中国国际问题研究院
资助出版

地区组织网络安全治理

肖莹莹◎著

Cyber Security Governance:
From the Perspective of Regional Organizations

时事出版社

中国国际问题研究院
资助出版

地区组织网络安全治理

肖莹莹◎著

Cyber Security Governance:
From the Perspective of Regional Organizations

时事出版社
北京

图书在版编目（CIP）数据

地区组织网络安全治理/肖莹莹著. —北京：时事出版社，2019.2
ISBN 978-7-5195-0274-4

Ⅰ.①地… Ⅱ.①肖… Ⅲ.①计算机网络—网络安全—研究
Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2018）第 248353 号

出 版 发 行：时事出版社
地　　址：北京市海淀区万寿寺甲 2 号
邮　　编：100081
发 行 热 线：（010）88547590　88547591
读者服务部：（010）88547595
传　　真：（010）88547592
电 子 邮 箱：shishichubanshe@sina.com
网　　址：www.shishishe.com
印　　刷：北京旺都印务有限公司

开本：787×1092　1/16　印张：16.5　字数：300 千字
2019 年 2 月第 1 版　2019 年 2 月第 1 次印刷
定价：98.00 元
（如有印装质量问题，请与本社发行部联系调换）

中国国际问题研究院资助出版

目录

Contents

第一章

绪论

一、研究的背景

在世界多极化、经济全球化、文化多样化深入发展，全球治理体系深刻变革的背景下，人类迎来了信息革命的新时代。以互联网为代表的信息技术日新月异，引领了社会生产新变革，极大地促进了社会经济的繁荣，创造了人类生活新空间，拓展了国家治理新领域，提高了人类认识世界、改造世界的能力。网络空间越来越成为信息传播的新渠道、生产生活的新空间、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、交流合作的新纽带、国家主权的新疆域。国际电信联盟（ITU）2017 年 7 月发布的《2017 年全球网络安全指数》报告显示，2016 年全球互联网用户达到 35 亿人，约占世界总人口的一半；到 2020 年，接入互联网的终端设备预计将达到 120 亿台。[①] 中国互联网络信息中心（CNNIC）2018 年 1 月发布的第 41 次《中国互联网络发展状况统计报告》显示，截至 2017 年 12 月，中国网民规模达 7.72 亿，普及率

① ITU，“Global Cybersecurity Index 2017”，July 2017，https：//www. itu. int/dms_pub/itu-d/opb/str/D-STR-GCI. 01 – 2017 – PDF-E. pdf.

达到55.8%，超过全球平均水平（51.7%）4.1个百分点，超过亚洲平均水平（46.7%）9.1个百分点。[①] 作为人类社会的共同财富，互联网让世界变成“地球村”，各国在网络空间互联互通、利益交融、休戚与共。维护网络空间和平与安全，促进开放与合作，共同构建网络空间命运共同体，符合国际社会的共同利益，也是国际社会的共同责任。[②]

网络空间给人类带来巨大机遇，同时也带来了新的问题和挑战，网络空间的安全与稳定成为攸关各国主权、安全和发展利益的全球关切。互联网领域发展不平衡、规则不健全、秩序不合理等问题日益凸显。

国家和地区间的“数字鸿沟”不断拉大。经济落后的发展中国家缺乏研发和使用信息技术的能力，正在成为“数字贫穷”国家，不仅难以享受信息技术高速发展带来的好处，而且几乎没有技术能力抵御形形色色的网络攻击，网络安全、经济安全和政治安全都面临严峻挑战。相关数据显示，发达国家的家庭上网的可能性几乎是发展中国家的2倍，是最不发达国家的5倍以上，个人用户的互联网访问率也有类似的差异；欧洲人上网的可能性是非洲人的3倍多，并且能享受到更快的访问速度。[③]

