DOI:10.13415/j.cnki.fxpl.2013.04.022

2011 年“伦敦进程”与网络安全国际立法的未来走向

黄志雄*

内容提要:作为一个新的全球性问题,网络安全在近年来受到各国的极大重视,但现有全球治理机制仍然存在很大不足。2011 年发起的“伦敦进程”,是当前围绕网络安全问题一个独特的国际磋商和对话进程。该进程一方面对于弥补现有多边机制的不足有着重要意义,另一方面在代表性、民主性以及议事日程等方面有着较为严重的缺陷。尽管这一问题涉及各国间深刻的意识形态和价值观分歧,网络安全的国际立法仍然势在必行。

主题词:伦敦进程 网络安全 国际立法

随着互联网的迅猛发展和网络攻击、网络犯罪等问题的日益凸显,网络安全在各国国家安全战略中的地位不断上升,并逐渐成为晚近国际关系中一个重要的全球性议题。在此背景下,各国不仅纷纷加强网络安全领域的国内法律和政策制定,还越来越多地谋求通过各种国际组织和国际会议来协调有关政策。发起于 2011 年的“伦敦进程”(London Process),就是当前围绕网络安全相关问题的一个颇为独特和重要的国际磋商和对话进程。尽管这一多边进程尚在发展、演进之中,最终能够达成何种成果还难以定论,但它提出了一系列值得重视的问题。本文试图对这些问题及其启示加以探讨。

一、网络安全:一个新的全球性问题

简单地说,网络安全是指为保护网络基础设施、保障安全通信以及防范网络攻击所采取的措施。① 在互联网已经得到极大普及的今天,网络安全日益成为一个影响社会方方面面的问题。就国家层面而言,网络犯罪、网络攻击和网络间谍的行为尤其受到关注。

近年来,一些重大的网络安全事件时有发生。例如,2007 年 4 月底开始,爱沙尼亚遭受了“已知第一例针对国家的网络袭击”,其总统府、议会、几乎全部政府部门、主要媒体和商业机构的网站连续三周遭遇三轮网络攻击,使得爱沙尼亚这个欧洲网络化最彻底、网络办公发展最迅猛的国家几乎遭受“灭顶之灾”。② 又如,2010 年 9 月,据信是由美国和以色列联合研制的“震网”病毒爆发,导致伊朗纳坦斯离心浓缩厂的上千台离心机报废,刚封顶的布什尔核电站被迫延期启动,伊朗的核项目倒退数年。③

由此,网络安全日益成为国家安全战略中的重要议题,越来越多的国家抓紧制定相应的国内法律和政策。例如,美国不仅是当今世界唯一的超级大国和互联网技术最为发达的国家,同时也是网络安全立法方面最发达的国家之一。在国际恐怖主义等因素的影响下,早在乔治·布什政府期间,美国就将网络安全纳入其国土安全计划,并组织制定了《确保网络安全国家战略》。④ 奥巴马总统更是声称“网络威胁是我们国家面临的最为严重的经济和国家安全挑战之一,……美国在 21 世纪的经济繁荣将有赖于网络安全。”⑤自“9·11 事件”以来,美国先后通过了《爱国者法》、《国土安全法》、《保护美国法》等法令,对互联网加以更为严密的

* 武汉大学国际法研究所教授、博士研究生导师。

① 参见程群《美国网络安全战略分析》,载《太平洋学报》2010 年第 7 期。

② 参见唐岚《欧洲加快筑造“数字防护网”》,载《世界知识》2009 年第 14 期。

③ 参见吴翔、翟玉成《网络军控:倡议、问题与前景》,载《现代国际关系》2011 年第 12 期。

④ White House, National Strategy to Secure Cyberspace, February 2003, https://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strtegy.pdf.

