联合国 A/AC.292/2024/2

大 会

Distr.: General
22 January 2024
Chinese
Original: English

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

第七届实质性会议

2024 年 3 月 4 日至 8 日，纽约

摸底调查联合国内外以及全球和区域层面的能力建设方案和举措的概况

秘书处编写的文件

一. 导言

1. 在题为“从国际安全角度看信息和电信领域的发展”的文件(A/78/265)附件所载工作组关于议程项目 5 讨论情况的进度报告第 46 段中，请联合国秘书处与有关实体协商，开展“摸底调查”，以调查联合国内外以及全球和区域层面的能力建设方案和举措的概况，包括通过征求会员国的意见。还请秘书处编写一份内载“摸底调查”结果的报告，并将该报告提交定于 2024 年 3 月 4 日至 8 日举行的 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七届会议，以支持各国努力评估现有的信通技术安全能力建设工作，并鼓励这些工作之间进一步协同增效、相互协调。本报告根据这一要求提交。

2. 2023 年 10 月 2 日，裁军事务厅向所有常驻联合国代表团分发了一份普通照会，提请它们注意上述报告第 46 段，并邀请它们就联合国内外以及全球和区域层面的信息和通信技术能力建设方案和举措的概况提出意见。答复的截止日期定为 2023 年 11 月 10 日，后来延长至 11 月 16 日。截至 2024 年 1 月 22 日，以下国家提交了书面意见：澳大利亚、比利时、巴西、布基纳法索、柬埔寨、智利、哥伦比亚、古巴、捷克、爱沙尼亚、法国、德国、印度、伊朗伊斯兰共和国，荷兰王国、黎巴嫩、墨西哥、葡萄牙、卡塔尔、大韩民国、俄罗斯联邦、新加坡、斯洛伐克、斯洛文尼亚、瑞士、土耳其、大不列颠及北爱尔兰联合王国、美利坚合众国和乌拉圭。

3. 裁军事务厅还通过 2023 年 10 月 2 日的信函请联合国系统相关实体发表意见。于 2024 年 1 月 22 日，以下联合国实体提交了书面意见：国际电信联盟、反恐怖主义委员会执行局、联合国开发计划署、联合国裁军研究所、联合国区域间犯罪和司法研究所、反恐怖主义办公室、信息和通信技术厅、法律事务厅和联合国毒品和犯罪问题办公室。

4. 2023 年 10 月 2 日，还通过电子邮件向相关非政府利益攸关方实体发出了征求意见的呼吁。截至 2024 年 1 月 22 日，以下利益攸关方实体提交了书面意见：进步通信协会、德里国家法律大学通信治理中心、外交基金会、全球网络专业知识论坛、国际商会、斯 • 拉贾拉南国际研究学院国家安全卓越中心、信息技术提供商 SafePC Solutions、Third Eye Legal 公司和 Write Pilot 机构。欧洲联盟也提交了意见。还收到以下联合书面意见：阿根廷、巴西、智利、哥伦比亚、哥斯达黎加、厄瓜多尔、萨尔瓦多、危地马拉、多米尼加共和国、巴拉圭和乌拉圭联合提交的意见；捷克国家网络和信息安全局、红十字国际委员会、北大西洋公约组织(北约)合作网络防御卓越中心、埃克塞特大学、美国海军战争学院和武汉大学联合提交的意见。

5. 所有收到的书面意见，包括在正式延长的截止日期之后收到的意见，均可在 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网站上查阅。[1] 鼓励各国查阅会员国、联合国系统各实体和非政府利益攸关方实体提供的书面材料全文，因为本报告并不代表其中所述所有活动的详尽清单。

6. 本报告主要借鉴了上述会员国、联合国系统实体和非政府利益攸关方实体提供的资料，但不影响其各自的立场。本报告还介绍了从公开来源获得的其他信息，以期呈现联合国内外以及全球和区域层面现有能力建设方案和举措的平衡而生动的全貌。

7. 本报告介绍了能力建设方案和举措的实例，首先着重介绍了区域和次区域层面的努力，然后提供了按主题大致分类的信息。这些说明并不代表所有能力建设举措和方案的详尽清单，而是试图以说明的方式提供活动的总体情况。没有暗指活动的优先次序或等级。

8. 本报告最后载有秘书处的意见和结论，以期支持各国在全球、区域和次区域各级采取更加有效、可持续和高效的能力建设举措。

二. 各国关于多边层面能力建设的讨论和结论概述

9. 鉴于各国在国际安全方面使用信息和通信技术所产生的威胁不断变化，各国继续特别强调指出，正如 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(A/78/265)申明，迫切需要加强所有国家的能力，以遵守和执行负责任国家行为不断演变的累积框架。

[1] 可查阅 https://meetings.unoda.org/meeting/57871/documents。

10. 各国着重强调，应促进更好地了解发展中国家的需要，以便通过有针对性的能力建设努力缩小数字鸿沟。各国特别强调，除技术技能、体制建设和合作机制外，还迫切需要外交、法律、政策、立法和监管等一系列领域中的建设能力和良好做法。各国不同程度地强调南南合作、三边合作、次区域合作和区域合作作为南北合作的补充的价值。各国还回顾了培训员培训办法的价值，即通过设立专门培训和针对特定需要的课程及专业认证，向相关对应方传授必要的知识和技能。

11. 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框架内，各国继续就能力建设工作提出注重行动的具体建议，其中除其他外，包括三项建议，分别涉及开发全球网络安全合作门户网站；鼓励进一步就信息和通信技术威胁进行技术交流，以识别和检测恶意活动，并协助对这些活动做出知情应对；在能力建设领域，包括为培训和研究目的，促进非政府利益攸关方有意义的参与和伙伴关系。

12. 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本身已被确认为一个平台，继续就能力建设工作交流意见和想法，包括如何最好地利用现有举措，以支持各国发展体制力量，落实负责任的国家行为框架。

