

CAICT 中国信通院

中国-东盟网络安全合作 与发展研究报告 (2020 年)

中国信息通信研究院安全研究所
2020 年 12 月

版权声明

本报告版权属于中国信息通信研究院，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院”。违反上述声明者，本院将追究其相关法律责任。

前 言

自 1991 年中国—东盟建立对话关系和 2003 年中国—东盟建立战略伙伴关系以来，双方的互信程度不断加深，在经贸等领域的合作取得了丰硕成果。东盟国家处于“一带一路”的陆海交汇地带，是中国推进“一带一路”建设的优先方向和重要伙伴。2020 年为中国—东盟数字经济合作年，以“集智聚力共战疫 互利共赢同发展”为主题，是中国和东盟继中国—东盟创新年、中国—东盟媒体交流年等活动之后的又一重要活动。中国—东盟关系已进入全方位发展的新阶段。

近年来，随着互联网的高速发展进入大数据信息时代，数字经济在不断发展的同时，网络安全、数据安全等问题频繁出现。尤其在今年疫情蔓延情况下，线上服务需求剧增，如何保障疫情间网络安全成为各国关注焦点。东盟部分国家网络安全发展速度较为缓慢，内部网络安全整体水平跨度较大，对网络安全需求迫切。因此，了解中国东盟网络安全发展特点，研究我国与东盟网络安全发展现状及合作趋势，对于优化我国网络安全外部形势，深入推动“一带一路”倡议建设有着重要意义。

为此，我院编写了《中国—东盟网络安全合作与发展报告（2020 年）》。本报告总结了中国、东盟网络安全发展现状，分析了双方网络安全领域合作中存在的不足，并提出了未来加强合作的可行建议。

目 录

一、当前中国-东盟地区网络安全形势	1
（一）贸易保护主义抬头反向促进与东盟安全合作	1
（二）中国与东盟积极寻求网络安全领域合作增长点	2
（三）中国东盟持续推进数据互联互通及应急协同处置	4
二、我国网络安全发展现状	5
（一）我国逐步形成自顶而下的网络安全监管体系	6
（二）我国网络安全技术手段发展机遇与挑战并存	8
（三）疫情和中美贸易摩擦影响网络安全产业发展	10
（四）国际合作持续开展为企业海外市场带来新机遇	12
三、东盟网络安全发展现状	13
（一）东盟发达国家凭技术管理优势，推动疫情期间产业发展	13
（二）东盟发展中国家积极探索对外合作，吸收创新治理经验	16
（三）东盟欠发达国家提升空间较大，完善自身实力为主要目标	19
四、中国-东盟网络安全合作面临的挑战和机遇	21
（一）突发疫情加大中国与东盟网络安全合作限制	21
（二）复杂环境下难以形成网络安全合作合力	24
（三）疫情下全球产业链格局变化为合作带来机遇	25
五、启示与建议	29
（一）持续深化安全技术及管理合作，打造“网络空间命运共同体”	29
（二）稳步推进“一带一路”倡议，建立常态化安全合作机制	31
（三）弥合数字鸿沟，优化生态重塑中国东盟供应链安全布局	33

图 目 录

图 1 我国 2017-2022 年物联网网络安全市场规模及预测	9
图 2 2019 年东盟各成员国每百万人安全互联网服务器数量	15
图 3 东盟地区发展中国家网络安全政策发展程度情况图	17
图 4 2014-2019 东盟发展中国家网络安全基础设施发展趋势	18
图 5 东盟地区欠发达国家互联网普及率	21
图 6 东盟与中国宽带网速	23
图 7 东盟网络安全投入走势	28

CAICT 中国信通院

表 目 录

表 1 2019 年全球芯片厂商销售额及市场份额排行..... 9

CAICT 中国信通院

近年来，互联网技术更新迭代为数字经济的发展创造了良好的环境，数字经济快速发展的同时网络安全风险也随之而来。2020年为中国-东盟数字经济合作年，网络安全与数字经济发展紧密相连，数字经济时代如何保障网络安全成为现在互联网发展的焦点。本报告分析了中国-东盟地区网络安全新形势和监管措施演进动向，并对中国-东盟网络安全合作面临的问题提出针对性建议以推动数字经济下中国-东盟网络安全合作发展。

一、当前中国-东盟地区网络安全形势

今年以来，受新冠疫情影响，网络安全在助力防疫抗疫、数字基础设施建设、产业数字化转型等方面发挥了不可替代的作用。同时，由于东盟地区整体新冠肺炎疫情防控措施较欧美地区相对和缓，加之中国与东盟经贸关系持续深化，双方在网络安全领域互联互通协同发展合作也不断加深。

（一）贸易保护主义抬头反向促进与东盟安全合作

1. 受美欧贸易限制及疫情叠加影响，区域和次区域¹网络安全合作成为中国-东盟网络安全领域发展重点

近年来，美国和欧洲针对中国的贸易限制和投资保护日益激烈，美欧政府对华贸易限制不断升级，包括启动“清洁网络”计划，全供应链范围内进行泛安全化打压等。在今年这场数字经济领域的竞争博弈下，中国地方政府与东盟地区围绕网络安全产业搭建创新试验区、创新联盟等开展紧密合作。特别是随着澜沧江-湄公河次区域合作、

¹ 次区域合作：指邻近国家地区间的边境省份或国家，精心界定、跨边界较小范围区域，为发展经济、维护边境地区社会稳定等需要而开展的经济与非经济等方面的合作。

大湄公河次区域合作、中国—中南半岛经济走廊、泛北部湾经济合作等项目建设不断推进，区域和次区域合作成为中国—东盟网络安全合作的新亮点和新增长点。

2. 全球网络安全供应链重塑趋势凸显，中国与东盟国家共同协作以谋求区域网络空间稳定发展

当前全球网络安全供应链格局正因疫情发生深刻变化，在发达国家推动贸易保护主义、经贸摩擦等一系列冲击下，全球供应链呈现区域化、多元化、本地化的趋势。相关分析指出，全球网络安全供应链的协调风险加剧，区域网络空间治理重要性凸显。今年5月29日，中国与东盟发表《中国-东盟经贸部长关于抗击新冠肺炎疫情加强自贸合作的联合声明》，强调双方致力于维护网络安全供应链稳定，谋求网络空间稳定发展的决心。

3. 东盟 ICT 投资政策环境成上游网络安全产业迁移首选，低成本经济效益反促中国信息产业原材料出口

受中美贸易摩擦及疫情影响，部分制造业上游公司将生产基地或供应商转移至越南、泰国等东盟国家。例如东盟国家当地人工成本较低及获得改善的基建和法律环境，吸引了日本、韩国的一些制造业将产业链转移，以此满足中国市场的需求。然而，中国作为全球供应链的重要一环，其低成本的经济效益仍然是吸引跨国制造基地从中国进口原材料、设备仪器、技术等的首选方向。

(二) 中国与东盟积极寻求网络安全领域合作增长点

1. 中国与东盟等新兴经济体逐步优化网络安全领域政策协作，共同深化网络空间安全共识

自 2009 年中国与东盟签订《中国—东盟电信监管理事会关于网络安全问题的合作框架》后，中国与东盟国家多次举行网络安全领域论坛。一方面，中国在东盟地区论坛的框架下，同东盟及其他国家就网络空间安全问题阐述各自立场、展开交流与沟通。另一方面，通过举办东盟地区网络安全论坛研讨会等形式，不断优化东盟地区论坛成员对网安全领域政策协作的认识。中国信通院定期主办中国—东盟网络安全交流与合作发展培训会，来自东盟 9 国等专家就网络空间安全治理、安全技术水平、人才培养、促进数字经济发展等议题进行了广泛深入交流。

