段所载各项原则，并鼓励其他行为体在其自身的能力建设活动中考虑到这些原则。

64. 各国继续自愿向秘书长通报其关于从国际安全角度看信通技术领域的发展的看法和评估意见，并补充说明能力建设方案和举措方面的经验教训和良好做法。

65. 各国自愿使用“联合国大会第 70/237 号决议执行情况全国调查”范本(将在线提供)来帮助开展这项工作。会员国还不妨在自愿基础上使用该示范调查来安排向秘书长通报其看法和评估意见的上述提交材料的结构。

66. 鼓励各国和其他有能力做到的行为体为能力建设提供财政、实物或技术援助，并进一步促进能力建设工作的协调和资源配置，包括相关组织与联合国之间的协调。

67. 各国继续考虑多边层面的能力建设，包括交流意见、信息和良好做法。

定期机构对话

68. 大会第 73/27 号决议所设不限成员名额工作组首次在联合国主持下提供了在所有国家间开展对话的专门平台，讨论从国际安全角度看信通技术的发展问题。

69. 工作组的目标是谋求所有国家之间的共识，除此之外，工作组还促进建立了外交网络，并增进了与会者之间的信任。非政府利益攸关方的广泛参与表明，众多行为体随时准备利用其专门知识支持各国实现其确保开放、安全、稳定、无障碍、和平的信通技术环境这一目标。工作组的讨论肯定了在联合国主持下就信通技术的使用问题进行经常和结构化讨论的重要性。

70. 与会国得出结论认为，联合国主持下的定期对话有助于实现在信通技术环境下加强国际和平、稳定和预防冲突的共同目标。与会国还得出结论认为，鉴于对

信通技术日益依赖，而且恶意使用信通技术造成巨大威胁，迫切需要继续增进共识，建立信任并加强国际合作。

71. 鉴于各国对国家安全、公共安全和法治负有主要责任，与会国申明定期进行政府间对话和确定在未来进程中让其他利益攸关方群体参与的适当机制十分重要。

72. 联合国对信通技术发展和国际安全的审议注重其国际和平、稳定和预防冲突层面。与会国得出结论认为，今后的定期机构对话不应该与注重其他问题所涉数字层面的联合国现有任务、努力和活动发生重叠。[8] 与会国得出结论认为，加强这些论坛与第一委员会所设进程之间的交流可有助于强化协同作用并增进一致性，同时要尊重每个机构的专家性质或特定任务。

73. 与会国得出结论认为，今后关于从国际安全角度看信通技术方面国际合作的对话，除其他外，还应提高认识，建立信任和信心，并鼓励进一步研究和讨论尚未达成共识的领域。与会国认识到以下方面的效用，即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以及制定更多规范和规则的机制。

74. 与会国得出结论认为，在联合国主持下今后进行定期机构对话的机制，应是一个有具体目标而且着重行动的进程，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。

工作组建议

75. 各国继续积极参加联合国主持下的定期机构对话。

76. 各国确保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的延续，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。

77. 各国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。

78. 各国在今后联合国主持下的定期机构对话过程中，考虑本报告的结论和建议。

79. 有能力做到的国家应考虑设立或支持赞助方案和其他机制，以确保广泛参与上述联合国进程。

[8] 见不限成员名额工作组主席发布的背景文件，“与工作组感兴趣的信通技术相关问题有关的联合国系统行为体、进程和活动初步概述，按主题分列”，2019 年 12 月，https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf。

C. 最后意见

80. 在整个工作组进程中，各国始终积极参与，从而进行了极其丰富的意见交流。这种交流的部分价值在于，提出了不同观点、新想法和重要建议，其中包括更多具有法律约束力的义务的可能性，虽然不一定所有国家都对上述观点、想法和建议表示赞同。不同观点载于所附的、关于议程项目“规则、规范和原则”下的讨论和具体措辞建议的主席摘要中。在今后的联合国进程中，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中，应进一步审议这些观点。

附件二*

主席摘要

A. 背景

1. 不限成员名额工作组为所有国家提供了一次历史性机会，使它们能够在联合国的主持下，从国际安全角度就信通技术相关事项进行平等、有重点、持续的讨论。工作组除了就报告所述的众多领域达成一致外，还通过开展包容各方和透明的讨论，增进了各国间的信任、信心和理解，帮助建立了一个由各国专家组成的全球外交网络，从而成为加强国际和平与安全的宝贵措施。所有代表团的积极和广泛参与显示了各国决心在这一对所有各方都至关重要的问题上继续共同努力。

2. 工作组的所有会议都有一个特点，就是各国之间而且与民间社会、私营部门、学术界和技术界开展实质性互动交流。各国和其他利益攸关方在工作组所有工作中表现出矢志不渝的决心，即使在一些会议已过渡到虚拟形式的情况下参与仍有增无减。这无可辩驳地表明，工作组所审议的议题日益具有普遍的现实意义，而且表明各方日益认识到迫切需要采取集体行动应对恶意使用信通技术对国际安全构成的威胁。

3. 本摘要由主席负责发布，反映的是主席本人对不限成员名额工作组各次会议期间讨论要点的理解。摘要可能无法反映所有代表团的全部意见，也不应被视为反映各国对其中所涉任何具体要点的协商一致意见。提交供分发的国家发言和建议的完整汇编可查阅 https://www.un.org/disarmament/open-ended-working-group。

B. 讨论概况

4. 工作组进程为所有国家以民主、透明、包容各方的方式表达观点、关切和愿望提供了机会。虽然工作组力求确定共同关注和具有共识的领域，但其讨论也记录了会员国的各种观点、想法和建议，可为今后工作奠定有益基础，推动就从国家安全角度看国家使用信通技术这一问题进一步达成共识。

5. 与会国在工作组的整个审议过程中，强调构成任务的每个要素都相互联系，存在协同作用：国际法约束国家间的行动和关系，自愿、不具约束力的规范则为何为负责任国家行为提供了额外指导。这两个要素体现了从国际安全角度看国家使用信通技术这一问题上的行为期望。因此，这两个要素也有助于增加各国之间的透明度和合作，从而促进建立信任，降低冲突风险。反过来，能力建设是所有国家能为加强全球稳定和安全作出贡献的使能因素。这些要素结合在一起共同构成应对信通技术领域现有和潜在威胁的合作措施全球框架。定期机构对话将促进各国之间形成共识、交流执行方面的经验教训和良好做法、建立信任和提高能力，从而为这一框架的进一步发展和发挥作用提供机会。