13. 各国继续促进关于从国际安全角度看国家使用信通技术方面的能力建设原则主流化，这些原则载于 A/78/265 号文件附件 C，并在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最后报告中首次阐述。[2] 各国赞同这些原则，认为能力建设应当是可持续的进程，包括注重成果的具体活动，同时也具有明确的目的，而且以证据为依据、政治上中立、透明、问责、不设条件。此外，各国一致认为，能力建设应以充分尊重国家主权原则的方式进行，以需求为导向，符合国家确定的需求和优先事项，并尊重人权和基本自由。不限成员名额工作组在其第二次进度报告(A/78/265)中建议各国制定并分享自愿清单和其他工具，以便将执行议定的能力建设原则纳入主流。

14. 通过 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讨论，各国继续提高对信息和通信技术使用安全的性别层面的认识，并在政策层面以及在能力建设项目的选择和实施方面促进对性别问题具有敏感认识的能力建设。各国继续鼓励努力开展促进性别平等的能力建设工作，包括将性别平等观点纳入国家信通技术及能力建设政策，以及编制清单或调查问卷，以确定该领域的需求和差距。

15. 各国认为，联合国可在协调能力建设努力方面发挥重要作用，评估各国的需求，通过各种工具和调查找出差距，并协助各国利用能力建设方案，包括通过目前的“摸底工作”。

[2] A/75/816，附件一，第 56 段。

三. 区域、次区域和跨区域合作

16. 各国一贯重申，区域和次区域组织支持执行在使用信息和通信技术方面国家负责任行为框架方面发挥重要作用，包括支持相关的能力建设举措。各国对可在区域、次区域和跨区域各级作出的努力进行了不同的反思，包括举办讲习班、培训班和交流最佳做法和经验教训。还鼓励各国支持能力建设方案，包括酌情与区域和次区域组织合作。[3]

17. 在跨区域合作方面，全球网络专门知识论坛是由 200 多个成员和伙伴组成的多方利益攸关方群组，其中包括来自所有区域的国家、国际和区域组织以及私营部门、民间社会和学术界的行为体。Cybil 门户网站是全球网络专门知识论坛的一个旗舰举措，是国际网络能力建设项目的在线储存库，并为感兴趣的利益攸关方提供了一个资源库。[4]

18. 2023 年 11 月，全球网络专家论坛与加纳、世界经济论坛、世界银行和网络和平研究所合作，举办了首届网络能力建设全球会议。会议包括专题会议和深入讨论的区域会议。会议产生了一份成果文件，即阿克拉网络复原力发展呼吁，其中包括一套不具约束力、自愿、确定方向的行动，旨在：(a) 加强网络复原力作为可持续发展推动力的作用；(b) 推进以需求为导向、有效和可持续的网络能力建设；(c) 促进更强有力的伙伴关系和更好的协调；(d) 释放财政资源和开启实施模式。[5] 会议宣布，下一届网络能力建设全球会议将于 2025 年 5 月在日内瓦举行，目标是在加纳会议取得进展的基础上再接再厉。

19. 为了加强各区域之间的合作，欧洲联盟-拉丁美洲和加勒比数字联盟主办了监管和网络安全对话，以及关于数字和空间问题的其他活动。该联盟旨在本着以人为本的数字经济和社会愿景，支持数字转型和创新。为了实现这些目标，联盟的活动包括建立两个区域数字政策对话；扩大建立欧洲与拉丁美洲联系方案；实施区域哥白尼战略，通过支持空间数据管理能力和战略使用来提高数字复原力；建立欧洲联盟-拉丁美洲和加勒比区域数字加速器，以促进创业和创新。

20. 正在进行的题为“加强亚洲内部和与亚洲的安全合作”项目得到欧洲联盟的支持以及法国和德国的资助，该项目旨在加强欧洲联盟与伙伴国家在政策和做法上的趋同，提高认识，并支持业务安全对话。[6] 该项目在四个专题领域开展活动：反恐和预防暴力极端主义、网络安全、海事安全和危机管理。目前的参加国是印度、印度尼西亚、日本、大韩民国、新加坡和越南。

---

[3] A/78/265，附件，第 51 段。

[4] 见 https://cybilportal.org/about-cybil/。

[5] 可查阅 https://gc3b.org/news/read-the-full-accra-call-for-cyber-resilient-development/。

[6] 见 www.eeas.europa.eu/sites/default/files/factsheet_eu_asia_security_july_2019.pdf。

21. 在中欧和东欧地区，法国、黑山和斯洛文尼亚于 2023 年 5 月启动了西巴尔干网络能力中心。[7] 该中心旨在支持六个参加国家和地区加强机构和业务网络能力。活动包括培训课程、编制网络课程以及交流信息和最佳做法，以支持西巴尔干国家的从业人员预防、防备和应对网络威胁。2023 年，该中心为公共行政部门提供了网络安防培训课程，为妇女提供了网络决策和国际谈判辅导方案，为司法当局和警察部队提供了网络犯罪课程，为重要基础设施的首席信息安全干事提供了课程。在编写本报告时，计划于 2024 年再举办 12 个培训班。同样，由捷克和爱沙尼亚共同牵头的一个欧洲联盟项目旨在通过发展以下方面支持西巴尔干国家网络安全能力建设：(a) 网络安全治理和认识；(b) 加强法律框架、网络规范和遵守国际法；(c) 风险和危机管理；(d) 业务能力，包括加强计算机安全事件响应小组。为支持抵御网络事件，还实施了欧洲联盟另一个题为“阿尔巴尼亚、黑山和北马其顿网络安全快速反应”的项目。

22. 欧洲安全与合作组织(欧安组织)跨国威胁部开展活动，以加强参加国应对信息和通信技术安全威胁的能力。活动范围包括促进对涉及关键基础设施的事件作出适当反应的演习、关于打击互联网被用于恐怖主义目的讲习班以及关于调查和起诉网络犯罪的培训。[8] 2023 年，该部在维也纳举办了国际网络外交培训班，重点是建设国家参与国际网络政策审议的能力。欧安组织实行国家网络事件严重程度等级和保护关键基础设施的相关措施，支持欧洲、中亚和其他国家制定危机沟通和管理程序以及事件分类方法。此外，欧安组织还是若干网络合作和能力建设讨论的多边论坛。

