网络安全治理的“东盟方式”*

袁正清　肖莹莹

内容提要：网络安全治理是全球治理的重要内容之一，地区组织在其中发挥着不可或缺的作用。根据自己的实际情况，东盟在网络安全治理方面积极探索治理之道，初步形成了“东盟方式”。它将网络安全更多地视为网络犯罪问题，并将网络恐怖主义归为网络犯罪；充分尊重成员国的互联网主权，偏好非正式的制度安排，主要采用声明、宣言、总体规划和行动计划等较为松散灵活的制度形式；采取“最小限度的组织性”，没有应对网络安全问题的常设机构，只是松散的合作框架；非国家行为体在东盟网络安全治理的过程中虽然有自己的声音，但影响有限；与域外大国进行网络安全对话，开展网络安全合作，但仍然保持自己的独立性。

关 键 词：网络安全　地区组织　非国家行为体　“东盟方式”

作者简介：袁正清，中国社会科学院世界经济与政治研究所研究员；
肖莹莹，中国社会科学院研究生院博士研究生

一、引　言

近年来，网络安全引起了各界普遍关注，网络安全治理亦成为全球治理领域的新议题。在多元化的治理主体中，地区组织是重要组成部分。由于各地区的网络技术发展水平和面临的威胁来源存在差异，地区组织对网络安全内涵的理解以及关注的重点也有所区别。相比欧盟和非盟，东盟在网络安全

* 本文得到了国家社科基金项目“国际组织分析的社会学路径研究”（项目编号：11BGJ003）的资助，感谢《当代亚太》编辑部约请的匿名评审专家提出的意见。文责自负。

治理方面取得了一定进展，特别是在打击网络犯罪和网络恐怖主义方面达成了多项共识，推出了一系列规划、宣言和行动计划等，呈现出独有的组织特色。目前，学界对于东盟网络安全治理问题的研究大体可以分为以下三类。

一是围绕东盟内部网络安全合作展开的研究。基本的看法是，在互联网技术已经成为全球经济和社会发展重要驱动力的情况下，东盟无法承担在网络安全方面落后的风险。作为一个整体，东盟有必要形成网络安全方面的全面策略，即东盟及其成员国和公民针对网络安全事件的准备和应对能力，以提高应对严重网络安全威胁的弹性。然而，东盟目前达成地区性网络安全全面框架的进程是缓慢和碎片化的。[①] 东盟国家需要进一步讨论如何在网络空间开展国家间以及国家与非国家行为体间的互动，以共同应对形形色色的网络安全威胁。[②] 与欧盟和北约相比，亚太计算机应急联盟组织（APCERT）更有望成为东盟在网络安全合作方面可以借鉴的模式。这是因为，不干涉内政和国家主权原则是东盟坚持的两大基本原则，东盟没有权力干涉其成员国内政，而且多数东盟成员国都已经加入 APCERT，[③] 以其模式为基础塑造东盟网络安全框架的难度较小。但是，APCERT 的合法性不及欧盟和北约，其成员都只是技术实体，缺乏做出重大政策改变的政治能力，如果东盟采取 APCERT 的合作模式，其营造的合作将与 APCERT 的议程重叠，并且不足以在政府层面做出实质性改变。[④]

二是聚焦于东盟与域外国家的网络安全合作。有东盟学者提出，东盟应当与对话伙伴国等进一步加强合作，共同应对跨境网络安全挑战，并且东盟

---

① Caitríona H. Heinl，“Regional Cyber Security：Moving Towards a Resilient ASEAN Cyber Security Regime”，RSIS Working Paper No. 263，September 2013，http：//www. rsis. edu. sg/wp-content/uploads/rsis-pubs/WP263. pdf；Caitríona H. Heinl，“Enhancing ASEAN-wide Cybersecurity：Time for a Hub of Excellence?” RSIS Working Paper No. 133，July 2013，http：//www. rsis. edu. sg/wp-content/uploads/2014/07/CO13133. pdf；Caitríona H. Heinl & Stephen Honiss，“Cybersecurity：Advancing Global Law Enforcement Cooperation”，RSIS Working Paper No. 111，May 2015，http：//www. rsis. edu. sg/wp-content/uploads/2015/05/CO15111. pdf.

② Elina Noor，“Securing ASEAN’s Cyber Domain：Need for Partnership in Strategic Cybersecurity”，*RSIS Commentary*，No. 236，November 2014，https：//www. rsis. edu. sg/rsis-publication/rsis/co14236-securing-aseans-cyber-domain-need-for-partnership-in-strategic-cybersecurity/.

③ 东盟十国中，只有柬埔寨和菲律宾两国尚未加入该组织。参见 http：//www. apcert. org/about/structure/members. html。

④ Khanisa，“A Secure Connection：Finding the Form of ASEAN Cyber Security Cooperation”，*Journal of ASEAN Studies*，Vol. 1，No. 1，2013，pp. 41-53.

成员国应当就“网络空间负责任国家行为的共同规范”形成统一立场。[①] 俄罗斯学者指出，在政治动机驱动下的网络攻击日渐增加的情况下，与东盟国家达成建立信任措施（CBMs）符合俄罗斯的利益，俄罗斯和东盟国家在网络安全领域的共同利益主要基于打击网络犯罪和网络恐怖主义两大议题。[②] 中国学者认为，网络安全是中国和东盟在网络空间治理上的最大公约数，中国与东盟开展合作的最终目标应该是使双方成为彼此网络安全的战略大后方。[③] 中国和东盟的网络空间合作需要处理各种相互交织的线上和线下矛盾，在尊重文明、文化和宗教多样性的同时，要共同应对宗教极端主义在网上日益扩大的影响力和西式言论自由极端主义在亚洲的滥觞。[④]

三是主要从国别层面探讨东盟国家的网络安全治理情况。研究对象主要是新加坡、马来西亚和泰国等网络普及率较高的东盟国家，研究内容侧重于这些国家在网络安全方面的机制建设等。新加坡在这方面独具特点。它是世界上第一个公开宣布对互联网实行管制的国家，其在网络内容管理方面实行“三管齐下”的方针，即实施轻触式管理制度、鼓励行业自律和提高公众网

① Caitríona H. Heinl，“Tackling Cyber Threats：ASEAN Involvement in International Cooperation”，*RSIS Commentaries*，No. 114，June 21，2013，http：//www. nationmultimedia. com/opinion/Tackling-cyber-threats-will-require-regional-coope-30209055. html.

② PIR，“Common Agenda for Russia and ASEAN in Cyberspace：Countering Global Threats，Strengthening Cybersecurity，and Fostering Cooperation”，*Security Index*：*A Russian Journal on International Security*，Vol. 20，No. 2，2014，pp. 75-87.