2. 中国与东盟积极开展网络安全技术优势互补，不断深化区域网络安全共识

网络安全技术是国家维护网络空间秩序、防范网络空间犯罪的前提基础。政府和互联网企业均是革新网络安全技术、推进网络安全技术合作的主体。中国与东盟积极推进 5G 网络、智慧城市、人工智能、物联网等新兴领域前沿技术优势互补，网络安全维护等领域工作，不断推进与东盟各国在构建新兴国家网络安全行业标准体系上凝聚共识、相向而行。2019 年第 35 届东盟峰会及东亚合作领导人系列会议上，双方发表《中国—东盟智慧城市合作倡议领导人声明》，支持中国和东盟智慧城市建立伙伴城市关系，推动相关安全政策沟通、标准制定、能力建设等方面合作。

3. 中国与东盟依托地缘优势促进市场和供应商多样化发展，稳步推进信息产业供应链安全

当前全球供应链格局正因疫情发生深刻变化，出于维护自身供应链安全考虑，中国与东盟国家以及相关跨国公司倾向于把供应链向区域、双边或本国内集中。在此情况下，中国与东盟依托地缘优势，鼓励网络安全企业双向投资，共同促进市场和供应商多样化发展，稳步推进供应链安全。今年11月15日，由东盟国家发起的《区域全面经济伙伴关系协定》（RCEP）正式签署，该协议达成后会进一步促进中国与东盟地区供应链安全，为区域网络安全一体化注入强劲动力。

（三）中国东盟持续推进数据互联互通及应急协同处置

1. 中国继续加强与东盟在新兴领域安全合作，重点推进与经济较发达东盟国家在数字基础设施安全领域合作

在新一轮科技革命与产业变革的历史机遇下，中国作为全球数字化转型领袖之一，中国继续加强与东盟在5G技术、大数据、区块链、电子商务、智慧城市等领域的安全合作。重点推进与马来西亚、泰国、新加坡等经济较发达的东盟国家在数字经济和智慧城市等领域的安全合作，打造新的经济增长点。2020年6月，在新加坡通信传媒部（MCI）与中国深圳市政府智慧城市合作联合执委会第一次会议上，双方签署8份合作谅解备忘录，旨在加强城市间合作，推动区域数字经济安全有序发展，为中国、东南亚乃至世界其他国家提供可复制的安全治理模式。

2. 中国与东盟国家积极推进互联互通，合力提升区域信

息基础设施安全水平

部分东盟国家由于数字产业发展水平和治理效能的原因，信息基础设施安全水平仍相对滞后。今年在疫情“封锁”背景下，中方与东盟国家持续推进“一带一路”倡议与《东盟互联互通总体规划 2025》对接，将数据互通作为重点，合力加强网络设施、网络数据在互联互通过程中的网络安全保障，助力本地区提升互联互通水平，为实现“无缝链接的东盟”目标共同努力。

3. 中国与东盟共同加强互联网安全监测及态势感知能力，促进建立安全应急机制

近年来，网络安全隐患层出不穷，世界各国纷纷加强网络安全领域的战略合作，以应对复杂多变的网络安全形势。当前中国与东盟从各国面临的共性威胁与挑战入手，积极搭建互联网安全监测及感知平台，重点打击网络攻击、网络犯罪及反对网络恐怖主义，保障关键基础设施、重要信息系统等领域开展合作。期间，国家计算机网络应急技术处理协调中心(CNCERT)举办十届中国-东盟网络安全应急响应能力建设研讨会，与会代表就国家网络安全新挑战、网络安全信息共享最佳实践和技术平台建设等议题进行了广泛深入交流。

二、我国网络安全发展现状

近年来，我国网络安全体系逐步成熟。网络安全立法愈加完善，技术手段不断创新升级。虽受疫情影响网络安全产业发展短期内停滞不前，但长期来看网络市场需求依然增大。同时，中国-东盟等国际合作活动以线上方式持续开展，为中国-东盟网络安全合作搭建沟通

交流平台。

(一) 我国逐步形成自顶而下的网络安全监管体系

1. 我国形成法律-制度-标准相结合顶层设计体系

我国不断强化网络安全顶层设计，从国家全局出发做出长远部署和谋划，形成法律-制度-标准相结合顶层设计体系，巩固网络安全监管。一是网络安全相关立法密集出台。自《网络安全法》出台后，极大地规范了网络空间安全管理，促进我国网络安全发展。近期我国密集出台各安全领域相关立法。2020年1月1日起正式实施的《中华人民共和国密码法》，为保障我国网络与信息安全的核心密码技术管理提供法律支撑，也为最近快速发展的区块链技术提供密码管理保障。2020年7月，《中华人民共和国数据安全法（草案）》、2020年10月，《中华人民共和国个人信息保护法（草案）》在全国人大网发布，向社会公开征求意见。2020年11月，国家发布《“十四五”规划和二〇三五年远景目标》强调统筹发展和安全，全面加强网络安全保障体系和能力建设，保障数据安全加强个人信息保护，并建立更安全可靠的产业链供应链，国家网络安全重要性进一步凸显。同时，《电信法》等相关法制列入十三届人大常委会立法计划，相关研制论证工作逐步开展。相关立法有序推进为中国-东盟数据跨境交流、新兴技术合作发展安全保障提供管理依据。二是网络安全相关制度持续完善。今年4月，十二部委联发《网络安全审查办法》正式出台，明确了网络安全审查的对象、重点。《关于促进网络安全产业发展的指导意见》发布，进一步促进网络安全产业升级，为中国-东盟网络安全产业合

作奠定基础。同时,《网络安全漏洞管理规定》、《网络安全等级保护条例》等制度相继完成,面向社会征求公开意见,近期进入修改完善阶段。三是网络安全相关标准不断发布。2020年3月国家市场监督管理总局、国家标准化管理委员会发布国家标准 GB/T35273-2020《信息安全技术个人信息安全规范》完成修订,给予发布。5月,《信息安全技术 防火墙安全技术要求和测试评价方法》等26项国家标准正式发布。相关标准不断更新完善,为行业网络安全监管提供指导,同时也为国际标准制定合作提供基础。

2. 重点领域配套监管政策安全要求明确

一是在网络安全防护方面,细化对关键信息基础设施安全防护监管。关键信息基础设施是各国重要战略资源,尤其是新型关键信息基础设施的发展与国家国计民生结合更为紧密。在新基建安全防护上,我国出台《关键信息基础设施安全保护条例(征求意见稿)》等相关指导文件,明确了关键信息基础设施监管部门职责和安全管理人员的责任和义务,细化了关键信息基础设施保护的监测预警、应急处置等流程,进一步加大对关键信息基础设施防护力度,为关键信息基础设施提供多方位保障。二是在数据安全方面,加强数据安全和用户个人信息保护。去年5月,网信办出台《数据安全管理办法(征求意见稿)》、《个人信息出境安全评估办法(征求意见稿)》,明确了个人信息、重要数据、数据跨境处理使用的合规要求。今年7月《中华人民共和国数据安全法(草案)》、10月《中华人民共和国个人信息保护法(草案)》公布,标志着我国从立法层面确立了数据安全治

理与监管体系，逐步规范强化对数据安全和用户个人信息安全的管理。三是在供应链安全方面，加大对供应链产品和服务的审查检测。从去年至今，美国多次对我国高新技术企业实施管制，我国越发重视供应链安全管理。2020年4月正式出台《网络安全审查办法》，标志着我国在供应链安全监管方面的进一步强化。办法从以确保关键信息基础设施供应链安全为主要目标，对供应链中面临的非法控制、断供、合规操作等网络安全风险进行重点审查，规范审查流程，提高供应链的完整性及安全性。