23. 俄罗斯联邦与东南亚国家联盟(东盟)地区论坛举办若干年度研讨会和在线讲习班，内容涉及信息和通信技术安全和使用领域的术语、打击为犯罪目的使用信息和通信技术行为以及互联网的可持续和安全发展和数字取证。俄罗斯联邦还在亚洲相互协作与建立信任措施会议上主办了关于调查与信息和通信技术有关的贪污犯罪的培训。

24. 国际电信联盟(国际电联)与应对网络威胁国际多边伙伴关系合作，在阿曼的支持下设立了阿曼-国际电联区域网络安全中心。[9] 该中心设在阿曼计算机应急小组所在地，旨在加强阿拉伯区域网络安全、保护关键基础设施和能力建设领域的能力、实力、准备状态、技能和知识。

25. 美洲国家组织(美洲组织)美洲反恐怖主义委员会通过其网络安全方案，支持成员国建设技术、政治和外交能力，以预防、查明、应对网络事件并从中恢复，并促进网络空间国家负责任行为。[10] 除其他活动外，该方案还协助制定国家网络安全战略和建立国家网络安全事件响应小组。该方案还为决策者、工业界和民间

[7] 见 https://cybilportal.org/projects/western-balkans-cyber-capacity-centre-wb3c/。

[8] 见 www.osce.org/secretariat/cyber-ict-security。

[9] 见 www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.spx。

[10] 见 www.oas.org/ext/en/security/prog-cyber。

社会提供援助和培训、工具包和指南，并在美洲运营网络安全事件响应小组半球网络，该网络在美洲组织 20 个成员国的 29 个网络安全事件响应小组中分享威胁和情报信息。该方案还支持将性别平等视角进一步纳入网络安全决策和多边进程代表性的主流。

26. 伊比利亚美洲网络防御论坛于 2023 年 10 月在巴西举行。[11] 约 13 个国家参加了论坛，目的是深化区域一体化与合作，以防止、查明和应对网络威胁。活动包括模拟演习和演练，包括网络卫士 5.0 演习和开发恶意软件信息共享平台。

四. 按重点专题领域分列的能力建设举措的非详尽说明性概览

国际法

27. 各国承认，在信息和通信技术安全方面，特别需要在国际法领域采取能力建设举措。各国特别强调，迫切需要继续开展此类能力建设工作，包括确保所有国家都能平等地参与就国际法如何适用于信息和通信技术的使用达成共识。这些努力包括在国际、区域间、区域和次区域各级举办讲习班、培训班和交流最佳做法。各国还注意到提供能力建设的价值，以期编写关于国际法适用于国家使用信息和通信技术的国家立场文件。

28. 关于国际法领域能力建设的全球现有在线资源包括网络法工具包，由捷克国家网络和信息安全局、红十字国际委员会、北约合作网络防御卓越中心、埃克塞特大学、美国海军战争学院和武汉大学。[12] 该工具包免费提供给政府和法律专业人员，目前包括：(a) 28 种情景，探讨国际法对网络行动的适用性；(b) 关于对信息和通信技术的使用适用国际法的国家立场的信息，包括与主权、不干涉或国际人道法关于何为攻击的规定有关的立场；(c) 50 多个网络事件页面，提供关于最近的攻击或正在进行的武装冲突的信息。

29. 2020 年，牛津道德、法律和武装冲突研究所与微软公司合作，启动了牛津网络空间国际法保护进程。[13] 在编写本报告时，牛津进程已经产生了五份“关于国际法保护的牛津声明”，这些声明是全球国际法律专家合作的产物，旨在确定和澄清适用于各种情况下网络作战的国际法规则，包括保护保健部门、保障疫苗研究、防止选举干预以及对信息业务和活动及勒索软件业务的监管。

30. 关于国际人道法对网络空间的适用性，红十字国际委员会为决策者提供资源，包括研究论文、讲习班和专题讨论会，并设立了红十字国际委员会网络空间代表团，该代表团设在卢森堡并得到卢森堡的支持。最近开展的活动包括：与剑桥大学艺术、社会科学和人文研究中心合作启动人道主义行动方案；与日内瓦国际人道法和人权学院合作，主办于 2023 年 9 月 28 日和 29 日在日内瓦举行的国际专家会议，内容涉及国际人道法，以及让平民在武装冲突期间更多地参与网络和其

[11] 见 https://dialogo-americas.com/articles/brazil-leads-ibero-american-cyber-defense-forum/。

[12] 见 https://cyberlaw.ccdcoe.org/wiki/Main_Page。

[13] 见 www.elac.ox.ac.uk/the-oxford-process/。

他数字行动；与国际法研究学会合作，于 2023 年 5 月 17 日在伊斯兰堡举行了关于网络战的圆桌会议。

31. 澳大利亚、荷兰王国和新加坡与网络法国际任凭，面向东盟和欧安组织成员国的国家官员协调提供关于网络作战国际法的国际网络法培训课程。

32. 日本国际协力机构通过关于国际法和政策制定方面能力建设的培训，加强确保网络安全的措施，为发展中国家政府机构官员和国家计算机应急小组提供有效制定执行网络安全政策所需的国际法和政策知识和技能。

33. 各国还进行了各种协商，以便有空间就国际法的适用性进行对话。例如，美洲国家组织与美洲法律委员会和红十字国际委员会合作，主办了关于适用于网络空间的国际法的协商会议。[14] 此外，墨西哥与宾夕法尼亚州天普大学法律、创新和技术研究所以及微软公司合作，主办了三个虚拟讲习班，内容涉及国际法在网络空间的适用、促进和平行为的规则和规范以及弥合数字鸿沟。该项目编制了关于在网络空间适用国际法的多方利益攸关方良好做法和建议汇编，于 2023 年 12 月在信息和通信技术安全和使用安全不限成员名额工作组第六届实质性会议上发布。

34. 欧安组织与荷兰王国合作，并在意大利、斯洛伐克、瑞士、大不列颠及北爱尔兰联合王国、大韩民国和网络法国际的额外支持下，举办了关于网络作战国际法的行政课程，包括 2023 年 2 月 13 日至 17 日在斯科普里举办的课程。

