第 7 卷第 1 期　　全球传媒学刊　　Vol. 7，No. 1：102-115
2020 年 3 月　　Global Media Journal　　March 2020

论联合国信息安全政府专家组在网络空间规范制定进程中的运作机制

鲁传颖[1]，杨　乐[2]

摘　要　随着大规模网络监听、网络黑客攻击、网络冲突等网络安全事件的频发，网络空间的和平与发展受到了严峻威胁，以网络规范为基础的秩序构建成为网络空间全球治理最紧迫的任务。联合国信息安全政府专家组是主权国家参与构建网络空间规范的主要国际机制，在构建网络空间规范方面取得了一定的成果。然而，主要大国之间的认知差距、利益分歧，对专家组网络规范制定工作带来了挑战。本文首先对专家组机制的运行情况和特征进行梳理；其次，对专家组机制在推动形成网络规范方面的作用和挑战进行深入分析；最后，对中国如何通过参与专家组工作引领国际网络规范进程提出建议。

关键词　网络规范；网络空间治理；联合国信息安全专家组；开放式工作组

DOI　10.16602/j.gmj.20200007

网络空间是一个由技术推动并在与人类活动的交互中快速形成的虚拟空间。网络技术所具有的颠覆性功能，使得这一空间具有动态性和复杂性的特征，增加了行为体之间就网络空间秩序达成共识的难度。如卡斯特所言，网络空间的意义在于技术与社会、经济、文化、政治之间的互动，技术在改变传统社会的同时，人类之间的象征性沟通、人与社会的生产、经验和权力也开始向网络空间扩张、延伸和映射（卡斯特，2009，pp. 8-14）。然而，由于缺乏相应的国际法和治理机制，网络空间的和平与发展面临着大规模网络监听、网络作战部队急速发展、网络渗透等国家行为的挑战。因此，建立网络规范成为当前网络空间治理中的优先议程，联合国、区域性组织和非政府组织等多国际组织纷纷加强了构建网络规范的工作。

1. 鲁传颖：上海国际问题研究院网络空间国际治理研究中心秘书长，副研究员。
2. 杨乐：上海国际问题研究院网络空间国际治理研究中心研究助理。

一、国际规范及其在网络空间的延伸

从词源上来说，规范对应的英文为“Norm”，《韦氏新国际英语词典》对其的多项解释暗含着正确的、正面的、广为认可的等褒义前缀。国际政治领域对于“规范”普遍接受的定义是：赋有某个给定身份的行为体所应该采取的适当行为的集体期望（卡赞斯坦，2009，p. 45）。这种期望是一种道德性、共识性的体现，适当行为的共有观念、期望、信念等因素使世界有了结构、秩序和稳定（Finnemore & Sikkink，1998，pp. 887-917）。在全球治理中，国际规范和区域规范规定了适当的国家行为准则，规范限制了国家可以选择的行动范围，因而约束了国家的行动（鲁传颖，2013，pp. 48-54）。在网络空间的治理中，规范是一种对网络空间中负责任国家行为的一种集体的期待，这种期待是积极、正面的，有助于网络空间的和平、稳定、发展、繁荣。

现有网络空间秩序是有关互联网原则与规范的演进产物，也是国际机制与组织扩散的客观体现（王明国，2016，p. 25）。在网络空间国际规范形成进程中，现存国际力量格局和不同利益相关方的立场都对规范形成产生着影响。玛莎·芬尼摩尔认为在建立网络空间行为规范的过程中，国家网络能力差异、网络空间特殊性和网络空间复杂综合性阻碍着规范的形成（Finnemore &，Hollis，2016，pp. 425-479）。首先，国家在网络技术、网络市场和网络资源等方面的差距使各国难以达成一种均势的力量对比和相互制约，大国易于采取进攻性和开放性的政策，弱国则倾向于采取防御性和封闭性的网络政策。其次，现行的国际体系难以对具有匿名性、跨国性、即时性等特点的网络行动采取约束性管理。最后，网络空间治理是一个跨领域、跨专业的综合议题，需要来自不同领域的专业知识分析，也需要国家、私营部门和民间团体的共同参与。因此，网络规范建立是一个漫长而艰难的协调过程。