互联网带来的问题和挑战也在不断增多。网络恐怖主义成为全球公害，恐怖分子利用网络宣传恐怖极端思想，策划和实施恐怖主义活动。网络犯罪呈蔓延之势，聚焦数字经济的网络犯罪产业化发展态势并没有得到遏制，网络勒索、电信诈骗、电子色情服务等网络犯罪活动持续升级。据估算，2016年，互联网对全球经济的贡献高达4.2万亿美元，

① “第41次《中国互联网络发展状况统计报告》全文”，中国互联网络信息中心，2018年1月31日，http://www.cac.gov.cn/2018-01/31/c_1122347026.htm。

② “网络空间国际合作战略”，新华网，2017年3月1日，http://news.xinhuanet.com/2017-03/01/c_1120552767.htm。

③ ITU，“Measuring the Information Society Report 2017”，November 2017，https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf.

但同时网络犯罪的成本高达4450亿美元，后者在2019年可能增至2万亿美元。[①] 滥用信息通信技术干涉别国内政、从事大规模网络监控等活动时有发生。用户个人信息、企业商业秘密甚至政府和政党的政治机密遭到大规模泄露，围绕大选等重大政治事件的黑客攻击成为国家间意识形态战略博弈的新形式。关键信息基础设施存在较大风险隐患，针对重要关键信息基础设施和工业系统的攻击更加智能、隐匿且影响巨大。2017年5月，勒索病毒肆虐全球150多个国家，大量受影响的设备都属于关键信息基础设施，遍布金融、能源、通信等各个行业，破坏性极其巨大，让大部分人从“围观者”被迫成为“受害者”。全球互联网基础资源管理体系难以反映大多数国家的意愿和利益，少数发达国家在网络信息资源和技术等方面占有垄断或优势地位，实际操控着全球网络空间的治理权，形成了对其他国家极为不平等的状况。

网络空间缺乏普遍有效规范各方行为的国际规则，这令其自身发展受到制约。2013年6月以来，斯诺登及其引爆的“棱镜门”事件使网络安全问题引起各国的高度关注，国际社会逐渐开始形成共识——在网络安全带来的问题和挑战面前，任何国家都难以独善其身，各方必须就网络安全问题加强国际协调和合作，以规则为基础实现网络空间全球治理。

然而，在网络空间威胁日益加剧的背景下，全球网络空间规则的制定仍处于初试阶段，各国政府至今仍未建立全球政策框架。2017年6月，第2016—2017届联合国信息安全政府专家组（UNGGE）在纽约开完最后一次会议，25个国家官方代表进行的谈判最终破裂，未能就网络空间行为规范形成共识性文件。因此，全球网络空间的规则治理依然

① CIGI and Chatham House, “Global Commission on Internet Governance”, 2016, pp. i – iv, https://www.chathamhouse.org/sites/default/files/publications/research/2016 – 06 – 21 – global – commission – internet – governance.pdf.

任重而道远，各国应继续积极推动双边、区域和全球协商合作，坚持多边和多方参与，发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各主体作用，构建全方位、多层面的治理平台。

在多利益攸关方框架中，不同行为体既有其专长，也有其缺陷。政府可以凭借其政治权威整合不同资源，提供必需的公共产品，但其在具体政策的执行过程中却不得不依赖私营机构或公民社会的配合。私营机构是互联网发展和技术创新的重要推动力量，但在涉及整体规划和统筹方面则又离不开政府的支持。互联网社群因其技术特长而具有相比于政府和企业的不对称优势，而且在互联网治理中，个人或公民社会的配合也不可或缺。

二、问题的提出

网络空间的全球性、虚拟性和无国界性使网络安全成为全球公共产品的一种类型，具备公共产品的基本特征——非排他性和非竞争性，[①] 并因此无法逃避外部性和搭便车问题。这意味着，如果每个国家都根据本国利益为其网络提供安全措施，作为公共产品的网络安全在全球层面很可能是供给不足的，这也决定了网络安全全球治理的必要性。全球治理是20世纪90年代开始兴起的国际关系概念。学界一般把国家、国际组织、市场和由众多非政府组织组成的公民社会看作全球治理的重要主体。如今，各类国际组织正发挥着越来越重要的作用。