政策，包括制定国家战略

35. 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在 A/78/265 号文件所载第二次年度进展报告附件 B 中，商定一份自愿性全球建立信任措施初步清单。在这些措施中，有一项措施鼓励各国继续在自愿基础上分享概念文件、国家战略、政策和方案。此外，各国还认识到，必须具备必要的能力，为营造安全的信息和通信技术环境制定必要的政策、立法和战略。在此背景下，开展了各种能力建设努力，以支持各国制定国家政策、拟定战略并建立国际安全背景下具备相关信息和通信技术能力的必要机构和结构。

36. 在全球一级，联合国裁军研究所(裁研所)主办年度网络稳定会议，讨论促进安全稳定的网络空间、规范和国际法以及支持关于网络安全问题的多边对话。在以往的会议中，学者们作了专题简报，支持各国阐述本国的观点，包括与和平解决国家使用信息和通信技术有关的争端的法律问题，以及保护各部门关键基础设施和服务的政策和技术问题。以往会议还侧重联合国主持下的相关政府间进程。下一次网络稳定会议将于 2024 年 2 月 29 日和 3 月 1 日在纽约举行。

37. 各国还确认裁研所网络政策门户网站的价值，该网站是各国通过分享相关信息、政策、立法和其他良好做法自愿采取透明度措施的有用形式。[15] 截至 2023 年

[14] 见 www.oas.org/en/sla/dil/International_Law_Applicable_to_Cyberspace_2022.asp。

[15] 见 https://cyberpolicyportal.org/。

12 月，已有 1 528 份文件上传到网络政策门户网站数据库，以 55 种语言提供文件，并公布了关于 897 个能力建设项目的信息。2023 年，门户网站的访问量约为 23 000 次。

38. 2023 年 12 月，网络政策门户网站整合了全球网络专门知识论坛 Cybil 门户网站的近 900 个能力建设项目。数据交换包括项目详情，如项目名称、受益人信息、供资者以及项目起止日期，并以联合国六种正式语文提供。该倡议通过提高对现有资源的认识、促进利益攸关方之间的合作以及鼓励提高网络能力建设工作的透明度，加强信息和通信技术的安全和使用。

39. 国际电联与世界银行、联合国贸易和发展会议(贸发会议)和英联邦电信组织合作，为建立有效的国家网络安全框架提供政策支持。为此，国际电联于 2021 年出版了第二版《国家网络安全战略制定指南》，[16] 为政策制定者概述了战略制定过程，同时考虑到各国的具体国情、文化和社会价值观。此外，国际电联还提供在线培训课程，通过四个电子学习模块和一个基于《指南》的在线桌面演练，帮助国家政策制定者以及公共和私营部门的网络安全从业人员做好准备。[17] 还可在线查阅更新的国家网络安全战略资料库，其中载有国家政策、行动计划和与网络安全有关的其他相关内容。[18]

40. 联合国-新加坡网络研究金方案每年举行两次为期六天的会议，被提名的国家官员参加会议，以建设关于国家网络和数字安全政策、战略和行动的能力和网络。继该方案的前三次会议之后，计划于 2024 年再举行两次会议。该方案有一个由代表 62 个会员国的 70 多名研究员组成的校友网络。

41. 荷兰王国与美国观察员研究基金会共同资助了全球网络政策对话系列。两年多来，该项目支持制定国家网络安全战略，并在东南亚、西巴尔干、中东和北非、南部非洲以及拉丁美洲和加勒比主办了区域网络政策对话。该项目还旨在促进安全的数字化转型和公私伙伴关系，确定能力建设需求和差距，并支持继续制定网络空间国家行为规范。

42. 作为数字促进发展中心的一部分，欧洲联盟、德国、法国国际合作署、国际和伊比利亚美洲行政和公共政策基金会以及非洲之角倡议开展合作，在非洲之角区域实施了一项数字政府和网络安全倡议。[19] 该项目旨在协助参加国(吉布提、肯尼亚和索马里)通过安全的数字渠道加强公共部门服务的提供。该项目包括通过区域技术委员会开展对话和信息交流，以及审查各国正在实施的路线图和数字化项目。

[16] 见 https://ncsguide.org/the-guide/。

[17] 见 www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx。

[18] 见 www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx。

[19] 见 www.fiiapp.org/en/proyectos_fiiapp/d4d-initiative-for-digital-governance-and-cybersecurity-idgc-for-the-horn-of-africa-initiative/。

43. 在双边方面，法国和塞内加尔在达喀尔建立了面向区域的国家网络安全学校，除其他活动外，该学校提供培训，加强合作，并提高非洲国家对网络安全的认识。[20] 葡萄牙支持正在与安哥拉、佛得角、几内亚比绍、莫桑比克、圣多美和普林西比和东帝汶合作开展的战略合作方案，这些方案加强法律和行政结构，以防止、查明和应对网络犯罪、网络恐怖主义和网络事件，这也是目前许多双边方案的一个例证。

44. 在亚洲，设在大韩民国的全球网络安全促进发展中心应请求向各国提供援助，以建设公共部门网络专门知识和网络复原力。可应以下方面举办研讨会：起草国家网络安全战略和框架；建立和运作国家计算机应急小组；发现、分析和应对网络事件；分享关于网络趋势和威胁的信息。[21] 最近在哥斯达黎加、老挝人民民主共和国和塞尔维亚主办了关于网络安全战略制定、事件处理、网络安全和复原力等主题的研讨会。

45. 作为其网络和关键技术合作方案的一部分，澳大利亚外交和贸易部支持其电子安全专员开发全球在线安全资源，并与亚洲和太平洋各国政府合作制定国家办法，以保障公民在线安全。[22] 该方案与工业界、学术界、民间社会、澳大利亚政府机构和其他志同道合的捐助者合作，支持东南亚和太平洋地区超过 25 个国家促进和保护其在网络空间的集体利益。

46. 在美洲，加拿大、墨西哥和美利坚合众国在 2023 年 1 月举行的北美领导人峰会的框架内参加了网络安全圆桌会议，以加强与会国在制定执行网络安全政策方面的合作。2023 年 10 月 8 日至 14 日，哥伦比亚和捷克共同召开了关于网络安全与人工智能交叉领域的讨论，重点关注立法、国家政策和战略。