网络空间各利益攸关方对网络规范有着不同的认知，也阻碍了规范的达成。如各国对于网络主权和网络自由存在不同的认知，实际背后的分歧在联合国两大法理支柱中已经存在。如联合国宪章（*Charter of the United Nations*）和世界人权宣言（*The Universal Declaration of Human Rights*）在涉及主权和人权的表述时，并没有区分两者的高下，而是采取包容的姿态。网络空间中的情况比现实社会更加复杂，国家的行为规范不仅需要考虑人权与主权之间的差异，还需要进一步考虑国际法在网络空间中的适用性问题。立场的差距既来自现实的利益分歧，也来自不同文化背景下形成的认知差异。因此，网络空间中的国家行为规范不仅需要利益上的妥协，也需要加强在认知层面的沟通，特别是关于行为规范的标准和内涵。联合国信息安全政府专家组（UN Group of

Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNGGE)是以主权国家为基础,构建网络规范的主要国际机制。UNGGE 规范构建进程推动了国际社会对主权国家在网络空间行为的集体希望形成,有助于国际社会客观评估国家活动和意图,降低大国之间的网络冲突,促进以和平手段利用通信技术,保障网络空间的和平与安全(UN General Assembly Document A/70/174, 2015)。

二、联合国信息安全政府专家组机制

UNGGE 是网络规范构建领域由主权国家主导的主要机制,在该机制下达成的网络空间规范具有高合法性和权威性。目前,UNGGE 机制已经组织了五届专家组,发布了三份共识报告,建立了多项有影响力的网络规范。同时,UNGGE 机制也面临着代表性不足的挑战,这也致使联合国层面建立了信息安全开放式工作组机制作为 UNGGE 的平行机制来解决其代表性不足的问题,但也在客观上分散了 UNGGE 在网络空间规范制定进程中的权威性。

第一,UNGGE 的诞生和发展过程一直处于网络空间全球治理的重要领域。进入 21 世纪以后,随着网络空间安全形势的整体恶化和大国之间的博弈陷入困境,各国逐渐认识到建立网络空间的规范和规则成为保障各国在网络空间国家利益的重要途径。联合国大会中的裁军和国际安全委员会(第一委员会)根据联合国秘书长的指令(Mandate)于 2004 年建立 UNGGE 作为秘书长顾问,以研究和调查新出现的国际安全问题并提出建议。UNGGE 的主要宗旨是服务于联合国建立一个“开放、安全、稳定、无障碍及和平的信通技术环境”(Kavanagh,2017,p. 3)。

UNGGE 作为国家间对话的中心平台,主要讨论对国家使用信通技术所适用的有约束力和无约束力的行为规范,涵盖面从现行国际法在信通技术环境中的适用到国家在网络空间的责任和义务,问题涉及关键基础设施保护、网络安全事件防范、信任和能力建设以及人权保护等(Kavanagh,2017,p. 11)。议题经讨论后由区域、次区域、双边、多边或专门机构进行运作和实践(Kavanagh, 2017,p. 15)。尽管 UNGGE 报告并不具备强约束力,但被视为增强网络空间稳定性的重要基石。广泛传播的 UNGGE 共识强化了国家间及和其他利益攸关方之间的信心建立,加强了发展中国家的网络能力。

2018 年联合国大会 A/RES/73/266 决议开启了 2019 年 UNGGE 组会进程,并要求 UNGGE 成员与非洲联盟、欧洲联盟、美洲国家组织、欧洲安全与合作组织、东南亚国家联盟区域论坛等有关区域组织合作举行一系列协商,在

UNGGE 会议前就 UNGGE 会议所涉议题交换意见。这一协商会议是新开启的不限成员名额开放式工作组(Open-ended Working Group，OEWG)，该工作组的参与成员来自联合国会员国、产业界、非政府组织和学术界。OEWG 和 UNGGE 是联合国主持下的重要独立协商机制，两者并驾齐驱相互补台(United Nations Institute for Disarmament，2019)。OEWG 先于 UNGGE 会议召开，这将便于 OEWG 代表讨论的议题和建议融入此后的 UNGGE 会议中，间接性扩大 UNGGE 参与成员。OEWG 首届会议于 2019 年 12 月 2—4 日在纽约召开，100 个主权国家和 113 个机构组织注册参加，是 UNICT 首次就网络威胁与挑战议题召开这种开放式的全球多利益攸关方的会议。

