联合国与全球网络安全治理*

□ 张蛟龙

〔提　　要〕联合国通过建立包容性治理框架，制定网络规范，纾解网络空间安全困境，实现了对全球网络安全治理的协调性引领，已成为推动全球网络安全治理的主要场所。然而，对联合国在全球网络安全治理中的角色，发达国家与发展中国家认知不同。受大国战略博弈影响，联合国网络安全治理进程面临激烈的制度竞争和规范冲突。这说明国际社会尚未确立统一的网络空间秩序愿景，地缘政治竞争有向网络空间渗透的趋势。各国应践行真正的多边主义，加快联合国网络安全常设机制建设，提升联合国网络安全规范有效性，推动联合国在全球网络安全治理中发挥更大作用。

〔关 键 词〕网络空间治理、联合国、全球治理、国际秩序

〔作者简介〕张蛟龙，中国国际问题研究院国际战略研究所助理研究员

〔中图分类号〕D81

〔文献标识码〕A

〔文章编号〕0452 8832（2023）6 期 0098-21

随着全球数字化加速，人类社会的发展高度依赖网络空间。由信息与通信技术（简称信通技术）驱动的网络成为现代社会的关键基础设施。国家和非国家行为体恶意使用信通技术的范围、规模、严重性和复杂性与日俱增，

* 本文是国家社会科学基金重点项目“人类命运共同体视域下的全球公域治理路径研究”（项目编号：21AGJ006）的成果。

如何维护网络安全成为全球治理的核心议题之一。联合国[1]已经成为解决网络发展不平衡、理念不一致、规则不健全等全球网络安全治理矛盾的主要平台。评估联合国在全球网络安全治理进程中的作用，对中国参与联合国网络安全治理、推动构建网络空间命运共同体、维护以联合国为核心的国际体系具有重要意义。

一、联合国对全球网络安全治理的协调性引领

为应对网络安全领域的挑战，联合国已建立诸多网络安全治理机制，推动达成了一系列网络安全规范，促进了全球网络空间的稳定性，为世界各国和各类行为体参与全球网络安全治理作出重大贡献。

（一）建立多层多元的网络安全治理机制

机制是治理的基础，也是治理效果的保障。联合国网络安全治理机制主要分为三个层次：第一层是政府间谈判机制，负责制定具有国际软法功能的网络安全规范规则；第二层是多种行为体共同参与并分享经验、专门知识及最佳实践的论坛机制；第三层是联合国本身能动性引发的治理机制，旨在调和不同行为体的网络空间治理诉求。联合国通过举办全球峰会、设立主题论坛、任命工作组等多种方式，逐渐建立起多层次、多行为体参与共治的包容性全球网络安全治理机制，起到了设置议程、促进对话、凝聚共识的作用。

1. 政府间谈判机制

一是政府专家组。2004 年，联合国大会通过第 53/70 号决议，成立“从国际安全角度看信息和电信领域发展政府专家组”（GGE），目标是探讨网络空间威胁以及国际合作。2004 年至 2021 年，联大成立了六届 GGE，形成了四份经联大审议通过的共识报告，成为联合国网络安全规范的基础。2021 年 GGE 共识报告通过后，联合国网络安全政府间谈判转移到了不限成员名额工

[1] 此处泛指包括专门机构在内的联合国系统。

作组。

二是不限成员名额工作组。2018 年，联大通过第 73/27 号决议，设立“信息和通信技术安全和使用问题不限成员名额工作组”（OEWG），不仅邀请所有联合国会员国参加，还举行了与行业、非政府组织和学术界的磋商会议。2020 年 12 月，联大第 75/240 号决议提出设立第二届 OEWG（2021—2025），确保包容、透明的联合国网络安全政府间治理进程的延续。2021 年，OEWG 达成第一份共识报告，为未来机制建设明确了方向。[1]

三是不限成员名额特设政府间专家委员会(Open-ended Ad Hoc Intergovernmental Committee of Experts，OECE)。这一专门针对网络犯罪问题的谈判机制源于 2010 年 4 月第 12 届联合国预防犯罪和刑事司法大会通过的《萨尔瓦多宣言》。2010 年 12 月，第 65 届联大通过第 65/230 号决议，成立对网络犯罪问题进行全面研究的不限成员名额政府间专家组（简称网络犯罪政府专家组），就网络犯罪的立法、定罪、国际合作、预防等进行研究讨论。在此研究基础上，2019 年联大第 74/247 号决议设立 OECE，计划在 2024 年 2 月之前起草一份新的网络犯罪公约，并向第 78 届联大提交公约草案。相关谈判于 2022 年 1 月启动，截至 2023 年 5 月已经举行了五次会议。

四是致命自主武器系统领域与新兴技术相关的政府专家组。以信通技术为基础的人工智能加速在军事领域应用，致命自主武器系统（LAWS）对国际安全以及战争伦理的影响受到国际社会的极大关注。[2] 与人工智能相关的网络武器引入联合国裁军进程就成为了重要议题。2016 年，联合国《特定常规武器公约》（Convention on Certain Conventional Weapons，CCW）第五次审查大会决定建立不限成员名额的LAWS 领域新兴技术政府专家组(CCW-GGE)，

[1] 晓安：《联合国网络安全进程取得重要进展》，《中国信息安全》2021 年第 9 期，第 72 页。

[2] Katharina E. Höne, et al., “Mapping the Challenges and Opportunities of Artificial Intelligence for the Conduct of Diplomacy,” DiploFoundation, January 2019, https://www.diplomacy.edu/resource/mapping-the-challenges-and-opportunities-of-artificial-intelligence-for-the-conduct-of-diplomacy/.

