CAICT 中国信通院

中国-东盟网络安全产业发展现状研究报告

（2019 年）

中国信息通信研究院
安全研究所

2019年12月

版权声明

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

编委会成员：谢玮、廖璇、丰诗朵、李慎之、高婧杰、王榕、缑文琦、郭骁然、李跖、曹珩

参与单位：中国信息通信研究院

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。近年来，中国—东盟关系呈现多层次、宽领域、全方位的发展势头，关系发展路径“更明”、战略互信水平“更高”、经贸合作增长“更稳”、人文友好交往“更热”、国际地区意涵“更广”。中国—东盟关系已进入全方位发展的新阶段。

当前，国际及地区局势严峻复杂，网络安全成为各国交流、博弈的重点领域。东盟各国多数处于网络与信息化建设起步期，对网络安全高度重视，需求迫切。然而，多数东盟国家网络安全基础相对薄弱，安全产业发展不成熟，仅靠自身力量难以完成网络安全建设。因此，了解东盟东盟网络安全产业发展特点，研究我国与东盟网络安全产业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。

为进一步推进实施亚洲区域合作专项资金“中国-东盟网络安全产业现状调研及合作发展策略研究”项目，了解我国及东盟网络安全产业现状，为双方开展务实合作夯实基础，我院编写了《中国-东盟网络安全产业发展现状研究报告（2019 年）》。本报告总结了中国、东盟网络安全产业发展现状，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

版权声明.....I
前 言.....II
一、中国-东盟安全产业发展态势.....1
（一）网络安全重要性不断凸显，安全产业发展备受各国关注.....1
（二）东盟位于“一带一路”关键地区，成为中国通向世界的国际大通道..2
（三）通过安全合作促进“一带一路”落实，提升网络安全产业竞争力....3
二、中国安全产业现状.....5
（一）安全产业规模持续增长，各方积极协同合作，总体趋势稳定.....5
（二）积极落实“一带一路”倡议，强化多边交流，把握国际网络安全市场拓展新机遇.....7
（三）我国安全产业结构、技术实力和应用创新与全球产业存在差距，有待进一步提升.....8
三、东盟安全产业现状.....10
（一）各成员国网络安全需求不同，网络安全产业发展不均.....10
（二）政府积极调整政策，改善安全产业发展环境.....12
（三）与域外大国密切合作，不断提升安全防护能力.....14
四、中国-东盟合作面临的问题与机遇.....16
（一）我国与东盟合作面临复杂环境，网络安全产业合作发展长期以来受到限制.....16
（二）“一带一路”倡议带来国际合作新机遇，中国和东盟安全产业合作迎来发展期.....19
五、启示与建议.....20
（一）缩小网络基础设施安全技术鸿沟，改善东盟国家合作底层环境.....20
（二）搭建中国-东盟合作机制，引领增进合作的积极性和主动性.....22
（三）优化安全产业生态环境，提高与东盟国家网络安全产业对接能力...23

一、中国-东盟安全产业发展态势

（一）网络安全重要性不断凸显，安全产业发展备受各国关注

随着科技的进步，计算机网络已渗入到社会生活，且涉及政治、经济、军事、民生等各个层面，网络安全产业作为网络安全技术、产品与服务的提供者和实施者，逐渐成为保障社会稳定和国家安全的核心，因此各国对安全产业的发展重视程度不断提高。**一是将网络安全产业纳入国家重点支持的战略产业。**近年来，各国纷纷出台国家网络安全战略，通过改革政策、经济扶持等手段支持安全产业的良好发展，将壮大网络安全产业纳入维护国家网络空间主权和利益的战略选择。**在国内方面**，我国发布《关于促进安全产业发展的指导意见》等一系列政策，明确发展方向及重点任务，为网络安全产业健康发展提供法律和政策性的保障。2019 年《国家网络安全产业发展规划》也提出了安全产业发展新目标、加快建设国家网络安全产业园区与网络安全高端产业集聚示范基地等“五大基地”，驱动行业加速发展。**在国际方面**，各国加大网络安全产业国家投入力度，美国出台《网络安全人力框架》，提供网络安全产业人才培训标准，并在“2019 财年国防授权法案”中将网络安全预算增加至 300 亿美元，从强化政企合作，提高安全技术能力等方面为安全产业提供经济支持。以色列提出三年产业发展计划，斥资 2443 万美元支持网络安全技术研发。欧盟《安全产业政策：具有创新性和竞争力的安全产业行动计划》也通过提出采取政策措施的方式推动无壁