第二，UNGGE 机制达成的主要共识包括负责任的国家行为准则、国际法在网络空间的适用性和建立信任措施等主要方面。首先，负责任的国家行为准则。2010 年 UNGGE 第一份报告中就认识到当前部分国家开始将信息通信技术(Information Communication Technology，ICT)用于作战和情报搜集等政治目的，并且提出当前国际社会缺乏对可接受的国家行为(Acceptable State Behavior)的共同认知，这会造成国家间的不稳定和误解(Note by the Secretary-General A/65/201，2010)。首次提出了网络空间应该对主权国家行为形成共同的期望，从而约束国家行为。2013 年的报告明确提出负责任的国家行为(Responsible Behavior by States)这一概念，并确定国际现有规范如国际法、《联合国宪章》、《世界人权宣言》等适用于信息通信领域，将国家主权、管辖权、人权、国家间合作等物理世界中国家间交往的概念运用于网络空间(UN General Assembly Document A/68/98，2013)。2015 年 UNGGE 报告中负责任的国家行为准则内容更加翔实，从“负面清单”式的要求各国不得做某些事，到鼓励各国回应他国援助请求、保障本国 ICT 供应链安全，促进国家间信息分享、国际合作。总体而言，UNGGE 机制下兴起的负责任的国家行为准则规范经历了概念提出、明确现有规范适用性、细化规范内容的发展历程。

其次，国际法在网络空间的适用性。UNGGE 机制的任务之一是明确现有国际规范在网络空间的适用性。从 2013 年的报告开始就明确强调了国际法适用于各国处理信通事务，承认主权国家和源自主权的国际规范和原则适用于国家进行的信通活动，以及国家对在其领土内对通信技术基础设施有管辖权(UN General Assembly Document A/70/174，2015)。2015 年的 UNGGE 报告肯定了国家主权、主权平等、以和平手段解决争端、不干涉他国内政的国际法原则，武装冲突法原则中的人道原则、必要性原则、相称原则、区分原则都适用于信通领域；国家在信通领域也需履行国际法规定的义务，享有国际法规定的权利，其中明确指出各国不得使用代理人利用 ICT 进行国际不法行为，并且力求不让非国家行为体利用其领土实施此类行为(UN General Assembly Document A/70/

174,2015)。在 UNGGE 机制下,国际法在网络空间适用性经历了从国际法未曾进入议程设置,肯定国际法在网络空间的适用性到逐步明确国际法既定原则适用性和国际法权利、义务适用性的过程。

最后,建立信任措施机制。建立信任措施是消除国家意图的恶意揣测、增强事件的可预测性、减少国家间的行为误判的有效途径。2010 年 UNGGE 报告将建立信任机制应对国家使用通信技术的影响纳入关注议题(Note by the Secretary-General A/65/201,2010)。2013 年的报告从多方面阐述了加强国家合作促进信任建立。合作机制上,呼吁建立双边、多边、区域的协商框架,双边的国家计算机应急小组交流对话,以及联合国定期主持广泛参与的对话。合作内容上,促进国家自愿交流关于国家战略和政策、最佳做法、决策过程,呼吁各国就加强应对 ICT 安全事件的信息分享;合作形式上,提出开展讲习班、研讨会、不同场合的对话(UN General Assembly Document A/68/98,2013)。2015 年的 UNGGE 报告则在政策和技术、交流内容、合作方式上对信任建立机制具体操作进行了更为具体的补充(UN General Assembly Document A/70/174,2015)。从三份报告对建立信任措施机制的内容来看,形成了议程设置、合作内容确定和合作操作指南制定的发展过程。

第三,UNGGE 面临代表性不足挑战。UNGGE 机制迄今已发展了近二十年,由于代表名额有限,并且除了联合国安理会常任理事国之外,其他国家基本按照地区均衡的原则轮流当选。因此,该机制所存在的代表性不足问题一直被诟病。据统计,连续参加六次 UNGGE 的国家仅有 6 个,参加五次的为 4 个,参加四次的为 3 个,参加三次的为 5 个,参加两次的为 4 个,只参加一次的高达 18 个(Kavanagh,2017,p. 17)。直到目前为止,UNGGE 组会参会代表都未曾超过 25 人,而且由于 UNGGE 在组建过程中使用轮流机制,印度、日本、巴西这样的中等大国对于不能连续参加 UNGGE 工作有很大不满。类似于新加坡、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,也不满足于几年甚至更长时间才能轮到一次参与 UNGGE。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也一直对不能参与相关工作表达了强烈不满。

