东盟多管齐下加强网络安全合作

文／刘 磊

图片来源/ACICE官网

2023年7月18日，东盟成员国在新加坡樟宜海军基地开设了网络安全和信息卓越中心（ACICE），新加坡国防部长黄永宏以及东盟成员国国防部官员和相关学者出席揭牌仪式。

2023年7月，为了加强网络安全区域合作，东盟成员国在新加坡樟宜海军基地开设了网络安全和信息卓越中心(ACICE)。该机构成立的主要目的是应对“网络安全、虚假信息和错误信息对国防机构构成的独特威胁”。它的开设将使成员国能够通过信息共享和改进政策协调来增强其防御性网络能力。近几年，由于地缘政治紧张局势加剧和犯罪机会主义上升，东南亚网络威胁形势日益恶化。

“数字鸿沟”和网络空间的治理呈现明显的分散化、碎片化特征

截至2022年12月，东盟地区的互联网用户高达4亿人，占全部人口的70%左右，数字技术已经成为东盟经济发展、产业转型的重要推动力量。但与之相伴，网络攻击的手段、规模、频次也在不断升级，而且隐蔽性、危害性、破坏性都在提高。频发的网络安全事件使东盟国家正在蒙受巨大的经济和社会损失。

数据泄漏、勒索攻击、针对基础设施攻击是东盟网络安全的三大威胁。据统计，2022年新加坡面临的网络攻击较前一年上升了145%，越南上升了40%左右。菲律宾和马来西亚75%的企业都曾遭遇过网络安全问题，越南因电脑病毒造成的损失高达8.6亿美元。而作为东盟国家经济支柱的中小企业已经成为网络攻击的重灾区。据卡巴斯基实验室（Kaspersky Lab）披露，2022年上半年，网络犯罪分子对东南亚国家中小企业进行了约1130万次的网络攻击，其中37万多个特洛伊木马-PSW窃取信息，导致大量数据泄露与经济损失。日益增长的网络犯罪正在严重阻碍东盟区域一体化进程。

由于东盟各国经济发展水平迥异，网络基础设施建设和技术水平也有较大差距，而且数字经济发展的重点不一致，因此东盟国家的“数字鸿沟”和网络空间的治理呈现明显的分散化、碎片化特征，由此导致在网络安全的应对上存在机制性短板与合作障碍。目前东盟70%的数据中心集中在发展水平较高的新加坡、印度尼西亚和马来西亚。作为东盟网络空间治理“领头羊”的新加坡已经提出了《智慧国家2025年规划》，拟建设覆盖全岛数据收集、连接和分析的基础设施与操作系统，并根据所获数据预测公民需求，以提供更好的公共服务。但对于老挝、柬埔寨和缅甸等国家来说，互联网建设的普及才是发展重点。据世界互联网统计中心（IWS）统计，截至2022年7月，老挝和缅甸等国的互联网渗透率才达到50%左右。老挝发布的《2016～2025年信息通信技术战略发展计划及2030年发展愿景》，将发展的重点放在邮政、电信服务行业的数字化上，希望通过发展数字通信来满足民众的基本需求。柬埔寨的《数字经济和数字社会政策框架（2021～2035）》

将数字基础设施建设确定为未来网络发展的重点内容。

多管齐下提升综合网络安全治理能力

东盟近年来先后出台《东盟数字数据治理框架》《东盟信息通信技术总体规划2020》《东盟跨境数据流动机制的关键方法》《东盟数据管理框架》等文件，确立起统一的数据流动和技术标准。在《东盟数字总体规划2025》中提出将东盟建成一个由安全和变革性的数字服务、技术和生态系统所驱动的领先数字社区和经济体。新加坡、泰国等国相继出台《网络安全法》，马来西亚制定了网络安全技术框架，文莱、新加坡、印尼、马来西亚等国成立网络安全机构，东盟国家通过不断完善网络技术标准和法制建设，来提升综合网络安全治理能力。

此外，2021年东盟启动《东盟网络安全合作战略（2021～2025）》。2022年1月东盟数字部长会议启动《第二届东盟网络安全合作战略（2021～2025）》，进一步强调加强区域网络安全合作的重要性。2022年10月成立计算机应急响应小组，商讨构建网络安全保护网络。至此，东盟基本形成了以《东盟数字总体规划2025》等文件为指导，依托东盟地区论坛、东盟打击跨国犯罪部长级会议、东盟网络安全部长级会议等区域性安全合作机制的网络安全治理体系。

除此之外，东盟还加强了与域外国家和国际组织在应对网络安全威胁方面的合作。2021年新加坡与美国签署网络空间合作谅解备忘录，将网络安全合作制度化和扩大到军事领域。2023年11月7日，东盟和美国发表《第四届东盟—美国网络安全对话联席声明》，再次强调东盟将加强与美国在网络安全能力建设方面的区域合作。2022年日本在印尼建设该地区最大规模的数字中心，以支持东南亚不断增长的数字经济。从2019年起联合国反恐办公室开始为东盟国家培训网络技术人员，帮助东盟提升打击网络恐怖主义的能力。同时，东盟积极在数据流动规则建立方面与欧盟加深合作，新加坡等国从2022年3月开始与欧盟协商制定一项将欧洲和亚洲的数据隐私框架连接起来的数据治理计划，越南也向欧盟借鉴建立关键信息基础设施网络安全保护、跨境数据管理、关键领域数据保护等方面机制建立的经验。

中国与东盟网络安全合作日益密切

早在2020年，第23届中国—东盟领导人会议就通过了《中国—东盟关于建立数字经济合作伙伴关系的倡议》，并建立起中国—东盟网络事务机制，发表《首轮中国—东盟网络事务对话共同主席声明》。2022年1月第二次中国—东盟数字部长会议通过了《落实中国—东盟数字经济合作伙伴关系行动计划（2021～2025）》和《2022年中国—东盟数字合作计划》，双方在新兴技术、数字技术创新应用、数字安全、数字能力建设等方面的合作共识持续巩固深化。中国与印尼签署《关于发展网络安全能力建设和技术合作的谅解备忘录》，与泰国签署《关于网络安全合作的谅解备忘录》。2022年11月中国发布《携手构建网络空间命运共同体》文件，强调中国秉持共商共建共享理念，不断深化网络空间国际交流合作，深化数字经济国际合作，共同维护网络空间安全。目前中国与东盟的网络合作呈现多议题、宽领域、多维度合作的态势，合作内容涵盖网络犯罪、数据安全、基础设施建设、安全政策协调、网络空间安全治理等议题。

随着共建“一带一路”倡议进入高质量发展阶段，中国与东盟的网络安全合作也迎来重要机遇期。中国和东盟除了合作应对当前猖獗的网络恐怖主义、网络犯罪、电信诈骗等跨境犯罪问题之外，双方在完善和加强网络安全合作机制建设，尤其是推动基础技术领域的研究合作，推动技术研发与产业发展，防范数据信息和关键基础设施领域的安全风险等方面还有很大的合作空间。

（作者为中国社科院亚太与全球战略研究院馆员）