审查包括人工智能在内的 LAWS 领域新兴技术带来的国际安全挑战。[1] 2023 年 CCW 缔约方会议决定继续通过 CCW-GGE 探讨 LAWS 领域新兴技术的运作框架，并发布了两次会议的备忘录。[2]

2. 多利益攸关方机制

联大信息社会世界峰会（The World Summit on the Information Society，简称 WSIS）对联合国构建包容性的多利益攸关方网络安全治理机制具有决定性意义。2002 年联大通过第 56/183 号决议，要求国际电信联盟（ITU）牵头召开 WSIS。[3]2003—2005 年，WSIS 先后通过了《日内瓦原则宣言》《日内瓦行动计划》《突尼斯承诺》《突尼斯议程》，确定了互联网治理的 11 条行动方针，形成了 WSIS 论坛和联合国互联网治理论坛（IGF）两个多利益攸关方机制。

一是 WSIS 论坛。2006 年 WSIS 授权成立论坛机制，由 31 个联合国机构组成的联合国信息社会小组负责组织，重点是协调联合国系统落实 WSIS 成果。作为《突尼斯议程》行动方针 C5 的主要内容，网络安全一直是 WSIS 论坛的主要议题之一，主要关注能力建设、网络犯罪以及新兴技术前沿等。WSIS 委托 ITU 作为 C5 行动方针的协调机构，ITU 于 2007 年启动全球网络安全议程（Global Cybersecurity Agenda，GCA），作为网络安全领域的国家合作框架。2022 年，ITU 理事会批准 GCA 使用指南，不定期发布全球网络安全指数，助力各国加强网络安全。[4]

二是联合国互联网治理论坛。与 WSIS 论坛的重点是联合国各机构的网

---

［1］ “GGE on Lethal Autonomous Weapons Systems,” Digital Watch, July 14, 2023, https://dig.watch/processes/gge-laws.

［2］ United Nations Office for Disarmament Affairs, “Convention on Certain Conventional Weapons—Group of Governmental Experts on Lethal Autonomous Weapons Systems(2023),” https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2023.

［3］ The World Summit on the Information Society, “Basic Information: About WSIS,” https://www.itu.int/net/wsis/basic/why.html.

［4］ 《全球网络安全指数 GCIv5 参考模型（方法）》，国际电联电信发展部门（ITU-D）网络安全项目，https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2C.pdf。

络安全议程协调不同，IGF 主要推进包括政府、非政府组织、企业、学术界等各类行为体间的对话交流和共识建构。2022 年 IGF 共举行 24 场网络安全活动，虽然它没有决策功能，但每年通过 IGF 网络安全最佳实践论坛（BPF）促进全球对网络安全最佳实践的理解，并将这些理解输送到 GGE、OEWG 等联合国政府间谈判机制中去。[1]

3. 联合国秘书长发起的网络安全治理机制

联合国秘书长设立的一系列网络安全相关机制，旨在协调国际社会有关网络空间的不同战略利益诉求，推动联合国网络安全治理进程取得更大成果。2018 年，联合国秘书长古特雷斯将网络安全纳入其裁军议程“保护我们的共同未来”，成立数字合作高级别小组（UNHLPDC），发布报告《数字相互依存的时代》。在该报告基础上，2020 年 6 月秘书长发布《数字合作路线图》，提出改革 IGF、建立“全球人工智能合作多方咨询机构”等网络空间治理举措。[2]2021 年，秘书长任命技术特使，成立秘书长技术特使办公室，加强和统筹联合国在数字空间领域的领导能力。同年 9 月，秘书长发布《我们的共同议程》报告，提出改革联合国网络空间治理机构，推进人工智能监管，制定《全球数字契约》。2023 年，联合国秘书长技术特使就《全球数字契约》的网络安全、人工智能等八个主题与国际社会不同行为体进行协商，为未来峰会作准备。

（二）多个网络安全议题形成了初步治理规范

在联合国框架下的网络安全治理进程中，规范建设取得了初步成果，各方就一些大的规范原则和框架达成了初步共识。

一是网络安全规范。联合国网络安全规范建设是一个渐进累积共识的过程。2002—2010 年间，联大通过多份关于全球网络安全文化的决议，确立了

[1] “IGF 2022 Best Practice Forum on Cybersecurity Output Document,” IGF 2022 Best Practice Forum on Cybersecurity, January 2023, https://www.intgovforum.org/en/filedepot_download/56/24125.

[2] UN General Assembly, “Roadmap for Digital Cooperation: Implementation of the Recommendations of the High-level Panel on Digital Cooperation: Report of the Secretary-General,” A/74/821(2020), May 29, 2020, https://digitallibrary.un.org/record/3864685.

保护关键基础设施、尊重主权等一系列网络安全规范的基本要素。[1] 这些共识与要素后来成为 GGE 等联合国网络安全政府间进程共识的重要组成部分。联大第 70/237 号决议将 2015 年 GGE 报告作为使用信通技术的指南，确立了网络空间规范的四个支柱：11 条非约束性《网络空间负责任国家行为规范》（简称《行为规范》）、现存国际法适用性的共同理解、信任建设措施以及能力建设。这四个支柱成为后来 GGE、OEWG 等进程制定网络安全国际规范的主要框架。2021 年 GGE 报告则对这四个支柱进行了更加详细的解释，尤其是细化了 11 条《行为规范》。2021 年 OEWG 报告重申了 GGE 报告所确立的网络空间规范框架，也增添了新的构成要素，包括细化网络威胁、指派国家联络点、制定能力建设具体原则等。第二届 OEWG（2021—2025）正在进一步细化网络空间规范框架，在国际法网络空间适用问题上寻找国际共识。