UNGGE 代表性不足的问题也引起了各方对 UNGGE 有效性的质疑。联合国成立 UNGGE 的目的是召集全球该领域的专家为联合国大会就该领域的事项提出专业建议,但纵观参与会议的代表身份背景,UNGGE 平台已然成为各国政府外交博弈的舞台。现今参与 UNGGE 的专家代表越来越多来自一国的外交部门,因此 UNGGE 的议题设置和议题讨论都受到较大域外政治因素影响。俨然,UNGGE 成为了国家间谈判的代理场所,国家间直接的、正式的谈判都可能被此取代。

三、UNGGE 机制与网络空间治理的规范形成进程

UNGGE 机制为网络空间全球治理提供了规范治理的基本框架，其推动的负责任的国家行为准则、国际法在网络空间中的适用性和建立信任措施三大规范治理领域也成为国际社会构建网络空间秩序的主要努力方向。虽然 2017 年的 UNGGE 报告由于在网络空间中的“国家责任”“反措施”“自卫权”等方面的规范上未能达成共识，最终未能完成任务。这次失败被认为是网络空间规范形成进程的一次重大挫折（Markoff，2017）。但回首历届 UNGGE 工作，既有成功之处，也面临着重大挑战。

（一）UNGGE 共识推动国际网络规范发展

UNGGE 机制下形成的规范是自愿性和非约束性，表明国家可以自主选择是否加入遵守规范的行列，对于违反规范的行为不会依据报告进行实质性的惩罚。非强制性虽然降低了规范的效力，但在当前网络空间技术、战略和法律不断完善的情况下采取的一种较为妥当的妥协举措。虽然国际法无法禁止违反负责任国家行为规范，但由于作为一种国际社会的集体期待和标准，违反规范的国家依旧会感受到来自全球的强大压力。从这种意义上而言，规范能够促进国际安全，减少冲击网络空间和平与稳定的行为。

2015 年 UNGGE 报告就负责任的国家行为提出了 11 条具体的规范，主要涉及信息共享、隐私保护、关键基础设施保护、供应链安全和计算机应急响应机构等。其中“各国不应当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服务的关键基础设施的利用和运行的信息通信技术”；“国家应回应其他国家在关键基础设施受到攻击时发出的援助请求，以及减少从其领土发动的针对他国关键基础设施的攻击”，这两条规范暗含国家不应当对其他国家的关键基础设施进行攻击，如果攻击被发现了，受害国提出了抗议，攻击方应当减少和停止继续攻击。尽管规范预设了很多条件，但对于关键基础设施的保护有非常重要的作用，表达了国际社会对于网络安全问题的高度期待。

UNGGE 在推动国际法在网络空间适用性中，肯定了主权平等、和平解决争端、不使用武力威胁、尊重人权和基本自由、不干涉他国内政和《联合国宪章》原则在网络空间适用。支持各国对其国内的信息通信基础设施拥有主权，现有的武装冲突法（LOAC）中的人道原则、必要性原则、相称原则和区分原则等适用于网络空间。UNGGE 报告中的这六项原则中最为核心的两项是“主权”在网络空间中的适用和武装冲突法的四项原则的适用（黄志雄，2015，pp. 146-159）。这是国际社会对此进行妥协的产物，发展中国家强调主权的适用，发达国家强