⑤ The White House, Remarks by the President on Securing our Nations Cyber Infrastructure, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

监控。随着网络安全形势的日益严峻,美国网络安全立法议案数量明显增加,以期构筑更为完备的网络安全防御体系。例如,2012 年 4 月 26 日,美国众议院通过了《网络情报共享与保护法令》和《联邦信息安全修正法令》;27 日,又连续通过了《2012 年网络安全加强法》和《促进美国网络和信息技术研究与开发法案》。而这几个议案只是众议院正在考虑的网络安全立法中的一部分,充分反映了美国对网络安全立法的重视程度。

互联网跨越国界、全球联通的基本特点,决定了网络安全必然是一个全球性问题。尽管各国制定的网络安全立法对于填补相关立法空白无必不可少,但这不足以从根本上遏制国际社会在网络安全领域所面临的问题和挑战。正因为如此,在欧盟、联合国、国际电信联盟等国际组织的议事日程中,网络安全问题的重要性正在不断上升。

以联合国为例,作为当今世界最具普遍性和权威性的一般政治性国际组织,它在上世纪末就开始对网络攻击、网络犯罪等问题加以关注,并每年进行相关的讨论和审议。就网络安全而言,相关讨论始于 1998 年俄罗斯向联大第一附属委员会(裁军与国际安全委员会)提交的“国际安全背景下信息和电信领域的发展”决议草案,以及在此基础上形成的联大第 53/70 号决议。⑥ 近年来,美国、俄罗斯等主要国家围绕该问题的对话与合作有所加强。2010 年 7 月,包括美俄在内的 15 个国家共同向联合国提交了一份关于全球网络安全问题的建议稿。2011 年 9 月,中国与俄罗斯等 4 个国家联合向联大提交了一份“信息安全国际行为准则”的草案,旨在为全球制订网络安全国际公约提供范例。尽管如此,各方在实质问题上的分歧仍然较大。就网络犯罪而言,根据联大 2002 年第 56/121 号决议,该议题主要由经社理事会下设的预防犯罪和刑事司法委员会(CCPCJ)进行相关讨论。该委员会在 2004 年年度报告中首次提出要订立一个联合国的网络犯罪公约,并将这一建议提交了第 11 届预防犯罪与刑事司法大会。但是,相关讨论迄今未能取得突破性进展。

就区域性国际组织而言,欧盟有关网络安全的立法和实践都走在了世界的前沿。例如,在网络犯罪问题上,早在 2001 年,欧洲委员会就发起制订了《网络犯罪公约》(即《布达佩斯公约》),⑦这是迄今为止全球范围内针对网络犯罪达成的唯一一项多边公约,也是欧盟打击网络犯罪所适用的首要法律手段。经过多年的规划,欧盟又在 2012 年 3 月宣布设立“欧洲网络犯罪中心”(European Cybercrime Center,EC3),并于 2013 年 3 月正式投入使用。该中心的建立,是欧盟集合各方资源共同应对网络犯罪的一个重要里程碑。不过,无论欧盟的相关立法和实践多么先进,网络安全问题的全球性决定了欧盟国家不可能在这一问题上“独善其身”。正因为如此,近年来,欧盟各国开始寻求将欧盟的立法和实践向其他国家推广,包括极力推动《布达佩斯公约》在全球范围内得到接受,但欧盟以外的不少国家则对此持反对或保留态度。

总之,作为一个新的全球性问题,网络安全在近年来受到各国的极大重视,但现有全球治理机制仍然存在很大不足。这一现状,正是“伦敦进程”发起的一个重要背景。

二、“伦敦进程”的发起和进展

(一)伦敦网络空间会议

2011 年 11 月 1-2 日,由英国外交和联邦事务部主办的网络空间会议(下称“伦敦会议”)在伦敦举行,这是国际上第一次以网络安全和网络空间治理为主题的大规模会议,共有来自 60 多个国家的 700 余名代表与会。本次会议的一个重要特点是:与会代表除了各国政府官员和国际组织代表外,来自互联网企业(如 Facebook、谷歌、华为等)、非政府组织以及各国智库和学界的人士也占据了相当的比例。而且,后者可以与政府官员和国际组织代表同等的地位参加所有全体会议和专题会议的发言及讨论。与会代表构成的上述特点,体现了会议发起者所倡导的网络空间治理中的“公私伙伴关系”(public-private partnership,PPP)。⑧

在为期两天的会议中,与会代表主要围绕“经济增长和发展”、“社会福利”、“网络犯罪”、“安全可靠的

---

⑥ United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/53/70), 4 January 1999.