47. 欧洲联盟网络外交倡议(网络直通)支持网络外交领域的广泛政策支持、研究、外联和能力建设，包括维护网络外交工具箱和主办年度欧洲网络外交对话。[23] 在许多其他方案和举措中，“网络直通”为来自伙伴国家的初级和中级网络或数字专家主办了一个研究金方案，即来自东欧国家集团、非洲国家集团、拉丁美洲和加勒比国家集团或亚洲-太平洋国家集团的非欧洲联盟成员。[24] 此外，在该区域，在爱沙尼亚信息系统管理局牵头下，爱沙尼亚、芬兰、德国和卢森堡之间的联盟管理和实施欧洲联盟 2019-2025 年网络倡议，[25] 该倡议在 40 多个责任领域建立了一个有 300 多名网络专家的群组，以支持网络能力发展。

[20] 见 www.diplomatie.gouv.fr/en/country-files/senegal/news/article/regionally-oriented-national-school-for-cyber-security-opens-in-dakar-senegal。

[21] 见 www.kisa.or.kr/EN/201。

[22] 见 www.internationalcybertech.gov.au/cyber-tech-cooperation-program。

[23] 见 https://eucyberdirect.eu/。

[24] 见 https://eucyberdirect.eu/news/eu-cd-fellowship。

[25] 见 www.eucybernet.eu/。

48. 日内瓦安全部门治理中心实施了一个网络安全治理方案，支持国家行为体制定网络安全法律和政策，以加强问责框架和建设能力。[26] 最近的一个项目建立了西巴尔干国家网络安全研究网络，除其他活动外，该网络根据各国国情，对网络安全和人权、弱势群体的网络安全需求以及性别平等问题进行研究。日内瓦安全政策中心同样提供网络安全培训课程和讲习班。[27] 外交基金会也设在日内瓦，支持因特网治理和数字政策领域的能力发展，为此提供网络安全、数据、人工智能和其他新出现问题方面的在线课程、讲习班和模拟演练，并推广和开发数字化工具，促进包容性和有影响力的治理和决策。[28]

49. 由荷兰王国支持的 Cyberspace4All 项目旨在通过创建国际网络治理的共同语言和参考，促进包容性和提高认识，提高对联合国关于网络问题主要发展动态的认识，并帮助为国家网络规范政策提供信息。在第一阶段，该项目制作了一期“网络政策期刊”、若干关于网络能力建设的短视频以及一档题为“谁统治网络空间？”的播客。第二阶段由查塔姆研究所联合实施，旨在就实施联合国网络空间能力建设和负责任国家行为的规范和原则提出建议、提高认识并提供支持。

50. 还通过各种渠道提供网络外交领域的能力建设。例如，作为多边主义和数字化方案的一部分，与爱沙尼亚外交部、电子政务学院和爱沙尼亚国际发展中心合作，组织了塔林网络外交暑期学校。其主要目的是为从事网络外交政策制定的外交官以及对复杂网络问题感兴趣的其他政府官员提供培训。美洲组织美洲反恐怖主义委员会的网络安全方案同样提供了网络外交培训方案，以支持在这一领域工作的官员。就联合国秘书处而言，目前在裁军教育看板上提供的在线网络外交课程将于 2024 年更新。[29]

计算机应急小组、技术培训和其他相关支助

51. 各国一直呼吁对能力建设采取具体的务实办法。各国得出结论认为，此类具体措施可包括向计算机应急小组或网络安全事件响应小组提供支助，并设立专门培训和针对特定需要的课程，包括培训员培训课程和专业认证。各国还表示关切的是，对现有和潜在威胁缺乏认识，以及缺乏发现、防范或应对恶意信息和通信技术活动的适当能力，可能使它们更容易受到攻击。

52. 还突出强调了对信息和通信技术领域人员进行技术培训的重要性，包括在以下领域进行培训：信息安全、在开放信息系统中发现和反击计算机网络攻击的方法、保护信息免被未经授权访问的战术、技术和程序、收集开放源数据、调查涉及国际和平与安全和这一领域国际合作的信息和通信技术相关犯罪的技术、计算机取证、打击利用信息和通信技术及国际邮政服务贩毒和盗窃资金以及查明和调查数字资产非法交易，包括加密货币及其用于资助恐怖主义。

[26] 见 www.dcaf.ch/cybersecurity-governance。

[27] 见 www.gcsp.ch/。

[28] 见 www.diplomacy.edu/。

[29] 见 https://cyberdiplomacy.disarmamenteducation.org/home/。

53. 在全球一级，国际电联不断协助各国建立国家计算机应急小组。[30] 最近的例子包括在国际电联的协助下，在巴哈马、巴巴多斯、布基纳法索、科特迪瓦、塞浦路斯、冈比亚、加纳、牙买加、肯尼亚、吉尔吉斯斯坦、黎巴嫩、马拉维、黑山、特立尼达和多巴哥、乌干达、坦桑尼亚联合共和国、和赞比亚成立了这种小组。在每种情况下，这些小组都是查明、管理和应对网络威胁的中央协调机构。

54. 事件应对和安全小组论坛维护一个拥有超过 700 个参与计算机应急响应团队的网络，以支持合作，主动和被动地应对网络安全事件。除其他活动外，该论坛在其成员之间交流最佳做法，并促进技术座谈会、课程、出版物、网络服务、特殊利益群体和事件应对年度会议的发展。[31]

55. 印度电子和信息技术部部长 Alkesh Kumar Sharma 在印度担任二十国集团主席国期间，为 400 多名国内和国际参与者主持了二十国集团网络安保演习和演练的开幕式。印度计算机应急小组以混合形式举行了网络安全演习和演练。来自约 12 个国家的国际参与者在线参加。来自金融、教育、电信、港口和航运、能源以及信息和通信技术等部门的国内参与者以到场和虚拟方式参加。

56. 联合王国在担任英联邦轮值主席期间，在英联邦网络安全方案的职权范围内开展了一系列能力建设活动，以支持 2018 年《英联邦网络宣言》的目标。[32] 该方案支持英联邦成员国开展国家网络安全能力自我评估，并就网络安全和网络犯罪威胁提供技术援助、培训和咨询。通过该项目，在 32 个国家举办了 140 多次活动，6 000 多人接受了培训。