调武装冲突法的适用，双方对此都表示满意（UN General Assembly Document A/70/174，2015）。

UNGGE 关于能力建设的规范倡导，引领了各国政府以及国际组织开展合作的方向。UNGGE 规范中提倡的能力建设主要是呼吁国家主导开展合作和援助，缩小国家间的数字鸿沟和信通能力鸿沟，从而保障全球 ICT 的安全和稳定。2016 年，中俄两国在元首会晤后发出的声明中承诺两国将“加强信息网络空间领域的经济合作，促进两国产业间交往并推动多边合作，向发展中国家提供技术协助，弥合数字鸿沟”（新华网，2016）。与此同时，G20 作为保障全球金融稳定的国家间组织，已经开始在 ICT 领域开展能力建设实践。2017 年 3 月，G20 财长和央行行长承诺加强全球金融体系抵御恶意使用 ICT 的能力（Germany，2018）。网络空间的互联互通性使得网络空间的安全与繁荣是一种“一荣俱荣，一损俱损”模式的博弈，UNGGE 提倡的能力建设规范正是基于强调加强各国网络能力建设，鼓励网络空间能力强国分享其最佳实践，提高网络能力较弱的国家增强其网络韧性。

（二）UNGGE 机制面临网络空间国家博弈的挑战

由于网络空间规范制定的战略性和复杂性，UNGGE 机制也面临着各种挑战，特别是大国之间、发达国家与发展中国家之间在网络空间国家行为准则、国际法适用等网络规范领域的博弈，不仅使得相应的规范难以达成，也使得 UNGGE 本身也陷入了停滞和分裂。

一是大国博弈阻碍规范形成。随着网络安全对国家安全、国家利益、国家战略的影响逐渐加深，网络空间成为大国间博弈的新场所，且呈愈发激烈之势。UNGGE 作为政府间组织，早在成立之初就蒙上了大国斗争的阴影。1998 年俄罗斯就向联大提出国际安全信息和电信技术的决议草案，美国认为俄罗斯的提案并不是出于关心和保护互联网领域，而是为了消灭美国在网络空间的能力，特别是俄罗斯呼吁缔结一项网络空间的军控协定，美国认为此协定是为了抑制美国将互联网优势转化为军事优势，在 2005—2009 年期间美国一直对该提案投反对票。而且，美国认为俄罗斯会以加强信息和电信安全为由限制信息自由，俄罗斯对信息战和网络空间的治理模式过于强调控制大众媒体的内容，意图影响国外和国内的看法（Ford，2010，p. 95）。

2017 年 UNGGE 未能达成共识的主要原因是各方在《联合国宪章》中的自卫权、一般国际法中的反措施（counter measures）、国际人道主义法在网络空间的适用性接受态度各不相同。2017 年 UNGGE 未能达成共识报告的消息一经发出，美国 UNGGE 代表米歇尔·马可夫就发表官方声明，表明美国积极推进国际法、国际人道主义法、国家责任法等现有原则在网络空间的适用，认为不愿

意肯定这些国际法和原则适用性的国家是为了在网络空间的行动不受任何限制或约束（Rodriguez，2017）。德国代表在随后的声明中也强调支持现行的国际法包括《联合国宪章》等适用于网络空间，恶意的网络行动应该受国际法的制裁，对于反制措施、禁止使用武力和自卫权等概念适用于网络空间也都持支持态度（Fitschen，2018）。然而，俄罗斯官方代表安德鲁·克鲁斯基赫在接受采访时说道，“自卫权、反制措施等概念本质上是网络强国追求不平等安全的思想，将会推动网络空间军事化，赋予国家在网络空间行使自卫权将会对现有的国际安全架构如安理会造成冲击”（Krutskikh，2017）。

时任中国外交部条约法律司副司长的马新民在 2016 年亚非法律协商组织会议上曾表明，将现有的武装冲突法直接移植至网络空间需要进一步的审视，将战争法、国家负责任的法等军事性范式（military paradigm）直接运用于网络空间可能会加剧网络空间的军备竞赛和军事化，网络空间发生的低烈度袭击可以通过和平、非武力手段解决（Ma，2016，pp. 19-33）。

此外，国家间冲突和国际阵营化敌对也影响着 UNGGE 最终成果。美俄围绕着“黑客干预大选”的冲突升级对 2017 UNGGE 影响很明显，马可夫在会议中坦言，缺乏政治意愿是导致 UNGGE 未能达成共识的主要原因（鲁传颖，2017a）。网络空间的大国博弈形成的阵营化对峙也阻碍国家间共识性规范达成，例如在 2016—2017 年 UNGGE 在国家是否有权自主判定和反击网络攻击议题上未能达成共识。中国明确地反对网络空间军事化，反对给予国家在网络空间合法使用武力的条款，欧盟在很大程度上与中国是持相同立场的，但因为欧美阵营的存在，不得不支持美国立场（鲁传颖，2019，pp. 121-136）。