* 未经正式编辑印发。

现有和潜在威胁

6. 与会国在工作组讨论中提出了各种不同的现有和潜在威胁，突出表明各国对来自信通技术环境的威胁或许看法不同。工作组包容各方的组成形式使各国有机会深入了解其他国家如何看待信通技术环境下的行动和行为，并倾听其他国家认为最大的威胁和风险是什么。

7. 一些与会国对为不符合维护国际和平与安全宗旨的目的发展或使用信通技术能力的做法表示关切。一些与会国表示关切的是，信通技术环境的特点可能助长采取单方面措施，而不是以和平手段解决争端。一些与会国对为军事和其他可能破坏国际和平与安全的目的发展信通技术能力的做法感到关切。另一些与会国指出，一国违反国际法规定的义务使用此类能力，才是威胁所在。此外还有与会国关切囤积漏洞以及缺乏透明度和明确的披露程序、利用有害的隐藏功能、全球信通技术供应链的完整性以及确保数据安全的问题。一些与会国担心信通技术可被用来干涉内政，包括通过信息行动和造谣运动等手段进行干涉。与会国提出的一项具体关切是信通技术活动越来越追求自动化和自主性，并关切可能导致连通削弱或中断、局势意外升级或殃及第三方的行动。一些与会国还指出，私营部门的责任不明确本身也是令人关切的问题。

8. 与会国强调，促进负责任国家行为的措施仍应保持技术中立，特别指出令人关切的不是技术本身，而是滥用技术。与会国认识到，技术进步和新的应用虽然可能提供发展机会，但也可能扩大攻击面，放大信通技术环境中的薄弱之处，或被利用从事新的恶意活动。在这方面，与会国重点指出具体的技术趋势和发展，包括机器学习和量子计算方面的进展；互联设备无处不在(“物联网”)；通过分布式账本技术和云计算存储和访问数据的新方式；大数据和数字化个人数据的扩张。

国际法

9. 与会国本着维护和平与稳定、促进开放、安全、稳定、无障碍、和平的信通技术环境以及增进共识的目标，根据工作组的任务规定，就国际法如何适用于信通技术的国际安全层面交换了意见。

10. 与会国在工作组讨论中回顾，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。在这方面，与会国强调需要采取步骤，避免和不采取任何不符合《联合国宪章》和国际法的措施，因为这种措施妨碍受影响国家的民众充分实现经济和社会发展，并且不利于他们的福祉。与此同时，与会国还重点指出需要进一步了解国际法如何适用于国家使用信通技术的问题。

11. 与会国重申的国际法具体原则包括国家主权；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。

12. 与会国回顾，国际法是国家间关系稳定和可预测的基础。特别是，国际人道法降低武装冲突中平民和民用物体以及战斗人员面临的风险和潜在伤害。与此同时，与会国强调，国际人道法既不鼓励军事化，也不使任何领域诉诸冲突的行为合法化。

13. 与会国还指出，根据习惯国际法，国家对国际不法行为的责任也包括其对信通技术的使用。

14. 与会国回顾国家不得利用代理人使用信通技术实施国际不法行为，并应努力确保按照国家指示或在国家控制下行动的非国家行为体不利用其领土实施此类行为。与会国还指出，国家对其拥有或控制的实体负有责任。

15. 与会国回顾，表明一项信通技术活动从一国领土或信通技术基础设施发起或以其他方式产生，本身可能不足以将该活动归于该国，对国家提出的组织和实施不法行为的指控应得到证实。在这方面，一些与会国强调了真实、可靠和充分证据的重要性。

16. 一些与会国认为，现有国际法，加上反映各国共识的自愿、不具约束力的规范，目前就足以解决国家使用信通技术的问题。还有国家提议，应着重通过制定补充指导意见，使各国就如何适用已经商定的规范框架达成共识，并通过改进所有国家的执行情况，落实框架。与此同时，另一些国家认为，由于构成威胁的环境迅速演变，而且风险严重，因此需要有一个国际商定的具有法律约束力的信通技术框架。还有国家表示，这种具有约束力的框架可望推动在全球范围内更有效地履行承诺，并为追究行为体的行为责任奠定更坚实的基础。与会国强调，建立任何国际法律框架来解决对国际和平与安全有影响的涉及使用信通技术的问题，都应考虑所有国家的关切和利益，并以协商一致为基础，在所有国家积极和平等参与的情况下在联合国内开展工作。

17. 与会国重点指出，虽然现有国际法没有具体提及从国际安全角度使用信通技术的问题，但国际法可逐步发展，包括通过法律确信和国家实践发展。会上提到今后在执行规范的同时制定具有约束力的配套措施的可能性。此外，与会国提出，政治承诺是今后可以努力的方向之一。

18. 与会国回顾国际法、特别是《联合国宪章》适用于使用信通技术的问题，同时重点指出一些关于国际法如何适用于使用信通技术的问题有待明确澄清。一些国家提议，此类问题应包括可能被其他国家视为是使用或威胁使用武力(《宪章》第二条第四款)，或可能使一国有理由援引其自卫之自然权利(《宪章》第五十一条)的与信通技术有关的活动类型；还包括人道原则、必要性原则、相称原则、区别原则和预防原则等国际人道法原则如何适用于信通技术活动的有关问题。在这方面，一些国家指出，需要以审慎态度讨论国际人道法适用于国家使用信通技术的问题。与会国指出，今后的讨论需要进一步研究这些重要议题。

19. 此外，就前进道路而言，与会国提议，要澄清问题和进一步形成共识，关键的第一步是各国在国际法如何适用于国家使用信通技术的问题上加强交流和深入讨论。与会国指出，这种交流本身就可以成为建立信任的重要措施。一些与会

国还提出了各国自愿分享对国际法如何适用问题的看法的几种方式，包括利用秘书长关于从国际安全角度看信息和电信领域的发展的年度报告、[9] 联合国裁军研究所的网络政策门户网站，或调查各国在适用国际法方面的做法。与会国还重点指出了区域和其他安排围绕如何适用国际法的问题交流看法和形成共识所取得的进展。

20. 与会国从维护和平和预防冲突的角度出发，申明需要进一步注重通过和平手段解决争端，不使用武力或以武力相威胁。在这方面，与会国回顾预防与和平解决争端的现有机构、机制和工具。一些国家表示，在联合国主持下，通过交流良好做法，铭记尊重国家主权的原则，在技术层面对信通技术事件来源形成一个普遍接受的共同办法和认识，可望加强问责制和提高透明度，并可有助于支持恶意行为的受害者进行法律追索。