57. 东盟-新加坡网络安全卓越中心通过提供研究、培训、与计算机应急小组有关的技术支持、交流关于开源网络威胁、攻击和最佳做法的信息，以及通过培训和演练，支持东盟成员国促进该区域的网络能力建设。[33] 该卓越中心自成立以来已实施 50 多个方案，参加国的 1 600 多名高级官员参加了这些方案。从 2024 年开始，东盟区域以外的国家可以参加卓越中心的方案。为了支持定期协调与合作，东盟国防部长会议加网络安全专家工作组自 2016 年以来定期举行会议，作为东盟成员国之间建立信任和制定规范的平台。

58. 东盟网络能力方案旨在通过加强复原力和区域应对威胁的能力，建设东盟成员国的能力。[34] 活动包括讲习班、研讨会、一年一度的新加坡国际网络周、美国-新加坡联合网络安全讲习班和东盟网络安全部长级会议。在 2023 年第八届新加

[30] 见 www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx。

[31] 见 www.first.org/。

[32] 见 https://assets.publishing.service.gov.uk/media/60538ad98fa8f55d38ea34c3/UK_Commonwealth_Cyber_Security_Programme_six_case_studies.pdf。

[33] 见 www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence。

[34] 见 www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace。

坡国际网络周上，启动了新加坡网络领袖与校友方案。该方案向所有国家的被提名者开放，为官员提供基础、执行和高级课程，以加深他们在网络外交概念和程序、国际法、网络空间规范以及国际网络政策的业务和技术考虑方面的专门知识。此外，还设想设立“网络领袖校友研究金”，将网络安全卓越中心主办的能力建设活动的前参加者联系起来，举行一系列闭门会议，讨论网络安全的趋势和国际论述，并交流劳动力和技能发展、法律框架和负责任的网络行为等领域的最佳做法。

59. 自 2016 年启动网络安全共同进步联盟以来，大韩民国一直是该联盟的东道国。该联盟的重点是促进参加国之间的合作和能力建设。[35] 在编写本报告时，来自 49 个国家的 67 个组织加入了该联盟。

60. 2023 年，韩国互联网与安全局与江原国立大学、江陵原州大学和文莱科技大学合作，启动了东盟网络盾牌项目。该项目旨在加强东盟成员国之间在网络安全方面的合作，将在该区域开设网络安全在线课程，开展关于网络安全证书制度的研究，主办东盟黑客马拉松和网络安全学生交流活动。[36]

61. 2017 年至 2019 年，国际电联开展了一个项目，支持太平洋小岛屿国家建立国家、次区域和区域网络安全框架，并提高这些领域的技能。该方案旨在评估巴布亚新几内亚、萨摩亚、汤加和瓦努阿图建立国家计算机应急小组的准备情况，并为这些小组设计和制定执行计划。通过该项目，国际电联主办了提高认识和技能的培训讲习班，200 多名参加者和 70 多个组织在讲习班上交流了在事件应对和保护重要信息基础设施领域的经验。随后，根据牛津大学马丁学院全球网络安全能力中心制定的国家网络安全能力成熟度模型中的指标，对评估工作的结果进行了衡量。[37]

62. 作为澳大利亚网络和关键技术合作方案的一部分，太平洋网络安全业务网络是太平洋区域工作级网络安全专家的网络安全业务网络。[38] 该网络维持一个网络安全业务联络点登记册，使成员能够分享网络安全威胁信息，为技术专家提供分享工具、技术和想法的机会，并促进合作与协作，特别是在网络安全事件影响该区域的情况下。

63. 还开展了各种侧重于技术能力的双边活动。例如，新西兰太平洋网络安全能力建设方案在以下方面向太平洋岛屿国家提供双边支持：制定国家网络安全战略；建设计算机应急小组的能力；提高认识；按照国际标准起草网络安全和网络犯罪立法；按照此类立法进行调查和起诉。该区域最近举行的会议包括 2023 年 9 月 13 日至 15 日在大韩民国举行的应对网络犯罪国际研讨会，以及 2023 年 10 月 2 日至 4 日在斐济举行的太平洋网络能力建设与合作会议。

[35] 见 www.cybersec-alliance.org/camp/index.do。

[36] 见 www.k.kangwon.ac.kr/english/contents.do?key=2356&。

[37] 见 https://gcscc.ox.ac.uk/the-cmm。

[38] 见 https://pacson.org/。

64. 通过网络和关键技术合作方案，澳大利亚支持太平洋和东南亚合作伙伴加强应对网络威胁的技术和治理复原力。[39] 该合作方案成立于 2016 年，并于 2021 年扩大到包括关键技术合作。截至 2023 年 11 月，该方案已为该区域 21 个国家的 126 个项目提供支助。项目包括开展活动，以加强网络安全能力、利用技术支持经济增长和发展、倡导在线保护人权和民主、预防和起诉网络犯罪以及支持执行联合国认可的从国际安全角度使用信息和通信技术的负责任国家行为规范框架。作为合作方案的一部分，2019 年 8 月启动了网络训练营项目，旨在就共同的挑战和机遇为东南亚各国政府官员提供实用的专门知识建设和技能培训。

65. 2022 年成立的拉丁美洲和加勒比网络能力中心得到欧洲联盟的支持，总部设在多米尼加共和国，为拉丁美洲和加勒比国家提供应对网络安全和网络犯罪方面的培训和能力建设。活动包括就国家网络安全和数字化转型以及就网络安全问题开展国家和区域协商向决策者提供培训材料和课程、提高认识并提供支持。还开展双边努力，支持建立国家计算机应急小组，包括巴西合作署支持在苏里南建立网络安全事件应对中心的项目。

66. 2016 年至 2019 年，由大韩民国和世界银行伙伴基金资助的全球网络安全能力方案向跨区域六国集团提供了针对特定需要的国家和区域技术援助。[40] 每个参加国都根据国家网络安全能力成熟度模型进行了评估，并在此基础上提供了分析报告、培训、讲习班和技术援助。该项目旨在协助参加国在网络安全决策者和相关利益攸关方的参与下加强国家网络安全环境。影响评估衡量了干预措施的有效性。