③ 李欲晓：《中国和东盟在网络空间治理上的最大公约数》，载《网络传播》2014 年第 10 期，第 71～75 页。

④ 徐培喜：《中国—东盟网络空间论坛：嵌入全球互联网治理的现实版图》，载《网络传播》2014 年第 10 期，第 79～81 页。

络安全意识。[①]

本文将在已有研究的基础上，从地区组织层面分析东盟所面临的网络安全威胁，系统梳理东盟官方在网络安全方面的制度安排，评估域外大国和非国家行为体对东盟网络安全治理的影响，最后阐释网络安全治理的“东盟方式”。

二、东盟网络安全现状

网络安全是东盟安全的重要部分。相比其他地区，东盟的网络安全既有共同之处，也有自己的特点。主要体现在以下几个方面：

第一，信息通讯技术的迅速普及给东盟国家带来了日益严重的网络安全挑战。尽管东盟是一个由小国组成的地区性国际组织，但总体来说，其成员国的信息通讯技术发展状况并不落后，新加坡、文莱和马来西亚的互联网普及率接近发达国家水平，越南、菲律宾和泰国的互联网普及率也都高于亚洲平均水平（见表1）。与之相随的是，这些国家的网络犯罪案件也在持续增加。在马来西亚，从2007年到2012年的6年内，网络犯罪案件从1139起增加到4738起，造成的经济损失从1140万林吉特（约合1893万元人民币）增加到9610万林吉特（约合1.596亿元人民币）。[②] 在新加坡，与电子商务有关的诈骗案从2013年上半年的96起大幅增加至2014年同期的504起，其中最常见的是网购多重付款案件，由13起增加到302起，涉案金额至少23.7万新元（约合118.5万元人民币）；第三方付款担保相关的电邮欺诈从

① 此类研究参见 Ter Kah Leng，“Internet Regulation in Singapore”，*Computer Law & Security Report*，Vol. 13，No. 2，1997，pp. 115-119；Australian Strategic Policy Institute，“Cyber Maturity in the Asia-Pacific Region 2014”，April 2014，https：//www. aspi. org. au/publications/cyber-maturity-in-the-asia-pacific-region-2014；Pinsent Masons MPillay，“Singapore Ramps up Its Cybersecurity Efforts”，September 2013，http：//www. pinsentmasons. com/PDF/singapore _ramps _up _cybersecurity _efforts _Sept2013. pdf；Warren B. Chik，“The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy Reform”，*Computer Law & Security Review*，Vol. 29，2013，pp. 554-575；Garry Rodan，“The Internet and Political Control in Singapore”，*Political Science Quarterly*，Vol. 113，No. 1，1998，pp. 63-90；刘杨钺：《泰国的互联网发展及其政治影响》，载《东南亚纵横》2014年第1期，第39～44页；李静、王晓燕：《新加坡网络内容管理的经验及启示》，载《东南亚研究》2014年第5期，第27～33页；肖永平、李晶：《新加坡网络内容管制制度评析》，载《法学论坛》2001年第5期，第65～71页。

② Data Released by Royal Malaysia Police，http：//www. skmm. gov. my/skmmgovmy/media/General/pdf/DSP-Mahfuz-Majid-Cybercrime-Malaysia. pdf.

4 起增至 35 起，涉案金额至少 3.9 万新元（约合 19.5 万元人民币）；网络爱情骗局从 22 起增加至 82 起，受害者被骗取的总金额至少 310 万新元（约合 1550 万元人民币）；网络敲诈案也从 38 起增加至 132 起。①

表 1　东盟国家的互联网普及率

国　家	人　口	2000 年的互联网用户数量	互联网用户数量	互联网普及率
文　莱	429，646	30，000	318，900	74.2%
柬埔寨	15，708，756	6，000	5，000，000	31.8%
印　尼	255，993，674	2，000，000	78，000，000	30.5%
老　挝	6，911，544	6，000	985，586	14.3 %
马来西亚	30，513，848	3，700，000	20，596，847	67.5%
缅　甸	56，320，206	1，000	7，100，000	12.6 %
菲律宾	109，615，913	2，000，000	47，134，843	43 %
新加坡	5，674，472	1，200，000	4，653，067	82 %
泰　国	67，976，405	2，300，000	38，000，000	55.9 %
越　南	94，348，835	200，000	47，300，000	50.1%
亚洲整体	4，032，466，882	114，304，000	1，622，084，293	40.2%

说明：除特别标明的时间外，表内数据均截至 2015 年 11 月 30 日。

资料来源：作者根据相关资料整理而成，参见 http：//www. internetworldstats. com。

第二，网络安全的内涵多样。由于东盟国家在历史、文化和经济发展阶段等方面存在着较大的差异，其网络安全也各有特色。在穆斯林占人口绝大多数的印尼，政府将网络上的色情内容和反伊斯兰言论视为威胁。2008 年 4 月，印尼政府要求所有的网络服务提供商暂停视频网站的文件共享功能，以阻止一部反伊斯兰电影的传播；2009 年，印尼政府又要求网络服务提供商关闭一个涉嫌侮辱伊斯兰教先知穆罕默德的漫画博客。而作为君主立宪制国家，泰国将网络上诽谤、侮辱或威胁国王及王室的行为视为威胁。因传播侮辱国王的视频，泰国政府多次关闭视频网站 YouTube，并于 2011 年逮捕了一名在博客中上传冒犯国王言论内容的美国人。但在受美国自由主义思想影响较深的菲律宾，政府就很难将上述内容建构为安全威胁。比如，2012 年，

① 陈济朋：《新加坡网络犯罪案件激增》，新华网，2014 年 8 月 13 日，http：//news. xinhuanet. com/newmedia/2014-08/14/c _126869564. htm。

由菲律宾国内人权组织、律师、媒体和博客写手发起的示威活动使得政府不得不推迟实施《预防网络犯罪法案》。该项法案旨在打击网络上的黑客、盗窃、欺诈、滥发垃圾电邮及色情活动等，同时它也将一些在线诽谤视为犯罪行为，示威者们担心该法案将导致网络自由言论受到审查和压制。①

第三，网络威胁的“安全化”程度有限。② 与欧美按严重程度“浓墨重彩”地描述网络安全威胁不同，东盟及其成员国对网络安全威胁的描述只能用轻描淡写来形容。东盟官方文件中难以找到将网络安全威胁视为“存在性威胁”或首要威胁等类似的表述。迄今为止，东盟也没有推出网络安全方面的战略和法规。在东盟已公布的与网络安全相关的正式或草案文本中，甚至都没有对网络安全这一核心概念的明确定义。东盟的网络安全主要涵盖网络犯罪和网络恐怖主义，对数据和隐私保护重视不足，对网络战争（防御）更是鲜有提及。根据东盟秘书处提供的资料，③ 东盟最初只是将网络犯罪作为跨国犯罪的一种类型加以讨论，在 2001 年 10 月于新加坡举行的第三届东盟关于跨国犯罪的部长级会议上，各国同意将网络犯罪作为共同打击的跨国犯罪的一部分。后将网络犯罪作为单独议题并设立相关工作组，此后才开始讨论网络恐怖主义、数据和信息基础设施保护等。不过，尽管东盟一直将网络恐怖主义作为单独议题加以讨论，比如，2004～2007 年举行了东盟地区论坛（ARF）第一至第四届关于网络恐怖主义的研讨会，各国仍旧认为网络恐怖主义只是网络犯罪的一种形式。东盟地区论坛 2006 年 7 月通过的《关于合作打击网络攻击和恐怖分子滥用网络空间的声明》专门指出，恐怖分子滥用网络空间是网络犯罪的一种形式，是犯罪分子对信息技术的滥用。④ 东盟官

① 张睿：《东南亚各国探索建设“安全网络”》，比特网，2013 年 6 月 25 日，http：//sec.chinabyte. com/247/12646747. shtml。

② “安全化”指的是特定的安全问题被当作“存在性威胁”加以提出，并赋予行为主体采取紧急行动和超越常规政治规则的权利的过程。参见巴里·布赞、奥利·维夫、迪·怀尔德：《新安全论》，朱宁译，浙江人民出版社 2003 年版，第 32～37 页。

③ “ASEAN’s Cooperation on Cybersecurity and Against Cybercrime”，presented by the ASEAN Secretariat at Octopus Conference：Cooperation Against Cybercrime，December 4，2013，Strasbourg，France，https：//www. coe. int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/Presentations/Workshop1/ASEAN%27s _Cooperation _on _Cybercrime _and _Cybersecurity. pdf.