负责任国家行为的规则、规范和原则

21. 与会国在工作组讨论中回顾，自愿、不具约束力的负责任国家行为规范并不改变或取代，而应被视为符合国际法以及联合国的宗旨和原则，包括维护国际和平与安全和促进人权的宗旨和原则。与会国还注意到 1965 年大会题为“关于各国内政不容干涉及其独立与主权之保护宣言”第 2131(XX)号决议。

22. 与会国回顾，大会第 73/27 号决议在提出一套 13 项国家负责任行为的规则、规范和原则的同时，除其他外申明了“第 71/28 号决议以协商一致方式通过并推荐的关于从国际安全角度看信息和电信领域的发展政府专家组 2013 年报告和 2015 年报告所载的”11 项自愿、不具约束力的规范。[10]

23. 与会国强调指出需要提高对现有规范的认识，并在制定新规范的同时支持落实现有规范。与会国特别指出，需要就如何落实规范的问题提供指导。在这方面，与会国呼吁交流和传播落实规范的良好做法和经验教训，并提出了协助落实工作的各种合作办法，例如由国家制定路线图，以及开展旨在交流经验教训和良好做法的自愿调查。

24. 与会国认识到，规范可帮助在信通技术环境中防止冲突，并有助于和平利用和充分实现信通技术，以促进全球的社会和经济发展。与会国重点指出，按规范行事不应对国际合作和转让技术造成不当限制，也不应阻碍为和平目的进行创新以及各国在公平和非歧视环境中发展经济。与会国还强调指出规范、建立信任和建设能力之间的相互联系，并特别指出需要将性别平等视角纳入规范执行工作。

25. 与会国在讨论中，就进一步完善现有规范提出了建议。与会国重申，保护所有向公众提供基本服务的关键基础设施，包括医疗和保健设施，同样至关重要。与会国还提请注意，鉴于对跨界或跨管辖区提供服务的关键基础设施的任何破坏可能造成的影响，务必合作保护此类基础设施，并且务必确保因特网的普及和健全。与会国回顾大会题为“创建全球网络安全文化以及评估各国保护重要信息基

[9] A/RES/75/32。

[10] A/RES/73/27，执行部分第 1 段。

础设施的努力”的第 64/211 号决议。[11] 此外，与会国还提议进一步确保信通技术供应链的完整性，对于在信通技术产品中创建有害隐藏功能表示关切，指出一旦发现重大漏洞就有责任通知用户。与会国还对囤积漏洞的做法表示关切。一些国家建议制定关于供应链安全的客观国际规则和标准。

26. 除上段所述外，与会国在工作组就进一步完善现有规范、执行指南和制定新规范的问题提出的书面建议载于本摘要的附件。

27. 一些与会国还注意到 2015 年提出的信息安全国际行为守则提案。[12]

28. 一些与会国认识到，在落实规范的问题上，需要鼓励和支持区域进一步努力，并与私营部门和技术界等其他利益攸关方合作。例如，可以建立此类伙伴关系，确保能力建设工作可以持续，克服执行能力方面的差异。在这方面，与会国回顾大会第 73/27 号决议执行部分第 1.13 段，其中除其他外，强调“各国应鼓励私营部门和民间社会发挥适当作用，改善信通技术的安全和使用，包括信通技术产品和服务的供应链安全”。与会国指出，必须采取必要步骤开展外联与合作，确保包括公私部门和民间社会在内的各种利益攸关方履行其在使用信通技术方面的责任。

建立信任措施

29. 与会国在工作组讨论中指出，政府专家组协商一致报告中建议的建立信任措施依然具有现实意义。与会国强调指出了几项需要优先关注的措施，例如就以下问题进行定期对话和自愿交流信息：已有和新出现的威胁，国家政策，立法框架或理论，国家对国际法如何适用于国家使用信通技术问题的看法，各国界定关键基础设施的方式及对信通技术相关事件进行分类的方式。与会国建议，交流数字取证方法和调查恶意网络事件方面的良好做法既可加强合作也可建设能力。与会国还重点指出对概念和术语达成共识的益处，认为这是进一步开展国际合作和建立信任的切实步骤。其他此类措施包括制定关于实施建立信任措施的指导方针、对外交官的培训、就建立和运用安全危机沟通渠道的经验教训进行交流、人员交流、政策层面情景演练以及计算机应急小组或计算机安全事件响应小组之间在技术层面的行动演练。与会国还建议采取国家透明度措施，如自愿分享对执行情况调查作出的回复，或发表遵守负责任国家行为框架的国家宣言，以此作为建立对国家意图和承诺的信任和信心的其他途径。

30. 与会国考虑到区域机构在建立和维护联络点网络方面的经验，并借鉴现有网络，讨论了建立联络点全球中央名录的可行性。与此同时，与会国指出，这种名录的安全及其运作模式对其发挥实际效益至关重要，避免各种安排出现重叠或过于细琐同样至关重要。与会国还强调了定期在联络点网络之间进行演练的益处，因为这有助于保持预备状态和反应能力，确保联络点名录不断更新。

31. 由于建立信任措施可在双边、区域或多边各级制定，因此与会国还讨论了在联合国主持下建立一个全球建立信任措施资料库的可取性和可行性，目的是分享

[11] 该决议附有国家保护重要信息基础设施努力自愿自我评估工具。

[12] A/69/723，在 A/70/174 第 12 段中提到。

有关建立信任措施执行工作的政策、良好做法、经验和评估意见，并鼓励同行学习和对能力建设进行投资。此类资料库还能协助各国确定更多适合其国情和区域实情的建立信任措施，并为其他地方的调整适用提供潜在模式。与会国指出，任何新的全球资料库都不应与现有安排重叠，而且运作模式还需要进一步讨论。

32. 与会国还提请注意包括民间社会、私营部门、学术界和技术界在内的其他行为体在促进国家、区域和全球各级建立使用信通技术的信任和信心方面的作用和责任。与会国注意到各种多利益攸关方倡议。这些倡议通过制定原则和作出承诺，已经建立起新的交流、协作和合作网络。同样，针对特定部门或领域的倡议表明，人们已日益认识到其他行为体的作用和责任，并认识到其他行为体可以通过自愿承诺、专业守则和标准为信通技术安全作出的独特贡献。

