东盟国家网络安全治理体系差异与中国—东盟合作

韦　红　郝　雪

摘要：网络安全已成为东盟面临的重大非传统安全威胁。东盟国家在网络安全管理体制、网络安全立法、网络安全技术和能力建设、全社会共同参与和国际合作等方面存在差异，大致可分为三个类型：新加坡、马来西亚为网络安全治理“体系完善群体”，印度尼西亚、泰国、越南、菲律宾和文莱为“体系欠缺群体”，缅甸、老挝和柬埔寨为“体系落后群体”。这一差异给中国与东盟国家的网络安全合作带来了不一样的机遇与挑战。机遇主要体现为：“体系完善群体”为双方创新网络安全技术、培养网络安全人才创造了条件；“体系欠缺群体”为双方提升网络安全能力、创新网络安全治理经验提供了可能性；“体系落后群体”为双方加强信息基础设施建设创造了机会。挑战表现在：中国与“体系完善群体”合作容易受到域外国家的遏制和阻挠；“体系落后群体”网络安全意识薄弱且缺乏网络安全基本需求，将削弱双方合作的意愿和必要性；东盟整体层面上坚持不干涉原则和基于共识决策的独特合作方式，将阻碍中国与东盟整体合作。鉴于中国与东盟国家网络安全合作面临的机遇和挑战，中国宜抓住机遇，因国施策，分层合作，将中国和东盟网络安全合作落到实处。

关键词：东盟国家；中国；网络安全；网络安全治理体系；网络安全合作

收稿日期：2023-05-19

作者简介：韦红 (1964—)，华中师范大学政治学部教授，主要研究领域：亚太地区国际关系；郝雪 (1990—)，华中师范大学政治与国际关系学院博士研究生，主要研究领域：亚太地区热点问题研究。

随着互联网用户数量急剧增加，中国与东盟国家已成为网络犯罪的高发地带，加强双方网络安全合作有利于维护中国与东盟国家安全。为推动双方网络安全合作顺利展开，需要对东盟国家网络安全治理体系进行系统分析，准确把握东盟国家网络安全治理现状及其可能给中国与之合作带来的影响。

一、研究现状

目前，国内外针对东盟网络安全治理的研究集中在三个方面：一是关注东盟成

《南亚东南亚研究》2023 年第 3 期，第 22—36 页。

员国的网络安全治理状况。如：突出新加坡作为东盟网络安全治理领导者的角色；[①] 强调菲律宾通过加强伙伴关系，持续提高菲律宾网络安全能力；[②] 关注东盟次区域国家柬埔寨、老挝、越南和缅甸的网络安全法律、技术、能力建设和合作措施研究。[③] 二是从地区层面探讨东盟网络安全治理机制。如：袁正清和肖莹莹提出网络安全治理的“东盟方式”；[④] 刘杨钺系统分析东亚地区网络安全合作机制的现状与挑战。[⑤] 国外学者关注东盟网络安全法规现状和发展困境，[⑥] 如：东盟国家在网络安全和数据保护方面的立法和政策；[⑦] 东盟网络安全规则的内容、挑战和机遇；[⑧] 东盟网络安全治理平台等。[⑨] 三是从东盟与域外国家合作的角度论述东盟的网络安全治理，主要集中在美国、日本、澳大利亚和中国。其中，有关中国与东盟网络安全合作的研究较为丰富。学者们从中国与东盟面临的带有共性的威胁与挑战入手，重点讨论双方在打击网络犯罪、反对网络恐怖主义、保障关键基础设施和重要信息系统等领域开展的合作。[⑩] 也有学者从目前中国与东盟网络安全合作的不足之处入手，认为由于双方网络基础设施发展水平不同、网络安全立法存在差异、域外大国干扰等因素，中国与东盟网络安全合作还处于较低水平，尚未建立统一的网络安全合作机制，难以产

① Benjamin Ang, “Next Steps for Cyber Norms in ASEAN”, *RSIS Commentary*, Vol.10, No.174, 2018, pp.1-3; Benjamin Ang, “Singapore, ASEAN, and international cybersecurity”, In Eneken Tikk, et al.(eds.), *Routledge Handbook of International Cybersecurity*, London:Routledge, 2020, pp.218-226; 汪炜：《论新加坡网络空间治理及对中国的启示》，《太平洋学报》，2018 年第 2 期，第 35—45 页。

② Mark Bryan Manantan, “How to Build a Cyber-Resilient Philippines”, *Strategic Insight*, Vol.1, No.1, 2019, pp.51-55; Amparo Pamela H. Fabe and Ella Zarcilla-Genecela, “The Philippines’ cybersecurity strategy: Strengthening partnerships to enhance cybersecurity capability”, In Scott N. Romaniuk, et al.(eds.), *Routledge Companion to Global Cyber-Security Strategy*, London:Routledge, 2021, pp.315-324.

③ Ratha Lim and Kunvath Sok, “Sub-regional views on international cybersecurity: CLMV countries”, In Eneken Tikk, et al.(eds.), *Routledge Handbook of International Cybersecurity*, London:Routledge, 2020, pp.227-233; 米良：《越南网络治理评析》，《前沿》，2017 年第 9 期，第 49—53 页。

④ 袁正清、肖莹莹：《网络安全治理的“东盟方式”》，《当代亚太》，2016 年第 2 期，第 80—101 页。

⑤ 刘杨钺：《东亚地区网络安全合作机制：现状与挑战》，《东南亚纵横》，2015 年第 4 期，第 48—53 页。

⑥ Gohwong Srirath Goi, “The State of the Art of Cybersecurity Law in ASEAN”, *International Journal of Crime, Law and Social Issues*, Vol.6, No.2, 2019, pp.12-23; Lqbal Ramadhan, “Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations(ASEAN)”, *Journal of Social and Political Sciences*, Vol.3, No.4, 2020, pp.983-995.

⑦ Jirapon Sunkpho, Sarawut Ramjan and Chaiwat Ottamakorn, “Cybersecurity Policy in ASEAN Countries”, paper presented at Information Institute Conferences, Las Vegas,USA, March 26-28, 2018, pp.1-7.