④ “ASEAN Regional Forum Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyberspace”，Issued at the 13th ASEAN Regional Forum，July 28，2006，Kuala，Lumpur，http：//www. mofa. go. jp/region/asia-paci/asean/conference/arf/state0607-3. html.

方文件中几乎没有有关网络战争（防御）的内容，这既与网络战尚未真正来临、东盟国家对其认知有限有关，也与东盟不愿因之引发成员国冲突、影响友好氛围有关。

与欧盟和非盟都已通过有关数据和隐私保护的条例或公约相比，东盟对待该问题的态度可以用“漠视”来形容——由表 2 可以看出，东盟只是在第十届东盟电信和信息技术部长会议（TELMIN）上通过的《东盟信息通信技术总体规划 2015》中提到，应当在东盟内部分享数据和信息基础设施保护的最佳实践。不论是威权体制色彩较浓的越南或缅甸，还是已经实行民主体制的新加坡、菲律宾、马来西亚和印尼，都难以在互联网自由、数据和隐私保护等方面达到欧美国家的水平，也难以在东盟层面达成强有力的数据和隐私保护机制。

三、东盟网络安全治理的路径

考虑到东盟本身的结构性特点和网络安全这一议题的特殊性，东盟网络安全治理的路径可从东盟、域外大国和非国家行为体三个层面加以解析。

（一）东盟层面的制度安排

东盟讨论网络安全问题的机制主要包括：东盟关于跨国犯罪的部长级会议（AMMTC）、东盟关于跨国犯罪的高官会议（SOMTC）、东盟地区论坛、东盟电信和信息技术部长会议、东盟电信高官会议（TELSOM）、东盟电信监管理事会（ATRC）和东盟关于社会福利和发展的高官会议（SOMSWD）（见表 2）。这七种机制可以分为四大类型。第一类是关于跨国犯罪的机制，即东盟关于跨国犯罪的部长级会议和东盟关于跨国犯罪的高官会议。前者负责审查东盟各国关于跨国犯罪的工作，为开展区域合作打击跨国犯罪设定方向；后者负责审查工作计划的政策战略和执行情况，同时要向前者汇报工作进展。它们不仅是东盟最早关注网络安全问题的机制，也是打击网络犯罪方面最为专业的机制。从 2001 年至今，两大机制应对网络犯罪方面的工作取得了很大进展：先是同意将网络犯罪列入东盟打击跨国犯罪的工作项目，随后通过了东盟网络犯罪执行能力建设的共同框架，继而批准建立了关于网络犯罪的工作小组，并完成了东盟在打击网络犯罪方面的路线图。

第二类是偏重技术合作的机制，即东盟电信和信息技术部长会议、东盟

电信监管理事会和东盟电信高官会议。这些机制关注的是东盟信息基础设施的安全，多使用互联网安全（network security）的术语。比如，东盟电信和信息技术部长会议先后通过了《新加坡宣言》、《东盟信息通信技术总体规划2015》和《麦克坦—宿务宣言》（Mactan Cebu Declaration），以此推动成员国建立计算机安全应急响应组（CERT）并开展合作，实现在东盟内部的安全交易，提高公众的网络安全意识。2012 年 2 月，老挝邮电部批准建立老挝计算机安全应急响应组，标志着东盟十国已全部设立该组织。再比如，东盟电信监管理事会在 2005 年通过了互联网安全合作框架与行动计划，并在2013 年通过了互联网安全合作框架的修改版，拓宽了互联网安全的范畴，将与其他机构间的合作也囊括在内。

由于在技术领域涉及主权的内容较少、各方更容易达成共识，东盟在此类机制下开展的国际合作更为广泛。从中国方面的资料来看，自 2006 年以来，中国多次应邀参加中国—东盟电信监管理事会圆桌会议，并于 2009 年与东盟签订了《中国—东盟电信监管理事会关于网络安全问题的合作框架》；中国国家互联网应急中心（CNCERT）自 2007 年起每年参加东盟计算机安全应急响应组的应急演练，并邀请东盟各国计算机安全应急响应组及其政府主管部门代表参加在中国举办的六次中国—东盟网络安全研讨会。2015 年 1 月，第九次中国—东盟电信部长会议审议通过了 2015 年度中国—东盟信息通信合作项目，支持中方提出的关于建立中国—东盟计算机应急响应组织合作机制的倡议，并责成东盟电信高官会议加以落实。[①] 此外，东盟电信监管理事会和日本自 2008 年开始每年举办信息安全政策会议，自 2009 年开始每年举办互联网安全专题研讨会。在东盟电信监管理事会机制下，2011 年 7 月在马来西亚召开了东盟—欧盟关于网络犯罪的执法、法官和检察官培训。

第三类是偏重社会安全的机制，即东盟关于社会福利和发展的高官会议。在该机制下召开了以“建设根除网络色情和网络卖淫行为的东南亚”为主题的会议。会议建议：根据现行的国际人权标准，强化各国立法，针对各种对儿童和青少年进行性剥削的行为（特别是网络色情和网络卖淫行为）进行定义、禁止并入罪；推动东盟在域外管辖权和法律互助方面的合作，以有效控告各种对儿童和青少年进行性剥削的行为；强化电讯监管，使其涵盖商

① 中国工业和信息化部：《尚冰出席并主持第九次中国—东盟电信部长会议》，2015 年 1 月 23 日，http：//www. miit. gov. cn/n11293472/n11293832/n11293907/n11368223/16421515. html。

业和非商业领域，并将服务供应商的数据截留政策标准化；在东盟成员国监督、报告和处理与网络色情和网络卖淫有关的案情和受害者时，形成清晰的行为准则和机构间协调机制。

第四类是多边安全对话与合作机制，即东盟地区论坛。与其他几类机制不同，东盟地区论坛自成立之日起就是跨区域的多边机制，其成员目前共有27个，除了东盟十国外，还包括中国、日本、韩国、印度、俄罗斯、美国、加拿大、澳大利亚和欧盟等域外国家和组织。更为重要的是，东盟地区论坛已成为亚太地区最主要的官方多边安全对话与合作渠道，该机制下展开的网络安全问题讨论最能体现各国在网络空间中的政治利益和国家安全考虑，也最能展示“东盟方式”在网络安全这一特定议题领域的特点。东盟地区论坛开展的与网络安全有关的项目较多，最初主要围绕网络恐怖主义问题展开，比如，2004～2007年举行的第一～四届东盟地区论坛关于网络恐怖主义的研讨会，2006年7月在第13届东盟地区论坛上通过的《关于合作打击网络攻击和恐怖分子滥用网络空间的声明》，2008年11月举行的东盟地区论坛关于恐怖主义和互联网的会议。2010年以后，东盟地区论坛有关网络安全的议题设置更多元化，并开始偏重能力建设和建立信任措施等方面。比如，2010年4月在文莱斯里巴加湾举行的东盟地区论坛网络犯罪能力建设会议，2012年3月在越南广南省举行的关于网络空间代理行为体的专题讨论会，2012年9月在新加坡举行的关于网络事故响应的专题讨论会（ARF Workshop on Cyber Incident Response），2012年9月在韩国首尔举行的关于在网络空间建立信任措施的专题研讨会，以及2013年9月在北京举行的“加强网络安全措施——法律和文化视角”研讨会。