能力建设

33. 与会国在工作组讨论中强调能力建设可以发挥重要功能，使所有国家增强权能，充分参与关于负责任国家行为框架的国际讨论，同时也有助于实现《2030 年可持续发展议程》[13] 等共同承诺。在这方面，与会国强调指出需要为能力建设方案分配足够的财政和人力资源。

34. 与会国重点指出国际组织、区域和次区域机构、民间社会、私营部门、学术界和专门技术机构等其他行为体在信通技术相关能力建设方面开展的重要工作，并鼓励思考如何促进这些努力相互协调、可持续、卓有成效并减少重叠的问题。

35. 联合国可以发挥重要作用，支持各国提高对能力建设的关注度，并利用联合国的召集力，支持更好地协调积极参与能力建设的各种行为体。与会国提议，可以利用联合国、其专门机构和广大国际社会中现有的平台加强既有的协调工作。可以利用这些平台分享各国对能力建设要求的看法，鼓励分享受援国和援助方的经验教训，并方便获取有关能力建设和技术援助方案的信息。这些平台还可支持筹集资源，或协助将现有资源与要求提供能力建设支持和技术援助的请求挂钩。与会国认为，在联合国主持下制定全球网络能力建设议程可有助于确保各项能力建设工作更加协调一致，并认为自愿的自我评估调查有助于各国认定并安排其能力建设需求的轻重缓急或提供支持的能力。

36. 与会国回顾，国家对维护安全、有保障和可信任的信通技术环境负有首要责任，但同时也强调必须采用多利益攸关方办法进行能力建设，以弥合社会所有相关部门的技术和政策差距。与会国特别指出，让地方民间社会、技术界、学术机构和私营部门行为体参与其中并与之结成伙伴关系的方式以及通过建立专家名册和中心可以加强能力建设的可持续性。在这方面，与会国还强调，采用跨部门、全盘统筹和多学科的能力建设方式可有助于国家保障信通技术安全，包括为此加

[13] 相关可持续发展目标和具体目标的例子包括但不限于以下各项：大幅提升信息和通信技术的普及度(9.C)；加强在科学、技术和创新领域的南北、南南、三方区域合作和国际合作，加强获取渠道(17.6)；加强国际社会对开展高效的、有针对性的能力建设活动的支持力度(17.9)。

强国家协调机构，在相关利益攸关方参与下评估方案的有效性。这种办法可能还有助于应对新兴技术带来的挑战。

37. 与会国呼吁注意“性别数字鸿沟”并敦促在国家和国际两级采取具体措施(包括收集按性别分列的数据)，解决性别平等以及妇女切实参与关于信通技术和国际安全的国际讨论和能力建设方案的问题。与会国对促进妇女参与多边信通技术安全讨论的方案表示赞赏，并强调指出需要加强这一专题与联合国妇女与和平与安全议程之间的关联。

38. 与会国指出，有许多障碍损害或降低能力建设的成效，重点指出在认定和完成各项能力建设工作时协调不力及缺乏互补是重大问题。与会国还提出一些实际关切问题，涉及对能力建设需求的认定、对能力建设援助请求的及时回应以及能力建设活动的设计、交付、可持续性和便于参与，而且缺乏衡量这种活动影响力的具体指标。在许多情况下，人力、财力和技术资源不足阻碍缩小数字鸿沟的能力建设工作和进展。能力建设一旦实现，一些国家便面临如何在竞争激烈的信通技术专业人员市场上留住人才的挑战。与会国提到，难以获得与信通技术安全有关的技术也是一个问题。

定期机构对话

39. 与会国在工作组讨论中回顾大会第 73/27 号决议为工作组规定的任务，即研究建立定期机构对话的可能性，并确认工作组在这方面的评估和建议将是其工作的核心成果。

40. 与会国对何种目标应成为今后定期机构对话的优先事项以及何种定期对话形式能够最有力地促进这些目标表达了各种不同的意见。一些国家表示希望定期对话优先关注已作承诺和建议的落实问题，包括制定支持和监测落实工作的指导方针；协调和加强能力建设成效；认定和交流良好做法。另一些国家则表示希望定期对话优先关注进一步深化已作出的承诺，并作出进一步的承诺，包括谈判达成具有法律约束力的文书以及支持该文书的体制结构。

41. 一些与会国就制定《行动纲领》推进网络空间负责任国家行为提出了具体建议，以期建立一个联合国常设论坛，审议从国际安全角度看国家使用信通技术的问题。与会国提议，该《行动纲领》将构成各国对商定建议、规范和原则所作的政治承诺；定期召开注重落实问题的会议；加强各国间的合作和能力建设；定期召开评审会议。此外，该《行动纲领》提议还设想广泛参与和协商。

42. 与会国注意到，通过 2020 年 12 月 31 日第 75/240 号决议设立了一个新的 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，该工作组应在第 73/27 号决议所设不限成员名额工作组工作结束后开始活动并审议其成果。

43. 与会国还表示希望国际社会最终回到在联合国主持下的基于共识的单一进程。在这方面，与会国指出，提议的不同对话形式并非一定相互排斥，认为不同的形式可以互补，或可以合并在一起，以便体现每种形式各自的特点，减少重复努力。

44. 此外，与会国还指出，有必要进一步考虑未来对话的时长和可持续性、对话应该是审议性的还是注重行动的问题、何时安排、可能的地点以及预算方面的考虑因素。

45. 与会国承认国家在本国和国际安全方面的独特作用和责任，但同时强调其他行为体的负责任行为对实现开放、安全、无障碍、和平的信通技术环境可作出重要贡献。在这方面，有人指出，增强多利益攸关方的合作和伙伴关系可有助于建立一个更有复原力和更安全的信通技术环境。

主席摘要的附件

议程项目“规则、规范和原则”下各代表团书面提交的具体语言建议

注意到许多代表团在其书面意见中提到了现有规范，以下内容仅反映其他语言建议。

亚美尼亚

- 各国将避免采取任何可能导致试图破坏关键基础设施和政府活动完整性的行动，并通过安全渠道及时作出澄清，以防止事态进一步升级。

澳大利亚、捷克共和国、爱沙尼亚、日本、哈萨克斯坦和美利坚合众国

为实施 2015 年规范 13(f)和(g)提供指导意见的案文

- 在为实施这些规范提供指导意见时，各国应注意，强调特定部门为关键基础设施并不是为了提供一份详尽的清单，不影响任何其他部门被国家指定或不被指定为关键基础设施，也不意味着暗中纵容针对未指定类别的恶意活动。