⑧ Zine Homburger, “The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace”, *Global Society*, Vol.33, No.2, 2019, pp.224-242; Candice Tran Dai and Miguel Alberto Gomez, “Challenges and opportunities for cyber norms in ASEAN”, *Journal of Cyber Policy*, Vol.3, No.2, 2018, pp.1-19.

⑨ Fauzia Gustarina Cempaka Timur, “The Rise of Cyber Diplomacy ASEAN’s Perspective in Cyber Security”, *KnE Social Sciences*, Vol.2, No.4, 2017, pp.244-250.

⑩ 王道转：《“一带一路”下中国与东盟国家应对网络恐怖主义研究》，《中国公共安全》（学术版），2018 年第 4 期，第 87—90 页；汪晓风：《网络恐怖主义与“一带一路”网络安全合作》，《国际展望》，2016 年第 4 期，第 116—132 页；蒋巍、蓝彩箫：《中国—东盟合作打击跨国网络犯罪问题研究》，《东南亚纵横》，2019 年第 6 期，第 84—89 页。

生实质性的合作成果。[①] 国外学者关于中国与东盟网络安全合作的研究还很少，一些学者强调东盟应当与中国就网络安全问题展开合作，但也只是将其作为双方非传统安全合作中的一小部分，且尚未就中国与东盟网络安全合作的现状、问题、领域、目标、路径等展开专门性、系统性研究。[②]

总体来看，目前国内外针对东盟网络安全治理研究产生了一批具有影响力的研究成果，但依旧存在一些局限：一是研究范围不够广，没有一项涉及东盟网络安全战略、负责机构、立法、技术、人才培养、社会参与以及国际合作等综合性的网络安全治理体系研究；二是缺少独特视角，现有的中国与东盟国家网络安全合作研究基本限于区域视角，即将东盟作为一个整体，探讨中国与东盟组织的网络安全合作，缺少在国别层次上探究中国与东盟国家的网络安全治理合作。为此，本文拟从网络安全管理体制、网络安全立法、网络安全技术和能力建设、全社会共同参与以及国际合作五个方面，全面分析东盟国家的网络安全治理体系现状。通过对东盟成员国网络安全治理体系的精准分析，研究中国与东盟各国及东盟整体在网络安全合作上面临的机遇与挑战，并在此基础上，探索中国与东盟网络安全合作的方向和路径。

二、东盟国家网络安全治理体系差异

面对愈发严峻的网络安全挑战，东盟国家加快了建设网络安全治理体系的步伐。网络安全治理体系建设涉及治理主体、治理机制、治理能力、治理路径等诸多方面内容，本文将从以下五个方面来分析东盟国家网络安全治理体系及其水平：网络安全管理体制，涉及国家网络安全战略、政策，负责机构等；网络安全立法，包括网络安全法、个人信息保护法等保障网络空间基础性法律；网络安全技术和能力建设，涉及网络安全技术研发、网络安全人才培养等；网络安全治理的社会参与，涉及建立公私合作伙伴关系、教学机构设立教育课程和项目，培养公民网络安全意识等；网络安全治理的国际合作，涉及双边协议、多边协议和参与国际机制等。根据这五个方面的评估，东盟国家大致可分为三种类型。

（一）“体系完善群体”：新加坡和马来西亚的网络安全治理体系

东盟国家中，新加坡、马来西亚信息化程度较高且对网络安全威胁高度重视，两国均建立起了较为完善的网络安全治理体系。

在网络安全管理体制方面，新加坡成立了网络安全局，作为监督和协调全国网

① 郑怡君、薛志华：《中国—东盟网络安全合作及其布局》，《东南亚南亚研究》，2017 年第 2 期，第 17—23 页；孙伟、朱启超：《东盟网络安全合作现状与展望》，《东南亚研究》，2016 年第 1 期，第 56—64 页。

② Erin Zimmerman, “Security cooperation in the Indo-Pacific: non-traditional security as a catalyst”, *Journal of the Indian Ocean Region*, Vol.10, No.2, 2014, pp.150-165; Ali Abdullah Wibisono, “ASEAN-China Non-Traditional Security Cooperation and the Inescapability of the Politics of Security”, *Jurnal Global dan Strategis*, Vol.11, No.1, 2017, pp.39-54.

络安全各个方面的中央机构，发布了《网络安全战略》，旨在打造富有弹性且值得信赖的网络环境。马来西亚成立了国家网络安全局，作为网络安全事务的国家牵头机构，致力于制定和实施国家级网络安全政策和战略，并采取应对网络威胁的措施，旨在解决关键国家信息基础设施潜在的安全风险，并确立网络安全立法和监管、网络安全技术、国际合作等八项重点建设项目。

在网络安全立法方面，新加坡颁布了东盟国家第一部《网络安全法》，与《滥用电脑和网络安全法令》《个人信息保护法》《电子交易法》等共同构成网络空间法律保障体系。马来西亚也有一系列保护网络环境的立法，如《计算机犯罪法》《电子商务法》《个人数据保护法案》《国家安全委员会法案》等。其中，《个人数据保护法案》用于保护个人姓名、地址、身份证或护照、电子邮件、电话号码等数据不被滥用，但是该法律仅适用于商业交易中的个人，不适用于马来西亚联邦政府或州政府。①

在网络安全和能力建设方面，新加坡政府积极协调新加坡国立大学、南洋理工大学等高等学府与以色列本古里安大学、印度班加罗尔大学等国外学术科研机构，新加坡国立研究基金会、国际信息系统安全认证联盟等非政府组织，以及新科电子、微软、霍尼韦尔等国内外企业互动合作，使新加坡成为东南亚甚至是亚太地区培养网络安全人才、创新网络安全技术的重地。马来西亚的“网络安全专业发展”平台，通过提供多样化的能力和专业认证课程，培养网络安全从业人员、行业专家和学者。