表2　东盟在网络安全和打击网络犯罪方面的合作

时　间	机　制	合作进展
2001年10月	第三届东盟关于跨国犯罪的部长级会议	各国同意将网络犯罪列入工作项目，以执行1999年第二届AMMTC上通过的《东盟打击跨国犯罪行动计划》。
2002年5月	第二届东盟关于跨国犯罪的高官会议	通过了《补充东盟打击跨国犯罪行动计划的工作项目》，网络犯罪被列入其中。
2003年9月	第三届东盟电信和信息技术部长会议	通过了《新加坡宣言》。该宣言强调，各方应努力建立东盟信息基础设施，以推进互联互通、网络安全和完整性；所有的东盟成员国应在2005年前根据相互认可的最低绩效标准建立和运营计算机安全应急响应组。

2005 年 8 月	第 11 届东盟电信监管理事会	通过了互联网安全合作框架与行动计划。
2006 年 7 月	第 13 届东盟地区论坛	通过了《关于合作打击网络攻击和恐怖分子滥用网络空间的 ARF 声明》。该声明要求各国：根据各自的国家情况并参照相关的国际文件和建议/指导，制定和执行网络犯罪和网络安全法；承认国家框架在合作应对犯罪分子（包括恐怖分子）滥用网络空间方面的重要性，并鼓励制定这样的框架；同意共同努力提高应对网络犯罪（包括恐怖分子滥用网络空间）的能力；承诺通过增进各国计算机安全事件响应小组（CSIRT）间的信任以及制定倡议和公众意识项目，继续共同打击网络犯罪。
2007 年 6 月	第七届东盟关于跨国犯罪的高官会议	通过了东盟网络犯罪执行能力建设的共同框架，以支持全球打击网络犯罪的行动。
2010 年 10 月	第 17 届东盟领导人会议	通过的《东盟互联互通总体规划》（Master Plan on ASEAN Connectivity）指出，“认识到更紧密的互联互通能够带来的可见收益，总体规划承认，跨国犯罪、非法移民、环境退化和污染以及其他跨境挑战带来的问题，应该得到妥善处理”。
2011 年 1 月	第十届东盟电信和信息技术部长会议	通过了《东盟信息通信技术总体规划 2015》。其中提到的六项战略互信中有两项都和网络犯罪相关：战略互信二中提到，推动在东盟内部的安全交易，开展活动提高网络安全意识；战略互信四中提到，为网络安全建立共同的最低标准，以确保东盟网络的覆盖率和安全性，为东盟建立网络安全“健康筛查”项目，为商业建立最佳实践模式和为所有行业建立灾难恢复能力，在东盟内部分享数据和信息基础设施保护的最佳实践。
2012 年 6 月	东盟关于社会福利和发展的高官会议	召开以“建设根除网络色情和网络卖淫行为的东南亚”为主题的首次会议。
2012 年 7 月	第 19 届东盟地区论坛	通过了《在确保网络安全方面开展合作的声明》。该声明包括在信息和通讯技术（ICT）的使用安全方面强化地区合作的措施：进一步考虑符合国际法及其基本原则、应对该领域新兴威胁的战略；推进与信任建立、稳定和降低风险有关的对话，以应对 ARF 参与者使用信息通讯技术中的各种问题；鼓励并推进网络安全文化方面的合作；制定在 ICT 使用安全方面的工作计划，聚焦在建立信任措施方面的实际合作；阐述与 ICT 使用相关的术语及定义。

2012 年 11 月	第 12 届东盟电信和信息技术部长会议	通过了《麦克坦－宿务宣言》。宣言指出，“要继续在东盟计算机安全应急响应组间开展合作活动，比如东盟 CERT 事故演练，以提高 CERT 间的事故调查和协作，支持东盟网络安全行动理事会（ANSAC）的活动”。
2013 年 4 月	东盟关于社会福利和发展的高官会议	召开以“建设根除网络色情和网络卖淫行为的东南亚”为主题的第二次会议。
2013 年 6 月	第 13 届东盟关于跨国犯罪的高官会议	批准建立关于网络犯罪的工作小组。
2013 年 8 月	第 19 届东盟电信监管理事会	通过了互联网安全合作框架的修改版。修改版拓宽了互联网安全的范畴，将与其他机构间的合作也囊括在内。
2014 年 5 月	东盟关于跨国犯罪的高官会议	成立了两个应对网络犯罪的新机制。一是 SOMTC 首个关于网络犯罪的工作组，该工作组完成了东盟在打击网络犯罪方面的路线图，旨在能力建设和培训、执法、信息交换、地区外合作等方面推进地区合作。二是东盟—日本网络犯罪首次对话会，双方讨论了在打击网络犯罪方面的战略合作。

资料来源：2013 年 8 月之前的内容参见“ASEAN’s Cooperation on Cybersecurity and Against Cybercrime”；2014 年 5 月的内容参见 ASEAN Secretariat，“ASEAN Steps up Fight Against Cybercrime and Terrorism”，May 30，2014，http：//www.asean.org/news/asean-secretariat-news/item/asean-steps-up-fight-against-cybercrime-and-terrorism。

（二）域外大国的嵌入

多元性和开放性是东盟开展地区合作的突出特点。在网络安全治理方面，东盟和域外大国存在广泛的合作和交流。

美国认为，网络安全正迅速成为其在亚洲外交活动中最需优先解决的问题之一。[①] 2013 年 7 月 1 日在文莱举行的美国—东盟部长级会议上，美国国务卿克里（John Kerry）表示，美国（在东南亚地区）有两项特别关心的事宜，即海洋安全和网络安全。“美国正在并且渴望进一步和东盟一起改善网络安全、打击网络犯罪，希望帮助东盟成员国加强能力建设，以确保所有人都免受网络威胁和降低这些网络威胁带来的风险。”[②] 克里的此番话语体现在美国与东盟发起的各种网络倡议上。比如，2012 年 3 月举行的东盟地区论坛首届关于网络空间代理行为体的专题讨论会，就是美国和越南合作开展的。

① Peter Jennings，“Rise of the Cyber-men in Asia”，July 5，2013，http：//www.aspistrategist.org.au/rise-of-the-cyber-men-in-asia/.

② U.S. Department of State，“U.S. Engagement in the 2013 ASEAN Regional Forum”，July 2，2013，http：//www.state.gov/r/pa/prs/ps/2013/07/211467.htm.