二是网络发达国家与网络发展中国家难以达成共识。以中美俄分歧凸显的大国博弈，其实很大程度上反映的是网络发达国家与网络发展中国家之间的分歧。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，必须采取自卫和反制措施，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（鲁传颖，2017a）。美国倾向于以现存的国际规范来保障其强者地位，推动网络空间规范发展能够创造可预测性并且威慑敌对势力的网络袭击（Lotrionte，2013，pp. 75-88）。

然而，网络空间国际法适用性密切涉及国家的战略考量，讨论国际法在网络空间的适用性不仅仅是学术问题更重要的是与国家战略利益和意识形态结合在一起（Henriksen，2016，pp. 51-64）。发展中国家出于对网络强权肆意使用武力和依据先进的网络能力谋取战略优势的担忧，主张以《联合国宪章》以及现有的国际安全架构来解决网络空间的冲突问题，避免将使用武力的决定权交由

网络强国。UNGGE古巴代表在2017UNGGE未能达成共识后的声明中陈述道:“某些国家欲将网络空间变为军事战场并为其单方面的惩罚性武力行动谋求合法化,包括对非法使用ICT的国家进行制裁甚至采取军事行动。”不接受将恶意使用ICT与《联合国宪章》中的“武装攻击”概念等同使用,这一主张其实是在为其使用自卫权谋求合法性(Rodriguez,2017)。在人道主义法的适用性上,不赞同完全适用于网络空间,认为这将使ICT背景下的战争和军事行动合法化,对这些现存国际法原则在网络空间的新解释很可能导致“丛林法则”出现,强大的国家利益永远占上风,而对弱小的国家永远不利(Rodriguez,2017)。

四、UNGGE的未来与中国的参与策略

联合国信息安全政府UNGGE是当前网络空间治理的主要机制和平台,虽然第五届UNGGE(2016—2017)未能预期达成共识,但UNGGE所具有的合法性以及各方的认可度都是其他机制难以企及的。包括中国和欧洲在内的国际社会主流声音依旧认可UNGGE发挥的作用,希望UNGGE能够延续。当然,也有观点认为UNGGE机制本身也存在着代表性不足,缺乏足够的资源等问题,应当借机对UNGGE机制进行改革等。目前UNGGE的改革方向主要包括,一方面,UNGGE机制代表性扩容。2019年开启的OEWG机制与UNGGE并驾齐驱的工作模式已经展现出扩大参与UNGGE代表性的举措,通过开放式的OEWG将多利益攸关方纳入UNGGE关注议题的讨论中,一定程度上扩大了联合国机制的参与代表性。但是UNGGE机制无论如何改革,都应当强调主权国家参与的基本原则(奈,鲁传颖,2017)。另一方面,也可以考虑适当地转变UNGGE的职能。过去几届UNGGE已经制定了足够多的规范,应当将重心转移到如何落实,而不是继续制定更多的规则。UNGGE还应当加强对其他区域性组织以及双边合作的指导工作,扮演好顶层设计的角色(Korzak,2017)。中国是UNGGE的重要成员,参与了所有六届UNGGE的工作,对UNGGE的成果做出了重要贡献。中国的《网络空间国际合作战略》明确提出要加强联合国在网络空间治理中发挥重要作用。无论UNGGE未来的改革走向何方,中国应继续支持联合国以及UNGGE的工作。

第一,加强UNGGE议题研究。针对当前UNGGE存在的主要问题和国际法在网络空间的适用性问题,应当加紧研究。网络安全问题错综复杂,任何片面的观点都不能客观、全面地反映问题的实质。在网络空间进行防御并没有问题,大多数国家都建立相应的网络防御力量。但是在国际人道主义法框架下授予国家行使自卫权是否适用于网络空间则需要进一步加强研究,网络空间的低烈度冲突不断,军事和情报活动难以区分、军用与民用技术不分、国家与非国家

行为体发动的攻击难以界定。这种情况下，国家轻易采取自卫权有可能会导致冲突升级和军事危机，并且会引起更多的附带伤害（collateral damage）。如何在国际法允许的情况下加强网络防御，需要结合国际法与网络冲突以及网络空间本身的属性来探索新的解决方案。