其他能力建设领域

67. 其他跨领域和专题领域的能力建设工作正在进行，包括以妇女、青年、学术界和工业界等特定群体为重点。其他重点领域包括提高公众认识、数字接入和数字素养以及打击网络犯罪。

性别和妇女参与

68. 妇女与国际安全组织和网络空间研究金方案于2020年启动，这是澳大利亚、加拿大、荷兰王国、新西兰、英国和美国的联合举措。[41] 该方案支持女外交官参加联合国主持的相关政府间进程的会议，包括信息和通信技术安全和使用安全不限成员名额工作组的会议，并主办谈判技能培训和讲习班。第二期方案支持代表东盟、亚洲及太平洋、南美洲和英联邦各国的 35 名女外交官参加不限成员名额工作组会议。研究员还接受联合国训练研究所关于多边谈判的培训，参加网络空间国际安全相关问题的介绍，并接受在纽约联合国从事这些问题工作的资深同事的指导。

[39] 见 www.internationalcybertech.gov.au/our-work/capacity-building。

[40] 见 www.worldbank.org/en/news/feature/2020/06/01/kwpfgscp。

[41] 见 https://eucyberdirect.eu/good-cyber-story/women-and-international-security-in-cyberspace-fellowship。

69. 国际电联目前管理一个题为“她的网络足迹”的方案，促进妇女在网络安全领域的平等、充分和有意义的代表性。[42] 该方案支持参加者培养参与国家和国际网络安全决策的技能，提高认识，减少妇女参与该领域的障碍，并增加妇女在网络安全工作队伍中的参与和代表性。在东南亚，国际电联实施了一个项目，以加强关键技术标准和框架的制定，支持妇女参与和融入并增强其权能。该项目支持政策制定、标准、框架和举措，以减少偏见，建立信任并加强包容性。该项目最初部署在印度尼西亚、马来西亚、菲律宾和泰国，以期扩展到该区域其他国家。

70. 国际电联还提供妇女网络辅导方案。该方案第一期于 2021 年国际妇女节推出，由国际电联、事件应对和安全小组论坛以及数字时代性别平等全球伙伴关系(也称为 EQUALS)联合组办。自该方案设立以来，73 个国家的近 300 名妇女通过该方案接受了培训和指导。

青年参与和提高认识

71. 为了提高对信息和通信技术安全感兴趣的青年的认识并促进其参与和能力建设，土耳其计算机应急小组主办了一次 24 小时在线夺旗网络安全竞赛，称为“网络之星”。2 万多名参赛者以团队和个人形式参加了 2019 年竞赛。该计算机应急小组还实施了一个称为“FETWTH”的网络方案，以进一步发展想要进入该领域的受训人员的技能。

72. 一些国家注意到在国家一级努力提高对网络安全领域良好做法重要性的认识。例如，墨西哥国民警卫队 10 月份推动开展活动，作为国家网络安全周的一部分，旨在汇集所有相关部门的代表，在保护关键基础设施、网络空间的公民安全、数字经济、隐私和统一国家立法框架方面分享良好做法和经验。

与产业界和私营部门互动协作

73. 各国不同程度上地强调了公私伙伴关系的重要性，并与产业伙伴互动协作，以建设网络复原力。各国指出，它们努力与主要公共和私营组织进行协商，以评估国家网络安全的总体水平。2023 年 10 月，库班网络安全会议接待了俄罗斯联邦高等教育机构、国家和市政当局、基础设施企业和设施负责人以及国际社会成员的代表，讨论挑战、任务和趋势。该活动还举办了题为“库班 CTF-2023”的以青年为重点的竞赛。[43]

74. 谷歌借鉴为政府和个人用户建立全球云和安全解决方案的经验教训和最佳做法，制定了一个网络安全路线图，供各国考虑。路线图的目的是支持各国制定国家网络安全战略，以保护关键基础设施、公民和经济繁荣。[44]

[42] 见 www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx。

[43] 见 https://kubcsc.ru/en#events。

[44] 见 https://safety.google/intl/en_uk/。

学术机构的资源和研究

75. 海牙国际网络安全方案对数字发展和网络规范进行研究，主办年度学术会议并编写学术研究与辩论摘要。[45] 最近的出版物涉及多利益攸关方参与网络安全规范制定进程和网络空间负责任行为等主题。

76. 国家网络安全能力成熟度模型界定了网络安全成熟度的五个层面以及达到这些层面所需的步骤。自 2015 年以来，在全球网络安全能力中心与国际组织、区域组织和其他伙伴组织合力推动下，该模型已在 90 多个国家部署 130 多次。展望未来，全球网络安全能力中心正在制定另一个衡量标准，作为该模型的一部分，以衡量人工智能能力，从而支持各国安全和可持续地适应和使用人工智能。

数字发展、数字接入和数字素养

77. 联合国开发计划署(开发署)实施了各种举措，以支持建设数字基础设施、促进数字素养或实施电子政务解决方案。[46] 开发署推出了数字准备情况评估，旨在确定和优先考虑数字干预措施，以此作为国家数字化转型之旅的一部分。该评估突出强调了一国当前数字环境-从基本数字基础可能缺乏或不完整的环境，到数字是国家增长和发展的核心要义的情况(称为数字准备阶段)。

78. 大不列颠及北爱尔兰联合王国政府的数字接入方案努力促进为巴西、印度尼西亚、肯尼亚、尼日利亚和南非的社区提供更具包容性、可负担、安全可靠的数字接入。[47]

79. 非洲之角国家数字政府和网络安全倡议支持吉布提、肯尼亚和索马里政府加强电子政务和发展以人为本的电子服务。2023 年 7 月，布基纳法索通过智慧非洲数字学院与智慧非洲合作，组织了云计算和网络安全认证培训课程。