与网络安全治理有关的国际组织可以划分为两种类型。[②] 一种是政

① 张宇燕、李增刚：《国际关系的新政治经济学》，中国社会科学出版社2010年版，第139—140页。

② David A. Gross, Nova J. Daly, M. Ethan Lucarelli and Roger H. Miksad, "Cyber Security Governance: Existing Structures, International Approaches and the Private Sector", in Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age*, CNAS, June 2011, pp. 110 – 113.

府间组织（Intergovernmental Organizations，IGOs）。公共产品理论指出，要解决免费搭车问题，政府必须扮演重要角色，以弥补公共产品的最优供给量和私人领域自愿提供部分之间的差距，可以通过征税的方式为公共产品的供给筹资，同时为那些提供公共产品的私人企业提供补贴。因此，作为公共安全的一种类型，网络安全需要由主权国家政府和由主权国家构成的政府间国际组织作为主导治理进程的行为主体。[①] 实践中，很多政府间国际组织都十分关注网络安全事务，它们当中既有全球性国际组织，也有地区组织；既有建立在条约基础上的国际组织（如联合国），也有较为松散的论坛性组织（如亚太经合组织）。由于网络技术应用广泛，涉及的领域众多，很多政府间组织都发起了网络安全倡议。另一种是国际互联网技术组织（International Internet Technical Organizations，IITOs），比如互联网名称与数字地址分配机构（ICANN）、国际互联网协会（ISOC）、互联网工程任务组（IETF）和万维网联盟（W3C）。这些互联网技术组织为非政府的治理机制，主要由学术界、公共部门或私营部门的研究人员及科学家创建，而且从技术层面制定了互联网领域的很多条约、标准等。

国际组织提供网络安全公共产品的能力取决于其能否以集体认同的标准认定、惩罚和约束搭便车者，进而帮助解决网络安全在全球层面的供给不足问题。就以上两种类型的国际组织而言，国际网络技术组织由于具有技术专长且谈判机制较为灵活，在规范设定方面的能力要高于政府间组织，但在执行力方面却要弱于后者。不管是在国内还是国际层面，国际网络技术组织都缺乏执行能力，只能为那些具备规范执行力的

① 尽管在网络安全这一议题上，政府及政府间国际组织扮演了治理主体的角色，但也不能忽略其他主体在治理过程中可能发挥的作用。比如，私营企业是互联网发展和技术创新的主要推动力量，社群在提高网络权利的认知度和加强行业自律方面则发挥了积极的作用，这些因素共同促进了网络安全的实现。从这个角度讲，网络安全治理仍然需要多利益攸关方的共同参与。

政府间组织提供技术支持。[①] 而且，互联网方面公共政策问题的决策权属于国家主权，政府间国际组织将在协调与互联网相关的公共政策中发挥重要作用。鉴于此，网络安全公共产品仍将以政府间国际组织为主要的供给主体。