二是网络犯罪规范。2011 年 1 月，网络犯罪政府专家组授权联合国毒品和犯罪问题办公室编撰《网络犯罪问题综合研究报告（草案）》。草案于 2013 年初完成，对网络犯罪定义、类型、应对措施等进行了全面研究并提出了诸多建议，成为《联合国打击网络犯罪公约》谈判的规范基础。2020 年设立 OECE 的联大第 74/247 号决议明确强调，在拟定新的网络犯罪条约时应充分考虑到现有国际规范，特别是网络犯罪政府专家组的工作和成果。OECE 已经发布了合并谈判文件，标志着网络犯罪规范制定进程向前迈进了一步。

三是网络人权规范。联合国人权理事会有关网络人权的决议成为联合国网络安全规范的重要组成部分。2012 年人权理事会通过关于在互联网上增进、保护和享有人权的第 20/8 号决议，确立国际人权法在网络空间的适用。在此之后，人权理事会先后通过了相同主题的第 26/13 号、47/L.22 决议，要求各国根据国际人权义务解决互联网安全问题。[2]2013 年斯诺登事件发生后，

---

［1］ 参见联大决议：A/RES/57/239；A/RES/58/199；A/RES/64/211。

［2］ United Nations General Assembly, “The Promotion, Protection and Enjoyment of Human Rights on the Internet,” A/HRC/47/L. 22(2021), July 7, 2021, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G21/173/56/PDF/G2117356.pdf?OpenElement.

联大先后通过“数字时代的隐私权”等多项决议，要求所有国家尊重国际法，包括《宪章》和人权规范中规定的义务。[1]2015 年 GGE 共识报告确立的 11 条负责任国家行为规范中，第五条专门规定了网络人权规范，并在 2021 年 GGE 报告中进行了细化。2021 年 OEWG 共识报告中，有关“能力建设”部分也强调了尊重人权的重要性。

四是网络新兴技术规范。在 OEWG 谈判过程中，各国积极商讨新兴技术对网络安全的挑战及国际合作方式。2021 年联合国教科文组织大会通过的《人工智能伦理问题建议书》是联合国框架下通过的首份人工智能国际规范。而新兴技术在军事领域引起的风险更受重视。CCW-GGE 迄今达成了 5 份共识报告，促进了成员国对人工智能在军事国防领域影响等方面的共识。2019 年，CCW 缔约方会议根据 CCW-GGE 报告，通过了 11 项指导原则，为人工智能等网络新兴技术在军事领域的应用确立了重要框架。[2] 联合国 CCW 第六次审议大会上，中国提交了《中国关于规范人工智能军事应用的立场文件》，是 CCW 下首份关于人工智能安全治理问题的立场文件。[3]

（三）降低网络空间秩序的不稳定性和竞争性

联合国网络空间治理机制有助于缓解网络空间碎片化、阵营化的趋势，纾解网络空间安全困境，缓和大国之间出现的数字冷战势头。[4] 通过 GGE、OEWG 等联合国网络安全机制，确保大国间的高频度和机制化互动，联合国推动了大国双边之间的网络外交，促进了大国间信任措施的建设，降低了大国网络空间竞争烈度。例如，2013 年的 GGE 报告，确立了联合国网络空间规范

---

[1] 联合国大会：《数字时代的隐私权》，UNGA Res 68/167，2013 年 12 月 18 日，https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/46/PDF/N1344946.pdf?OpenElement。

[2] 《特定常规武器公约》缔约方会议：《致命性自主武器系统领域新兴技术问题政府专家组确认的指导原则》，2019 年 12 月 13 日，https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/343/63/PDF/G1934363.pdf?OpenElement。

[3] 《中国首次就规范人工智能军事应用问题提出倡议》，中国政府网，2021 年 12 月 14 日，http://www.gov.cn/xinwen/2021-12/14/content_5660614.htm。

[4] 徐培喜：《解读联合国两份网络问题共识报告的五个视角》，《中国信息安全》2021 年第 9 期，第 77 页。

讨论的基本框架，推动了美俄网络关系的缓和。同年，八国集团峰会上，奥巴马和普京签署了一系列美俄在网络空间建立信任措施的协议，涉及建立工作组和美俄总统热线等。[1]2015 年中美两国达成了一系列网络空间共识，包括欢迎联合国达成 2015 年 GGE 报告，建立中美高级专家小组，继续推动制订国际社会网络空间国家行为准则等。[2]

联合国网络安全治理进程降低了网络空间无政府状态的负面效应。联合国大会、各专门机构等通过决议、举行专题会议、设立专业论坛（如 IGF）和多个政府间谈判机制（如 GGE、OEWG 等）在不同层次上应对网络安全议题。[3]这些联合国网络安全机制本身就是在建立信任措施，因为它们推动了各国在网络空间威胁认知、国家和其他行为体的负责任行为、国际法在网络空间适用等议题上交流意见，达成多份共识报告，从而降低各国在网络安全上的信息不对称，最终支持集体制定和实施网络安全国际规范。例如，在 2023 年 3 月举行的第二届 OEWG（2021—2025）第四次实质性会议上，各国对数字供应链中断风险、基于人工智能的网络工具对国际安全的影响等议题进行了详细讨论，提出了诸多建议，增加各国对彼此关切的理解。

二、对联合国在网络安全治理中角色的不同认知

由于所处发展阶段和利益诉求的不同，各国对联合国在网络安全治理中的角色持不同认知，形成不同的国家集团。但无论是发达国家还是发展中国家，都认识到推进自身网络安全利益、维护网络空间和平稳定离不开联合国。

---

［1］ The White House, “FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security,” June 17, 2013, https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperationinformation-and-communications-technol.