（二）我国网络安全技术手段发展机遇与挑战并存

1. 新基建网络安全防护成为发展热点

当前，以5G、物联网、大数据、人工智能等新技术为代表的新型基础设施在疫情防控、复工复产等方面发挥了重要作用。“新基建”拓展多元化应用场景，推动物联网高速发展，智慧城市、智慧社区、智慧家庭等通过5G实现万物互联与现实生活深度融合。而物联网依托智能感知、泛在接入等技术，实现人与人、人与物、物与物之间无障碍的信息获取、传递、存储、认知、决策与使用，带来了网络形态的持续快速变动，加大了网络安全边界变化延伸的不可预测性，安全保障需求更趋于多样化、差异化。以“新基建”中物联网等新型基础设施为例，在建设之初不仅要加强物联网的安全防护能力，而且要建立全局的态势感知体系，做到监测与实时响应，网络安全防护需求急增。据数据显示到2022年，我国物联网安全市场规模达到358亿元人民币（图1）。由此看来，5G、物联网、人工智能等技术为代表“新

“基建”的安全防护正成为发展热点，市场规模不断扩大，实现安全技术创新升级。



数据来源：赛迪顾问

图 1 我国 2017-2022 年物联网网络安全市场规模及预测

2. 核心关键技术的发展存在受制于人情况

近两年，我国在科技发展方面有了质的提升，但仍与发达国家技术实力上存在一定差距。一方面，我国的网络安全根基不牢，缺乏核心的芯片和系统内核源码，关键设备依靠国外进口，计算机网络核心技术的发展依旧受发达国家所牵制。据数据显示，2019 年全球芯片厂商销售额及市场份额排行 top10 我国无一家企业入榜（如表 1），国民经济重要部门如银行、制造业等 70% 以上信息设备依靠外国技术支持，网络安全隐患严重。另一方面，我国对互联网核心技术重视程度和研究力度不足，网络安全监测预警以及自主性的安全防护尚未得到有效实现，信息通信产业核心技术的发展势头还有待进一步提升。

表 1 2019 年全球芯片厂商销售额及市场份额排行

2019 年排名	供应商	国别	2019 年收入	2019 年市场份额 (%)
1	英特尔	美国	65,793	15.7
2	三星电子	韩国	52,214	12.5

3	SK 海力士	韩国	22,478	5.4
4	美光科技	美国	20,056	4.8
5	博通	美国	15,293	3.7
6	高通公司	美国	13,539	3.2
7	德州仪器	美国	13,203	3.2
8	意法半导体	瑞士	9,017	2.2
9	东芝储存	日本	8,797	2.1
10	恩智浦	荷兰	8,745	2.1
—	其他		189,169	45.2
—	总市场		418,302	100

数据来源: Gartner

(三) 疫情和中美贸易摩擦影响网络安全产业发展

1. 受疫情和中美关系影响，网络安全产业发展短期放缓

在疫情发展和中美摩擦升级情况下，短期来看，我国网络安全产业发展增速放缓。一方面，新冠疫情发展到现在，从政府到企业的最高优先级都是处理疫情相关事务，对于网络安全项目的启动、交流、招投标等活动大部分被延迟。对 2020 年全年网络安全项目的签约、开展和回款造成影响。网络安全企业在业务量萎缩的情况下，支出并未减少甚至还有增多的趋势，网络安全企业面临一定的资金链压力。另一方面，中美摩擦再次升级，2020 年 6 月 7 日，美国发布了最新实体清单，将 33 家中国机构和个人纳入实体清单，这些被列入清单的企业在涉及美国产品技术出口转让时会受到《出口管制条例》管制，其中包括中国最大的网络安全公司 360。通过对 360 调研显示，实体清单对于 360 供应链安全、海外业务开展、海外人才招聘方面都有冲击，产业发展短期内受到影响。

2. 政府加大扶持力度，促进安全产业经济建设

一是从中央到地方政府层层推进网络安全产业落实。腾讯生态安全中心发布《中国产业互联网安全发展研究报告》，截至2018年，国家22部委出台法律法规近200部，促进产业互联网安全发展。与此同时，地方政府也在加大网络安全产业扶持力度，长沙市政府发布《长沙市加快网络安全产业发展三年（2019-2021）行动计划》，打造具有特色的网络安全产业体系。成都市政府出台《加快推进网络信息安全产业体系建设发展意见》，推动做强做大网络安全产业。二是加大在网络安全产业方面的资金扶持力度。如：天津投资45亿元建设天津滨海信息安全产业园。湖北武汉建设国际网络安全人才与创新基地，在线项目总投资达2000亿元。四川成都网络信息安全产业园获得增资，目前总投资达500亿元，增资有助于进一步推动大数据安全、云安全等新兴安全产业发展。

3. 长期来看网络安全市场需求增大，人才队伍建设速度需进一步提升

虽然受疫情影响，我国网络安全产业发展进程暂时放缓，但从长期来看，网络安全行业处于我国发展的朝阳产业，体量小、发展稳定，近几年每年以20%的速度复合增长，我国网络安全市场需求依旧庞大，网络安全人才缺口逐年递增。目前，我国通过开展网络安全竞赛活动、攻防演练方式选拔人才。如：2020年，由工业和信息化部、人力资源社会保障部等主办的“2020年全国工业互联网安全技术技能大赛”，吸引了5279支队伍、万余名专业人才参赛，遴选出56支获奖队伍，刺激

了网络安全人才实战水平的提升。但总体网络安全人才的种类仍需多样化，专业队伍建设速度需不断加快，以保障市场供应需求。

(四) 国际合作持续开展为企业海外市场带来新机遇

1. 疫情不断蔓延背景下，网络安全交流合作以线上方式持续开展

在全球疫情不断蔓延情况下，各国外交活动受到不同程度影响，在此情况下，纷纷通过线上方式持续开展。今年为中国东盟数字经济合作年，6月12日中国东盟数字经济合作年开幕式通过网络视频形式举行，东盟国家信息通信主管部门部长围绕数字经济应对疫情、数据经济发展与创新进行发言交流，并在本合作年期间，双方将在线上举行网络安全、数字经济安全研讨会、培训会等一系列合作活动，助力中国东盟疫情下的网络安全防护能力提升，增强我国与东盟国家数字经济发展和网络安全领域优势互补合作。

2. 疫情波及海外业务发展，但为网络服务型市场开拓带来新机遇

疫情横行波及大部分企业的海外业务拓展，业务进度停滞不前对公司整体业绩造成一定影响。但对于网络安全服务型企业，疫情期间为避免传染交叉感染，众多行业加快互联网化、远程办公、在线学习等平台的投入，网络安全风险上升，网络安全服务需求增大。网络安全服务向远程化发展的同时，也为网络服务型市场开拓带来新机遇。如：腾讯安全战略中心业务结构偏向服务型，受疫情影响全球视频会议使用频率大幅增加，腾讯会议 app 因其安全性和合规性突出，

被联合国入选的官方推荐，服务器增加约 100 台。网络安全服务业务需求量加大，对互联网企业数字化发展带来机遇，催生了线上一波产业链发展。

三、东盟网络安全发展现状

当前，随着技术发展及政策重视，东盟互联网市场体量不断增长。但受经济发展水平影响，东盟各成员国网络安全产业发展情况存在较大差异，疫情全球蔓延则加剧其发展水平的差距。东盟各成员国积极应对疫情对网络安全的冲击，为未来东盟网络安全产业发展带来了更多机遇。

（一）东盟发达国家凭技术管理优势，推动疫情期间产业发展

1. 政策体系完善使安全防护能力不断提升，有效控制疫情期间网络安全风险

一是不断优化解决方案为提升安全防护能力创造条件。近年来东盟地区发达国家²多措并举优化网络安全问题解决方案，促进其安全防护能力全方位提升。提出了强化网络安全的四个主要抓手，分别是建立具有韧性的基础设施、组织安全的网络空间、促进有活力的网络安全生态系统、进一步加强国际合作伙伴关系。同时，新加坡在所修订的《网络安全法案 2018》中提出对关键基础设施的监管框架，在确保网络安全的同时平衡行业发展需求。而新加坡在 2020 年 5 月所发布的《个人数据保护法（修订）》草案中也完善框架并加大监管处罚

