

新形势下如何进一步 在联合国框架下加强国际网络安全治理

联合国信息安全政府专家组（下称专家组）是目前全球网络空间治理领域处理国际安全相关问题的主要机制，主要工作包括制定网络空间负责任的国家行为准则、国际法在网络空间的适用性以及建立信任措施等三大领域。目前联合国秘书长分别任命了5届专家组，其中三次达成共识并且发布了专家组报告。2017年专家组因各方分歧未能达成共识，是网络空间国际安全治理的一次重大挫折。

由于2015年专家组取得了成功，本届专家组成立之初，各方都抱有很高的期待。由于美英等国力推的在网络空间行使自卫权、反措施以及武装冲突法的适用等议题与中、俄以及其他部分发展中国家代表之间的分歧而未能达成共识。背后也反映出当前网络空间国际规则制定的博弈进入深水区，分歧开始凸显，各方缺乏妥协意愿，以及现有专家组机制无法应对新的挑战 and 满足更多的国家和非国家行为体参与网络空间国际规则制定的愿望。

第一，政治博弈成为影响专家组的主要因素。围绕着专家组的博弈已经成为美欧与新兴国家之间、非国家行为体与主权国家之间争夺全球治理话语权的主要平台。此外，美俄围绕着“黑客干预大选”的冲突升级对本届专家的影响也很明显。美俄外交部都在



鲁传颖
上海国际问题研究院全球治理所
副研究员

专家组未能达成共识后的第一时间发表官方声明，将责任归于对方。对此，担任美方专家组代表的迈克尔·马可夫在美国国务院网站公开声明，缺乏政治意愿是导致专家组未能达成共识的主要原因，这也是美欧与俄罗斯等国不愿意搁置在部分条款上的争议，就其余专家组建议达成共识的主要原因。

第二，网络空间军事化背后的深层次原因。美欧等国将网络空间定义为第五空间，认为网络空间采取军事行动是既成事实，为了维护国家安全，必须要采取自卫权和反措施，并且需要用武装冲突法等国际法为依据建立网络军事行动的基本准则。这一战略的背后实际上是要利用美欧领先的网络军事力量建立在网络空间的战略优势，增加对非西方国家的网络威慑能力。

第三，现有机制的有效性和代表性赤字。本届专家组未能达成共识，引发了各方对专家组机制有效性和代表性两方面的反思和质疑。在有效性方面，专家组原设计为联合国秘书长在信息安全领域的专家顾问，实际上成为了各国政府外交官博弈的舞台，因此受到了领域外因素，特别是政治因素的影响很大。另一方面，现有的专家组代表经过了两次扩容，从15人增加到20人和25人，依然有很多国家未能参与其中，特别是印度、日本、巴西这样的中等大国对于不能连续参

加专家组工作有很大不满。此外，类似于像新加坡、荷兰、韩国、比利时这样的中等国家在网络领域有一定的区域影响力，也不满足与几年甚至更长时间才能轮到一次。除此之外，以微软、国际红十字会为代表的私营部门和非政府组织一直对不能参与相关工作表达了强烈不满。

最后，网空国际规则制定主导权竞争将进入实质性的博弈阶段。专家组以失败告终拉开了新一轮网络空间治理博弈的帷幕。经过之前一轮的博弈，各方已经意识到网络空间国际规则制定已经从技术性、国际法和人权等议题转入国际政治博弈，联合国专家组取代 ICANN、伦敦进程、NetMundial 等机制，成为新一轮博弈的主要平台。今后联合国将会对专家组的未来做出新的抉择，无论结果是延续、改革还是取消现有机制，围绕着网空国际规则制定的博弈将会从联合国延伸到区域性组织、从国家延伸到非国家行为体，博弈将会更加复杂和激烈。对各方而言，今后的博弈将会是更加真刀真枪，鱼龙混杂，这对我国参与网络空间治理，争夺话语权提出了更高的要求。

联合国在网络空间治理中的主渠道作用不容置疑，专家组过去的工作对于网络空间的和平稳定有重要的意义。因此，应当继续推动联合国信息安全政府专家的相关工作。中美欧俄等网络空间大国应当继续推动联合国采取新的举措，同时继续探索在联合国框架下，采取双边和多边的合作形式。

第一，继续推动落实过去三届专家组报告的内容，特别是 2015 年专家组报告在国际法适用性、规范和关键基础设施保护等方面有很多有价值的共识依旧值得进一步落实。如报告强调了阐述了国际法和《联合国宪章》对通信技术的适用。强调了两者所倡导的主权平等、和平解决国际

争端、不对任何国家的领土完整或政治独立进行武力威胁或使用武力、尊重人权和基本自由、不干涉他国内政等基本原则适用于网络安全问题。网络规范对促进和平利用通信技术、充分实现将通信技术用于加强全球社会和经济发展的作用，在前两次报告基础上对负责的国家行为规范有了更明确、完善的补充。关键信息基础设施保护领域规定各国不应蓄意允许他人利用本国领土使用通信技术实施国际不法行为，一国应适当回应另一国因其关键基础设施受到恶意通信技术行为的攻击而提出的援助请求等。

第二，聚焦在关键信息基础设施保护。各国政府对于关键信息基础设施缺乏明确的定义阻碍了在这一领域的合作。各方应当在专家组报告的基础之上继续就关键信息基础设施的定义，以及就如何建立双边和多边的关键信息基础设施保护机制开展探讨。过去几十年互联网一直在发展，网络安全形势和威胁挑战也在不断变化，这对如何定义什么是关键信息基础设施带来了困难。在关键的功能、关键的设备 and 关键的信息之间，应当将重点放在关键的信息上，把那些信息是关键的先找出来，然后再考虑保护措施。也有代表认为，在认定关键基础设施时，应当从风险和威胁入手，改变过去的固有思维。

第三，如何共同应对来自第三方的挑战，如网络恐怖主义、网络犯罪对于网络安全带来的挑战。网络空间安全态势逐步的恶化已经成为威胁国际安全的重要风险来源。新一届专家组未能达成共识对国际合作打击网络恐怖主义和网络犯罪有一定的负面影响，不利于各国在联合国框架下开展合作。因此，退回到 2015 年专家组报告，从双边和多边层面继续推进落实相关的成果有助于克服目前网络空间治理进程陷入困境而带来的不利局面。 6