［2］ 《习近平访美期间中美关于网络空间的共识与成果清单》，中国网信网，2015 年 9 月 28 日，http://www.cac.gov.cn/2015-09/28/c_1116702255.htm。

［3］ 徐龙第：《联合国与网络安全：动力机制、可能前景和中国角色》，载中国联合国协会编：《联合国 70 年：成就与挑战》，世界知识出版社 2015 年版，第 387 页。

（一）西方发达国家战略上降低联合国在全球网络安全治理中的作用

长期以来，西方发达国家在全球治理体系中处于中心地位，是治理者，而发展中国家处于边缘地位，是被治理者。以美国为首的一些西方国家不愿放弃在国际秩序中的优势地位，其国际组织战略由“全球模式”转型为“俱乐部模式”，成员参与方式则由基于多元化的鼓励加入转变为根据其战略需求有条件准入，[1] 战略上降低联合国作用，重构所谓“以规则为基础”的国际秩序，增强有利于西方国家的全球治理体系。

美国网络空间战略倚重自身实力地位和联盟体系，打压其他国家，抑制联合国在网络空间治理中的作用。不论是 2022 年发布《国家安全战略》、在其国务院成立网络空间和数字政策局，还是 2023 年发布《网络安全战略》，美国始终强调盟友体系在其网络空间战略中的重要性，联合国被放在无足轻重的地位。[2]2022 年 4 月，美国联合 60 多个国家签署并发布《互联网未来宣言》，将网络空间作为大国竞争的新疆域，抢占网络空间治理主导权，挑起网络空间对抗。美国甚至对联合国秘书长设立的技术特使办公室保持高度警惕。

西方发达国家作为现存全球网络空间秩序的既得利益者，有意降低联合国在网络安全治理中的作用，只是将联合国视为向国际社会“教授”“自家帮规”的工具；而在治理路径上，它们强调以多利益攸关方为主导，即以西方跨国科技企业为主体的私人监管机制为主，不愿意将网络安全治理置于联合国体系下。[3]2011 年的“伦敦进程”、2018 年的《网络空间信任与安全巴黎倡议》、“网络空间负责任行为的日内瓦对话”等，都是西方国家试图在

---

［1］ 高程：《从规则视角看美国重构国际秩序的战略调整》，《世界经济与政治》2013 年第 12 期，第 81-97 页。

［2］ The White House, “The United States’ National Security Strategy,” October 2022, p.34, https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/; The White House, “National Cybersecurity Strategy,” March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

［3］ 李艳：《美国强化网络空间主导权的新动向》，《现代国际关系》2020 年第 9 期，第 5-6 页。

联合国体系外把持网络安全全球治理话语权和规则主导权的具体表现。[1] 北约先后发布两份《塔林手册》，七国集团在数据合作、人工智能、国际法适用等网络安全议题上建立诸多机制，提出统一立场。[2] 美欧等发达国家坚持多利益攸关方模式是为了巩固现有西方国家在数字经济领域的垄断地位、在网络空间国际治理机制的主导角色，干涉发展中国家主权、安全和发展的行动自由。[3]

（二）新兴市场和发展中国家主张联合国在全球网络安全治理中发挥核心平台作用

进入新世纪以来，新兴市场和发展中国家群体性崛起，要求扩大它们在全球治理体系中的话语权和代表性，维护以联合国为核心的国际体系，实现真正的全球治理。对于网络能力与话语权处于弱势的新兴国家和发展中国家而言，联合国是保障它们充分参与全球网络安全治理的最佳途径，有效缓解了全球网络安全治理的民主赤字。[4]

俄罗斯、中国等新兴市场国家主张在联合国框架下治理全球网络安全。2021 年俄罗斯发布《国家安全战略》，强调要在联合国框架下制定一项全球公约，分配国家、社会和技术公司的角色和责任。[5]2022 年中国发布《携手构建网络空间命运共同体》白皮书，主张尊重网络主权，维护网络空间和平、安全、稳定，营造开放、公平、公正、非歧视的数字发展环境，坚持多边参与、多方参与，支持联合国在网络空间全球治理中发挥主渠道作用，构建更加紧

---

［1］ 黄志雄：《2011 年“伦敦进程”与网络安全国际立法的未来走向》，《法学评论》2013 年第 4 期，第 57 页。

［2］ “G7 Digital and Technology-Ministerial Declaration,” April 28, 2021, https://www.gov.uk/government/publications/g7-digital-and-technology-ministerial-declaration.

［3］ 郎平：《网络空间国际秩序的形成机制》，《国际政治科学》2018 年第 1 期，第 44 页。

［4］ 耿召：《政府间国际组织在网络空间规治中的作用：以联合国为例》，《国际观察》2022 年第 4 期，第 129 页。

［5］ 于淑杰：《俄罗斯新版国家安全战略评析》，《俄罗斯东欧中亚研究》2022 年第 1 期，第 39 页。

密的网络空间命运共同体。[1]

联合国为发展中国家充分参与全球网络安全治理提供了最包容的平台。从行为体参与数量上，联合国网络安全治理进程经历了从少数国家参与到全体会员国参与的转变。GGE 成员国数量从第一届的 15 个增加到第六届的 25 个，而 OEWG 则面向联合国全体会员国开放。对于处于全球网络安全治理边缘的非西方国家而言，联合国是其最主要的网络安全治理参与平台。它们主张加强联合国在全球网络安全治理中的作用，实行多边主义治理模式，制定新的、符合国际现实的网络安全规范与规则，以便发展中国家能够掌握网络空间主权，缩小南北数字鸿沟，实行受监管的信息跨国流动。

（三）不同集团均认可联合国在网络安全治理中的合法性与权威性优势

联合国具有的合法性优势能够应对全球网络安全治理的复杂性。数字技术作为新科技革命的代表，对人类社会现有经济增长方式、社会互动模式以及政治治理范式产生了全局性、复杂性影响。全球网络安全治理必然需要一个综合性、民主性和包容性的制度平台。作为最具普遍性、权威性、代表性的国际组织，联合国是最恰当的平台。[2] 联合国在全球网络安全治理中的领导力增强，根源于其权威性和合法性，产生于其能动性和包容性。联合国为各国政府、其他国际组织和非政府组织充分参与全球网络安全治理提供了最包容的平台。联合国网络安全治理进程在促进网络空间国际合作、化解分歧、提升国际法治方面发挥着其他国际机制难以取代的桥梁作用。联大通过各类决议、设立 GGE、OEWG 等政府间网络治理平台，有助于降低国家适用国际法的主观性、私益性和矛盾性。[3] 例如，联大决议虽然没有法律约束力，但其