²根据联合国开发计划署的人类发展指数等指标综合评价，东盟地区内公认的发达国家仅有新加坡这一国家，因此本部分主要选取新加坡作为研究对象。

力度，同时引入数据可携带性条款，以提升类似事件应对能力。**二是多方面应用网络安全治理手段助力疫情防治工作。**东盟地区发达国家一贯注重提升网络安全态势感知能力，并将网络安全治理方法广泛应用于其他行业。如《2019新加坡运营技术网络安全总体规划》中提及，新加坡公共事业局通过网络安全行业提供的专业知识及基础设施，进行网络安全态势分析，以提升供水部门的网络安全恢复能力。而新加坡于2019年通过的《防止网络假信息和网络操纵法案》中也从多角度出发提高打击网络虚假信息的能力，遏制了疫情期间相关谣言传播。新冠疫情全球流行背景下，东盟地区发达国家网络安全治理收效良好，助力了疫情防治工作。

2. 政府大力推进网络安全技术创新，5G网络安全受疫情反向刺激发展提速

一是技术创新拥有相应基础且受重视程度较高。相较于其他东盟国家，东盟地区发达国家网络安全基础设施建设较为完善，且在技术方面也有一定优势。仅以安全互联网服务器数量³为例，2019年新加坡每百万人安全互联网服务器数量远超东盟其他成员国（图2）。在网络安全领域相对较强的技术实力及完善的基础设施，为新加坡的网络安全技术创新提供了条件。同时政府也十分重视技术创新升级，在《新加坡网络景观2019》中提出大力倡导网络安全创新，开发创新网络安全生态系统以推动行业创新及前沿研究。**二是受需求扩大影响5G网络安全市场竞争增大。**5G技术加强网络与物理空间互连，安全风险

³ 安全互联网服务器，即互联网交易过程中使用加密技术的服务器，这一指标可以从一定程度上衡量一个国家网络安全基础设施的发展水平。

随之增大。因此东盟地区发达国家在大力推动 5G 发展的同时极为重视 5G 网络安全。新加坡在 2019 年 6 月表示已拨出 4000 万新元来支持 5G 创新研究，其中安全性是研究关键。受疫情影响，居家办公与线上学习等新常态提升了民众对互联网依赖性，需求扩大刺激了 5G 技术及网络安全加速发展，5G 网络安全市场竞争也随之增长。如新加坡在颁发 5G 网络牌照时吸引多家国内外企业竞标，由于其十分注重对运营商安全性的监管，安全方面的考察使市场竞争更加激烈。



数据来源：世界银行

图 2 2019 年东盟各成员国每百万人安全互联网服务器数量

3. 为开展新兴领域网络安全国际合作奠定基础，应对新技术挑战并促进网络安全同步发展

一是新兴领域网络安全国际合作愈加深入。新加坡在广泛开展网络安全国际合作的基础上，增强了在人工智能、5G、物联网等新兴领域的安全技术交流与信息共享，以增强对新技术网络威胁的应对能力。如 2019 年新加坡与英国签署《安全设计：英国和新加坡就物联网进行合作的联合声明》，旨在加强两国在物联网设备安全方面的合作，多方面推进物联网产业安全技术发展创新。二是人才培养全面发展为新兴领域安全储备力量。近年来，一方面，新加坡在网络安全教

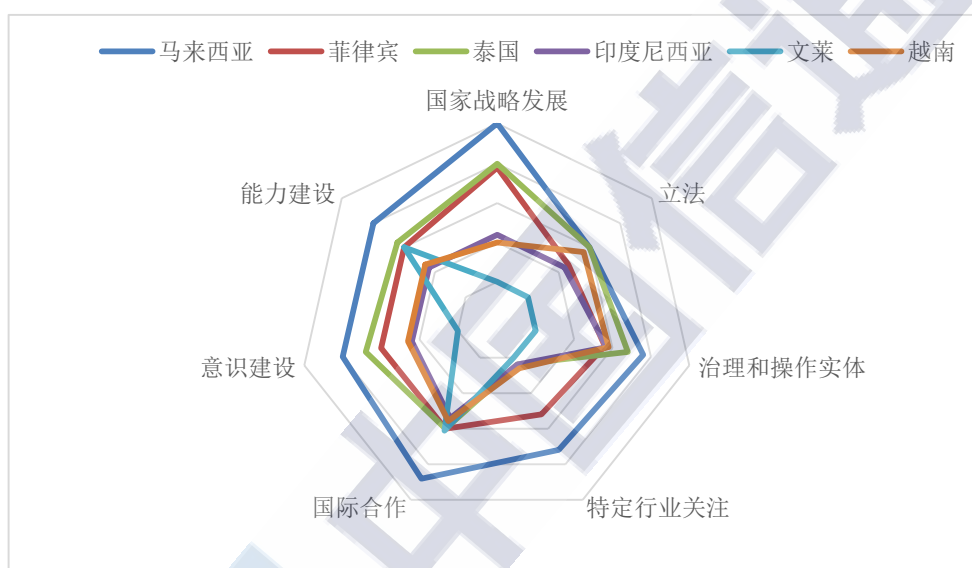
育及人才培养上实现了全覆盖，具有专门针对中学生、大学生、行业人士、女性的不同网络安全培养计划，并设置了相关奖学金。另一方面，新加坡通过交流合作，积极应用网络课堂、线上培训等新方式培养新技术安全人才。例如，2020年华为于新加坡开设了一所“虚拟”人工智能学院，提供关于人工智能、5G、云计算等新技术相关课程，其中也计划提供网络安防培训课程，以帮助中小型企业更好地抵御网络安全威胁，助力新加坡新兴领域安全人才培养。

（二）东盟发展中国家积极探索对外合作，吸收创新治理经验

1. 完善政策并推进标准认证，监管范围扩充内容细化

一是促进安全标准制定互认多角度完善政策体系。近年来东盟地区发展中国家虽然网络安全政策发展程度不同（图3），但皆多方面着手完善网络安全策略，并制定安全领域标准，旨在为产业发展提供良好条件。一方面，东盟地区发展中国家积极开展网络安全标准制定认证。2019年印尼成为CCRA认证成员国，可运用国际通用标准去对设备进行检测，并且国家成员单位进行进一步认证。同时，印尼也在提高对于IT产品的独立安全分析。马来西亚也在积极推进网络安全培训方面的国际互认。另一方面，在政策上，印尼于2020年1月初向其立法机关提交了《个人数据保护法案（草案）》，加强了个人数据保护的立法，在保护数据并维护数据主权的同时，确保创新及商业投资机会的开放。同时，越南也开始实施《网络安全法》，以创造安全健康的网络空间。二是网络安全监管范围扩大且惩处力度强化。

泰国在 2019 年通过的《网络安全法》中制定了严格且较为详细的监管条例，且将部分个人信息言论纳入监管范围；在内容治理方面成立了打击假新闻中心，以加大网络虚假信息打击力度。马来西亚、印尼等国也极其重视安全监管，通过立法与技术创新等举措进行网络威胁监测预警，打击非法网络活动、严格监管网络虚假信息，以引导网络安全产业良性发展。