政府间国际组织提供公共产品的能力也有很大不同。以联合国为代表的全球性国际组织在国际参与范围和授权能力（mandate）方面是独一无二的，但其在规则的设定方面却存在程序繁琐、耗时较长、专业性不足等缺点。从实践层面来看，近年来，联合国围绕网络安全开展的全球性协商也的确因各方分歧和多头决策危机而进展缓慢。早在 2001 年 12 月，联合国大会就接受国际电信联盟的倡议，决定举办信息社会世界峰会（WSIS）。峰会分两阶段举行：2003 年 12 月在瑞士的日内瓦举行了第一阶段峰会；2005 年 11 月在突尼斯的突尼斯城举行了第二阶段峰会。而且，峰会首次采取多利益攸关方共同参与的方式，吸引了众多国家、国际组织、民间团体和私营部门的广泛参与。但是，由于发达国家和发展中国家在缩小数字鸿沟和互联网国际管理两个主要议题上存在较大分歧，无论是日内瓦峰会上通过的《原则声明》和《行动计划》，还是突尼斯峰会上通过的《突尼斯承诺》和《突尼斯议程》，都只是一些倡议和声明，与网络安全条约的标准还相距甚远。举例来说，《突尼斯议程》就网络犯罪问题的表述是，“我们强调惩治网络犯罪的重要意义，包括惩治在一个司法辖区实施、但对另一辖区产生影响的网络犯罪。我们进一步强调必须在国家和国际两个层次采用实用高效的工具和机制，重点促进网络犯罪执法部门间的国际合作。我们呼吁各国政府与其他利益攸关方合作，制定查处网络犯罪的立法，并注意现有的法律框架，例如有关‘打击违法滥用信息技术’的联大第 55/63 和 56/121 号

① Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age*, CNAS, June 2011, pp. 114 – 116.

决议以及欧洲委员会（Council of Europe）的《布达佩斯网络犯罪公约》”。[①] 值得关注的是，该议程特别提到了欧洲委员会的《布达佩斯网络犯罪公约》。后者是当时也是截至目前唯一一份具有法律效力的专门解决与计算机相关犯罪行为的多边文件，但该公约是由发达国家制定的，反映的也多是发达国家的利益主张和价值诉求，故而其公平性和代表性存疑。此后，联合国为了推动网络犯罪全球性规范的达成还做了很多努力，但最终收效甚微。比如，2010 年 4 月，在巴西召开的第 12 届联合国预防犯罪和刑事司法大会上，俄罗斯提出了有关网络犯罪全球条约的提案，获得中国等发展中国家的支持，但最终因美欧的反对而遭到否决。[②] 美欧的立场是，不需要新的网络犯罪条约，因为与网络犯罪有关的《布达佩斯网络犯罪公约》自 2001 年就已存在；若要在联合国签署网络犯罪条约，将耗时很久，因此当务之急是提高能力建设，不需要为一个全新的未经验证的条约再浪费时间。事实上，与网络战争、数据和隐私保护等议题相比，各国在网络犯罪议题上的分歧相对较少，同时网络犯罪也被各国普遍认同为最亟需应对的网络安全问题，但是即使在这个最有可能达成共识的议题领域，依然没有达成全球性的治理规范。

相比之下，一些地区性国际组织（简称“地区组织”）已经在网络安全的机制建设方面走在了全球性国际组织的前面。比如，欧洲委员会早在 2001 年 11 月就已推出全世界第一部针对网络犯罪行为的国际公约——《布达佩斯网络犯罪公约》。截至 2018 年 8 月，全球共有 61 个国家批准/加入了该公约，包括美国、日本、澳大利亚、加拿大、菲律宾等欧洲委员会的非成员国，对世界多数国家的有关立法产生了重要影

① 《信息社会突尼斯议程》，2005 年 11 月，http://www.un.org/chinese/events/wsis/agenda.htm。

② Mark Ballard, “Conflict over Proposed United Nations Cybercrime Treaty”, April 15, 2010, http://www.computerweekly.com/news/1280092581/Conflict-over-proposed-United-Nations-cybercrime-treaty.

响。欧盟自1992年就开始推出网络安全方面的法规和政策，目前已建立全面系统的网络安全政策法规体系，并拥有组织完备的机构设置。非盟也在2014年6月推出了《网络安全和个人数据保护公约》。东盟尚无具有约束力的网络安全规范，但也推出了一系列有关网络安全的行动计划、工作项目、声明、宣言、框架、总体规划等。因此，在网络安全全球治理框架暂难推出的大背景下，地区层面的合作相比而言更容易获得长足发展。而且，未来要建立网络安全全球治理框架，还可以将其建立在地区组织的框架之上。