在网络安全治理的社会参与方面，新加坡着力在全社会营造一种网络安全优先的意识，政府部门举办“网络安全意识日”活动、推出“网络健康运动”项目，资助民间公益组织“触爱社区服务社”提升全民网络安全意识。非政府组织网络健康指导委员会制定“网络礼仪”，培育公民网络素养。新加坡工商联合总会主办全国安全大会，重点讨论如何应对网络犯罪，增强全民网络安全技能。马来西亚也着重在全社会打造使用互联网服务时的安全文化。“网络安全马来西亚”是马来西亚政府设立的提供网络安全服务的机构，其目标是通过组织和创建活动，在儿童、青少年、父母中建立一种安全文化，以提高网络安全意识水平。②

在网络安全治理的国际合作方面，新加坡既突出与东盟整体的合作，参加并举办东盟网络安全部长级会议，推出东盟网络能力计划，帮助成员国进行网络空间治理，还积极开展与发达国家、周边国家和地区的合作，与美、英、法等国签署双边网络安全合作备忘录。马来西亚相继与澳大利亚、印度、韩国签署网络安全谅解备忘录，

① Hunton and Williams, “Malaysian Data Protection Law Takes Effect”, December 19, 2013, https://www.huntonprivacyblog.com/2013/11/19/malaysian-data-protection-law-takes-effect/.

② Ministry of Communications and Multimedia Malaysia, “Frequently Asked Questions”, March 14, 2022, https://www.cybersecurity.my/en/media_centre/media_faqs/media_faqs/main/detail/1691/index.html.

交流共享网络安全知识与经验。在多边领域，马来西亚与印度尼西亚和菲律宾召开网络安全问题三方会议，共同打击网络恐怖主义，与欧盟在网络安全司法领域签署合作协议。

综合而言，新加坡、马来西亚都已将网络安全定调为国家议题，给予高度重视，并逐步完善管理机构、政策制度和法律保障体系，努力构建更为安全的网络空间。同时，新加坡、马来西亚突出网络安全人才的重要性，协调政府、学术界和企业界共同开展网络安全先进技术研发。在推进网络安全教育的同时，新加坡、马来西亚还注意提高全民网络安全意识和防范网络威胁能力，将网络安全国际合作作为对外活动的首要议题之一，推动全球网络安全生态系统更具活力。

（二）“体系欠缺群体”：印度尼西亚、泰国、越南、菲律宾和文莱的网络安全治理体系

印尼、泰国、越南、菲律宾、文莱五国十分重视网络安全问题，积极投入网络安全治理体系建设，并取得了一些成绩，但在一些方面的建设仍有所欠缺。

在网络安全管理体制方面，印尼成立了国家网络和加密机构作为全国网络安全负责中心，确保政府部门、关键信息基础设施和数字经济的信息安全，增强国家对网络威胁的防御能力并提高公众对网络安全的认知。[①] 军方组建的印尼国民军网络部队，负责保护军队数据免遭盗窃，增强网络防御能力。在泰国，军方领导的国家网络安全委员会（NCSC）主要负责制订有关国家网络安全维护的各项政策和计划，供内阁批准，并在政府机构、监管机构以及关键信息基础设施组织之间举行公开听证会。[②] 网络安全监管委员会作为中层机构，根据 NCSC 的政策和计划监控网络威胁，并评估其影响。另外，还有数字经济与社会部、电子交易局、高科技犯罪科共同协调和处理网络安全问题。越南各部委之间分工明确：信息和通信部负责国家网络安全，公安部负责打击网络犯罪，国防部负责网络防御。信息和通信部下设越南计算机应急响应小组（VNCERT）、信息安全局和国家电子认证中心三个机构，其中，VNCERT 专门负责网络安全事件协调，定期与该地区的其他国家计算机应急响应小组合作组织培训课程、网络安全演习和研讨会。在菲律宾，信息和通信技术部是有关国家信息通信技术事务的牵头机构，负责信息通信行业的政策制定和发展电子政务以及确保关键信息基础设施的安全。其附属机构网络犯罪调查协调中心，负责制订国家网络安全计划、建立国家计算机应急响应小组以及促进有关网络安全事务的

① Jacqueline Kelleher, “Indonesia Launches Cyber Security Agency”, October 27, 2017, https://opengovasia.com/indonesia-launches-cyber-security-agency.

② Gohwong Srirath Goi, “The State of the Art of Cybersecurity Law in ASEAN”, *International Journal of Crime, Law and Social Issues*, Vol.6, No.2, 2019, p.13.

国际合作。[①] 文莱网络安全局负责制定国家网络安全政策和实施框架，并监督和协调相关部门应对网络威胁和网络犯罪。《数字政府战略（2015—2020）》制定了国家网络安全框架，并确定了包括网络安全在内的六个重点关注领域，力求最大限度地发挥网络空间使用潜力。

在网络安全立法方面，印尼颁布了《电信法》和《信息和电子交易法》两部与网络安全直接相关的法律，但没有具体的《网络安全法》，《个人数据保护法》还在起草阶段。在泰国，《计算机相关犯罪法案》《网络安全法》《个人数据保护法》已全面实施。在越南，现行保护网络环境的立法有《信息技术法》《网络信息安全法》《网络安全法》等。越南是唯一一个依托《网络信息安全法》同时处理网络安全和个人数据保护的东盟国家。[②] 在菲律宾，目前与网络安全相关的法律有两部，《网络犯罪预防法》旨在保护计算机、通信系统、数据库不被滥用和非法访问；《信息和通信技术部法案》主要规定了信息与通信技术部的职责。在文莱，《计算机滥用法》规定了未经授权访问或修改计算机任何程序或数据的犯罪行为；[③]《电子交易法》则为电子交易的安全使用制定了规范。

在网络安全和能力建设方面，泰国启动了耗资约 3.5 亿泰铢的培训计划，部署约 1,000 名人员从事网络安全保护措施，促进泰国跻身全球网络安全措施前 20 名国家之列。[④] 越南政府提出了“99 计划”[⑤]，将网络安全知识纳入初高中的信息学课程和课外活动中，还与国内 8 所大学合作开设网络安全学学位课程。在菲律宾，信息与通信技术部与国防部合作推出“Cyber Bayanihan 2.0”项目，项目引入来自微软、思科等众多企业的军事和民用信息技术专家，以补充政府公私合作计划，提高国家网络防御能力。信息和通信技术部与教育部联合发起“BeCyberSafe”项目，旨在教育菲律宾儿童保护自己免受网络暴力。

在网络安全治理的社会参与方面，印尼还未形成协调一致的国家举措，只有少数机构和企业着眼于加强网络安全能力和技术，如国家情报局、印尼大学、银行、

---

① The Department of Information and Communications Technology, “Cybercrime Investigation and Coordinating Center (CICC)”, March 16, 2022, https://dict.gov.ph/cybercrime-investigation-and-coordinating-center-cicc/.