- 工作组在 COVID-19 大流行的背景下编写了这份报告。在此情况下，工作组强调，就规范(f)和(g)而言，所有国家都认为医疗服务和医疗设施是关键基础设施。

白俄罗斯

- 各国应重申其对放弃现有信通技术军事化、放弃创建专门为损害其他国家的信息资源、基础设施和关键设施而设计的新信通技术这一原则的承诺。

加拿大

建议将规范指导意见案文列入第 41 段

虽然 2015 年政府专家小组规范阐明了各国应该采取或不应该采取的行动，但各国强调需要就如何实施这些规范提供指导意见，并就这些规范提供了以下指导意见。根据工作组的理解，规范和指导意见都不妨碍、也不以任何方式改变或减少各国根据国际法享有的现有权利和义务。

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；(2015 ¶13(a))。

一. 本规范具有普遍性。实施整套规范以及下文提供的具体指导意见将有助于进一步落实本规范。各国应采取协作方式相互合作，并与包括工业界、学术界和民间社会在内的非政府利益攸关方合作。

二. 为此，各国应酌情并尽可能：

- 制定和实施全面的国家网络安全战略。这些措施应尽可能促进网络安全方面的国际合作

- 建立和维护事件响应职能，例如有能力进行协调、分享良好做法并在应对信通技术事件时进行合作的计算机应急小组

- 发表声明，大意是其将按照 2015 年联合国政府专家小组报告中阐述的网络空间负责任国家行为框架行事

- 参与旨在制定和实施建立信任措施的区域和双边举措。

三. 应鼓励会员国汇编和精简它们提供的关于其执行公认规范的信息。

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(2015 ¶13(b))。

一. 各国可以建立促进认真审议严重信通技术事件和确定适当应对措施所必需的国家结构、政策、程序和协调机制。

二. 一旦这些结构和程序到位，各国就可以制定信通技术事件评估或严重程度模板，以评估和评价信通技术事件。

三. 该等模板的透明化和区域组织对该等模板的协调统一可确保各国在审议信通技术事件时的共同性并改善各国之间的沟通。只要有可能，模板应与现有做法保持一致并避免重复。

四. 在考虑信通技术事件的所有相关信息时，各国应对可能产生的性别平等影响进行研究，并与所有利益攸关方进行包容性合作，以了解信通技术事件的更大背景，包括其对享有男女同性恋、双性恋和跨性别者权利和妇女权利的影响。

五. 各国应考虑信通技术事件对人权(包括表达自由的权利、和平集会和结社权利、不受任意或非法干涉隐私的权利以及残疾人的权利)的影响。

六. 各国应认识到，应对安全事件往往需要各利益攸关方的参与，而不仅仅是国家计算机应急小组/网络安全事件响应小组的参与，并应通过与所有利益攸关方群体开展培训和能力建设来改善协作。各国应鼓励包括民间社会在内的利益攸关方

进行旨在预防安全事件的数字安全培训和其他能力建设并提供援助，特别是针对脆弱社区和其他面临风险的用户开展这些工作。

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(2015 ¶13(c))。

一. 关于本规范的实施情况：

- 如果一国确定有源自另一国领土或网络基础设施的恶意网络活动，第一步可以通知后者。计算机应急小组对于能够识别此类活动至关重要。

- 鉴于信通技术事件可以源自第三国或涉及第三国，不言而喻，通知一国并不意味着该国对该事件负有责任。

- 被通知国应通过有关国家联络人确认收到请求。

- 当一国知悉其领土或网络基础设施正被用于利用信通技术进行的国际不法行为、且这种行为很可能在另一国产生严重不利后果时，前者应努力在其领土和能力范围内采取符合其国内和国际法义务的合理、可用和可行的措施，以促使停止该国际不法行为，或减轻其后果。

- 一国可在接到受影响国家的通知后获知该等行为。该等通知必须善意地作出并应附有佐证资料。佐证资料可包括共享可能的入侵指标，例如用于恶意信通技术行为的 IP 地址和计算机以及恶意软件信息。

- 应鼓励各国确保防止包括私营部门在内的非国家行为体为其自身目的或国家或其他非国家行为体的目的而进行恶意信通技术活动，损害第三方，包括位于另一国领土上的第三方。可以通过与私营部门合作使用基于风险的方法确定准许行动以及开发认证程序、最佳做法指南、事件应对机制和视情况而定的国家法规等具体工具来实现这一目标。

- 本规范不应被解释为要求一国主动监测其领土内的所有信通技术或采取其他预防措施。

二. 一国若意识到有害信通技术活动源自其领土但缺乏应对能力，可以选择向其他国家寻求援助，包括通过标准援助请求模板。

- 在此等情况下，可以向其他国家或私人实体寻求援助，如果提供援助，则应以符合国内法和国际人权法的方式提供。

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。(2015 ¶13(d))。

一. 在实施本规范时，各国应：

– 酌情考虑支持联合国预防犯罪和刑事司法委员会的工作，包括延长不限成员名额政府间专家小组的任务期限，并支持其正在进行的全面研究网络犯罪问题的努力。

– 支持联合国毒品和犯罪问题办公室继续根据请求并根据国家需要，通过网络犯罪问题全球方案及其区域办事处等，在预防、侦查、调查和起诉各种形式的网络犯罪方面，向会员国提供技术援助和可持续能力建设，以应对网络犯罪，同时认识到与会员国、相关国际和区域组织、私营部门、民间社会和其他相关利益攸关方的合作可为这一活动提供便利。

– 以符合其义务的方式实施现有措施，并考虑采取新措施，例如以符合各国人权义务并确保司法保证的方式通过打击网络犯罪的国家立法。

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、保护和享有人权的决议 A/HRC/RES/20/8 和 A/HRC/RES/26/13 以及大会关于数字时代的隐私权的决议 A/RES/68/167 和 A/RES/69/166，保证充分尊重人权，包括表达自由权。(2015 ¶13(e))