第二，继续支持联合国和 UNGGE 的工作。中国应继续支持联合国以及 UNGGE 网络空间国际治理中发挥重要作用。特别是在当前 UNGGE 陷入困境，前景不明的情况下，中国应拿出更多的资源来推动联合国在网络事务上的影响力。欧美等国不顾广大发展中国家的利益，总希望绕开联合国，将其自身制定的标准推广为国际标准。但是联合国所拥有的合法性是任何区域性组织所不具备的，长期来看，联合国的地位依旧不可撼动，中国以及金砖国家应当承担起更多的责任，开展建设性的行动，把中国在网络空间治理上的成功经验逐步推广到国际社会，赢得更多国家对中国提出的国际互联网治理主张的支持和认同。同时，也需要通过网络空间国际治理工作为建立网络强国保驾护航。要做到这一点，就应当注重网络空间国际规则制定的基础性研究，充分发挥好政府、科研机构和智库之间的协同合作。

第三，积极推动落实 UNGGE 已达成的共识。在双边和区域层面加强对 UNGGE 已有共识的落实，进一步增加 UNGGE 的合法性和权威性。2013 年、2015 年 UNGGE 报告中在建立信任措施、能力建设等方面取得的成果并没有很好地落实到实际中。中国可以与上合组织、欧盟、东盟，以及非洲国家等进一步加强在上述领域的合作。相比美欧之间的合作而言，中国目前主要的合作还是在上合组织层面，缺乏有实质性举措和影响力的网络安全国际合作项目。中国作为 UNGGE 的重要成员，支持 UNGGE 过去达成的共识也经过了反复权衡，认为符合我国国家利益和战略需求。在这种情况下，进一步加强对 UNGGE 报告的落实对于维护我国的网络安全乃至网络空间国际安全都有非常重要的意义。

五、结论

由于网络空间的战略性地位，规范形成进程并不会一帆风顺，UNGGE 的工作也面临着巨大的不确定性。整体而言，联合国的合法性和 UNGGE 过去的工作都表明了 UNGGE 的不可替代性。问题在于主要的大国既想通过 UNGGE 来维护网络安全，又不愿意放弃谋取在网络空间的战略优势，由此导致了各方根本性冲突。但是网络空间的特点决定任何国家都无法追求绝对的安全，集体安全才是客观的需求。因此，UNGGE 已经制定的规范应当被逐步落实，并且在未来发挥更加重要的作用。

本论文系教育部哲学社会科学研究重大课题攻关项目“构建全球化互联网治理体系研究”(项目号:17JZD032)的阶段性成果;本文系国家社科基金一般项目“网络空间大国关系与战略稳定研究”(19BGJ083)的阶段性成果。

注释

① Note by the Secretary-General(2010), 2010 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201.

② Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security(2013), UN General Assembly Document A/68/98.

③ Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security(2015), UN General Assembly Document A/70/174.

④ Germany (2017), G20 Communiqué, Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, 17-18 March, Retrieved from http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/G20-2016/g20-communique.pdf?__blob=publicationFile&v=7

参考文献

彼得·卡赞斯坦(2009):《国家安全的文化:世界政治中的规范与认同》(宋伟、刘铁娃译)(45页),北京:北京大学出版社。

黄志雄(2015):国际法视角下的“网络战”及中国的对策——以诉诸武力权为中心,《现代法学》,第37卷第5期,第146-159页。

鲁传颖(2013):试析当前网络空间全球治理困境,《现代国际关系》,第11期,48-54页。

鲁传颖(2017a):国际政治视角下的网络安全治理困境与机制构建——以美国大选“黑客门”为例,《国际展望》,第9卷第4期,33-48页。

鲁传颖(2017b年12月5日):专家组未能达成共识的原因及其对网空治理的影响,获取自http://www.sohu.com/a/208620660_761681。

鲁传颖(2019):网络空间大国关系面临的安全困境、错误知觉和路径选择——以中欧网络合作为例,《欧洲研究》,第2期,第113-128页。

曼纽尔·卡斯特(2009):《网络社会:跨文化的视角》(周凯译)(8-14页),北京:社会科学文献出版社。

王明国(2016)：网络空间秩序转型的国际制度基础，《全球传媒学刊》，第 3 卷第 4 期，24-35 页。

约瑟夫·奈，鲁传颖(2017)：网络规范还处于早期阶段，《信息安全与通信保密》，2017，第 10 期，6-8 页.