美国还与新加坡合作举办关于网络空间建立信任措施的专题研讨会。[①] 美国官方声称，由于国家安全利益越来越和网络空间联系到一起，旨在提高透明度和加强能力建设的各种建立信任措施将有助于降低未来的冲突风险。[②] 美国之所以如此积极地在东盟地区论坛框架下开展各种倡议，一方面是为了借助论坛传播其在网络安全方面的理念，实现其所倡导的行为规范的社会化；另一方面是为了将其偏好的安全议题引入讨论议程，并借助论坛实现与亚太地区其他大国之间的对话和交流。与东盟国家内部更为关注网络犯罪和网络恐怖主义议题不同，美国在东盟地区论坛上提出的倡议更符合其自身安全利益。近年来，中美之间围绕网络间谍和网络犯罪问题摩擦不断，美国经常指责中国借助代理行为体（proxy actors in cyberspace）对美国发起网络攻击，其在东盟地区论坛上发起关于网络空间代理行为体的专题讨论会，无疑是为了通过渲染问题的严重性，借力东盟，对中国形成压力。当然，为了掩饰其真实意图，美国往往也会给其各种倡议披上合法和看似合理的外衣，比如，宣称有关倡议是为了帮助东盟成员国加强能力建设以降低未来的冲突风险等。

美国还联合日本一起拉拢东盟国家。2014 年 6 月，日本官方宣布，将和美国一起帮助东盟提高调查网络犯罪的技术能力，两国将共同出资 40 万美元，以向东盟成员国派遣联合国毒品和犯罪问题办公室（UNODC）的专家。美日两国希望，首先对东盟国家完成证据收集和情报分析的培训，然后考虑设立一个咨询机构，实现与东盟的信息共享。日本政府毫不讳言此举背后的动机，直言帮助东盟提高打击网络犯罪的技术能力很重要，因为“中国被怀疑正在借助东南亚地区的服务器向日本、美国和其他国家发起网络攻击”。[③] 这一事件的背景是，仅仅在日本政府表态的数周前，美国司法部以所谓的网络窃密为由起诉五名中国军官，声称他们帮助中国企业窃取美国企业的商业信息。

---

① NATO CCD-COE，“ASEAN Regional Forum Reaffirming the Commitment to Fight Cyber Crime”，July 20，2013，https：//ccdcoe. org/asean-regional-forum-reaffirming-commitment-fight-cyber-crime. html.

② U. S. Department of State，“U. S. Engagement in the 2014 ASEAN Regional Forum”，August 10，2014，http：//www. state. gov/r/pa/prs/ps/2014/230479. htm.

③ Clint Richards，“New ASEAN Anti-Cyber Skills Aimed at China”，June 9，2014，http：//thediplomat. com/2014/06/new-asean-anti-cyber-skills-aimed-at-china/.

与美国相比，日本政府和东盟在网络安全方面的合作更加全面深入，与政治的关联程度也更高。例如，2012 年 9 月，日本政府单方面宣布对中国的钓鱼岛及其附属岛屿实施所谓的“国有化”，导致两国关系不断恶化，两国黑客针对对方国的网络站点实施了侵袭。同年 10 月，日本《读卖新闻》报道称，日本政府正推动建立由日本和东盟十国组成的网络防御体系，在该体系下，各国可以分享关于网络攻击模式和技术的信息，以防御网络攻击。该媒体还认为，因为东盟国家防御网络攻击的能力较为滞后，它们可能会对该体系感兴趣。[①] 在日常交流方面，自 2009 年 2 月开始，日本政府每年都联合东盟召开有关网络安全政策的会议（2011 年召开了两次）。2014 年 10 月，第七届东盟—日本网络安全政策会议在东京举行，与会者制定了保护关键信息基础设施的指导方针，并且确定了提高公众网络安全意识等方面的倡议。此外，日本还和东盟在打击网络犯罪方面开展合作，首届东盟—日本网络犯罪对话会于 2014 年 5 月在新加坡举行，双方讨论了在打击网络犯罪方面的合作，比如推进信息共享、国际合作和能力建设等。[②]

俄罗斯和东盟在网络安全领域的合作主要是在东盟地区论坛的平台内开展，没有上升到俄罗斯—东盟双边对话关系的高度。[③] 2010 年，根据东盟地区论坛第 17 次会议的决定，俄罗斯、马来西亚和澳大利亚共同主持了关于网络安全和网络反恐问题的会议。在 2012 年 7 月举行的东盟地区论坛第 19 次会议上，在俄罗斯的倡议下，通过了一份重要文件——《在确保网络安全方面开展合作的声明》。根据声明的条款，俄罗斯、澳大利亚和马来西亚开始讨论《ARF 有关信息通信技术使用安全的工作计划》。俄罗斯参与了东盟地区论坛框架内与网络安全有关的各项讨论，包括形成通用术语、建立信任措施、网络空间中的共同原则和行为规范、数据交换和分享最佳实践、打击跨境网络犯罪和网络恐怖主义、建立地区性竞争中心和专家网络等。不过，俄罗斯研究人员认为，在东盟地区论坛开展的各项活动应当进一步融入打击网络恐怖主义的内容。他们还认为，网络空间行为准则的制定、打击网络犯

① Alicia P. Q. Wittmeyer, “Japan, ASEAN Team up for Cyber Defense”, October 8, 2012, http://foreignpolicy.com/2012/10/08/japan-asean-team-up-for-cyberdefense/.

② ASEAN, “Overview of ASEAN-Japan Dialogue Relations”, January 22, 2015, http://www.asean.org/news/item/asean-japan-dialogue-relations.

③ ASEAN, “Overview of ASEAN-Russia Dialogue Relations”, October 2014, http://www.asean.org/news/item/overview-of-asean-russia-dialogue-relations.

罪、制定建立信任措施——这些可以借助“一轨半”外交的方式实现，即官方背景的专家和非官方背景的专家一起合作，这也是东盟国家比较喜欢的方式。[①]

与俄罗斯相似，中国与东盟在网络安全治理方面的合作起步较晚，这与中俄两国更为重视在联合国平台上推动网络安全国际规范有关。[②] 近年来，中国和东盟在网络安全治理方面的合作有逐渐升温之势。与西方国家不同，中国倡导的理念是，网络国际治理应遵循《联合国宪章》所确立的国家主权原则和不干涉内政原则，加强国际网络安全应当重视各国互联网公共政策背后的文化因素，在相互尊重和包容的基础上推进合作。[③] 这和以相互尊重主权、不干涉内政为特点的“东盟方式”相符合，有助于双方开展更进一步的合作。在上述理念的指引下，2013 年 9 月，中国首次举办东盟地区论坛框架下的网络安全研讨会，从法律和文化的视角探讨加强网络安全的措施。中国外交部部长助理郑泽光在研讨会上表示，中国愿与国际社会通过东盟地区论坛等多边机制拓展交流与合作，共同推动网络空间国际规则的制定和实施；应当重视和加强发展中国家的能力建设，推动建立公正、民主、透明的互联网国际管理机制，发挥联合国的主渠道作用，并通过东盟地区论坛等多边机制拓展交流与合作，共同推动网络空间国际规则的制定和实施。[④] 2014 年 9 月，首届中国—东盟网络空间论坛在广西南宁举行，这是在中国—东盟博览会框架下举办的首次网络空间论坛，主题是“发展与合作”。中国国家互联网信息办公室主任鲁炜在开幕式上发表题为《打造中国—东盟信息港　携手构建网络空间共同体》的主旨演讲，他提出，中国与东盟要加强互联互通，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 21 世纪“海上丝绸之路”的信息枢纽。中国—东盟信息港的具体内涵包括五个方面，即基础建设平台、技术合作平台、经贸服务平台、信息共享平台和人文交流平台。2015 年 9 月，在以“互联网＋海上丝绸之路——合作·互利·共赢”

① PIR，“Common Agenda for Russia and ASEAN in Cyberspace：Countering Global Threats，Strengthening Cybersecurity，and Fostering Cooperation”，pp. 75-87.