[1] 国务院新闻办公室：《携手构建网络空间命运共同体》，中国政府网，2022 年 11 月，https://www.gov.cn/zhengce/2022-11/07/content_5725117.htm。

[2] 钱文荣：《联合国应在全球治理中发挥核心作用——纪念联合国成立 70 周年》，《和平与发展》2015 年第 3 期，第 78 页。

[3] 刘碧琦：《联合国“双轨制”下网络空间国家责任认定的困境与出路》，《电子政务》2021 年第 2 期，第 102 页。

决议能够影响国际规范内容及其合法性，能够影响国际习惯产生方式。[1]

联合国的权威性使其成为全球网络安全治理中的规范制定者和倡导者。联合国网络安全规范成为地区多边机构和其他国际组织参与全球网络安全治理的基础性规范。联合国专门机构如 ITU、联合国教科文组织等也将 GGE 等机制中通过的共识报告作为它们制定相关网络空间规则的重要参考。在《欧盟数字十年网络安全战略》中，欧盟将 GGE 共识报告确立的《行为规范》框架纳入其战略规划中，强调联合国网络安全规范（尤其是其中建立信任措施的相关条款）对降低网络空间发生冲突的可能性至关重要。东盟也在《东盟网络安全合作战略》（2021—2025）中制定了相关措施，推动地区国家实施《行为规范》。[2]

三、围绕联合国网络安全治理的博弈

当前国际局势正发生深刻复杂变化，全球秩序正在进入转折期。网络空间秩序是全球秩序的重要组成部分，不同国家集团围绕权力博弈、制度偏好和价值观的博弈日益激烈，竭力争夺全球网络安全治理的主导权，试图重塑于己有利的全球新秩序。

（一）不同集团对网络空间秩序的认知差异凸显

西方国家认为，现存网络空间秩序是自由主义国际秩序下的产物，新兴市场国家群体性崛起推动了全球网络空间的“非自由主义”发展，削弱了自由主义国际秩序。[3] 西方国家是网络空间秩序建设中的“保守派”。它们主

---

［1］ 黄志雄：《网络空间负责任国家行为规范：缘起、影响和应对》，《当代法学》2019 年第 1 期，第 60-69 页。

［2］ H. E. Noor Qamar Sulaiman, “Statement on Behalf of ASEAN at the First Substantive Session of the OEWG (2021–2025),” December 13, 2021, https://documents.unoda.org/wp-content/uploads/2021/12/ASEAN-Statement-OEWG-First-Substantive-131221.pdf.

［3］ Constance Duncombe and Tim Dunne, “After Liberal World Order,” *International Affairs*, Vol.94, No.1, 2018, p.25; André Barrinha and Thomas Renard, “Power and Diplomacy in the Post-liberal Cyberspace,” *International Affairs*,Vol.96, No.3, 2020, pp.755-756.

张现有国际法适用于网络空间，以现存西方国家制定的相关规范为主要规范，反对在网络空间制定新国际条约，主张信息跨境自由流动。[1] 西方大国基于信通技术的先发优势和市场优势，试图通过维护原有网络空间治理安排，追求网络空间的绝对行动自由，维护对新兴市场和发展中国家的战略优势。

新兴市场和发展中国家寻求改革网络空间国际秩序，以适应新的政治经济格局。[2] 随着技术传播和创新，互联网基础设施、用户、数据以及大的信通技术公司越来越多地产生于新兴市场和发展中国家。它们认为，应在联合国框架下制定全新的国际条约，维护网络空间主权，监管信息跨境流动，构建更加公平合理、开放包容的网络空间新秩序。[3]

两种对网络空间秩序的根本性认知差异在 GGE 和 OEWG 等机制中一再体现出来，使联合国网络安全治理进程缓慢，甚至停滞不前。例如，六届 GGE 只产生了四份共识报告，其中 2004 年和 2017 年的 GGE 报告皆因各国在主权与人权、保护与开放等方面的分歧无疾而终。

（二）不同集团之间的制度竞争加剧

全球网络安全治理中的制度竞争反映了不同国家和国家集团对网络空间战略利益的争夺。西方降低联合国在网络空间中的功能，并不代表其放弃对联合国网络安全机制影响力的争夺。从双轨制到 OEWG 的制度化，联合国网络安全治理机制的成员资格、授权和进程主导权成为不同阵营国家争夺的对象。2017 年由于各国无法就国际法的适用问题达成共识，GGE 没能向联大提交报告。在此背景下，联合国出现了两个网络安全平行进程。2018 年，中俄等国

---

［1］ Henry Farrell and Abraham L. Newman, “The Janus Face of the Liberal International Information Order: When Global Institutions Are Self-Undermining,” *International Organization*, Vol.75, No.2, 2021, pp.333-358.

［2］ Michael Cox,“Power Shifts, Economic Change and the Decline of the West?,” *International Relations*, Vol.26, No.4, 2012, pp.369-381.

［3］ Mark P. Lagon and Theresa Lou, “The Dragon in Turtle Bay: The Impact of China’s Rise in the UN on the United States and Global Governance,” *World Affairs*,Vol.181, No.3, 2018, pp.239-255; Andrey Krutskikh and Veronika FilatKina, “New Horizons of Russian Cyber Diplomacy,” *International Affairs*, Vol.67, 2021, pp.72-82.