② Jirapon Sunkpho, Sarawut Ramjan and Chaiwat Ottamakorn, “Cybersecurity Policy in ASEAN Countries”, paper presented at Information Institute Conferences, Las Vegas,USA, March 26-28, 2018, p.6.

③ Brunei Daruaaalam, “Computer Misuse Act (Chapter 194)”, Revised Edition 2007, https://www.agc.gov.bn/AGC%20Images/LOB/PDF/Computer%20Misuse.pdf.

④ National News Bureau of Thailand, “six major infrastructure categories named for extra cybersecurity protection”, May 9, 2018, https://thainews.prd.go.th/th/website_th/news/news_detail/WNPOL6105090010009.

⑤ “99 计划”即 2014 年越南总理提出的第 99/QD-Ttg 号决定，批准“到 2020 年信息安全人力资源培训和开发”项目，项目目标为：(a) 派遣 300 名讲师和研究人员到国外进行信息安全培训，其中 100 人为博士水平；(b) 培养 2000 名本科及以上信息安全毕业生；(c) 派遣 1500 名信息安全人员到国外进行短期培训；(d) 为政府机构的 10,000 名网络安全官员组织短期信息安全和 IT 培训。

天然气和石油行业。[①] 在泰国，由电子交易发展署与政府机构、私营部门和公众合作组织的“泰国网络安全周”，旨在鼓励所有相关人员加强网络安全合作，提高网络安全意识。在越南，越南信息安全协会联合信息安全管理局等单位，每年举办“越南信息安全日”，通过面向全国大专院校的“学生信息安全”竞赛、网络安全最新问题系列研讨会、国内最优质信息安全产品和服务投票等活动，增强公众网络安全知识和鼓励私营公司创新网络安全产品。在菲律宾，信息与通信技术部在私营企业、公共部门和学术界建立了强大的合作关系。在文莱，计算机应急响应小组不仅与本地或国际计算机应急响应小组、网络服务提供商、安全供应商等相关组织进行协调，促进对互联网安全事件的检测、分析和预防，而且通过讲座、路演、小册子等形式，提高国民网络安全意识。

在网络安全治理的国际合作方面，印尼较为热衷于国际合作。在双边领域，印尼与澳大利亚多次举行网络政策对话，全方位讨论网络安全事务，加强网络安全实践、能力建设等领域的友好合作；与印度、所罗门群岛、中国签署谅解备忘录，加强打击网络犯罪合作；与俄罗斯、新加坡就网络安全措施、网络安全立法交流经验。在多边领域，印尼积极参加国际网络攻击模拟演习、东盟—日本网络演习、国际电信联盟网络演习等一系列国际或区域网络安全演习。同时，多次出席联合国“关于从国际安全的角度来看信息和电信领域发展的政府专家组”，与各方代表共同探索应对网络安全威胁的合作措施。泰国与澳大利亚、新加坡、孟加拉国、葡萄牙签订了网络安全和数字经济领域合作谅解备忘录；与俄罗斯、伊朗、黑山建立了稳定的沟通渠道，共同应对网络安全威胁和开发网络安全技术。在多边领域，泰国举办“加强东盟地区的网络安全合作：采取综合方法应对跨国犯罪”研讨会、“网络安全区域研讨会：网络空间规范”。越南也积极参与双多边合作，与以色列、俄罗斯、印度和捷克共和国签署网络安全合作谅解备忘录；与日本就确保信息基础设施方法和应对网络攻击措施加强协调；参与全球网络专家论坛、CLMV 国家网络安全政策和外交研讨会、国际网络安全演习等。菲律宾与马来西亚签署谅解备忘录，交流网络安全实践经验，提高双方网络安全事件响应能力；与印尼、马来西亚举行网络安全三方会议；与欧洲委员会联合举办网络犯罪问题会议，讨论改善区域网络环境和国际合作打击网络犯罪。同时，菲律宾还是网络安全共同进步联盟的创始国和全球网络专家论坛的成员国。文莱在国际合作方面积极性并不高，主要是与越南加强网络安全领域合作。在多边领域，文莱参与了联合国组织的相关网络安全和发展会议。

总体而言，上述东盟五国在网络安全治理体系建设方面取得不少成果，但与新加坡、马来西亚相比，它们在某些方面的建设仍存在欠缺。例如，在立法方面，除泰国、

① Yanyan M. Yani and Muhamad Rizal, “Cybersecurity policy and its implementation in Indonesia”, *Journal of ASEAN Studies*, Vol.4, No.1, 2016, p.72.

越南制定了《网络安全法》外，其他三国均未制定相关法律。越南尽管通过了首部国家《网络信息安全法》，但政府仍然在保护网络安全基础设施与对公民的网络空间活动加强管控之间左右为难。越南还未制定《网络安全战略》，且个人数据保护也不完善。印尼对动员企业、学术界、社会组织和广大网民共同参与网络安全维护不够重视；菲律宾在网络安全人才培养和网络安全技术研发方面也有不足；文莱在参与网络安全国际合作方面显得积极性不高。这些国家的网络安全项目通常与国内基础设施项目（如学校、医院、道路）相互竞争，而后者常在国家预算分配中占据优先地位，导致用于解决网络安全问题的资源分配有限。