② 2011 年 9 月，上合组织的四个成员国——中国、俄罗斯、塔吉克斯坦和乌兹别克斯坦——向联合国秘书长提交的关于国际信息安全的行为准则草案。

③ 《外交部：中国愿通过 ARF 拓展网络安全合作》，中央政府门户网站，2013 年 9 月 11 日，http：//www. gov. cn/jrzg/2013-09/11/content _2486292. htm。

④ 同上。

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。[①]

在国际合作方面，尽管美国和日本竭力“利诱”东盟国家，希望与东盟合作对付中国，但东盟与美、日在互联网自由、数据隐私保护等问题上存在诸多分歧，合作的道路并非平坦。相反，中国提出的“网络国际治理应遵循《联合国宪章》所确立的国家主权原则和不干涉内政原则”，“加强国际网络安全应当重视各国互联网公共政策背后的文化因素，在相互尊重和包容的基础上推进合作”等观点，与东盟的理念更为契合，双方的合作也将更具有可持续性。

（三）非国家行为体的影响

与传统安全不同，网络安全治理事关国家和非国家行为体等范畴广泛的利益攸关方，理想的治理模式应建立在各行为体广泛参与、平等协商的基础上。[②] 在东盟区域安全治理模式下，非国家行为体对东盟的影响主要通过第二轨道和第三轨道的对话协调机制实现。一般来说，第一轨道外交指以国家为中心的地区合作，第二轨道外交指以学术共同体为中心的地区参与形式，第三轨道外交是通过个人和组织的跨国支持网络建立的人与人之间的外交。[③] 东盟战略与国际问题研究所（ASEAN-ISIS）和亚太安全合作理事会（CSCAP）是第二轨道的两个代表性机制。第三轨道外交的主体通常是公民社会组织（CSO）。20 世纪 90 年代东南亚金融危机之后，公民社会组织在该地区获得巨大发展，[④] 开始积极参与东南亚的地区治理，以东盟人民大会（APA）和东盟公民社会会议（ACSC）最为知名。需要指出的是，第二轨道对第三轨道的运行有着重要影响。比如，东盟人民大会就是在东盟战略与国

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。

② 董青岭：《多元合作主义与网络安全治理》，载《世界经济与政治》2014 年第 11 期，第 52～72 页。

③ 周玉渊：《论东盟决策过程中的第三轨道外交》，载《东南亚研究》2010 年第 5 期，第 15～20 页。

④ 亚洲金融危机中，东盟在经济复苏中的明显缺位令外界质疑其目标和实践。东盟为此提出改革项目，其中之一就是提高决策系统的开放性，包容公民社会组织。政治家们提出“以人为本”的口号，并为公民社会组织创建了参与渠道。参见蒋佳丽：《东南亚地区主义与决策参与的局限》，肖玮译，载《国外理论动态》2015 年第 2 期，第 86～94 页。

际问题研究所的组织下开展活动的，后者将其角色定位为第一轨道和第三轨道间的桥梁。[①]

1. 第二轨道机制的代表——亚太安全合作理事会

亚太安全合作理事会成立于 1993 年，是对应和辅助东盟地区论坛的第二轨道组织，发挥着知识型领导作用，一方面推动东盟地区论坛合作议程的发展，另一方面深化其合作原则和规范。[②] 这种知识型领导作用主要借助研究小组（study group）的工作实现，网络安全研究小组就是其中之一。该小组在两次会议讨论的基础上推出了关于网络安全的备忘录。2012 年 5 月，这份名为“确保更安全的网络环境”的备忘录（亚太安全合作理事会第 20 号备忘录）获得了亚太安全合作理事会指导委员会的批准。

备忘录的建议部分涉及国家责任和区域合作两个层面。[③] 在国家责任方面，备忘录建议，政府应在协调各利益攸关方的参与方面发挥强力领导作用，制定全面的网络安全战略，提高政府、私人部门和社会整体的网络安全意识和知识，推动政府和私人部门之间的有效合作安排，制定有效的法律框架和提高执法能力以打击网络犯罪，建立和加强有着足够资源和权力的计算机安全应急响应组。在区域合作方面，备忘录建议，东盟地区论坛应当：加强机制建设，为信息和经验分享提供便利；执行有关能力建设和技术援助的措施；考虑拓展 APCERT 的角色和职责，使其成为传播信息和建议的协调中心；提高法制协调水平；建立地区性网络安全行动工作组（CSATF），为法制协调提供标准、机制和政策方面的建议。其中，在提高法制协调水平方面，应考虑东盟地区论坛成员已经接受或批准的国际网络安全公约，同时也应探索已有的地区性或全球性安排给法律的协调一致带来的便利。

尽管备忘录本身的内容有限，但亚太安全合作理事会网络安全研究小组在其两次会议中讨论的话题却十分广泛。尤其是在 2011 年 3 月于马来西亚

---

① Kelly Gerard，“From the ASEAN People's Assembly to the ASEAN Civil Society Conference：the Boundaries of Civil Society Advocacy”，*Contemporary Politics*，Vol. 19，No. 4，2013，pp. 411-426.

② 陈寒溪：《第二轨道外交：CSCAP 对 ARF 的影响》，载《当代亚太》2005 年第 4 期，第 37～38 页。

③ CSCAP Memorandum，“Ensuring a Safer Cyber Security Environment”，No. 20，May 2012，http：//www. cscap. org/uploads/docs/Memorandums/CSCAP％ 20Memorandum％ 20No％ 2020％ 20-％20Ensuring％20a％20Safer％20Cyber％20Security％20Environmenet. pdf.

召开的首次会议上，代表们讨论了与亚太地区相关的多项网络安全议题。[①]

第一，关于网络安全的定义。多数代表认为，与技术相关的对信息的可获取性、完整性、真实性和保密性的威胁都属于网络安全的范畴，比如钓鱼软件、恶意代码、黑客或僵尸病毒等。但是，对于那些与信息内容相关的威胁，各国却有不同观点。一些国家将借助网络传播某些内容（比如色情、煽动叛乱和诽谤等）的行为视为网络犯罪行为。但是，这些“非法内容”可能被另一些信奉言论自由原则的国家视为被保护的对象。由于这些差异的存在，与信息内容相关的威胁不在该研究小组的讨论范围内。

第二，各国在网络安全立法方面的差异比较显著，这是由各国在国家利益和威胁理念方面的差异导致的。代表们建议，研究小组不要过多地讨论应对网络安全的法律手段，只应声明各国愿意重审本国立法，将那些它们公认的网络技术威胁列为犯罪行为。同时，研究小组应强调非法律手段在应对网络安全问题方面的重要性，这些手段包括提高公众的网络安全意识、国家间的信息分享和技术援助以及能力建设等。

第三，强调政府、企业和公民社会开展网络安全合作的重要性，认为公私伙伴关系（PPP）是应对网络安全的双赢战略。代表们提出了加强政府、企业和公民社会合作的六点建议。一是制定和采用网络安全领域的高标准，以最大程度地确保安全，并增进各方对主要由私人部门拥有和管理的计算机网络的信心；二是确保政府和行业赖以运营的关键信息基础设施的弹性；三是政府和行业应运用市场手段，激励企业自愿将网络安全提高到理想的标准；四是确保企业和相关行业能够以协作和完整的方式应对任何网络危机；五是信息分享和早期预警；这种信息分享必须是双向的，以提供针对网络攻击和网络空间恶意活动的早期预警，并确保具备有效反击的时间；六是提高公众的网络安全意识和受教育水平，并加强公众和系统应对网络威胁的能力建设。

第四，网络安全方面存在领地管辖权和普遍管辖权挑战。现有的国际法律体系在应对跨境网络犯罪方面存在差距。尽管马来西亚、澳大利亚、印度、新加坡和菲律宾等国家已经“升级”了应对网络犯罪的法律，但亚太地

① “Report on the 1st Meeting of CSCAP Study Group on Cyber Security”, March 21-23, 2011, Putrajaya, Malaysia, http://www.cscap.org/uploads/docs/Cybersecurity/1CyberSec%20cochairs%20report.pdf.