在联大提出了“国际安全背景下信息与电信领域发展”草案获得通过，设立了 OEWG。[1] 这遭到西方国家反对，因为 OEWG 获得了“在联合国主持下定期开展机构对话的可能性”以及对所有国家开放等 GGE 没有的新授权，进而可能在联合国建立网络安全治理常设机制。

与此同时，美国为了与中俄引领的 OEWG 竞争，向联大提交“国际安全背景下促进网络空间负责任国家行为”的提案，并获得通过，组建第六届 GGE。[2] 第六届 GGE 的名称已从原来的“信息和电信领域发展”变为“推进网络空间负责任国家行为”，显示美西方国家要在联合国专注推进“网络空间负责任国家行为”规范框架，而不是建立联合国网络安全常设机制或是谈判新的网络安全法律文书。[3] 在谈判过程中，为了抑制联合国在网络空间治理中的作用，西方国家坚决反对 OEWG 机制化。在联大 2020 年围绕建立第二届 OEWG 机制展开讨论的阶段，西方国家甚至施加程序性压力，对草案第一条进行了单独表决。[4] 从西方国家组建新的 GGE 到反对 OEWG 的机制化，其目的都是削弱联合国在网络安全治理中的核心作用，防止西方国家塑造网络安全规范规则的能力受到限制。

新兴市场和发展中国家主张将 OEWG 作为网络安全治理唯一平台，而西方国家只愿将 OEWG 作为对 GGE 规范的社会化机构。随着 OEWG 成为联大唯一设立的网络安全规范谈判机制，且在联合国设立单一机制处理网络安全问题的趋势得到越来越多国家的支持，西方国家又向联大提交设立具有不同授权

---

［1］ United Nations General Assembly, “Developments in the Field of Information and Telecommunications in the Context of International Security,” A/RES/73/27(2018), December 11, 2018, https://digitallibrary.un.org/record/1655670.

［2］ United Nations General Assembly, “Advancing Responsible State Behavior in Cyberspace in the Context of International Security,” A/RES/73/266(2019), January 2, 2019, https://digitallibrary.un.org/record/1658328.

［3］ 戴丽娜、郑乐锋：《联合国网络安全规则进程的新进展及其变革与前景》，《国外社会科学前沿》2020 年第 4 期，第 41 页。

［4］ Andrey Krutskikh and Veronika FilatKina, “New Horizons of Russian Cyber Diplomacy,” *International Affairs*, Vol.67, 2021, p.75.

的新提案，意在反对 OEWG 作为联合国网络安全治理常设平台。2020 年 10 月，在 OEWG 起草报告的过程中，欧美提出《促进网络空间负责任国家行动纲领》（PoA）提案，核心是它们要主导联合国网络安全制度建设，以取代 GGE 和 OEWG，对非国家行为体更加开放，以与 OEWG 竞争。[1] 而在 2021 年 3 月 OEWG 第三次实质性会议期间，围绕“定期机构对话”的讨论最激烈，因为这将决定未来联合国网络安全谈判机制的走向。西方国家在会议期间要求 OEWG 授权任期结束后引入 PoA 机制。2022 年 11 月，尽管中俄等国反对，联大仍通过决议，提出在 OEWG 的授权任期于 2025 年结束后将 PoA 作为永久性、包容性、行动导向的机制。[2]

联合国内部的网络安全制度竞争从 OEWG 和 PoA 授权内容和范围的不同可见一斑。最重要的不同是 PoA 的授权范围比 OEWG 窄，限制了联合国在全球网络安全治理中的功能空间。因为 PoA 主要是为了落实“网络空间国家负责任行为”规范框架，一些新的网络安全议题无法被纳入。这实际上就排除了一些新兴市场和发展中国家提出的要为网络空间制定新的有约束力的国际规范的可能性。另外，OEWG 对网络人权的强调只在“能力建设”一部分中提到，而继承 GGE 的 PoA 规范框架中第五条专门论述了网络人权，可能为西方国家对发展中国家实施“信息干政”提供正当性。这种制度竞争仍在 OEWG 谈判中继续，2025 年 OEWG 授权结束后才能决定竞争结果。[3]

（三）不同集团竞逐宪法性规范在网络空间适用的解释权和执行权

网络空间的特殊性、国际规范生成规律以及各国不同的利益考量，致使

---

［1］ 王蕾：《自下而上的规范制定与网络安全国际规范的生成》，《国际安全研究》2022 年第 5 期，第 145 页。

［2］ United Nations General Assembly, “Programme of Action to Advance Responsible State Behavior in the Use of Information and Communications Technologies in the Context of International Security,” A/C.1/77/L.73(2022), October 13, 2022, https://digitallibrary.un.org/record/3991743.

［3］ Andrijana Gavrilović, et al., “What’s New with Cybersecurity Negotiations? OEWG 2021-2025 Fourth Substantive Session,” Diplo Foundation, April 6, 2023, https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-oewg-2021-2025-fourth-substantive-session/.

联合国网络安全治理面临严重的规范冲突。在规范制定上，西方国家通过七国集团、北约等排他性俱乐部建立符合自身偏好的网络空间规范，试图充当国际规范的倡导者，垄断对《联合国宪章》等宪法性国际规范在网络空间的解释权，以巩固自身在网络空间的有利地位。[1] 新兴市场和发展中国家认为网络空间是一个新兴领域，应在联合国框架下制定新的国际规范，其内容需体现包括降低“信息干政”风险、缩小南北数字鸿沟在内的诉求。这两种不同的观点是联合国网络安全进程产生规范冲突的根本原因。