⑦ Council of Europe, Convention on Cybercrime (opened for signature on 23 December 2001 and entered into force on 1 July 2004. 参见周文《欧洲委员会控制网络犯罪公约与国际刑法的新发展》,载《法学评论》2002 年第 3 期。

⑧ William Hague, Announcement of London Conference on Cyberspace: Chair's Statement, https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement.

网络接入”以及“国际安全”这五大议题，就网络空间的国际治理和规则制定问题展开了辩论。40 余位代表先后在全体会议和专题会议中发言，他们绝大多数来自欧美国家的政府官员（包括英国首相卡梅伦、美国副总统拜登、爱沙尼亚总统伊尔维斯等）、行业代表或西方的非政府组织以及智库代表。而从有关辩论的内容来看，西方国家关于互联网自由和人权保障的立场几乎占据了“一边倒”的优势，主张政府对互联网加以严格管理的国家（包括中国、俄罗斯等）则明显处于少数地位。西方国家及其立场居于主导地位，是伦敦会议（及其后续会议）的另一个重要特点。

参加伦敦会议的几乎所有代表都承认，开放和充满活力的互联网是经济增长和社会进步的巨大推动力，而网络安全和网络犯罪已经成为越来越严重的威胁，必须加以有效应对。但不可否认的是，网络空间的开放性与安全性之间常常存在着冲突乃至对立。如何处理网络自由和政府管制之间的矛盾，则涉及各国之间深层次的价值观和意识形态分歧。伦敦会议的第三个特点是：相比网络空间的规则制定问题，该会议更多地展现了各国之间不同价值观的辩论和交锋。西方国家认为，互联网在传播自由、民主、人权等价值观以及促进所谓“极权国家”转型（如“阿拉伯之春”那样）方面发挥着无可替代的作用，因此，这些国家在会场内外极力鼓吹“互联网自由”和“人权保障”，而对包括中国在内的有关国家依据本国法律对互联网的审查和管理加以指责。会议主席、英国外交大臣黑格代表东道国提出的“七项原则”以及《主席声明》所强调的“对网络安全的保障不能以牺牲基本人权为代价”，⑨都鲜明地反映了西方国家的声音和立场。

当然，伦敦会议也不可避免地涉及了网络空间可适用的国际法规则问题。西方国家比较一致的声音是，现有的国际法规则（特别是有关言论自由等问题的国际人权法规则以及关于战争和武装冲突的国际人道法等“普世规范”）在网络空间同样适用；不需要以条约形式为网络空间专门制定新的规则。例如，美国副总统拜登在会议期间发表的视频讲话中，强调“现有国际法原则既适用于现实世界，也同样适用于网络空间”。⑩不过，在打击网络犯罪问题上，美国和欧盟各国试图推动《布达佩斯公约》成为一项全球性的公约。另一方面，俄罗斯等一些国家则主张就达成一项网络军备条约举行谈判。

由于伦敦会议“价值观辩论”的色彩以及相关国家在有关问题上分歧较大，本次会议并未达成任何成果性文件，而只是以一份“主席声明”的形式对会议的主要议题和相关辩论进行了总结。但是，伦敦会议的召开，标志着“伦敦进程”的正式发起，并为两次后续会议——2012 年的布达佩斯会议和 2013 年的首尔会议）设置了议程。