（三）“体系落后群体”：缅甸、老挝和柬埔寨的网络安全治理体系

与其他东盟国家相比，缅甸、老挝和柬埔寨三国无论在网络安全管理机构、立法、能力建设方面，还是在国内社会力量参与、国际合作方面，均处于落后状态。

在网络安全管理体制方面，尽管三国不同程度地建立了一些机构，但这些机构的作用却很有限。在缅甸，信息技术与网络安全部是国家网络安全的主管机构，下设国家网络安全中心（NCSC），NCSC 设置计算机应急响应小组，其使命是通过与其他国家计算机应急响应小组合作，共享网络安全信息与建议、提供技术咨询与援助，并与国家执法机构合作打击网络犯罪，提高公众网络安全意识，但是由于财力、人力、技术和设备资源有限，严重影响了这些机构履行职责能力的提升。[①] 老挝邮电部是国家网络安全的主管机构，制定信息通信技术产业发展方向与计划，2021 年升级为技术和通信部，负责国家科技、创新、电信、互联网、网络安全，下设网络安全部、数字技术部、国家互联网中心等在内的 15 个部门。目前，老挝正在提议设立网络安全指导委员会和制定《国家网络安全战略》，现行的《国家 ICT 发展战略（2016—2025）》提出了推动云计算等新技术开发和应用、培养公众网络安全意识等几项优先事项。[②] 在柬埔寨，邮电部是国家网络安全的主管机构，下设信息和通信技术安全司，负责处理网络安全和网络犯罪问题。

在网络安全立法方面，上述三国还处于初级阶段。在缅甸，仅有三部与信息通信技术相关的法律，即《计算机科学发展法》《电子交易法》《电信法》，这些立法还不足以应对国内快速上升的网络威胁，而且由于警察和司法部门在调查、取证、起诉网络犯罪方面的资源、能力和技术都有限，导致现有的法律实施缺乏效力。[③] 老

① Myanmar Centre for Responsible Business, “Sector-Wide Impact Assesment of Myanmar’s ICT Sector”, September 24, 2015, https://www.myanmar-responsiblebusiness.org/swia/ict.html.

② Ministry of Posts and Telecommunications, “National ICT Development Strategy for 2016–2025”, October 3, 2015, https://cyberpolicyportal.org/en/states/laopeoplesrepublic.

③ Niels Nagelhus Schia and Lars Gjesvik, “Managing A Digital Revolution: Cyber security capacity building in Myanmar”, In Scott N. Romaniuk, et al.(eds.), *Routledge Companion to Global Cyber-Security Strategy*, London: Routledge, 2021, p.361.

挝在《预防和打击网络犯罪法》中将网络犯罪定为刑事犯罪，并开展活动以减少和预防网络犯罪。[①]《数据保护法》和正在制定中的《网络安全法》都将成为保障老挝网络安全的基本法规。柬埔寨在加强国家网络安全和打击网络犯罪方面存在着严重的法律不足。在东盟国家中，柬埔寨是唯一一个尚未就处理网络犯罪制定具体法律的国家。《电信法》只是规定了电信业的职责，确保提供有效、安全、优质、可靠和负担得起的电信基础设施、网络和服务。[②]

在网络安全治理的国际合作方面，三国开展的国际合作都比较有限，大多是参加网络安全培训及交流研讨会之类的活动，少有实质性的合作。缅甸与澳大利亚莫纳什大学开展合作，旨在加强缅甸网络安全能力，提高政府官员、IT 从业人员以及公众的网络安全意识；与日本和新加坡合作，发展军事网络安全能力和参与网络安全培训；参与亚太计算机应急响应小组网络演习和 CLMV 国家国际网络安全政策与外交研讨会。老挝有关网络安全的国际合作也主要局限于参与研讨会，如参与 CLMV 国家国际网络安全政策与外交研讨会、网络安全共同进步联盟年会以及中国—东盟数字经济年网络安全交流研讨会。柬埔寨也是如此，如主办了 2019 年亚洲网络安全会议，参加了 CLMV 国家国际网络安全政策与外交研讨会和网络安全共同进步联盟年会。

在网络安全和能力建设方面以及网络安全治理的社会参与方面，这三国基本上乏善可陈。总体而言，这三国在网络安全治理体系建设方面都还有很长的路要走。究其原因，主要因为这些国家尚处于数字经济发展的初级阶段，缺乏处于网络威胁之中的资产，从而导致对网络安全威胁的严重性认识不足。虽然这些国家都已建立了自己的计算机应急响应小组和成立了相关的网络安全机构，负责网络安全事件的咨询和处理，但它们仍面临多重挑战，包括用于投资 ICT 基础设施的人力与财政资源有限、民众的网络安全意识匮乏、国内缺少网络安全技术人才、网络安全立法和实施有限等，这些都进一步加剧了网络安全风险。

三、东盟国家网络安全治理体系差异给中国与之合作带来的机遇与挑战

受经济发展水平以及多方面因素的影响，东盟国家网络安全治理体系水平不一，给中国与之开展网络安全治理合作带来了一定的机遇和挑战。

（一）面临的机遇

从国家利益和发展需要出发，积极应对网络安全冲击，已成为多数东盟国家维护国家安全的首要任务，为中国与之开展网络安全合作带来了机遇。

---

① Ministry of Posts and Telecommunications, “Law on Prevention and Combating Cyber Crime”, July 16, 2015, https://laocert.gov.la/ftp_upload/Cyber_Crime_Law_EnVersion.pdf.

② Ministry of Posts and Telecommunications, “Law on Telecommunications”, November 30, 2015, https://mptc.gov.kh/en/laws-regulations/laws/13777/.