新华网(2016 年 6 月 26)，中华人民共和国主席和俄罗斯联邦总统关于协作推进信息网络空间发展的联合声明，获取自 http://www.xinhuanet.com//politics/2016-06/26/c_1119111901.htm。

Elaine K. (2017). UNGGE on Cybersecurity: The End of an Era?. The Diplomat. Retrieved from https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

Finnemore, M. & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, *52*(4), 887-917. doi: 10.1162/002081898550789

Finnemore, M. & Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. *The American Journal of International Law*, *110*(3), 425-479.

Fitschen, T. (2018). Director for the United Nations, Cyber Foreign Policy and Counter-Terrorism. *Federal Foreign Office of Germany*. Retrieved from https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/11/statement-by-germany-72-dmis.pdf

Ford, C. A. (2010). The trouble with cyber arms control. *The New Atlantis-A Journal of Technology & Society*. Retrieved from https://www.thenewatlantis.com/docLib/20110301_TNA29Ford.pdf

Henriksen, A. (2016). Politics and the development of legal norms in cyberspace. In Friis, K., Ringsmose, J. (Eds.), *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives* (pp. 151-164). New York: Routledge.

Kavanagh, C. (2017). The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century. United Nations Institute for Disarmament Research. Retrieved from http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

Krutskikh, A. (2017). Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere. Retrieved from https://coe.mid.ru/en_GB/sotrudnicestvo-v-sfere-pravoporadka/-/asset_publisher/jYpWpmrO5Zpk/content/otvet-specpredstavitela-prezidenta-rossijskoj-federacii-po-voprosam-mezdunarodnogo-sotrudnicestva-v-oblasti-informacionnoj-bezopasnosti-a-v-krutskih-n?inheritRedirect=false&

redirect = https% 3A% 2F% 2Fcoe. mid. ru% 3A443% 2Fen__GB% 2Fsotrudnicestvo-v-sfere-pravoporadka% 3Fp__p__id% 3D101__INSTANCE__jYpWpmrO5Zpk% 26p__p__lifecycle% 3D0% 26p__p__state% 3Dnormal% 26p__p__mode% 3Dview% 26p_p_col_id% 3Dcolumn-1% 26p_p_col_count% 3D1

Lotrionte, C. (2013). A better defense: Examining the United States' new norms based approach to cyber deterrence. *Georgetown Journal of International Affairs*, (14), 75-88.

Ma, X. M. (2016). Key issues and future development of international cyberspace law. *China Quarterly of International Strategic Studies*, *2*(1), 119-133. doi: 10.1142/S2377740016500068

Markoff, M. G. (2017). Explanation of Position at the Conclusion of the 2016—2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm

Rodriguez, M. (June 23, 2017). Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, *New York*, June 23, 2017. Retrieved from https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf

United Nations Institute for Disarmament. (2019). Developments in the field of information and telecommunications in the context of international security. Retrieved from https://www.un.org/disarmament/ict-security/

UNGGE Mechanism in Global Cyber Norm Building Process

Chuanying Lu, Le Yang

(*Research Center for Cyberspace International Governance, Shanghai Institutes for International Studies*)

Abstract Global governance in cyberspace has become an important agenda in the international community, as large-scale surveillance, hacking and other malicious actions threaten the development of cyberspace. The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) is the main international mechanism for nation states to participate in forming cyber norms. Since its establishment in 2004, China has made remarkable achievements in the formation cyberspace norms.

However, different attitudes among parties on the applicability of existing international norms in cyberspace, the definition of core concepts and other issues have hindered the formation of norms on cyberspace governance. First, this article reviews the situation and characteristics of the expert group. Secondly, it analyzes the development process and challenges of the UNGGE mechanism in creating norms of state behavior in cyberspace. Finally, it puts forward suggestions on how China can lead the process of international network standardization by participating in the work of the UNGGE.

Key Words　Cyber Norm; Cyberspace Governance; UNGGE; OEWG

（编辑：曹书乐）