地区组织如何开展网络安全治理？是否受到网络安全的非常规特征[①]——主权难以界定、合法性难以判定、身份难以限定、过程难以追踪、应对难以依靠单一主体的影响？不同的地区组织开展网络安全治理的方式方法有何异同？这与其原有的运行机制有着怎样的关系？概而言之，本书研究的核心问题是地区组织的特征如何影响其开展网络安全治理的路径。针对上述问题，本书拟从地区主义、安全治理、国际组织学相结合的理论视角，研究欧盟、东盟、非盟治理网络安全的路径及其特点，进而尝试对上述问题做出解答。

三、选题的意义

一方面，从地区组织的角度研究网络安全治理，既是研究视角的创新，也具有很强的理论意义。目前，国内对网络安全治理的研究多是从联合国或国别的角度切入，对地区组织开展的网络安全治理情况缺乏必要的考察，本书的研究能为全球网络安全治理提供地区组织的视角，具有一定的创新意义。面对网络安全全球治理的尴尬局面，地区组织治理是更为现实可行的治理路径。正如建构主义学者玛莎·芬尼莫尔（Mar-

① 廖丹子：“‘多元性’非传统安全威胁：网络安全挑战与治理”，《国际安全研究》2014年第3期，第25—39页。

tha Finnemore）所言，可以在现有的地区组织和功能性国际组织的平台上磋商网络安全规范，因为“与全球性国际组织相比，地区组织的成员数量少，关心的问题较为一致，更有可能迅速达成协议”。[①] 通过比较欧盟、非盟和东盟等地区组织在网络安全理念和治理方式上的异同，可以进一步丰富和发展地区组织理论和全球治理理论，为其提供更为全面的经验基础。

另一方面，选题具有现实性和较强的决策参考价值。“十八大”以来，党和国家高度重视网络安全问题，做出了在国家总体安全观的指导下，正确处理网络安全和信息化发展的关系，加快建设网络强国的战略部署。习近平主席在讲话中强调，“没有网络安全就没有国家安全”，“推进全球互联网治理体系变革是大势所趋、人心所向。国际网络空间治理应该坚持多边参与、多方参与，发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各种主体作用”。[②] 了解和掌握地区组织在网络安全治理方面的最新进展，对于中国确定国际谈判的立场，更好地在网络安全问题上开展国际合作具有现实意义。中国与东盟、非盟和欧盟等地区组织正在以及即将开展的网络安全合作，有助于推动网络空间命运共同体和“21 世纪数字丝绸之路”的建设，并将嵌入全球网络安全治理的现实版图。

其中，中国与东盟的网络安全合作已经迈出了坚实的步伐。2014 年 9 月，首届中国—东盟网络空间论坛在南宁举办。中方提出，中国与东盟在网络空间有着很多共同的理念和诉求，中方希望与东盟携手深化网络空间合作，共同打造中国—东盟信息港，使之成为建设中国—东盟

---

① Martha Finnemore, “Cultivating International Cyber Norms”, in Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age*, CNAS, June 2011, pp. 89 – 101.

② “习近平：自主创新推进网络强国建设”，新华网，2018 年 4 月 21 日，http://www.xinhuanet.com/2018 – 04/21/c_1122719810.htm。

命运共同体的重要平台。2015 年 1 月，第九次中国—东盟电信部长会议在泰国曼谷召开，会议支持中方提出的关于建立中国—东盟国家计算机应急响应组织合作机制的倡议，一致认为该机制是加强双方网络安全合作的重要平台。2015 年 9 月，在以“互联网 + 海上丝绸之路——合作·互利·共赢”为主题的中国—东盟信息港论坛上，中方就中国—东盟网络空间合作进一步提出八点合作倡议，包括共同打击网络恐怖主义，不让网络成为恐怖主义的温床，共同打击网络犯罪，打击窃取信息、侵犯隐私等行为，等等。[①] 2016 年 11 月，以“网络空间安全与社会管理”为主题的第一届中国—东盟网络空间安全高峰论坛在南宁开幕。2017 年 9 月，第四届中国—东盟网络信息安全研讨会在南宁召开，东盟多国专家增进交流与共识，并期待中国—东盟携手应对网络信息安全挑战。共筑网络安全合作空间已成为中国与东盟建立命运共同体的必然选择。加快推动中国—东盟网络安全合作，是推动中国与东盟各国以信息化促进区域经济社会繁荣发展的重要途径，也是落实国家“一带一路”倡议的重要举措，对于促进“21 世纪海上丝绸之路”的发展具有十分重要的战略意义。