一是“体系完善群体”不断提升新兴领域安全防护能力，为中国与之合作创新网络安全技术、培养网络安全人才创造了条件。近年来，“体系完善群体”国家在5G、人工智能、物联网、大数据等新兴领域蓬勃发展，催生新兴网络安全发展方向，相应的安全防范技术、安全人才培养成为发展热点。2020年新加坡网络安全局发布《新加坡更安全的网络空间总体规划（2020）》提出政府未来三年将要逐步实施的11项措施，包括：更好地保护5G网络免受网络威胁和漏洞的影响；加强云服务的网络安全；建立物联网威胁检测与分析平台等。[①]2020年《马来西亚网络安全战略（2020—2024）》提出，催化世界一流的创新、技术、研发和产业，来管理和实施马来西亚网络安全规划。[②]2021年马来西亚宣布启动建立东南亚第一个5G网络安全测试实验室，实验室将由国家网络安全专家机构、马来西亚网络安全机构、华为技术有限公司和天地通亚通（Celcom Axiata Bhd）共同建设。[③] 总之，“体系完善群体”国家都在不断加强对新兴领域安全防范技术的研究和安全人才培养，以应对新兴领域网络安全威胁并促进网络安全同步发展，这为中国与之开展网络安全合作奠定了基础，为提升共同安全防护能力创造了机会。

二是“体系欠缺群体”虽然网络安全治理体系存在不同方面的欠缺，但都积极探索对外合作，加速网络安全发展，为中国与之合作提升网络安全能力建设、创新网络安全治理经验提供了可能性。2021年中国—印尼签署《关于发展网络安全能力建设和技术合作的谅解备忘录》，双方一致同意进一步加强网络安全能力建设合作；2021年印尼发布第49号总统条例，放宽了对外国投资的限制，其中包括电信和技术部门。[④] 菲律宾因缺乏能够部署检测和预防攻击对策的称职网络安全专业人员与网络安全技术，而导致国家安全面临巨大风险。2017年菲律宾通过了《国家网络安全计划2022》，以全面的国家网络安全战略框架来适应新的网络安全管理和风险，计划内容包括：保证全国网络安全运行、实施网络弹性措施等。[⑤]2019年菲律宾启动了《网络安全管理系统项目》，希望建立双边合作伙伴关系，通过公私合营的方式，帮助

① Cyber Security Agency of Singapore, “Singapore’s Safer Cyberspace Masterplan 2020”, October 6, 2020, https://www.csa.gov.sg/docs/default-source/csa/documents/publications/safer-cyberspace-masterplan-2020.pdf?sfvrsn=d1834c15_0.

② National Security Council, “Malaysia Cyber Security Strategy 2020-2024”, October 12, 2020, https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf.

③ The Malaysian Investment Development Authority, “Malaysia to launch Southeast Asia’s first 5G cybersecurity test lab”, Feburary 22, 2021, https://www.mida.gov.my/mida-news/malaysia-to-launch-southeast-asias-first-5g-cybersecurity-test-lab/.

④ Steffen Hadi and Talitha V. Sahaly, “Legal Insight: Regulatory Aspects of the so-called ‘Super Apps’ in Indonesia”, February 24, 2022, https://www.lexology.com/library/detail.aspx?g=9fe1dc59-8cb1-4b6d-9e90-4840afef4ffe.

⑤ The Department of Information and Communications Technology, “National Cybersecurity Plan 2022”, May 2, 2017, https://dict.gov.ph/national-cybersecurity-plan-2022/.

本国应对当前和未来的网络安全挑战。此外，菲律宾信息与通信技术部正专注于创建网络安全研究中心和创新资金流，例如，2020—2030 年期间计划投入 2 亿菲律宾比索，来进一步发展网络防御能力。[①] 文莱为成功实现数字政府战略，支持“2035 宏愿”的国家发展战略，制定和实施了涵盖数字连通、个人数据保护、网络安全等主题在内的国家间网络安全合作框架，以确保现有信息基础设施和系统的安全，最大限度地发挥数据和信息在决策过程中的价值。[②] 这些举措为协调和推动中国企业、非政府组织参与印尼、菲律宾、文莱的网络安全建设创造了条件。

泰国《网络安全法》和《个人数据保护法》因授予国家网络安全机构访问、复制、监管个人和国内外企业网络账户和网络数据的广泛权力而备受争议。自由活动人士、互联网公司和商业组织都对此表示反对，认为这将牺牲隐私和法制，而为了符合规范要求可能会将外国企业赶出泰国。越南在网络安全立法方面也存在争议，《网络安全法》要求所有外国在线服务提供商在越南开设分支机构或代表处，在越南本地存储特定时间段内的用户数据。学者认为政策制定者应该对此条款保持谨慎，因为数据本地化存储可能会浪费越南开放商业环境吸引优质外国投资的机会。[③] 中国在《网络安全法》中规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。”[④] 鉴于中国在保护个人数据与维护数据跨境流动方面同泰国和越南存在相同的安全利益需求，以及类似的规范要求，有利于双方就个人信息数据保护和数据跨境流动监管展开密切的合作交流，增进双方对彼此网络安全法律、政策的认识与理解。

此外，文莱因积极采取措施使互联网对青少年和儿童更加安全而赢得联合儿童基金会的赞誉。文莱教育部将网络风险、危害和网络礼仪纳入教学大纲。从 2009 年开始的“互联网道德和网络安全警戒计划”专门针对学生、教师和家长举办研讨会，提升这些群体的网络安全和道德意识。中国也高度重视未成年人网络安全保护工作，2019 年 10 月 1 日起施行的《儿童个人信息网络保护规定》明确规定，任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息。2020 年 6 月 28 日，《未成

① Amparo Pamela H. Fabe and Ella Zarcilla-Genecela, “The Philippines’ cybersecurity strategy: Strengthening partnerships to enhance cybersecurity capability”, In Scott N. Romaniuk,et al.(eds.), *Routledge Companion to Global Cyber-Security Strategy*, London:Routledge, 2021, p.322.

② Mahendro Bhirowo, Fauzia Gustarina Cempaka Timur and Mardi Siswoyo, “Brunei Darussalam’s E-Government Strategy in Overcoming Cyber Threats”, *Jurnal Pertahanan*, Vol.4, No.3, 2018, p.155.

③ Phan Le, “Cybersecurity In a One-Party State Policies and implications for Vietnam’s economy and online freedom”, In Scott N. Romaniuk, et al.(eds.), *Routledge Companion to Global Cyber-Security Strategy*, London:Routledge,2021,p.310.