80. 国际电联“Cyber4Good”倡议旨在促进最不发达国家获得数字服务和工具，私营部门行为体参与了该倡议，大韩民国提供了支持。[48] 该项目的一项成果将是设立国际电联网络安全开发基金，该基金在咨询委员会的指导下按照治理模式运作。欧洲联盟的网络复原力促进发展方案支持公共和私营行为体在全球范围内加强网络安全和复原力。[49]

81. 世界银行数字发展伙伴关系支持全球 80 多个国家的包容性数字化转型。[50] 网络安全多捐助方信托基金于 2021 年启动，得到爱沙尼亚、德国、日本和荷兰王国的支持，通过在关键基础设施和高风险部门开展研究、方案支助、风险评估

[45] 见 www.thehagueprogram.nl/。

[46] 见 www.undp.org/digital。

[47] 见 www.oecd.org/development-cooperation-learning/practices/leaving-no-one-behind-in-a-digital-world-the-united-kingdom-s-digital-access-programme-e8b15982/。

[48] 见 www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=2GLO21119。

[49] 见 https://cyber4dev.eu/。

[50] 见 www.digitaldevelopmentpartnership.org/。

和缓解工作，为数字发展方案提供支持。世界银行的非洲数字经济倡议与非洲联盟合作，支持实施 2020-2030 年非洲联盟数字化转型战略。该战略以数字基础设施、服务、技能、有利的政策和监管环境以及创新和创业精神等基本支柱为基础，将网络安全、隐私和个人数据保护确定为一个贯穿各领域的主题。该战略概述了在数字发展、数字接入和数字素养方面进行能力建设的详细建议，包括通过提高公众认识运动、专业培训、研究与开发和计算机应急小组，促进人员和体制能力建设。[51]

打击网络犯罪

82. 联合国毒品和犯罪问题办公室全球打击网络犯罪方案于 2013 年设立。大会第 65/230 号决议以及预防犯罪和刑事司法委员会第 22/7 和 22/8 号决议规定了该方案的任务。全球方案一直根据这些决议运作，同时应指出，大会目前正在就一项条约进行谈判。该方案涉及打击网络犯罪的相互关联的方面：预防、侦查、调查、起诉和判决或裁定。

83. 国际刑事警察组织(国际刑警组织)通过其多利益攸关方网络情报融合中心，目前正在牵头拟定和提供针对信息和通信技术及网络犯罪问题的执法技术援助和能力建设。网络情报融合中心帮助成员国查明网络威胁，制定预防和阻断战略，并协调应对这些威胁。

打击为恐怖主义目的使用信息和通信技术行为

84. 网络安全和新技术全球反恐方案协助会员国及国际和区域组织制定实施有效对策，应对在打击恐怖主义方面信息和通信技术带来的新挑战和机遇。该方案的目的是发展知识和提高认识，并提高执行对策所需的技能和能力，同时保护关键基础设施免受涉及信息和通信技术的恐怖活动的影响，加强刑事司法能力。来自 150 个会员国的 4 000 多名官员通过该方案接受了培训，举办了 60 多次能力建设讲习班，并作为该方案一部分发行 12 个知识产品。作为该方案的一部分，还以反恐网络演练和桌面演练的形式提供了网络安全能力建设援助。

五. 秘书处的意见和结论

85. 从国际安全角度进行信息和通信技术领域的能力建设理所当然地仍然是各国最高优先事项之一。能力建设在很大程度上支持 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努力处理所有相关事项，即应对现有和新出现的威胁，并阐明国际法对国家使用此类技术和促进建立信任措施的适用性。许多国家还强调，在今后由联合国主持的关于信息和通信技术安全的任何定期机构对话中，都必须讨论能力建设问题。**在这方面，能力建设仍应是各国在联合国就信息和通信技术安全进行的所有相关讨论的一个贯穿各领域的基本支柱。要在从**

[51] 见 www.worldbank.org/en/programs/all-africa-digital-transformation。

规范到国际法再到建立信任措施的所有相关领域取得进展，就需要专门资源来执行相应的能力建设措施。

86. 秘书长特别强调，投资于数字素养和数字基础设施以弥合数字鸿沟至关重要(A/75/982)。同样，各国继续强调，并非所有人都能平等地享受数字技术带来的惠益，因此，着重强调在加快实现可持续发展目标的背景下，需要适当关注日益扩大的数字鸿沟，同时尊重各国的国家需求和优先事项。**因此，信息和通信技术领域的能力建设必须有效地服务于所有国家，特别是发展中国家的需要和优先事项，着眼于弥合数字鸿沟，包括性别数字鸿沟。能力建设努力还应成为可持续发展的推动力。**

87. 科学和技术的迅速发展对国际和平与安全的影响尚不完全清楚。预计包括人工智能和量子技术在内的新兴技术的快速发展所带来的机遇和风险将对各国在技术和政策层面的能力建设需求和优先事项产生深远影响。一方面，要使用信息和通信技术能力，如加强威胁检测和分析、事件应对自动化、加强恶意软件检测以及欺诈检测和预防工具，就必须提高能力。另一方面，能力建设工作对于各国掌握必要的知识和技能来应对挑战至关重要，这些挑战包括人工智能支持的恶意信息和通信技术活动、人工智能系统固有的偏见和歧视以及透明度问题等。**具体的能力建设倡议可侧重于增强对这些新兴技术影响的认知和积累相关专门知识，制定关于负责任设计、开发和使用新兴技术的国家战略，以及通过转让知识、最佳实践和经验教训加强网络复原力的国际合作机制。**

88. 有效和可持续的能力建设努力面临的一个持续挑战仍然是可能出现重复。在这方面，值得注意的是，在 2023 年 8 月通过的国际电信联盟理事会第 630 号决定中，授权国际电联为成员国开发一个资源，其中除其他外包括关于国际电联实施的能力建设方案以及其他相关方案的信息。[52] 要求更新该资源，以考虑到新的挑战和事态发展。各国经常提出在这方面利用协同作用和现有举措的问题。**鉴于信息和通信技术安全和使用安全不限成员名额工作组的普遍性，鼓励各国利用专门的政府间进程进一步阐明如何避免重复，以期尽可能做到需求与资源的最佳匹配。**

[52] 可查阅 www.itu.int/md/S23-CL-C-0124/en。