区还有很多国家没有这样做。导致的后果是，在很多国家看来十分严重的网络犯罪问题，却因犯罪发生地法律的不健全，让犯罪分子逍遥法外。[①] 而且，犯罪分子所在国也不能将其引渡到法律健全的国家，因为现有的引渡条约通常要求其行为在两国都被视为犯罪行为。一些国家的政策还规定，不得将本国公民引渡到国外。研究小组强调，让某一地区的所有国家批准一个提供普遍/地区管辖权的公约，将是非常困难甚至是不可能的。一个更现实的选择是，该地区所有国家重新审视各自在网络犯罪方面的立法，修改现有的或者引入新的网络犯罪法，使其包括域外管辖权和在调查中法律互助的条款。

由此可见，亚太安全合作理事会为其成员提供了分享网络安全问题和挑战的平台，但其研究小组是在判断东盟地区论坛需要的基础上开展研究。[②] 正如新加坡代表在网络安全研究小组第二次会议上提醒其他代表注意的那样，研究小组的备忘录应当提出的是有希望在东盟地区论坛指导委员会上被接受的建议，因此，有关的建议应当是明确和具体的。[③] 受到这种思想的推动，题为“确保更安全的网络环境”的备忘录自动屏蔽了很多可能不受官方欢迎的内容，比如公民社会组织在网络安全治理中的作用、数据和隐私保护、表达自由和人权等。事实上，在 2011 年 3 月网络安全研究小组的首次会议上，新西兰代表和印度代表分别分享了在“网络安全中的公私伙伴关系（PPP)”和“数据和隐私保护立法”方面的经验，但在提交给东盟地区论坛的备忘录中，相关内容并未得到很好地体现。此外，备忘录给出的建议多是框架性内容，很难判断它们是否已经被东盟地区论坛所接受，比如，建议在地区层面加强能力建设和技术援助，为信息和经验分析提供便利等，这些缺乏量化标准的内容多大程度上被接受和执行都是未知数。不过，备忘录提出的“建立地区性网络安全行动工作组（CSATF)”的建议，到目前为止尚未得到落实，这在一定程度上可以证明亚太安全合作理事会对东盟地区论坛影响的有限性。

---

① 比如，2000 年左右，从美国国防部到英国国会的计算机都遭到“我爱你”病毒的袭击，造成的损失约达 100 亿美元。该病毒的创造者是菲律宾的一个名为古兹曼的年轻学生。由于病毒在 2000 年 5 月爆发时，菲律宾还没有制裁计算机黑客行为的相关法规，菲律宾当局先是以盗窃及其他罪名起诉古兹曼，但在同年 8 月因证据不足而撤销。

② “Report on the 1st Meeting of CSCAP Study Group on Cyber Security”, p. 347.

③ “Report on the 2nd Meeting of the CSCAP Study Group on Cyber Security”, Oct. 11-12, 2011, Bengaluru, India, p. 232, http://www.cscap.org/uploads/docs/Cybersecurity/2CyberSec%20cochairs%20report.pdf.

2. 第三轨道机制的代表——东盟公民社会会议

东盟公民社会会议是东盟成员国的公民社会组织每年举行一次的常规性论坛，会议产生的联合声明和建议会提交给东盟秘书处和东盟国家的政府代表。2005 年 10 月，首届东盟公民社会会议在马来西亚召开，该组织还受邀参加随后举行的东盟峰会，递交其关于东盟共同体建设的建议报告。2006 年之后，东盟公民社会会议便由公民社会组织的倡议网络——“亚洲人民倡议团结”（SAPA）独立主办，自 2008 年起还同时举行东盟人民论坛（APF），其代表获得了在东盟峰会上陈述意见的机会。[①] 东盟公民社会会议讨论的议题广泛，涵盖人权、发展、贸易、环境、青年和文化等诸多领域。

近年来，东盟公民社会会议开始从人权的角度关注网络安全问题，并提出了与数据保护、线上表达自由和互联网准入权等有关的建议。2015 年 4 月，东盟公民社会会议举行了关于“东盟地区互联网、人权和治理”问题的专题研讨会，讨论了与互联网准入、基础设施、监管和人权相关的问题。该研讨会提出了关于互联网权利和自由的十条建议。[②]

其中，第一条建议提出，在《东盟信息通信技术总体规划 2015》（2011 年 1 月在第十届东盟电信和信息技术部长会议上通过并启动）的制订过程中，公民社会的参与度很低，未来的规划必须让公民社会参与到磋商和起草过程中。第二条建议将互联网准入视为人权的一部分，提出国家有义务给公众提供便利，让他们享有在互联网上自由表达的权利。互联网准入权不仅包括接入互联网的权利，还包括信息自由流动的权利。第三条指出，表达自由和人权的标准应适用于线上。任何信息通讯技术规划都必须尊重国际人权标准，包括自由表达权、信息权和隐私权。特别是，任何信息通讯技术规划都必须尊重联合国《公民权利和政治权利国际公约》，目前有六个东盟国家是该公约的签约国。参与执行东盟信息通讯技术规划的企业也必须遵从国际人权标准。第四条指出，数据保护需要成为东盟信息通讯技术规划中的优先考虑事项。目前并非所有的东盟国家都拥有数据保护法，那些制订了数据保护法的国家必须加快执行该法律。东盟国家现有的数据保护法没有要求机构披露导致个人数据丢失的安全漏洞，未来的法律中必须使之变成强制性要求。第六条提出，在审查或屏蔽网站

① 宋效峰：《公民社会与东盟地区治理转型：参与与回应》，载《世界经济与政治论坛》2012 年第 4 期，第 34～43 页。

② ACSC/APF，“Workshop on Internet，Human Rights and Governance in ASEAN”，April 21，2015，http：//aseanpeople.org/workshop-on-internet-human-rights-and-governance-in-asean/.