一. 各国应当：

– 在审议、制定或应用国家网络安全政策或立法时，或在设计和实施与网络安全有关的举措或结构(包括确保保护所有人权的措施)时，遵守国内法和国际法规定的义务。

– 为此，各国应在网络安全政策制定和执行的最早阶段纳入所有相关受影响利益攸关方的观点，以保障全面考虑网络安全措施的影响。

– 民间社会是促进国家履行人权义务和承诺的关键行为体，因此其参与尤为重要。

– 考虑到个人在网上与在网下享有同样的权利，并应铭记妇女和属于少数群体和弱势群体的个人在人权方面可能面临的不同威胁。

– 对国家或区域的网络安全政策进行性别平等审计，以确定需要改进的领域。

– 考虑将旨在解决信通技术对人权影响的措施纳入其工商业与人权问题国家行动计划。

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(2015 ¶13(f))。

一. 每个国家根据国家优先事项和关键基础设施分类方法确定其认为关键的基础设施或部门。提供基本公共服务的关键基础设施部门的例子可包括能源、水、环境卫生、健康、教育、金融、运输、电信和危机应对组织。关键基础设施还可包括对选举、公民投票或全民公决至关重要的技术基础设施以及对互联网的总体可用性或完整性至关重要的技术基础设施。强调这些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，也不姑息针对上文未具体阐述的关键基础设施类别的恶意活动。

二. 各国应考虑其信通技术活动对互联网总体可用性或完整性至关重要的技术基础设施的潜在有害影响。

g. 各国应考虑到大会关于创建全球网络安全文化及保护重要的信息基础设施的第 58/199 号决议和其他相关决议，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(2015 ¶13(g))。

一. 为了促进建设全球网络安全文化，各国应酌情考虑分享关于保护关键基础设施最佳做法的信息，包括本决议和以下内容中确定的所有要素：

- 基线安全要求；
- 事件通知程序；
- 事件处理工具和方法；
- 应急应对能力；
- 从过往事件中吸取的经验教训。

二. 建设全球网络安全文化的能力建设和其他措施应该以包容方式制定，并力求解决网络安全的性别层面问题。

三. 鉴于关键基础设施所有权的多样性和分散性，各国应酌情与相关利益攸关方协商，推广关键基础设施最低安全标准，并促进与私营部门、学术界和技术界在关键基础设施保护工作中的合作。

四. 各国应酌情参加有其他利益攸关方参与的自愿风险评估和业务连续性(应对能力、恢复和应急)规划举措，以针对现有和新出现的威胁加强在区域或国际层面提供服务的关键基础设施的安全性和应对能力。

五. 在开展保护关键信息基础设施的努力时应适当考虑有关隐私保护的适用国家法律和其他相关立法。

六. 在为实施规范(f)和(g)提供指导意见时，各国应注意，强调特定部门为关键基础设施并不是为了提供一份详尽的清单，不影响任何其他部门被国家指定或不被国家指定为关键基础设施，也不意味着暗中纵容针对未指定类别的恶意活动。

七. 工作组强调，就规范(f)和(g)而言，所有国家都认为医疗基础设施、医疗服务和设施是关键基础设施。工作组是在 COVID-19 大流行的背景下编写其报告的，因此对确认保护保健基础设施的必要性有特别强烈的感触。

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另一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。

一. 执行这一规范需要考虑适当的援助请求，并考虑可及时提供的援助的性质。在信通技术事件发生后收到适当援助请求的国家应在可能、合理和适当的情况下考虑：

- 通过相关国家联络人确认收到请求；

- 及时确定该国是否有能力和资源提供所请求的援助。这可能包括从一系列利益攸关方那里确定该国的专业技能；

- 在初步答复中，说明可能提供的援助的性质、范围和条件，包括提供援助的时限；

- 如双方商定将提供协助，迅速提供所安排的协助。

- 确保援助请求(包括框架和模板等相关进程和资源)以及回应符合人权义务。

二. 事先存在的国家架构和机制，包括国家联络人、援助请求模板和对拟提供援助的确认，以及有针对性的能力建设和技术援助，将进一步促进这一规范的实施。双边和多边合作倡议、国际和地区组织和论坛可在推动其发展方面发挥作用。

可以积极促进执行这一规范的办法可能包括：在国家和国际范围内加强公共-私营-民间社会组织的合作，特别是合作采取预防行动；通过有针对性的网络能力发展方式提高事件应对小组的能力；以及开展专门的培训，以建设国家各级和整个社会的网络能力。

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(2015 ¶13(i))。

一. 为实施这一规范，各国应：

- 采取步骤，包括通过现有论坛，防止恶意信通技术工具和技术的扩散。在这一过程中，各国应鼓励研究界、学术界、工业界、执法部门、计算机应急小组/计算机安全事故响应小组和其他网络保护机构开展合法活动，确保其信通技术系统的安全。

- 考虑就信通技术产品中与信通技术有关的漏洞和/或有害隐蔽功能开展信息交流。

- 努力实施基于风险管理的安全控制。

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，以限制并在可能情况下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(2015 ¶13(j))。

一. 为实施这一规范，各国应：

- 建立能够负责任地报告和处理信通技术漏洞的国家结构；

- 鼓励公共和私营部门实体之间建立适当的协调机制；

二. 此外，为避免误解或误读，包括因未披露关于可能有害的信通技术漏洞的信息而产生的误解或误读，鼓励各国酌情尽可能广泛地分享关于严重信通技术事件的技术信息，办法是利用计算机应急小组之间现有的协调机制，以及区域组织建立的机制(如联络人网络)。各国应确保负责任地处理此类信息，并酌情与其他利益攸关方协调。

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响应小组)信息系统的活动。一国不应利用授权应急小组从事恶意的国际活动。(2015 ¶13k))。

中国

- 各国应承诺，不应利用信通技术和信通技术网络开展有悖于维护国际和平与安全的活动。

网络空间中的国家主权

- 各国对本国境内的信通技术基础设施、资源以及信通技术活动行使管辖权。

- 各国有权制定符合本国国情的与信通技术有关的公共政策，管理本国的信通技术事务，保障公民在网络空间的合法利益。

- 各国不得利用信通技术干涉他国内政，破坏他国政治、经济和社会稳定。

- 各国应平等参与国际互联网资源的管理和分配。

关键基础设施保护

- 各国有权利和责任依法保护其重要的信通技术基础设施免受威胁、干扰和攻击破坏造成的损害。

- 各国应承诺不对他国的关键基础设施实施网络攻击。

- 各国不得利用政策和技术优势破坏他国的关键基础设施的安全性和完整性。

- 各国应就关键基础设施保护方面的标准和最佳做法加强交流，并鼓励企业开展此类交流。

数据安全

- 各国应平衡处理技术进步、商业发展与保护维护国家安全和公共利益的关系。

- 各国有责任和权利保护涉及本国国家安全、公共安全、经济安全和社会稳定的个人信息及重要数据的安全。

- 各国不得开展或支持利用信通技术开展的针对其他国家的间谍活动，包括大规模监控、窃取重要数据和个人信息。

- 各国应坚持发展与安全并重理念，推动数据依法有序自由流动。各国应加强这方面的最佳做法交流与合作。

供应链安全

- 各国不应利用其在信通技术领域的主导地位，包括在资源、关键信通技术基础设施和核心技术、信通技术产品和服务方面的主导地位，损害别国独立控制信通技术产品和服务及其安全的权利。