一是宪法性规范如何适用于网络空间。当前的国际法律秩序是以《联合国宪章》（简称宪章）为基础建立起来的，宪章是国际法普遍性的根本体现，而网络规范制定离不开对宪章的解释。西方国家与发展中国家围绕宪章适用性问题的第一个冲突点是在开战正义方面，各国争论的是宪章中的自卫权、武装攻击、主权等在网络空间如何定义。[2] 西方国家倾向于在网络空间扩大解释自卫权，降低网络空间中触发国家自卫权的武装攻击门槛。美国在 2015 年发布了与《塔林手册》相呼应的《美国国防部战争法手册》，扩大解释了网络空间自卫权，允许其受到网络攻击时以任何方式（包括常规武器）作出反应。[3]2016 年，七国集团发布《网络空间原则和行动》，将网络攻击和武装攻击等同起来，以激活《联合国宪章》第 51 条关于自卫权的条款，为使用传统武力进行反击寻求合法性。[4] 此后，西方国家一直在联合国网络安全治理谈判中坚持在网络空间扩大自卫权的规范解读。然而，新兴市场和发展中国家强调捍卫网络空间国家主权，不能任意扩大网络空间的自卫权触发条件，

---

［1］ 江天骄：《全球网络空间的脆弱稳定状态及其成因》，《世界经济与政治》2022 年第 2 期，第 142 页。

［2］ 王铮：《联合国“双轨制”下全球网络空间规则制定新态势》，《中国信息安全》2020 年第 1 期，第 43 页。

［3］ The United States Department of Defense, “Office of General Counsel Department of Defense, Department of Defence Law of War Manual,” June 2016, http://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June2015.pdf.

［4］ The Ministry of Foreign Affairs of Japan, “G7 Principles and Actions on Cyber,” http://www.mofa.go.jp/files/000160279.pdf.

反对网络空间军事化。俄罗斯认为使用武力不是对网络攻击的合法回应。古巴认为网络攻击不等同于武装攻击，因此在这种情况下不应行使自卫权。

第二个冲突点是交战正义如何在网络空间适用。具体表现在国际人道法是否适用于网络空间，必要性、区分性、相称性等原则如何适用等，这些问题尚无国际共识。北约率先发布《塔林手册》等，主张国际人道法完全适用于网络空间，试图抢占网络战规则制定权。[1] 发展中国家反对将国际人道法适用于网络空间，认为一旦国际人道法自动适用于网络空间，将使网络空间军事化和在任何领域诉诸冲突合法化。2021 年 GGE 报告在这一问题上仍然处于模糊的搁置状态，指出国际人道法仅适用于武装冲突局势，需要进一步研究这些原则如何以及何时适用。在 2023 年 OEWG 谈判中，国际人道法在网络空间的适用性讨论占据主导地位，上文提到的这两种分歧仍然存在。

第三个冲突点是推出新的网络犯罪国际规范的必要性。西方国家反对制定“联合国打击网络犯罪公约”，认为网络犯罪规范已经存在，即 2001 年达成的《布达佩斯网络犯罪公约》，现在的任务是将其“国际化”，不需要制定新的国际规范。《网络犯罪问题综合研究报告（草案）》一直无法通过就是这种抵制的表现。然而，一些新兴市场和发展中国家要求推出新的国际规范，以应对网络犯罪的新变化。2019 年联大决定启动“联合国打击网络犯罪公约”的谈判后，西方国家也并没有严肃对待。欧盟在 2020 年发布的《欧洲数字十年网络安全战略》中坚称，不需要任何新的、联合国层面的网络犯罪规范，因为联合国层面的谈判可能会扩大分歧，阻碍有效的网络犯罪国际合作。[2] 网络犯罪规范的冲突源于西方国家与中俄等国在主权保护与人权保护的平衡取舍方面存在根本分歧，具体表现在跨境数据流动、司法协助、数字证据等

[1] 王孔祥：《评＜国际法适用于网络战的塔林手册＞》，《现代国际关系》2015 年第 5 期，第 59-60 页。

[2] The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade*, December 16, 2020.

方面，这在 2023 年 OECE 第五次会议上表现得尤为明显。[1]

二是如何落实网络安全规范。这种冲突的实质是围绕网络安全规范有效性的主导权竞争。虽然西方国家不愿意在联合国制定有约束力的网络安全规范，但却强调现有网络规范的有效性。换言之，它们既要垄断网络安全规范的解释权，也要主导这些规范的实施权。西方国家试图主导归因、问责、制裁这些具体议题的规范制定。[2] 例如，美国企图通过北约、五眼联盟、欧美贸易与技术理事会（TTC）等将美国主导的归因标准国际化，抢占网络归因主导权。有评论指出，联合国网络空间治理规范的最重要贡献，是为西方国家对不遵守网络空间“规则”的国家采取共同行动提供正当性。[3] 这是西方国家持续在联合国参与网络安全规范谈判的动力所在。2019 年 9 月，美国及其盟友在联合国发表了《关于推进网络空间负责任国家行为的联合声明》，开始就所谓对违反网络空间规范的国家“集体追责”展开协商。[4] 然而，新兴市场和发展中国家坚持归因仅仅是指向性的，无直接证据归因不应被允许。鉴于这种分歧，2021 年 OEWG 报告和 GGE 报告均强调指控网络攻击来源需要证实，呼吁谨慎归因。

四、推动联合国在网络安全治理中发挥更大作用

面对全球网络安全治理的诸多矛盾，开放、包容的联合国网络安全治理

---

［1］ “Countries Clash over Cybercrime Negotiations at the UN,” April 24, 2023, https://dig.watch/updates/countries-clash-over-cybercrime-negotiations-at-the-un.

［2］ Jürg Lauber and Lukas Eberli, “From Confrontation to Consensus: Taking Stock of the OEWG Process,” The Global Commission on the Stability of Cyberspace(GCSC) and The Hague Centre for Strategic Studies, September 2021, p.34, https://hcss.nl/report/from-confrontation-to-consensus-taking-stock-of-the-oewg-process/.

［3］ James Lewis, “Private Actors’ Roles in International Cybersecurity Agreements – Unlearned Lessons,” *The Cyber Defense Review*, Vol.7, No.1, 2022, pp.33-40.