④ 中共中央网络安全和信息化委员会办公室：《中华人民共和国网络安全法》，2016 年 11 月 7 日，http://www.cac.gov.cn/2016-11/07/c_1119867116.htm。

年人保护法》修订草案新设“网络保护”专章，对未成年人的网络保护理念、网络环境建设、网络企业责任等作出全面规范。这些为中国与文莱相互学习，彼此借鉴，共同维护未成年人网络安全营造了条件。

三是“体系落后群体”因为资金有限，导致信息基础设施投资不足、发展水平缓慢，易遭受网络攻击和安全威胁，为中国与之合作改善信息基础设施建设创造了机会。面对信息基础设施落后带来的网络安全问题，“体系落后群体”积极谋求国际合作以获得资金和技术支持，以图建立具有韧性的信息基础设施。尤其是新冠疫情暴发后，“体系落后群体”国家使用互联网的人数激增，受限于信息基础设施建设水平，接入难、频繁掉线、网络崩溃等基础网络问题时常发生。2020 年老挝政府颁布一项法令，通过公私伙伴关系促进国内外投资者参与基础设施和公共服务项目的发展，重点包括开发全新的信息基础设施和服务。[①]2021 年柬埔寨政府发布《数字经济和数字社会政策框架（2021—2035）》，提出包括发展数字基础设施在内的五大发展目标，[②] 以多项利好措施，积极吸引外资投入。缅甸颁布新的《外国投资法》，给予投资者相应的税收减免优惠和提供必要的协助，旨在进一步吸引外资，实施包括现代信息技术在内的基础设施建设。[③] 而中国在信息基础设施建设上具有成熟经验与丰厚积累，能为其提供必要的资金和技术支持，有利于双方搭建合作桥梁。

（二）面临的挑战

不同水平的网络安全治理体系，会反过来影响国家在网络成熟度、政策优先级和处理安全威胁等方面的水平、认知和能力，这将给中国与东盟国家网络安全合作带来挑战。

一是“体系完善群体”在东盟地区网络安全治理中发挥着关键作用，是域外国家竞相合作的对象。受域外国家联合他国、遏制中国的网络安全合作政策影响，中国与之合作的努力遭遇阻力。新加坡作为全球重要的金融、航运、物流中心，每天在承担巨量线上交易的同时，也遭受各式的网络威胁。而马来西亚已经成为被封锁的主要可疑网络活动的全球主机。[④] 中国更是持续遭受来自境外有组织、有目的的网络攻击。开展联合行动，发挥各方优势，共同打击网络犯罪是有效遏制中国与东盟国家愈演愈烈网络犯罪活动的重要举措，但因受美国、日本、澳大利亚等域外国家的影响，双方在打击网络犯罪合作上受到一定的阻碍。以美国为例，美国长期将中

① Lao People’s Democratic Republic, “Decree on Public-Private Partnership”, December 21, 2020, https://investlaos.gov.la/wp-content/uploads/formidable/18/PPP_Decree_No.624.Gov_Dated_21.12.2020_English_Print.pdf.

② The Royal Government of Cambodia, “Cambodia Digital Economy and Society Policy Framework 2021-2035”, October 5, 2021, https://mpwt.gov.kh/en/documents/policy/436.

③ The Parliament of the Union of Myanmar, “The Republic of the Union of Myanmar Foreign Investment Law”, November 2, 2012, https://www.burmalibrary.org/docs15/Foreign_Investment_Law-21-2012-en.pdf.

④ ATKearney, “Cybersecurity in ASEAN: AN Urgent Call to Action”, January 3, 2018, https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-in-asean/files/assets/common/downloads/publication.pdf.

国视为网络攻击最大来源国，2021 年中美关系因国家间的网络攻势而持续恶化，在此背景下，美国高官密集出访亚洲。2021 年 8 月 23 日，美国副总统哈里斯将新加坡作为亚洲外交访问的第一站，两国签署了三份有关网络安全合作的“谅解备忘录”，以扩大双方在国防、金融和研发领域的网络安全合作，这些举措包括扩大网络威胁和防御措施信息共享，联合开展跨境网络安全演习，促进员工培训与学习访问等。[①] 值得注意的是，合作内容增加了对中国的关注。美国负责网络和新兴技术的副国家安全顾问安妮 • 纽伯格证实，拜登政府正在就针对中国网络行动的反制措施建立国际共识，[②] 反映出拜登政府欲拉新加坡联合制裁中国的意图。

二是“体系落后群体”国家公民和互联网企业大多是新手，网络安全意识薄弱，对开展网络安全合作认识不足，不利于增强中国与之合作的意愿。在全球范围内，大多数网络安全漏洞和网络犯罪是人为错误引起的，而不是计算机系统或硬件的脆弱性导致的。[③] 例如，根据 2018 年网络安全事件响应统计数据，老挝 43% 的网络安全事件是由于网民错误进行网络连接导致的。[④] 缅甸直到 2014 年才接入互联网，与其他国家的成熟用户相比，缅甸网民缺乏必要的在线自我保护意识。例如，他们通常会与朋友或销售 SIM 卡的代理商分享密码，以致发生网络犯罪，如移动资金损失、社交媒体账户被黑、银行账户被盗等，这些事件在缅甸很常见，[⑤] 而这些只需提高网民安全意识就可以预防。另外，“体系落后群体”信息基础设施尚未搭建完成，政府对信息基础设施的关注与需求远大于网络安全风险防范。例如，根据对东盟国家网络安全研究成果的总结分析，从 2014 年到 2019 年，柬埔寨和老挝皆没有就网络安全问题进行过研究。[⑥] 因而，相较于网络安全合作，这些国家更希望通过接受他国的技术、资金和人才等援助，以提高本国的网络发展水平。

三是东盟整体层面上坚持不干涉原则和基于共识决策的双边合作独特方式，差

---

① Cybersecurity and Infrastructure Security Agency, “United States and Singapore Expand Cooperation on Cyberspace”, August 23, 2021, https://www.cisa.gov/news/2021/08/23/united-states-and-singapore-expand-cooperation-cybersecurity; U.S. Department of the Treasury, “The United States Department of the Treasury and the Monetary Authority of Singapore Finalize a Memorandum of Understanding on Cybersecurity Cooperation”, August 23, 2021, https://home.treasury.gov/news/press-releases/jy0331.

② Dan Gunderman, “US, Singapore Sign Cybersecurity Agreements: Nations Agree to Collaborate on Information Sharing, Training”, August 23, 2021, https://www.healthcareinfosecurity.com/us-singapore-sign-cybersecurity-agreements-a-17349.