（二）布达佩斯网络空间会议

2012 年 10 月 4 - 5 日，由匈牙利外交部主办的网络空间国际会议在布达佩斯举行（下称“布达佩斯会议”），来自 60 多个国家和地区的近 600 名与会者就相关议题展开了讨论。与伦敦会议相比，布达佩斯会议在代表组成、主要议题设置等方面有一脉相承之处。例如，本次会议的五个主要议题分别是“经济增长与发展”、“社会利益与人权”、“网络安全”、“国际安全”以及“网络犯罪”，这与伦敦会议有关议题并无明显不同。⑪ 在本次会议上，占据主导地位的仍然是欧盟、美国为代表的西方国家，其主流的声音是倡导网络空间的自由、开放和人权保护，反对国家对互联网的监管和干预。与此同时，欧盟国家（特别是作为东道国的匈牙利）继续大力宣扬《布达佩斯公约》在惩治网络犯罪国际合作中的重要作用，并积极推动该公约在全球范围内的适用。

作为伦敦会议的后续会议，在布达佩斯会议上，各国围绕相关议题开展了更加深入的辩论，也呈现出一些新的态势和实践。例如，英国作为伦敦会议的主办国和伦敦进程的主要推动者之一，在布达佩斯宣布将设立一个全球网络安全能力建设中心，帮助发展中国家缩小“数字鸿沟”、更好和更加安全地利用网络空间。欧盟和其他一些发达国家也提出了类似行动方案。当然，在一定程度上，这也是西方国家为争取发展中国家支持其网络空间政策主张而采取的举措。

---

⑨ Supra note 8.

⑩ The White House, VP's Remarks to London Cyberspace conference. http://www.whitehouse.gov/the-press-office/2011/11/01/vps-remarks-london-cyberspace-conference.

⑪ Final Programme of the Budapest Conference on Cyberspace, http://www.cyberbudapest2012.hu/draft-programme.

布达佩斯会议的另一个新态势是,经过伦敦会议的交锋,中国、俄罗斯等在“伦敦进程”中属于“少数派”的国家得以有备而来,更加全面、系统地提出本国的互联网政策以及对网络空间国际合作的基本立场。例如,中国代表团团长、外交部条法司黄惠康司长在第一次全体会议上发言,阐述了互联网在中国经济和社会发展中所发挥的重要作用及中国政府有关互联网的基本政策,并提出网络空间应遵守“网络主权”、“国际合作”、“平衡”、“和平利用”、“公平发展”等五项原则。⑫ 这一发言在本次会议上引起了较大反响。

与伦敦会议一样,布达佩斯会议也没有出台任何成果性文件,而只是通过一份主席声明对会议加以总结,并商定了下一次后续会议(首尔会议)的具体会期为 2013 年 10 月 17 – 18 日。

三、几点初步评价

过去二十年左右,互联网的快速发展给人类社会带来了前所未有的机遇,但随之而来的挑战特别是各种安全威胁也日益严重。应当如何在有效应对这些挑战的同时,充分利用互联网给人类带来的机遇和福利?如何协调主权国家在网络空间的管制权与保障互联网自由之间的潜在矛盾?⑬ 质言之,应当为网络空间构建何种秩序、确立何种行为准则?这些问题表明,网络空间的发展和相应的政策制定已经来到了一个何去何从的十字路口。伦敦进程正是在这一背景下发起的。

本质上说,伦敦进程是一个由西方国家发起和主导的、围绕网络安全及网络空间秩序构建开展的对话和辩论议程。这一性质,决定了该进程在以下三方面有着不同程度的“先天不足”:第一,受邀参加伦敦会议和布达佩斯会议的国家都只有 60 多个,广大发展中国家特别是非洲国家鲜有出席者。从两次会议议程和发言者的安排来看,欧美发达国家的声音更是占据压倒性优势。显然,伦敦进程的代表性和民主性都有着较为严重的缺陷。第二,由于主要发起国最终将该进程的重心放在网络空间的相关政策辩论,而放弃使之成为一个正式的国际立法谈判框架,因而伦敦进程更多地表现为各国围绕网络安全国际规则制定的一场“前哨战”,而不可能直接催生任何有实质性影响的重要国际条约。第三,伦敦进程没有常设的秘书处之类的制度性安排,更不是一个正式的国际组织。这固然可以使该进程保持必要的灵活性和适应性,但反过来也不利于加强对该进程的信心。对于该进程的前景和可能产生的结果,目前各国还远未达成共识。