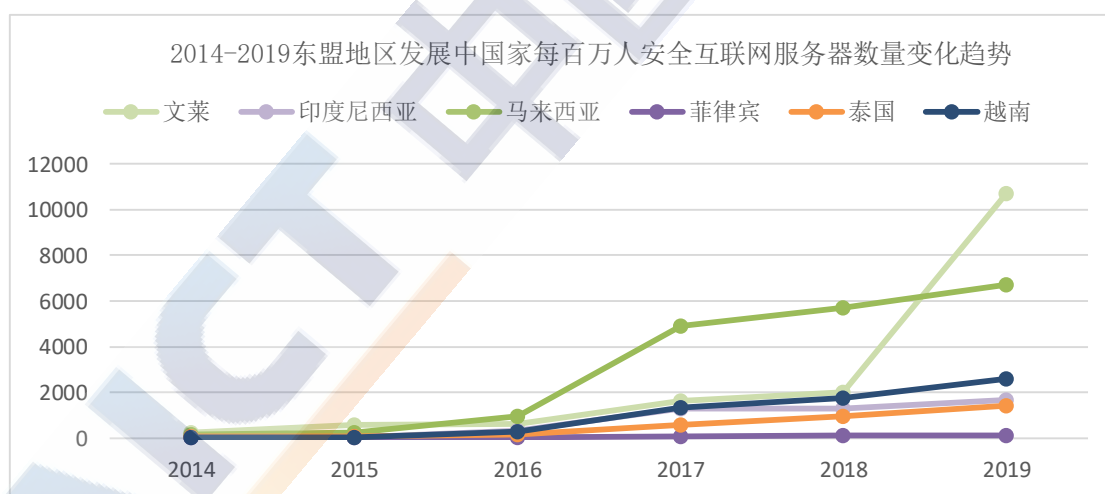
数据来源：Cyber Security in ASEAN: An Urgent Call to Action (2017)

图 3 东盟地区发展中国家网络安全政策发展程度情况图

2. 网络安全技术发展迅速，疫情期间人工智能等新技术安全关注度不断提高

一是战略重视推动网络安全技术水平快速提升。在网络安全环境持续变化的背景下，东盟地区发展中国家在网络安全战略中，纷纷明确对技术创新的重视，设置网络安全基础设施建设相关目标。如印尼在《国家网络安全战略》中列出提高网络创新能力，并要建设安全可靠的国家网络基础设施。马来西亚也将“促进高质量创新技术研发和工业”，作为其网络安全战略五大支柱中的一项。在战略重视的推动

下，东盟地区发展中国家网络安全技术快速发展，且安全基础设施发展程度不断提升，仅以安全互联网服务器数量⁴为例，近年来呈持续上涨趋势（图4）。二是新兴技术网络安全问题逐渐成为关注焦点。新技术不断迭代使网络安全风险更加复杂化，给网络安全防护能力带来更大挑战，因此近年来东盟地区发展中国家愈发重视新技术网络安全的发展。例如马来西亚在《国防白皮书》中提及要提升网络威胁应对能力，并关注了人工智能、物联网、云计算等技术进步带来的威胁因素。但与此同时，人工智能等新技术在网络安全领域具有很大的发展前景，可用于开辟网络安全新路径。在疫情期间，人工智能等技术在日常生活中更是发挥了重要作用，通过远程服务降低了疫情对人们工作生活的冲击，因而关注度进一步提升。



数据来源：世界银行

图4 2014-2019 东盟发展中国家网络安全基础设施发展趋势
(以每百万人安全互联网服务器数量为例)

3. 国家产业推动力有待加强，需优化培养机制以增大网络安全专业人才储备

⁴ 安全互联网服务器，即互联网交易过程中使用加密技术的服务器，这一指标可以从一定程度上衡量一个国家网络安全基础设施的发展水平。

一是基础设施及技术创新能力仍存在提升空间。虽然东盟地区发展中国家在战略上重视网络安全产业，但是由于网络安全基础设施建设不够完善，同时在技术创新方面也较为薄弱，往往更多依赖于国际合作技术交流来进行提升，例如越南的很多网络安全技术就是由国外提供。因此东盟地区发展中国家安全产业原生动力仍有待进一步增强，从而促进产业发展提速。**二是需进一步完善人才培养机制以增加专业人才储备。**目前在网络安全产业快速发展的趋势下，东盟地区发展中国家在专业人才储备上存在一定缺口。例如菲律宾网络专业人士较少，只有 150 人拥有 CISSP 认证，同时其中一半在海外工作。2020 年菲律宾人才数字进一步增加，但还不足以满足不断增长的网络安全人才需求。而越南在缺乏高质量人才的同时也缺少网络安全培训项目。在战略方面，虽然马来西亚已经在相关战略及计划中涉及人才培养相关内容，以推动新人才队伍的构建。菲律宾也在《国家网络安全规划 2022》设定了提升社会网络安全教育程度的目标，并开展多项相关培训活动。但就东盟地区发展中国家整体而言，其专业人才培养及储备机制仍具有较大提高空间。

(三) 东盟欠发达国家⁵提升空间较大，完善自身实力为主要目标

1. 网络安全防护意识逐步提高，但立法体系远未完善

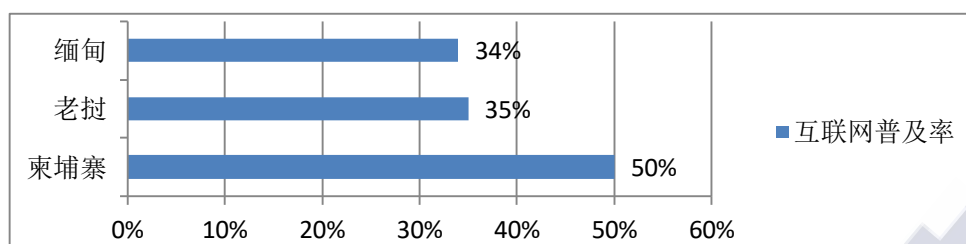
一是国家发展战略中网络安全内容占比提升。东盟地区欠发达国家对于网络安全防护逐渐重视，将网络安全列入相关发展战略中，并

⁵ 根据联合国贸易和发展会议所列名单，目前联合国将 47 个国家指定为“最不发达国家”，东盟国家中柬埔寨、老挝、缅甸在此列。

开始网络安全相关立法工作。例如柬埔寨在《柬埔寨 ICT 总体规划 2020》中明确要通过建设网络安全来确保互联性。老挝也制定了网络政策和规划，在其 2020 年 9 月份通过的数字经济宏观规划中涉及网络安全框架和数字经济基础设施，包括网络安全立法研究等十项起草网络安全政策的具体措施。**二是仍缺少完善的网络安全政策法律体系。**由于经济发展水平发展缓慢以及网络基础设施较为贫乏，发展较为缓慢国家相比之下对网络安全整体需求较少。因此其网络安全相关政策及立法也较为空白，还没有构建完善的网络安全政策法律体系，在立法上仍有较大发展空间。

2. 技术发展较国际水平差距大，缺乏安全产业布局谋划

一是技术实力发展滞后为产业发展造成阻碍。受限于经济发展等因素，东盟地区欠发达国家网络基础设施发展水平相对缓慢，以互联网普及率为例普遍较低（图 5），因此其网络安全产业发展硬件基础薄弱，同时其网络安全防护能力较弱，为网络安全产业发展带来了不利影响。面对技术发展速度缓慢情况，东盟欠发达国家积极谋求技术发展及提升，对国际合作以及技术交流需求较大。**二是安全产业缺少整体统筹布局与发展计划。**虽然东盟地区欠发达国家逐渐认识到网络安全的重要性，并努力提升自身网络安全技术水平，以图追赶世界网络安全产业新发展。但其网络安全发展还处在初阶阶段，受制于基础设施建设水平等条件限制，