③ Ross Kelly, “Almost 90% of cyber attacks are caused by human error or behavior”, March 3, 2017, https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/.

④ Ratha Lim and Kunvath Sok, “Sub-regional views on international cybersecurity: CLMV countries”, In Eneken Tikk, et al.(eds.), *Routledge Handbook of International Cybersecurity*, London:Routledge, 2020, p.229.

⑤ Lennon Y. C. Chang and Nicholas Coppel, “Building cyber security awareness in a developing country: Lessons from Myanmar”, *Computers & Security*, Vol.97, No.10, 2020, p.3.

⑥ Nor Shazwina Mohamed Mizan, et al.(eds.), “CNDS-Cybersecurity:Issues and Challenges in ASEAN Countries”, *International Journal of Advanced Trends in Computer Science and Engineering*, Vol.8, No.1.4, 2019, p.117.

异化的网络安全治理体系阻碍了中国与东盟整体网络安全合作。在基于共识决策的要求下，网络安全合作的达成要求成员国就网络空间一系列集体期望和网络领域共同身份达成一致，以便为正在进行的国际和区域倡议最终联级和内部化提供可能性。然而，东盟国家不尽相同的网络安全治理体系，使得成员国通常在确保本国利益和实际需求之前，支持和参与东盟倡导的整体对外合作。这就导致中国在谋求与东盟合作时，因无法满足各国具体的政策要求，或因合规成本过高而无法达成。比如，2015 年联合国信息安全政府专家组达成的 11 项自愿性、非约束性的网络空间负责任国家行为规范，有助于促进中国与东盟国家以和平手段利用网络技术，保障网络空间和平与安全。尽管东盟强调对 11 条规范作出更强有力的承诺，但各国也强调在区域执行方面，灵活性将是关键。[①] 正如有学者指出，考虑到东盟成员国之间网络成熟度水平的差异，对于 11 条规范的共同承诺不应被视为理所当然。[②] 为此，在严格遵守不干涉原则和未能形成统一共识之下，中国与东盟只能在涉及经济、技术等敏感度较低、协调性较高的领域进行网络安全合作，而在文化、法律等“高政治”领域达成网络安全合作较为困难。

四、中国和东盟国家开展网络安全合作的策略选择

鉴于中国与东盟国家网络安全合作面临的机遇和挑战，因国施策，分层合作，将是中国和东盟网络安全合作的最优选择。

一是对“体系完善型”国家采取知识密集型、技术导向型协同创新合作。增强在新兴领域的安全技术交流与信息共享，共同形成前沿技术优势互补，网络安全共同维护的局面，并通过推广受国际认可的网络安全技术认证机制、制定可满足业界需求的教材等方式，将双方研发的网络安全方案与技术打入全球市场，在全球网络安全治理中发挥引领作用。借助第三方合作桥梁——位于新加坡的国际刑警组织全球创新中心，互相沟通网络风险信息，加强双方在打击网络犯罪行动、推动技术和人才领域的交流与合作，并为全球网络安全威胁分析、预防和打击网络犯罪等长期战略提供支持服务。同时，深化在亚太计算机应急响应小组内的相互协作，为该组织培养专业网络安全人才、制定网络威胁方案和促进情报共享提供财务、人力和法规支持与服务。

二是对“体系欠缺型”国家采取因地制宜、能力建设型多元化合作。中国应鼓励以大学为代表的学术研究机构和私营企业进入印尼、菲律宾本地网络市场，在技术研发上与当地大学和企业合建研发实验室，专注于网络安全防护、检测、管理技

① Elina Noor, “Positioning ASEAN in Cyberspace”, *Asia Policy*, Vol.15, No.2, 2020, p.114.

② Elina Noor, “ASEAN takes a bold cybersecurity step”, October 4, 2018, http://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/.

术的研发，以对抗各方遭遇的不断升级的高端网络威胁；在人才培养上与当地社会组织和政府相关部门，通过设立奖学金和资助计划吸引更多学生从事网络安全研究，并着手成立专门的网络安全学院对学生进行系统培训。中国可以同泰国和越南在《区域全面经济伙伴关系协定》框架下，展开数据保护与流动监管的相关议题讨论，推动三国达成统一的数据安全倡议。中国计算机网络应急处理协调中心可以与文莱计算机应急响应小组合作，开展政府公务员网络安全知识、技能、意识培训计划。同时，两国可以共同推动国际社会建立起在联合国国际电信联盟之上的在线儿童保护框架，共同支持国际电信联盟为保护网络世界中的儿童和青少年建立起一套规则，以便国际社会采取协调一致的行动。

三是对“体系落后型”国家采取信息基础设施、网络安全意识建设型合作。中国要适当转变信息基础设施建设的思路，从主动帮助转为应邀共建，通过对接目标国发展规划，提供更多、更好的适应其需求的信息基础设施建设项目，推动双方合作项目更好地落地。中国企业要聚焦基础通信能力、云计算、大数据等重点基础设施，与当地政府和通信企业开展业务创新合作，提供从规划设计、施工、到维护运营全流程服务，不断提高双方信息基础设施建设合作水平。同时，将网络安全意识建设纳入投资项目，帮助当地公民更加了解网络风险与威胁，以提升公民网络安全防范意识。

最后，鉴于东盟协商一致的共识决策模式，宜采用先行先试、随时加入的灵活性合作方式。先行先试是指在推进中国与东盟网络安全项目合作进程时，考虑到东盟各国网络安全治理体系存在差异，如果有成员国没有准备好执行项目安排，两个或更多的成员国可以先行尝试，并表明该合作项目正式启动，而无需等待所有成员国一致行动。随时加入是指先前未加入或未启动项目者，在准备充分或条件成熟之后，可以随时申请加入或启动项目。这既允许部分国家在尚未准备好承诺特定倡议或项目的情况下灵活参与，又能使那些准备进行更深入合作的国家能够在不受阻碍的情况下向前迈进，有利于推进中国与东盟网络安全合作持续深入开展。

[责任编辑：郑佳]