尽管如此,笔者认为,伦敦进程对未来网络安全的国际治理乃至更广泛意义上的国际关系都将产生不可忽视的影响力。在伦敦进程发起的前 10 年即 21 世纪的第一个 10 年,网络安全问题在各国国家安全战略和国际治理体系中就已经日益受到重视。除了在联合国等国际组织中就这一议题进行的讨论外,各种双边和区域性对话机制也日益增多。⑭ 2011 年伦敦会议的召开,则标志着国际上第一个也是迄今唯一一个专门针对网络安全和网络空间治理问题的多边进程正式发起。从伦敦会议和布达佩斯会议与会代表的规格来看,许多国家纷纷派出国家元首、政府首脑或部长级高官,对本国的网络安全政策和相关的国际政策构想加以宣示,显示出对这一议题的极大重视。这足以表明,网络安全已经进入国际关系的主流议程,其重要性将与日俱增。

2013 年首尔会议后,伦敦进程何去何从?从目前的情况看,该进程几种可能的前景是:第一,在伦敦进程从伦敦到首尔三次会议辩论的基础上,发起一个正式的网络空间国际立法进程;第二,召开新的后续会议,继续该进程内的辩论以寻求各国间的共识;第三,以主席声明的形式,对三次会议加以总结并结束这一进程,并在会后转而推动相关国际习惯法和“软法”的形成。目前来看,第三种前景的可能性较大。

可以预见,在今后若干年,网络安全都将作为各国共同面临的一个挑战而持续受到关注。那么,应当如何通过国际合作来为这一新的全球性问题寻求全球性对策?特别是,应当如何看待国际法在应对网络安全威胁方面的现实状况和应有作用?这一问题颇为值得思索。

---

⑫ 《外交部条法司司长黄惠康在网络问题布达佩斯国际会议上的发言》(2012 年 10 月 4 日,布达佩斯),http://www.fmprc.gov.cn/chn//pds/wjb/zzjg/tyfls/xwlb/t977343.htm。

⑬ 例如,关于网络空间的表达自由与相关的政府管制问题,参见罗楚湘《网络空间的表达自由及其限制——兼论政府对互联网内容的管理》,载《法学评论》2012 年第 4 期。

⑭ 例如,在近几年的美俄、中美、中欧战略对话中,网络犯罪、网络攻击等网络安全相关议题都占据着十分重要的地位。

关于就网络安全问题制定新的国际条约，西方学术界已经进行了相关探讨并达成了一些共识。[15] 在伦敦会议召开之前，英国政府也曾经考虑将发起新的网络安全国际条约谈判作为主要议题之一，但最终根据美国政府的建议而放弃了这一议题。[16] 英美等国的这一立场，主要是出于两方面的考量：其一，担心即使制定了相关的国际条约，其执行和效力也会存在很大问题；其二，更重要的是，这些国家担心国际条约的制定会加强“极权国家”控制网络空间的能力，从而与其推动“互联网自由”的战略相悖。因此，它们转而强调现有国际法（特别是国际人权法、国际人道法等）应在网络空间得到适用。但是，为什么在网络犯罪问题上，欧洲国家早早就制定了《网络犯罪公约》，并且还要积极向其他国家和地区推广呢？事实上，由于网络空间本质上是一个全球性空间，国际法往往比很多国家已经大量制定的国内法更适合对互联网相关问题加以规制。[17] 而在很多重要的网络安全问题上，现行国际法要么没有相关的规制（如对于“网络间谍”行为），[18] 要么存在诸多模糊和有待澄清之处（如对于国际人道法在网络攻击中的适用）。[19] 这表明，网络空间相关规则的制定和完善仍然势在必行。