数据来源: ASEAN CYBERTHREAT ASSESSMENT 2020, INTERPOL

图 5 东盟地区欠发达国家互联网普及率

3. 疫情冲击整体经济形势，国际合作助推安全产业发展

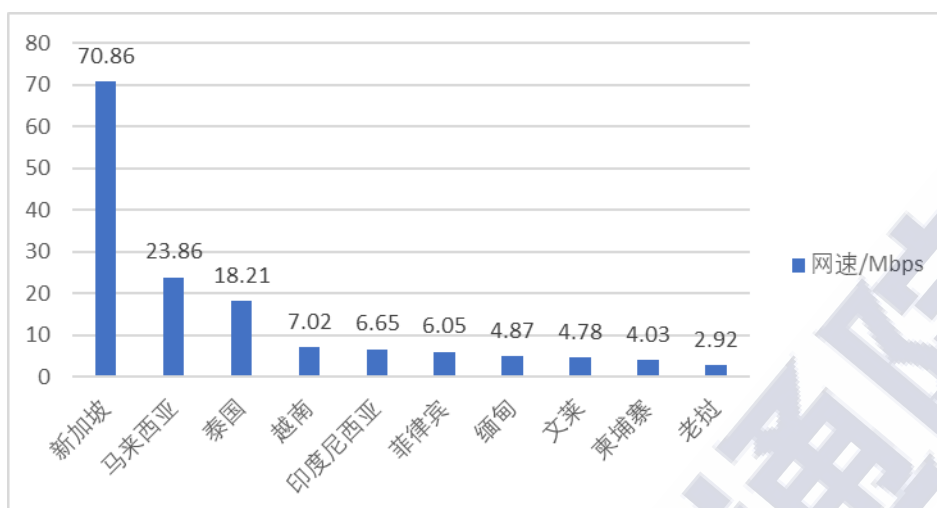
一是疫情冲击整体经济为网络安全带来一定不利因素。一方面新冠疫情蔓延给东盟地区欠发达国家各大产业带来了经济上的冲击，如柬埔寨包括旅游业在内的服务业受疫情影响严重萎缩，整体经济形势不佳侧面影响了对网络安全产业的投入。**另一方面**疫情扩散使得各国实行更加严格的边境管控政策，对技术交流合作造成不利影响，东盟地区欠发达国家在疫情期间得到技术援助及指导的机会变少。**二是通过国际合作谋求网络安全产业发展及技术提升。**一直以来，东盟地区欠发达国家积极寻求安全领域的国际合作，疫情带来的负面影响更促使其加强与域外大国合作以获得技术帮助与信息共享，帮助加强自身网络安全能力建设。例如柬埔寨和其他的亚洲国家，如中国、日本都在进行网络安全合作，其中 2019 年东盟和日本联合进行了网络安全演习，此外还和新加坡进行了网络应急演练。2020 年 6 月，中国-东盟数字经济合作年通过网络视频形式举行开幕式，中国与东盟地区欠发达国家展开多方面合作，包括共同推进网络安全务实合作，加强网络安全能力建设等。

四、中国-东盟网络安全合作面临的挑战和机遇

(一) 突发疫情加大中国与东盟网络安全合作限制

1. 基础设施资源存在差异，影响疫情期网络安全需求

一是东盟各国存在信息基础设施“硬实力”差异，疫情期需求侧重点不同影响我国对外产品出口。新冠肺炎疫情爆发以来，全球各地不乏面临伪装成疫情信息传播的网络病毒、钓鱼邮件、恶意链接，以及医疗机构、疫情防控物资生产企业所属网络系统存在受控、安全漏洞等的一系列网络安全风险。新加坡也发布了《网络安全更新：COVID-19》^{*}，意识到不断增加的网络安全风险，并采取相应的远程工作防护措施，加强数据保护和安全管理。然而，根据调研结果显示，我国安全企业在对外输出网关设备、防火墙等安全产品、漏洞检测软件时，普遍认为东南亚部分发展缓慢国家的市场拓展难度较大，主要原因因为缅甸、老挝等地区基础设施目前尚未搭建完善，政府基础设施不完备，无法满足疫情期间增长的远程办公需求，对于基础设施建设的的需求仍远大于网络安全风险防护。二是东盟较为不发达国家互联网连接能力不足，网络安全发展滞后。据最新 SEASIA 发布的 2019 年全球宽带网速排名来看，新加坡位居全球第二，平均下载速率到达了 70.86Mbps，而柬埔寨、老挝的平均下载速率仅达到 4.03Mbps 和 2.92Mbps。缅甸等发展水平较低的国家在疫情爆发后，使用网络的人数激增，因宽带速率较低，则放大了设备难接入、掉线、网络崩溃等基础网络常见问题，因此更关注于解决基础网络问题，从而相对减少了安全防护层面的考虑和要求。



数据来源: Rank of Countries Internet in The World 2019, SEASIA

图 6 东盟国家宽带网速

2. 突发状况下各国安全风险应对措施不完善，影响线上线下交流效率

一是缺少保障远程工作的安全风险评估和安全办公指导。疫情爆发以来，多数员工常在未开启防火墙和没有其他安全防护措施的情况下进行远程工作，从而加剧了隐私泄露、数据泄露的网络安全风险。如：印尼疫情期间网络流量增加了 23%，网络犯罪数量在不断增加并达到新高。⁶部分黑客利用新型冠状病毒肺炎疫情相关热词对我国开展网络攻击行为，导致用户文件被窃取等。由此可见，中国与东盟多数企业并未制定远程办公和公司系统访问方面的基本规则，对远程办公中 VPN 的使用、定期检查帐户特权及本地系统帐户、以及有关身份验证、电子签名等的指导和规定仍有待加强。二是合作渠道单一导致市场拓展能力受限。我国企业大多依靠政府交流带动拓展海外东盟网络安全市场，达成国际合作。虽然目前国内企业依靠政府带动已取

⁶ 信息来源于中国 2020 中国—东盟数字经济合作年网络安全培训交流会印尼专家演讲材料

得了良好效果，但是合作渠道仍较为单一，国内安全企业的国际知名度较低，缺乏独立出海的信任度和竞争优势，受疫情影响中国与东盟政府间交流减少，导致海外市场拓展力度随之大幅降低。因此，还需考虑如何更大限度的发挥政府资源优势，通过线上会议交流等机会，实现疫情期间中国与东盟各安全企业间业务与合作需求的有效对接。

(二) 复杂环境下难以形成网络安全合作合力

1. 东盟缺乏统一安全框架，网络安全政策约束力较薄弱

一是东盟整体层面未形成便于管理的统一网络安全框架。由于东盟各国对网络安全认知、立法政策、个人数据安全等要求与我国不同，甚至各成员国之间都存在差异，缺乏整体层面上对安全审查、供应链安全等方面的机制建设，导致我国与东盟安全企业进行合作时，无法对各国、各领域的具体政策要求进行详细了解。此外，东盟各国近两年不断发布数据保护相关政策，如：新加坡于2020年5月发布《个人数据保护法案（修订）》草案，马来西亚、泰国考虑推出强制性数据泄露通知法案。由于未形成统一框架，为符合当地政策要求，合规成本也将进一步增加，加大了我国企业打入东盟市场并在当地有序发展的难度。**二是各地政策不同影响安全产业的市场活跃度。**东盟各成员国的用户信息安全和网络安全政策受当地政府态度和既有国家制度的影响，如：泰国、菲律宾、新加坡对信息建设管理的工作是市场化的，主要以解决多边和两边信息化问题为主，政府间互动频繁以解决需求，更易对外交流合作。而老挝、越南国家整体相较封闭，发展方向主要参照国家的整体思路，因此市场灵活性较低。此外，东盟并

未采取措施促进全境内的自由流动或建立内部的统一市场，发展较为发达的国家未能带动发展欠发达国家的市场活跃度。

2. 政策成为制约因素，各领域合作覆盖面有待拓展

一是各国数据跨境流动政策严格一定程度上限制国际贸易。随着全球跨境电子贸易、国际贸易的增加，中国与东盟为保障国家安全，更关注于数据跨境流动方面的安全问题。东盟成员国中，多数发展中国家由于在双、多边贸易中处于弱势地位，数据跨境流动对其而言意味将要承担更多的安全风险，因此对数据跨境流动的监管日趋严苛，如：马来西亚选择限制数据自由流动政策，要求企业在境内设置数据服务器；越南的数据则受政府保护禁止出境。相关安全政策的不断收紧将对国际贸易合作造成一定的影响。二是我国与东盟在安全认证等领域方面缺乏合作。虽然近年来，我国已在安全政策、技术研究、电子贸易、应急响应等多方面进行了长期的合作和交流，但在设备安全认证方面合作相对较少。2019年印尼成为共同准则互认协定（CCRA）认证的成员国⁷，与美国、加拿大、日本、韩国等多个国家加强了双方有关IT产品认证和国际化的交流。马来西亚为得到全球的认证，近年来也在加强安全认证方面的培训。然而，我国目前未加入网络安全产品认证检测国际认证，交流培训的议题涉及较少，与东盟的安全合作有待加强。