［4］ 《关于在网络空间促进负责任的国家行为的联合声明》，美国驻华大使馆和领事馆网站，2019 年 9 月 26 日，https://china.usembassy-china.org.cn/zh/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace-zh/。

进程最符合国际社会整体利益，有望获得更大的发展动力。

（一）践行真正的多边主义，维护联合国在网络安全治理中的核心地位

推动全球网络安全治理，离不开对联合国权威和地位的维护。大国能否维护联合国的核心地位，能否坚持真正的多边主义，对联合国在网络安全治理中的功能空间起着关键作用。正如 GGE、OEWG、PoA 等联合国网络安全治理机制所展现的，大国权力关系动态一定程度上决定着联合国网络安全制度安排架构（平台数量及其关系、任务授权、行为体参与数量与类型等），决定着网络空间规范演进速度（什么时候达成共识），决定着网络规范的有效性。

充分发挥联合国在全球网络安全治理中的潜能，需要世界各国维护以联合国为核心的国际体系。当前，美国等将网络空间视为大国博弈的新领域，纷纷加强网络外交能力建设，发布网络安全战略，将价值观冲突和自身战略利益置于网络空间稳定性和统一性之上，在网络空间硬件（数字基础设施）方面实行“脱钩”战略，在网络空间软件（规范规则）方面依赖自身主导的国际机制制定网络空间规范，排挤联合国主导的政府间磋商模式，削弱联合国网络安全治理的有效性。[1] 国际社会应坚持以联合国为核心平台的全球网络安全治理体系。各国应秉持共商共建共享理念，创新合作模式，捍卫和提高联合国的权威与作用，推动全球网络安全治理体系向着更加公正合理有效的方向改革完善。

（二）加快联合国网络安全常设机制建设，提升联合国的引领力

建立开放包容、授权广泛的联合国网络安全常设机制。OEWG2023 年的年度进展报告（简称年度报告）确立了未来网络安全常设机制的要素：由国家牵头、由联合国主持的单一轨道的常设机制，向联合国大会第一委员会报告，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，以 GGE 和 OEWG 以往报告的共识协议作为工作基础，能够根据各国的需要以及技术环

[1] 姚琨、韩一元：《联合国面临的困难与挑战》，《现代国际关系》2020 年第 12 期，第 44-50 页。

境的发展而演进等。[1] 与此同时，年度报告也列出了未来联合国网络安全机制的不同方案，供以后的会议讨论。新兴市场和发展中国家应加大对 OEWG 进程的参与，在未来常设机制的制度设计、议程设置、行为体类型等多方面提出自身诉求，努力在未来联合国网络安全机制中增强自身话语权，提高联合国在全球网络安全治理的主渠道地位。

加强联合国与区域性组织和非政府行为体的合作。区域性组织和非政府行为体已经成为全球网络安全治理的重要组成部分。联合国网络安全机制应通过制度化安排加强与它们的互动，提升联合国在全球网络安全治理体系中的地位，利用其合法性和包容性优势增强引领力。第六届 GGE 和 OEWG 都组织了与非盟、欧盟、美洲国家组织、欧安组织等区域性组织的一系列磋商。[2]OEWG、PoA 和 IGF 都体现出联合国网络安全治理机制中多利益攸关方与多边治理模式的混合与妥协特征。[3] 未来的联合国网络安全常设机构应更好地设计与区域性组织、非政府行为体的互动方式，不断提升联合国网络安全进程的包容性和代表性。

（三）把握联合国网络规范建设主方向，提升网络安全规范有效性

坚持网络和平与网络主权的国际规范建设主方向。无论围绕网络安全规范的争论如何激烈，主权规范与和平规范都是国际社会的共同诉求，网络主权规范是实现网络和平的根本途径。只有维护网络空间和平，人类才能真正利用信通技术带来的利益。和平是促进开放、安全、稳定、无障碍和可互操作的信通技术环境的前提和基础。如果不坚持这两个规范建设方向，只会加剧网络空间武器化趋势，促使网络空间的所有要素都成为新的武器，并导致

---

［1］ 联合国大会：《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报告》，2023 年 8 月 1 日，https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/227/58/pdf/N2322758.pdf?OpenElement。

［2］ The United Nations Office for Disarmament Affairs, “Group of Governmental Experts,” https://www.un.org/disarmament/group-of-governmental-experts/.

［3］ Jürg Lauber and Lukas Eberli, “From Confrontation to Consensus: Taking Stock of the OEWG Process.”

更多的行为体参与到网络冲突中来。[1] 各国政府应遵守《联合国宪章》的宗旨与原则，和平利用网络，以和平方式解决争端。

建立网络军控国际机构，提高联合国网络安全规范的有效性。网络空间的特殊性之一是其开发和使用的门槛较低，网络行为的透明度低、虚拟性和跨国性强，导致参与的行为体较多，技术溯源难度大，难以确定国家和非国家行为体是否遵守网络安全规范。无法衡量对网络规范的遵守情况，削弱了联合国网络安全规范的有效性，也降低了各国继续推动规范建设的动力。因此，可以参照核武器等军控领域经验，建立国际网络安全领域的实体性国际机构，履行第三方机构监督与核实机制，开展溯源行动，为判断网络攻击等事件的性质提供依据。[2] 这一机构的建立，长远看也有助于推动自愿性的联合国网络安全规范向具有政治约束力和法律约束力的网络安全国际法转变。

【责任编辑：肖莹莹】

[1] 郎平：《从俄乌冲突看网络空间武器化倾向及其影响》，《中国信息安全》2022 年第 6 期，第 69 页。

[2] 鲁传颖：《全球网络安全形势与网络安全治理的路径》，《当代世界》2022 年第 11 期，第 51-52 页。