- 各国应要求信通技术产品和服务供应方不得通过在商品中设置后门非法获取用户数据、控制和操纵用户设备和系统。各国还应要求信通技术产品和服务供应方不得利用用户对其产品的依赖谋取不正当利益，强迫用户升级其系统或设备。各国应要求信通技术产品和服务供应方作出承诺，如果在其产品中发现严重漏洞，及时通知其合作伙伴和用户。

- 各国应致力于维护公平、公正和非歧视性的营商环境。各国不应以国家安全为借口限制信通技术的发展与合作，限制信通技术产品的市场准入和高科技产品的出口。

反恐怖主义

- 各国应禁止恐怖组织利用互联网开设网站、在线论坛和博客来进行恐怖活动，包括制作、发布、存储和传播恐怖音视频，宣扬暴力恐怖言论和思想，筹集资金、招募人员、煽动实施恐怖活动等。

- 各国应开展打击恐怖主义的情报线索交流和执法合作。例如，一国应在他国提出有关网络恐怖主义案件的协查请求时，及时留存和收集相关网络数据和证据，协助调查，并快速反馈。

- 各国应在打击网络恐怖主义方面与国际组织、企业和公民发展合作伙伴关系。

- 各国应要求互联网服务供应方关闭恐怖组织宣传网站和账户，删除恐怖主义和暴力极端主义内容，切断涉恐信息的在线传播渠道。

克罗地亚、芬兰、法国和斯洛文尼亚

- 应鼓励各国采取措施，防止包括私营部门在内的非国家行为体为其自身或其他非国家行为体开展有损第三方(包括位于另一国领土的第三方)的信通技术活动。

- 可以通过与私营部门合作，使用基于风险的方法确定可允许的行动，并开发认证程序、最佳做法指南、事件响应机制等具体工具和酌情颁布国家法规来实现这一目标。

古巴

这种情况要求执行对国际法构成补充的具体条例，除其他外，这些条例旨在解决以下同等重要的问题：

- 防止采取有碍于各国普遍获得信通技术所提供惠益的单边措施和针对国家措施的反制措施。
- 在面对网络攻击的情况下减轻认定责任归属的恶性影响。
- 防止网络空间军事化。
- 通过推动这方面的国际法规，更有效地保护公民的私人数据。
- 对网络恐怖主义立法进行补充，以应对网络安全事件和问题，如网络攻击。以协商一致的方式界定对网络攻击的理解。
- 以更大的客观性实施这一领域的国际法原则。

捷克共和国

- 各国不应进行或蓄意支持会损害医疗服务或医疗设施的网络活动，并应采取措施保护医疗服务不受到危害。[14]
- 在审议、制定和适用国家网络安全政策和立法时，需要遵守国际人权法规定的现有义务。[15]
- 需要在网络安全政策制定的最初阶段纳入所有相关和受影响利益攸关方的观点，以确保全面考虑网络安全措施对人权的影响。[16]

厄瓜多尔

- 关于规范 13.b(政府专家小组 2015 年建议)的指导意见：[17]

㈠ 各国可以建立必要的国家结构、政策、程序和协调机制，以便认真审议严重的信通技术事件，并确定适当的应对措施；

㈡ 然后，各国可以开发信通技术事件评估或严重性模板，以评价和评估信通技术事件；

[14] https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-buildinternational-law。

[15] https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf。

[16] https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf。

[17] 一旦发生信通技术事件，各国应考虑所有相关信息，包括所发生事件的更广泛背景，信通技术环境中归责方面的困难，以及后果的性质和范围。

㈢ 区域组织对此类模板保持透明和统一，可确保各国在审议信通技术事件时采取共同的方式，并改善各国之间的沟通；

㈣ 在审议信通技术事件的所有相关信息时，各国应就其对不同性别的可能影响进行研究，并以包容的方式与所有利益攸关方进行合作，以了解信通技术事件的更广泛背景，包括其对妇女享有权利的影响。

- 为执行规范 13.c 提出了以下指导意见：[18]

㈠ 如果一国发现源自另一国区域或网络基础设施的恶意网络活动，首先可通知该国。要能识别此类活动，计算机应急小组的作用至关重要；

㈡ 鉴于信通技术事件可能来自第三国或涉及第三国，应当理解的是，通知一国并不意味着该国对该事件负有责任；

㈢ 被通知国应通过有关国家联络人确认收到请求；

㈣ 当一国知悉其领土或网络基础设施被用于可能对另一国造成严重不利后果的国际不法行为时，应根据其国内法和国际法义务，努力在其领土和能力范围内采取合理、可用和可行的措施，使该国际不法行为停止或减轻其后果；

㈤ 这一规范不应被解释为要求一国主动监测其领土内的所有信通技术，或采取其他预防措施；

㈥ 当一国意识到有害信通技术活动源自本国领土但缺乏应对能力时，可以选择向其他国家寻求援助，包括通过标准的援助请求模板寻求援助；

㈦ 在这种情况下，可以按照符合国家法律的方式向其他国家或私人实体寻求援助。各国承诺在发生危机时与其他国家合作并提供援助是非常重要的，应特别强调信通技术事件对发展中国家特定基础设施可能产生的不同影响。

- 草案还应包括新的规范；其中包括：

“各国不应开展信通技术行动破坏选举、全民投票或全民表决等政治进程所必需的技术基础设施。”

印度

- (关于第 39 段)：有关新规范的提案涉及的问题是：有必要制定关于网络空间基本安全的商定标准，界定在保护公众的同时优化有应用前景的技术的最有效方式。为此，各国应大力支持广泛采用和验证实施基本的网络卫生。