当然，对于网络安全国际立法进程的长期性，我们也应当有充分的认识。在这一过程中，以下几个因素尤其值得重视。

首先，不同价值观的冲突与融合，将对网络安全领域未来国际合作和国际法规则的塑造产生巨大影响。网络空间的形成，是现代科学技术发展的结果。然而，网络安全的国际治理却绝不仅仅是单纯的技术问题，而是涉及各国深刻的意识形态和价值观分歧。在很大程度上，伦敦进程正是西方国家开展“价值观外交”的一个前沿阵地。2013 年 2 月出台的新版《欧盟网络安全战略》，表达了欧美国家试图在伦敦进程中传递的价值观

“开放和自由的网络空间推动了世界范围内的政治和社会包容；它打破了国家之间、社区之间、公民之间的壁垒，促成了全球范围的信息和观念的互动和共享；它提供了自由表达和行使基本权利的场所，并使人民在追求民主和更加公正的社会时变得强大——‘阿拉伯之春’就是一个最突出的例证。……为了保持网络空间的开放和自由，那些欧盟在现实社会所支持的规范、原则和价值也应当在网络空间得以运用。基本权利、民主和法治应当在网络空间得到保护。”[20]

当然，这种“互联网自由”优先于网络安全的价值观，在实践中常常呈现出某种双重标准。例如，在伦敦会议期间，英国首相卡梅伦大谈“各国政府不应当以网络安全为借口，对互联网加以审查或使本国人民丧失互联网提供的机会”，对中国、俄罗斯等国加强互联网监管的立法和措施大加指责。[21] 而在此前 2011 年 8 月伦敦骚乱中，鉴于 Facebook、Twitter 等社交网络在骚乱者联络沟通中发挥的重要作用，卡梅伦首相却表示将授权警方临时中断社交网络服务。另外，美国和其他西方国家一再在没有确凿证据的情况下指责中国政府支持网络黑客行为，但颇具讽刺意味的是，包括美国主流媒体在内的各方舆论普遍认为，2010 年伊朗核设施

---

[15] See Robert K. Knake, Internet Governance in an Age of Cyber Insecurity (Council on Foreign Relations Special Report No. 56, September 2010), http://i.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf; Stein Schjolberg and Solange Ghernaouti-Helie, A Global Treaty on Cybersecurity and Cybercrime (2nd edition), 2011.

[16] Joseph Menn, Elites Disagree at London Cyber Conference, http://blogs.ft.com/tech-blog/2011/11/london-cyber-conference/.

[17] Antonio Segura-Serrano, Internet Regulation and the Role of International Law, in Armin von Bogdandy and Rudiger Wolfrum (eds.), Max Planck Yearbook of United Nations Law, Vol. 10 (2006), p. 192.

[18] See David P. Fidler, Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law, American Society of International Law Insights, Vol. 16, Issue 22 (June 20, 2012), http://www.asil.org/insights120620.cfm.

[19] See Johann-Christoph Woltag, Cyber Warfare, in Rudiger Wolfrum (ed.), The Max Planck Encyclopedia of Public International Law, Oxford University Press, 2008-, online edition, www.mpepil.com.

[20] European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (JOIN(2013) 1 final), 7 February 2013, p. 2.

[21] Prime Minister's Speech on Cyberspace (1 November 2011), http://www.number10.gov.uk/news/cyberspace/.

受到的“震网”病毒攻击是美国和以色列联合研制的。[22] 因此,西方国家有必要摒弃其“傲慢与偏见”,理解其他国家在网络安全问题上的合理关切,在此基础上开展建设性合作。