（三）疫情下全球产业链格局变化为合作带来机遇

⁷ 信息来源于中国2020中国—东盟数字经济合作年网络安全培训交流会印尼专家演讲材料

1. 联合发表声明支持数字经济合作伙伴关系倡议与东盟发展规划对接，大形势下网络安全合作前景广阔

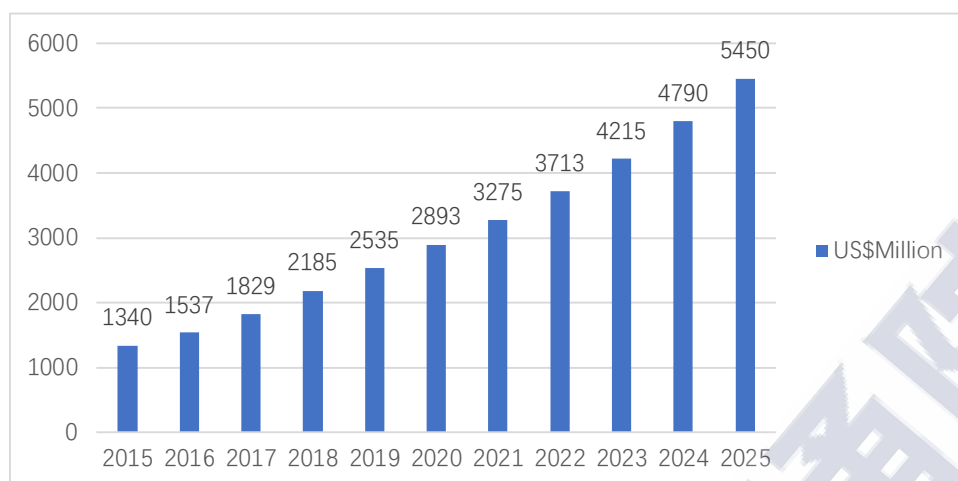
一是发布中国与东盟数字经济伙伴关系倡议。疫情期间中国与东盟互动频繁，2020年11月12日，23次中国—东盟（10+1）领导人会议以视频方式成功举行，会议发表了《中国—东盟关于建立数字经济合作伙伴关系的倡议》，双方同意抓住数字机遇，打造互信互利、包容、创新、共赢的数字经济合作伙伴关系，网络安全是未来六大重点合作领域之一。主要内容为深化数字技术在疫情防控中的应用，共同加强数字基础设施网络安全保障，共建跨境网络安全事件响应信息共享体系，增进双方网络安全法律、政策理解，提升双方地区能力建设合作。5月29日发表了《中国—东盟经贸部长关于抗击新冠肺炎疫情加强自贸合作的联合声明》，共同抗击疫情，加强两方自贸合作。同日，还在印尼的雅达加举办了视频会议“中国—东盟关系雅加达论坛”，聚焦当前形势下如何加强中国和东盟的关系与合作、维护产业链和供应链的稳定，并提出促进地区经济社会恢复和发展的积极举措^{*}。加强“一带一路”倡议与东盟发展规划对接，有利于推动中国与东盟在网络安全领域建立密切的合作关系。

二是先期合作积累建立互信，东盟与我国的伙伴关系不断深化。自贸易摩擦以来，各国网络安全相关政策不断收紧，疫情爆发后，各个网络安全国际对话机制也置若罔闻，使得中国与美、欧等关系愈发紧张。在此情形下，东盟与我国在网络基础设施互联互通和电子商务贸易融合等已有一定的合作基础，我国与东盟政府间的互信程度较高，网络安全企业普遍反应中国与东

盟睦邻互信的伙伴关系未受到全球安全大形势的影响，且维持了良好的伙伴关系，共同推进网络安全产业的发展交流。

2. 疫情期间确保网络设备的安全稳定成为重点，我国积极帮助东盟提高关键信息基础设施安全

一是东盟各国对网络设备、产品和服务的需求增加。疫情爆发后，东盟各国对更高端的设备、满足远程工作和交流的安全软件需求增加。6月，马来西亚电信公司（Telekom Malaysia Bhd）和华为技术有限公司（Huawei Malaysia）互相签署了协议备忘录，将云计算、人工智能和最先进的网络安全实践与技术相结合以实现云计算运营，为用户带来下一代创新体验。此外，为开展一系列的中国与东盟的线上交流活动，我国网络安全企业也不断为老挝等发展水平相对缓慢国家提出解决方案并提供接入设备。二是东盟市场潜力较大网络安全投资呈提高趋势。根据世界经济论坛（WEF）的最新报告，面对当前新冠疫情危机，各国最大的担忧之一即网络攻击和数据诈骗的增加，该报告也引起了东盟各国专家的重视，并表示东盟各成员国正通过与遴选的合作伙伴建立战略关系以完善安全路线图和体系结构、优化基础架构来加速其安全转型。目前，东盟仍未在网络安全方面投入足够的资金，东盟专家建议：东盟成员国还需要投资其国内生产总值的 0.35% 至 0.61%，即 1,710 亿美元用于维护网络安全*。投资增加的趋势有利于我国与东盟拓宽合作与技术创新发展。



数据来源: The ASEAN Post

图 7 东盟网络安全投入走势

3. 疫情促使中国与东盟打造全新产业链条，共同维护供应链的安全稳定

一是目前形势为中国与东盟双向投资创造有利条件。疫情原因，当前全球产业链供应链格局发生变化，欧美等部分国家因经济受创、安全市场需求减少，且供应链网络安全隐患日趋严重，出现了 ICT 制造业回流现象。在此情况下，中国与东盟合作加强安全产业链供应链整合对疫情应对尤为重要，借欧美企业退出东盟市场的时机，提高我国与东盟在 ICT 供应链安全方面的国际合作，同时把握联合扩大网络安全企业、加强生产能力，是打造全新产业链条的良好时机。二是中国与东盟因地制宜合作发展空间较大。总体来看，我国在对东盟的投资中，制造业占比最高，研发类占比较小。因此，中国可以因地制宜对东盟国家展开网络安全领域投资，如：以技术导向型投资为主，加大对新加坡安全技术应用、产业融合投资；马来西亚、泰国、印尼则以市场导向型为主，从外卖、打车软件的安全性入手打入东盟网络安全市场；对越南、老挝、柬埔寨等较发展相对缓慢国家开展工业发展

型投资，完善其信息基础设施建设，加强供应链产业链完整性，有效促进双方贸易与网络安全的国际合作。

五、启示与建议

中国-东盟网络安全合作依然面临着由于基础设施资源存在差异导致网络安全需求不同、缺乏统一合作框架等挑战，对此，我国应整合国内网络安全力量，深入落实“一带一路”倡议，弥合数字鸿沟，建立统一合作机制优化中国-东盟网络安全合作生态，打造中国-东盟网络空间命运共同体。

（一）持续深化安全技术及管理合作，打造“网络空间命运共同体”