- 保护关键信息基础设施是各国负责任的行为。对关键信息基础设施的威胁会破坏信息的完整性，损害国家的经济和经济发展。各国必须考虑通过公私伙伴关系保护关键信息基础设施。各国不应开展破坏关键信息基础设施的信通技术行动。各国不应在信通技术产品中设置有害功能。各国应负责在发现重大漏洞时通知用

[18] 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。

户，并通知供应商修补漏洞。各国应合作开展关键信息基础设施活动，交流有关威胁的信息，分享缓解工具和技术。

伊朗伊斯兰共和国

- 各国对维护有保障、安全和可信赖的信通技术环境负有首要责任，应加强它们在全球一级信通技术环境治理，包括政策和决策方面的作用。设想的治理应以加强国家主权的方式实现，不应影响各国在信通技术环境中选择发展、治理和立法模式的权利。

- 各国应避免在信通技术环境内或通过信通技术环境武力威胁或使用武力危害任何国家的领土完整或政治独立。

- 任何国家都无权通过与网络有关的方式和手段，直接或间接、以任何理由干涉别国的内政或外交事务。应谴责和防止对各国政治、经济、社会和文化系统以及与网络有关的关键基础设施的一切形式的干预和干扰或威胁企图。(联合国大会 1965 年 12 月 21 日第 2131 号决议)

- 各国不得将信通技术进步用作实施经济、政治或任何其他类型的强制性措施的工具，包括限制和阻止针对目标国的措施。(联合国大会 1965 年 12 月 21 日第 2131 号决议)

- 各国应确保采取适当措施，以期使具有域外影响的私营部门，包括平台，对其在信通技术环境中的行为负责。各国必须对其管辖范围内的信通技术公司和平台实施应有的控制，否则它们将对蓄意侵犯其他国家的国家主权、安全和公共秩序负责。

- 各国应避免并防止滥用在其控制和管辖下开发的信通技术供应链来制造或协助开发产品、服务和维护方面的漏洞，损害目标国的主权和数据保护。

日本

作为对确保供应链完整性的规范(i)的指导意见，日本向不限成员名额工作组提出的新建议是增加以下措辞：

- “各国有权利和责任确保使用值得信赖的信通技术设备和系统供应商，特别是在解决国家安全问题和保护隐私方面。合理的步骤可能包括立法或行政措施，以确保供应链安全，支持可靠和值得信赖的技术和工业的发展，使供应商多样化。”

荷兰

- “国家和非国家行为体既不应进行也不应允许蓄意实质性损害互联网公共核心的普遍可获得性或完整性，从而损害网络空间稳定性的活动”[将是]执行联合国政府专家小组 2015 年建议 13(f)的指导，因此也属于联合国政府专家小组 2015 年建议 13(g)的范围。

- “国家和非国家行为体不得从事、支持或允许旨在破坏选举、全民投票或全民表决所必需的技术基础设施的网络行动，”[将是]执行联合国政府专家小组2015年建议13(f)的指导，因此也属于联合国政府专家小组2015年建议13(g)的范围。

不结盟运动

- 应鼓励会员国汇编和精简它们提交的关于其执行国际规则的信息和相关的拟议存放处，以期从国际安全的角度规范国家使用信通技术的各具体方面，并确定共同关注的领域。

- 会员国不应开展或蓄意支持任何违反国际法、故意破坏或损害其他成员国关键基础设施使用和运营的信通技术活动。

- 应敦促会员国考虑就信通技术产品中与信通技术有关的漏洞和/或有害隐蔽功能交换信息，并在发现重大漏洞时通知用户。

- 会员国在开展所有与信通技术有关的活动时还应考虑到联合国大会第73/27号决议。

- 不结盟运动重申对越来越多诉诸单边主义的行为的强烈关切，并在此背景下强调，根据《联合国宪章》，多边主义和多边商定的解决方案是解决国际安全问题的唯一可持续方法。

- 不结盟运动重申，各国应避免在信通技术环境内或通过信通技术环境武力威胁或使用武力危害任何国家的领土完整或政治独立。

- 不结盟运动呼吁加强努力，保障网络空间不成为冲突的舞台，确保完全和平利用信通技术，使其能够充分发挥促进社会和经济发展的潜力。

- 不结盟运动强调，必须避免对和平利用信通技术、国际合作或技术转让施加不适当的限制，包括通过单方面胁迫措施。

- 不结盟运动强调，各国负有维护开放、安全、稳定、无障碍以及和平的信通技术环境的首要责任。

- 不结盟运动强调，所有国家都不应违反国际法规定义务故意开展或支持蓄意破坏或损害关键基础设施使用和运营的信通技术活动。

巴基斯坦

- 应鼓励会员国继续酌情考虑是否可能通过一项具有法律和/或政治约束力的文书，以规范国家在国际安全背景下使用信通技术的具体方面。

- 应鼓励会员国就什么是“关键基础设施”达成一致的共同定义，以期就禁止开展故意或蓄意破坏关键基础设施或以其他方式损害关键基础设施的使用和运营的信通技术活动达成一致。

- 应鼓励成员国开展合作，就禁止在信通技术产品中创建有害隐蔽功能或累积漏洞达成协议，并承诺及时、负责任地报告信通技术漏洞，分享有关此类漏洞可用补救措施的相关信息。

- 会员国应努力促进与信通技术产品和服务提供商的合作，以防止利用或滥用用户的数据和隐私。

- 会员国应承诺不利用信通技术开展有悖于维护国际和平与安全的活动，不利用信通技术以任何方式干涉别国内政。

- 会员国应合作应对信通技术环境中与认定责任归属相关的挑战。在联合国主持下，在全球适用的范围内制定共同的认定责任归属办法，仍然是这方面最有效的前进道路。

- 必须敦促会员国达成协议，禁止旨在破坏选举或全民投票或全民表决所必需的技术基础设施的信通技术活动。

- 应鼓励会员国制定和实施规范，避免对和平利用信通技术、该领域的国际合作或技术转让施加不必要的限制。

大韩民国

关于政府专家小组 2015 年建议第 13(c)段指导意见的建议：

- 当受影响国通知另一国信通技术事件源自或涉及被通知国领土，并提供合格信息时，被通知国应根据国际法和国内法，并在其能力范围内，在其领土内采取一切合理步骤，促使这些活动停止，或减轻其后果。

- 应当理解，上述通知并不意味着被通知国对该事件负有责任。

- 对合格信息的最低要求可能包括失陷指标，例如 IP 地址、犯罪人和用于实施恶意信通技术行为的计算机的位置以及恶意软件信息。