时，各国对哪些内容需要被屏蔽（比如钓鱼网站和恶意代码网站）应给出清晰和确切的定义。如果是因为宗教或道德原因屏蔽网站，就必须对屏蔽的标准做出清晰的定义。如果接收到屏蔽某一网站的请求，决定是否同意该请求的程序应该公开、负责和透明。跨太平洋伙伴关系协定（TPP）可能会允许私人部门请求屏蔽内容，但互联网服务提供商不应被允许仅凭私人公司请求就撤销内容，在屏蔽或撤销内容时，必须有相应的程序和责任方。

上述内容是东盟公民社会会议从人权角度出发提出的建议，涉及线上表达自由、数据和隐私保护、线上监视和内容管制等敏感问题，弥补了第一轨道和第二轨道对此关注不足的缺陷，也体现出受西方人权组织影响的印记，是东盟网络治理中的一种声音。

四、网络安全治理的“东盟方式”

“东盟方式”是东盟国家对本地区合作和外交特征的概括。一般认为，“东盟方式”具有非正式性、共识原则和不干涉内政等核心特点，但随着区域内外各种新形势、新挑战和新问题的出现，“东盟方式”的特点也发生了些许变化。[①] 网络安全具有与传统安全相异的特点，属于国际社会在近些年面临的新问题和新挑战。但从目前的情况来看，东盟治理网络安全的方式和传统的“东盟方式”并没有太大差异。这在一定程度上说明，地区组织固有的社会规范和文化是其开展网络安全治理的先天制度环境，将在很大程度上影响甚至决定地区组织网络安全治理的路径和效率。在其他地区组织中，欧盟的网络安全政策法规体系及组织机构设置最为系统完备，其网络安全政策注重民事权利，以打击网络犯罪和数据隐私保护为关注重点，体现的是其平等、自由、法治、人权等价值观。非盟于 2014 年 6 月通过《非盟关于网络空间安全和个人数据保护的公约》，是欧洲之外第一个通过数据保护公约的地区，其理念更多地是西方发达国家的“传授”以及非政府组织积极倡导的

① 以不干涉内政这一特点为例。越来越多的国际事件促使东盟国家领导人发出改革的呼声。东南亚金融危机期间，时任马来西亚副总理的安瓦尔·易卜拉欣在 1997 年提出“建设性干预”的概念，泰国外长素林随后也提出了类似的“灵活介入”概念。2000 年新加坡的东盟正式会议公开讨论了缅甸问题，这是“东盟首次讨论成员国的内政”。还有学者指出，在缅甸问题上，东盟谨慎地对缅甸进行了“柔性干预”，如多次发表声明敦促缅甸采取措施、释放昂山素季、改善人权等。

结果。[①] 相比之下，网络安全治理的“东盟方式”主要体现在以下几个方面：

第一，东盟网络安全治理以官方层面的非正式制度安排为主体，主要采用声明、宣言、总体规划和行动计划等较为松散灵活的制度形式（见表 2）。与欧盟和非盟都已拥有网络安全方面的地区性公约相比，东盟虽然推出了一系列声明、宣言和总体规划等，却没有专门的公约或其他具有约束力的制度，有限的合作方式主要集中于人员技术交流和各类论坛对话，这符合“东盟方式”的一贯特点。但其带来的问题是，面对数量和复杂性不断提高的网络威胁，东盟缺乏有效的集体行动能力，难以开展危机管理，真正意义上的网络安全合作难以开展。正如东盟学者所言，要确保合作，就应当在东盟成员国间达成更加强有力的正式协议，让成员国在网络犯罪的界定上达成共识，能在邻国调查网络犯罪案件并根据地区协议处理案件。[②]

第二，东盟网络安全的制度安排落后于其多数成员国国内水平。以成员国中互联网普及率最高的新加坡为例。早在 1993 年，新加坡就已经制定了《滥用计算机法》，之后于 1998 年和 2003 年两次进行修订，2013 年将其更名为《滥用计算机和网络安全法》，增加了有关网络安全的内容。2012 年，新加坡还通过了数据和隐私保护方面的立法。另据联合国贸发会议对东盟电子商务法律的审查情况，[③] 截至 2013 年 3 月，东盟十国中已经有 8 个国家制定了网络犯罪相关立法（柬埔寨和老挝当时还没有网络犯罪法），3 个国家拥有数据和隐私保护方面的立法（马来西亚 2010 年通过了隐私保护法、菲律宾和新加坡 2012 年通过相关法律）。[④] 而东盟层面不仅没有与数据和隐私保护相关的制度安排，在网络犯罪方面的制度安排也基本都是缺乏约束力的宣言或声明。这一点与欧盟和非盟有很大不同。非盟 2014 年通过的有关网络空间安全和个人数据保护的公约表明，其网络安全制度设计明显领先于其成员国，外部

① 参见肖莹莹、袁正清：《非洲网络安全治理：一项初步考察》，即将发表于《西亚非洲》2016 年第 3 期。

② Khanisa，“A Secure Connection：Finding the Form of ASEAN Cyber Security Cooperation”，pp. 41-53.

③ 据联合国贸发会议 2015 年 1 月发布的报告，贸发会议在 2008 年和 2013 年对东盟电子商务法律协调统一情况进行过审查。参见联合国贸易和发展会议：《推动电子商务发展的网络法律和法规：案例研究和经验教训》，2015 年 1 月，http：//unctad. org/meetings/en/SessionalDocuments/ciiem5d2 _ch. pdf。

④ UNCTAD，“Review of E-commerce Legislation Harmonization in the ASEAN”，New York and Geneva，2013，p. 5，http：//unctad. org/en/PublicationsLibrary/dtlstict2013d1 _en. pdf.

因素而非成员国是非盟制度设计的主要驱动力。作为一个超国家行为体，欧盟的制度安排也有很多领先于成员国国内水平之处，但其形式多样，既有对发布对象具有强制性，直接适用于成员国、公司及个人的“决定”，也有灵活性较强、允许成员国根据自身情况采取不同方式和手段去实现特定目标的“指令”。

第三，非国家行为体在东盟网络安全治理中发挥的作用有限。一方面，第二轨道机制对官方依附性太强，不愿提出与官方理念相左的建议，故而其建议效果不甚明显。以亚太安全合作理事会为代表的第二轨道机制非常重视网络安全问题，成立了专门的研究小组，并以备忘录的形式向第一轨道的东盟地区论坛等提交了建议，但这些建议基本都是在“迎合”官方的需要，因此也难言对官方产生了影响力。另一方面，以公民社会为代表的第三轨道机制受西方影响较大，提出的建议与官方理念有“云泥之隔”，在以协商达成共识为决策方式的东盟，这些有干涉各国内政之嫌的建议往往会遭到忽略或摈弃。例如，东盟公民社会会议在 2015 年 4 月召开了与互联网治理有关的研讨会，提出了有关线上表达自由、线上监视、网络内容审查、数据和隐私保护等方面的建议，这些建议至少到目前为止尚未引起东盟官方的关注。

第四，东盟的网络安全治理还体现了“最小限度组织性”的偏好。东盟虽然成立了关于网络犯罪的工作组，但还没有应对网络安全问题的常设机构，在网络安全治理方面所建立的仍旧只是松散的合作框架，既缺乏约束力，也欠缺执行力。而欧盟不仅早在 2004 年就成立了负责统筹协调欧盟、成员国和企业界网络安全合作的欧洲网络和信息安全局（ENISA），而且还在 2013 年 1 月成立了专门负责打击网络犯罪的欧洲网络犯罪中心。

第五，东盟的网络安全政策具有一定的独立性，不愿对域外大国盲目随从，但尚未形成“大国平衡”格局。截至目前，在东盟组织召开的多边会谈（见表 2）中，网络安全从未像南海问题和气候变化那样成为大国间博弈的焦点。原因包括两方面。其一，东盟本身对网络安全的重视程度尚有待提高，没有将其提高到足以威胁自身存在的战略高度，因此在东盟地区论坛等多边层面推动该议题的动力不足。其二，虽然美、日等国极力通过提供资金或技术援助的方式拉拢东盟共同对付中国，但东盟在网络安全的理念方面与美日存在较大差异，与中国的共识（如尊重国家主权、不干涉内政、在相互尊重和包容的基础上推进合作）更多，各种利益冲突使得东盟暂且没有推出“大国平衡”的策略，更多的是维持于各方的对话与合作。