1. 提高我国网络安全技术水平，助力东盟地区疫情期间网络安全发展

网络安全技术水平是体现国家网络安全实力和国际竞争力的重要因素。中国与东盟部分国家网络安全水平差异较大，尤其在疫情期间需求对接差异明显，合作受到一定影响。在此情况下，一方面，我国应持续优化网络安全技术防护体系，加大网络安全服务技术重视程度，疫情期间网络安全服务向远程化、云化、自动化、平台化的方向发展，提前定位实现安全服务线下能力线上化，数据化、可视化，并基于大数据分析、机器学习进行运营分析，提升网络安全服务能力水平。保障疫情期间各行业网络安全。另一方面，加大向东盟国家提供网络安全技术支持力度。疫情期间，可通过中国-东盟网络安全交流培训中心线上平台等加大对东盟网络安全技术培训，深化我国企业与东盟

国家相关网络安全企业交流合作，助力东盟国家在网络安全方面的技术升级，实现国家之间在网络技术领域的平衡合理发展。

2. 构建中国-东盟数据跨境合规管理体系，开展分级分类数据出境治理

一是建立统一的中国-东盟数据跨境管理体系。加强与东盟国家在数据跨境方面的交流，构建政府间、行业间、研究机构间多类型多线条的沟通模式，增进数据跨境领域国际互信。并建立数据跨境基本管理框架，形成中国与东盟国家统一的数据流动规则，促进在贸易活动、跨国科技交流方面的数据跨境传输，打通数据跨境流动壁垒。二是建立分级分类的数据治理机制。在分类监管上，对数据类型、企业性质、出境事由等进行分类，并按照出境国家地区政治环境、国际关系、数据保护水平等因素划分数据出境风险等级，制定低风险地区数据出境白名单，减少数据流动障碍。

3. 明确中国东盟网络安全战略发展目标，打造网络空间命运共同体

一是通过中国-东盟领导人会议、部长会议等现有机制，制定中国-东盟网络安全合作战略规划，达成双方共识，设定在网络安全领域共同的努力方向。同时，以高级别会议机制推动网络安全合作深入发展，形成总体性的框架协议，明确阶段性目标，通过自上而下、渐进性合作的方式，实现中国-东盟在网络安全合作上的整体推进。二是助力周边外交建设，在设立中国-东盟共同的网络安全目标情况下，提升科技创新，深化数字经济合作。积极将我国先进的网络信息技术

推广至东盟地区发展相对缓慢国家，在智慧城市、5G、人工智能、电子商务、大数据、区块链、远程医疗等领域打造更多新的合作亮点，深化中国同东盟国家的战略伙伴关系，共同应对跨境犯罪、信息窃取等网络安全问题。推动中国同东盟国家之间友好关系的进一步发展，打造中国-东盟命运共同体。

(二) 稳步推进“一带一路”倡议，建立常态化安全合作机制

1. 建立针对各行业、领域网络安全应急机制，协调处理疫情等不可抗力因素下安全风险

应急响应是处置突发重大事件的有效手段，在公共卫生领域的重大疫情事件下，各行业、领域网络安全攻击对象更具有针对性。在此情况下，中国东盟应针对各行业特点建立完善的网络安全应急管理体系。一方面，明确应急目标，做好网络安全事件的分级分类，建立监控预警机制和可行的应急预案和高效、全面的协同配合机制以确保突发事件下中国、东盟各行业网络安全合作正常推进。另一方面，开展与东盟国家行业网络安全应急演练活动，针对不同行业面临的高发网络安全风险，模拟突发情况下网络与信息安全事件，以检验应急预案的正确性，不断提高中国与东盟国家的安全意识和各行业应急响应配合工作的熟练程度。

2. 深入推进“一带一路”倡议落实，搭建中国-东盟网络安全交流平台

近年来，东盟内部存在意见不统一，部分国家的合作意愿不强等现象，对中国-东盟网络安全合作的推进形成阻碍。对此，一方面，稳步推进“一带一路”倡议。以区域一体化思路推进基础设施互联互通，强化对“一带一路”沿线国家网络基础设施安全保障，推动网络安全保障技术联合研发，从技术、产业、政策上共同发力，促进中国-东盟网络安全合作有序开展。另一方面，搭建中国-东盟网络安全交流平台。通过平台交流，合理协调东盟各国在网络安全合作推进中的问题，保障合作国家之间信息交流的相对对称性，提高信息交流质量。同时，加强同东盟国家在网络安全人才培养、产业升级方面的互利合作，提升双边政治互信。

3. 建立常态化中国东盟网络安全合作框架，推进双方安全领域有序发展

目前，在大部分东盟国家地区存在网络安全合作机制碎片化问题，统筹完善中国-东盟网络安全合作框架可以进一步推进中国-东盟网络安全合作持续化、常态化发展。一方面，网络安全合作机制可以结合东盟各国自身存在的网络安全发展现状，集中东盟各成员国在网络安全合作领域所关心的问题，制定相对适合各国的网络安全发展的合作框架，提高抵御网络安全风险的能力，增强合作的主动性。另一方面，长期以来中国-东盟网络安全合作缺乏机制化的领导组织机构，导致网络安全合作的顶层设计难以得到充分落实，网络安全合作机制可促使各成员国联合建立相关网络安全组织机构，帮助各成员国协调网络安全合作中面临的各种问题，提升合作效率。

(三) 弥合数字鸿沟，优化生态重塑中国东盟供应链安全布局

1. 平衡中美国际关系，重构供应链安全格局促进中国东盟安全产业升级

近期，美国不断升级对 ICT 供应链安全的进出口管制，压制相关国家网络安全产业创新发展，对此，我国应积极采取相关策略，一是加强中美高层关系对话，就涉及双边和多边网络安全议题进行广泛讨论，推进各领域务实合作和交流，妥善管控分歧和敏感问题，增强战略互信，确保中美关系向不冲突不对抗、相互尊重合作共赢方面发展。二是推动供应链多元化发展，重构供应链安全格局。借助“一带一路”倡议积极与东盟国家开展经贸合作，加快地区经济全面复苏。进一步实施好中国 - 东盟自由贸易协定，相互开放市场，推动产业链、供应链、价值链深度融合。扩大与东盟国家网络安全市场，促进双方网络安全技术不断创新和产业升级，共同应对供应链安全问题。

2. 疫情下加强中国-东盟网络安全人才交流，弥合技术鸿沟推动数字经济共同繁荣

疫情期间，各行业线上系统使用频率大幅增加，网络安全保障尤为重要，网络安全人才重要性凸显。一方面，可依托中国-东盟网络安全交流培训中心等平台，通过线上方式开展中国-东盟网络安全人才交流会，探讨网络安全防护最佳实践经验，通过理论与实践相结合的方式提升网络安全防护能力。提高相关人员网络安全意识，为双方输送高质量的网络安全人才队伍。另一方面，加快搭建网络安全仿真模

拟平台，并通过中国-东盟网络安全主题竞赛活动、网络安全演练等方式，着力选拔、培养双方实践能力和创新能力较强的网络安全人才队伍，弥合技术鸿沟，带动发展较慢的东盟国家信息通信技术和网络安全技术发展，推动中国-东盟数字经济共同繁荣。

3. 推动双方关键信息基础设施互联互通安全保障，为持续合作发展夯实基础

关键信息基础设施互联互通滞后成为经济增长、竞争力提升的阻碍，只有关键信息基础设施互联互通不断得到改善，中国-东盟网络安全合作全面发展才得以实现。东盟互联互通总体规划中，提升战略互信，深入对接发展规划。依托陆海新通道建设，加强基础设施互联互通合作，加快推进现有经济走廊和重点项目建设，各参与方把公共交通、能源需求、信息通信技术等领域确定为优先发展的领域。对此，东盟需要大量的基础设施投资，提高互联互通水平。在此情况下，一方面，加大对东盟关键信息基础设施发展人员、技术支持力度。共同推动互联互通安全发展。另一方面，共同加强网络设施、网络数据在互联互通过程中的安全保障，推动重点领域的网络安全技术应用，保障中国-东盟数字经济发展和用户利益。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304961

传真：010-62300264

网址：www.caict.ac.cn