作为战略合作伙伴，中国与欧盟也早已开展网络安全方面的磋商与合作。双方在 20 世纪 90 年代就建立了有关信息社会的高层对话。2005 年 7 月 1 日至 2009 年 6 月底，中国—欧盟开展了信息社会项目。该项目旨在通过信息化推动中国的经济和社会发展，加强中欧对话与交流，推动信息化有关法律框架比较研究，并通过实施示范项目，在中央级和省级部门开展培训，起到提高政府服务效率和缩小数字鸿沟的作用。项目组在支持中国政府制定和实施基本的法律、法规，改进法律、法规环境方面做了很多工作。双方对话内容涵盖整个信息社会方面的法律框

① 刘伟、汪军：“中国—东盟信息港论坛闭幕　中方提出八点合作倡议”，新华网，2015 年 9 月 15 日，http：//news. xinhuanet. com/newmedia/2015 - 09/15/c_134624461. htm。

架，包括基础结构（电信法）、安全问题（信息安全法、个人数据保护法）、透明度问题（政府信息公开条例）、电子商务问题（电子签名法、电子合同法、在线版权法和在线仲裁法）以及电子政务方面的法规等。[①] 2012 年 9 月，中欧网络工作小组（China-EU Cyber Task Force）会议在北京举行，双方认识到深化在网络问题上的理解与互信的重要性，愿加强交流与合作，应对障碍与威胁，并愿就共同面临的风险交换意见。2013 年，中欧领导人发表的《中欧合作 2020 战略规划》也涉及双方在网络安全方面的合作。2018 年 5 月，双方举行中欧数字经济和网络安全专家工作组第四次会议。2018 年 7 月发布的第二十次中国欧盟领导人会晤联合声明也多次提及双方在数字经济和网络安全方面的合作，指出“双方欢迎中欧网络工作组取得的进展，将继续利用工作组增进相互信任与理解，以促进网络政策交流与合作，并如联合国政府专家组 2010 年、2013 年、2015 年报告所述，进一步制订并落实网络空间负责任国家行为准则、规则和原则”。[②] 不过，到目前为止，欧盟和中国的网络安全合作仅停留在技术和法律援助等层面，还没有达到欧美之间已经开展网络安全联合演习的合作程度。

中国和非盟在网络安全方面的合作目前尚未全面展开。近年来，中国一直在国际社会积极打造负责任大国的身份和形象，不断扩大对非洲国家的各类援助规模，在非洲民众和国际社会中都有很好的口碑，但双方对网络安全这一新兴议题却似乎有些重视不足。2014 年 5 月，中国国务院总理李克强在尼日利亚出席第 24 届世界经济论坛非洲峰会全会时提出，合作建设非洲基础设施“三大网络”，即高速铁路网络、高速公路网络和区域航空网络，其中并没有提及正在非洲大陆迅速普及的移

① 王勇：“中国—欧盟信息社会项目成效显著”，《中国计算机报》2007 年 10 月 8 日，第 A16 版。

② “第二十次中国欧盟领导人会晤联合声明（全文）”，中华人民共和国驻欧盟使团网站，2018 年 7 月 18 日，http://www.fmprc.gov.cn/ce/cebe/chn/zoyws/t1578374.htm。