其次,各国特别是主要大国围绕相关议题和优先领域、谈判场所等方面的分歧不可忽视,有关网络安全话语权和主导权的争夺将呈加剧势头。尽管维护网络安全是当今世界各国共同面临的一大挑战,但不能不看到,由于各国国情、发展阶段等因素的差异,在网络安全领域所面临的具体问题和关切重点也有着较大差异。相对而言,打击网络犯罪是各方利益易于趋同、较易达成共识的问题,应是近期网络安全国际立法的优先领域。就谈判场所而言,鉴于伦敦进程主要受美欧发达国家的主导和支配,很多新兴国家对此抱有一定警惕,而主张突出联合国在网络安全领域的核心作用。近年来俄罗斯在联合国大会提交的有关决议草案、中俄等国在 2011 年 9 月向联大提交的“信息安全国际行为准则”以及 2012 年 9 月召开的首届新兴国家互联网圆桌会议等,都可以视为是这些国家反对美欧“互联网强权”和维护互联网主权的重要举措。随着网络安全国际立法进程的深入,各国在有关问题上的分歧和斗争还有可能加剧。

最后,在未来网络安全国际立法中,非国家行为体和“软法”的作用不可忽视。过去较长的一段时期内,以互联网域名地址分配机构(ICANN)为代表的非国家行为体对于互联网的发展发挥了主导性作用。在未来的网络安全国际立法中,尽管国家和政府间国际组织将扮演越来越重要的角色,非国家行为体仍将发挥不可或缺的作用。在 2011 年伦敦会议和 2012 年布达佩斯会议中,各种非国家行为体(包括行业性组织、非政府组织和智库等)俨然成为国家和政府间国际组织之外的“第三种力量”。尽管这种所谓的“公私伙伴关系”在一定程度上是西方国家推动的结果,它的确具有某种必然性和合理性。同时,由于各方在网络安全的诸多领域尚存在不同程度的分歧,制定有约束力的国际条约短期内尚不具备可行性,在此情况下,西方国家力图通过行业规范、企业标准等形成“软法”,并在此基础上推动反映其利益和主张的国际习惯趋于确定。因此,有必要高度重视非国家行为体和“软法”在网络安全国际立法中的作用,并采取必要措施加以应对。

对中国这样一个新兴的互联网大国来说,伦敦进程的发起以及未来网络安全国际立法的推进都提出了一系列新的挑战。中国外交部发言人在伦敦会议后指出:“中方希望,伦敦会议及相关论坛的讨论能够对于国际社会在联合国框架下讨论制订网络空间国际规则的进程形成有益补充。”[23]应该说,这代表了相当一部分国家对伦敦进程的定位,即这一议程对于弥补现有多边机制的不足有着重要意义,但它应当是对联合国框架下相关行动的补充而不是“另起炉灶”。能否达到这一步目标,接下来所面临的最大问题,就是相关国家如何凝聚共识,为伦敦进程的未来规划务实、合理的目标,同时采取建设性的合作行动,切实有效地为在全球范围内加强网络安全做出应有的贡献。

四、结语

随着互联网在人类生活中的重要性与日俱增,网络空间作为陆地、海洋、空气空间、外层空间之外的所谓“第五空域”(fifth domain),正成为各国特别是主要大国斗争与合作的新疆域。如果说 1990 年代是以互联网(包括网络安全问题)自发、自治发展为特征的 10 年,2000 年代是相关国内立法显著加快的 10 年,那么,2010 年代很可能是国际立法逐渐强化的 10 年。

当然,网络空间作为一个新的虚拟空间,还有许多独特的技术属性亟待人们加以深入认识,相关的国际规制也必将涉及各国之间错综复杂的意识形态和价值观念分歧。在多边主义日益面临危机的当今世界,有关网络安全的讨论注定不会一帆风顺。各国间围绕网络安全国际立法的博弈,将是一个长期和持续的过程。但是,全球性问题必然需要有全球性的解决方案。在网络安全问题上,除了积极谋求多边合作外别无他途。无论伦敦进程的前景如何,其意义之一正是在于推动各国为网络安全和网络空间的未来加强对话、寻求共识。

(责任编辑:黄德明)

---

[22] See e. g. David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, in New York Times, June 1 2012, at A1.

[23] 《外交部就中方未来空间国际合作、军事透明度等答问》,http://news.xinhuanet.com/world/2011-11/02/c_111141582_3.htm.