垒欧盟安全产品大市场的构建，提升欧盟安全产业竞争力。**二是网络安全产业领域国际合作日趋增加。**美国与以色列签署《高级研究伙伴关系法案》，加强双方企业、大学、非营利性组织间的联合研究与开发工作，日本也与以色列签署合作关系，以提升日本安全产业的网络安全技术能力。此外，各国大型企业间也维持着协同发展关系，例如美国工业互联网安全技术公司 Bayshore Networks 与韩国 SAMSUNG、中国思科、英国 BAE 系统等企业建立了战略合作伙伴关系，促进了全球网络安全产业的生态建设。

（二）东盟位于“一带一路”关键地区，成为中国通向世界的国际大通道

东盟地处亚洲东南部的中南半岛和马来群岛，与中国大陆相连，是太平洋、印度洋、大西洋与亚洲大陆之间相联系的地缘控制区。**一是东盟地理位置关键，成为域外大国争相合作的重点对象。**据统计，东盟国家总人口超过 6 亿，但从互联网应用水平看，东盟国家网民接近 2 亿，网络普及率不足 30%，且各成员国之间网络安全水平差距大，发展极度不均衡，对网络安全产业发展、技术研究、安全管理、设备引进等有着迫切需求。因此，东盟因其占据亚太地区重要的地缘位置和网络安全发展水平滞后等因素，逐渐成为多个域外大国借助网络外交施加影响力的角力场，美国、俄罗斯、日本、韩国等国家纷纷主动寻求与东盟建立网络安全合作机制，通过与东盟合作提高网络安全领域话语权。**二是我国借助“一带一路”机遇，通过与东盟合作提升国际影响力。一方面，**我国把东南亚地区划为

重点发展区域，积极开展多边和双边交流。在“一带一路”的有序推进、国际网络空间利益博弈日趋激烈的大背景下，成为东盟地区的全面战略合作伙伴，通过开展与东盟国家在网络安全领域的合作，建立中国-东盟合作的信息交流平台，扩大双方在网络空间领域的共识，加强互信程度，提高中国在全球网络空间治理中的话语权。**另一方面，**逐渐由东盟向西方国家扩大我国在安全领域的国际影响力。近年来，我国建设东盟电子信息产业基地，推动中国-东盟区域性中心城市信息化重点工程，提高了 40%左右的高新技术产品出口增长率，进一步加大了对海外市场的开拓。微步在线、360、安天、绿盟、安恒等公司也纷纷入围全球网络安全 500 强名单，加速了我国网络安全企业的国际化转型。

（三）通过安全合作促进“一带一路”落实，提升网络安全产业竞争力

东盟国家是“一带一路”倡议的重要参与者，是“一带一路”倡议落实与实施的助推力量，加强中国一东盟的网络安全合作能够有效推进 “一带一路” 倡议的落实与实施，促进中国同相关国家之间的互利合作，深化中国与东盟国家的友好关系。同时，增强中国与东盟国家对网络安全风险上的认知和了解，并达成维护网络空间安全的共识。为我国网络安全产业竞争力的提升带来新的机遇。**一是助力我国网络安全企业市场拓展，为网络安全产业海外发展铺路。**如：深信服在马来西亚、印尼、新加坡等东盟国家和地区设立子公司，形成了覆盖全国市场及部分海外市场的营销网络，可以更

好地了解用户需求，及时有效地推出满足市场需要的产品；绿盟科技公司中标马来西亚运营商网络安全项目，其集合 NTA 攻击检测、ADS 流量清洗和 ADS-M 集中管理的抗 DDoS 解决方案经过多轮国际竞争，产品更趋于成熟。加强由于东盟国家网络安全合作，大力推广我国具有优势的网络安全产品和服务，拓宽我国网络安全企业产品的覆盖面，以此提高我国网络安全产业在国际上的影响力，为网络安全产业海外发展铺路。**二是加强我国网络安全技术研发和人才交流，提高网络安全产业竞争力。在技术提升方面**，我国与东盟国家网络安全企业开展合作研发和应用推广,促进科技成果交流，推动我国企业对网络安全技术的创新和吸收。同时，国内网络安全企业间加强合作，有效提升网络安全监测、预警和应急处置能力。**在人才培养方面**，我国与东盟国家开展网络安全人才交流方面合作,如：观安信息与联合国亚太地区经济与信息化人才培训中心合作设立培训基地。数据广西集团公司建立网络安全交流培训中心计划，引入 360、绿盟、深信服等有针对性的网络安全产业培训机构，形成网络安全人才培养、技术创新、产业发展融合生长的良好生态环境。并通过网络安全国际会议和国际赛事选拔国际化高端网络安全人才，为我国网络安全产业发展和竞争提供了助力。

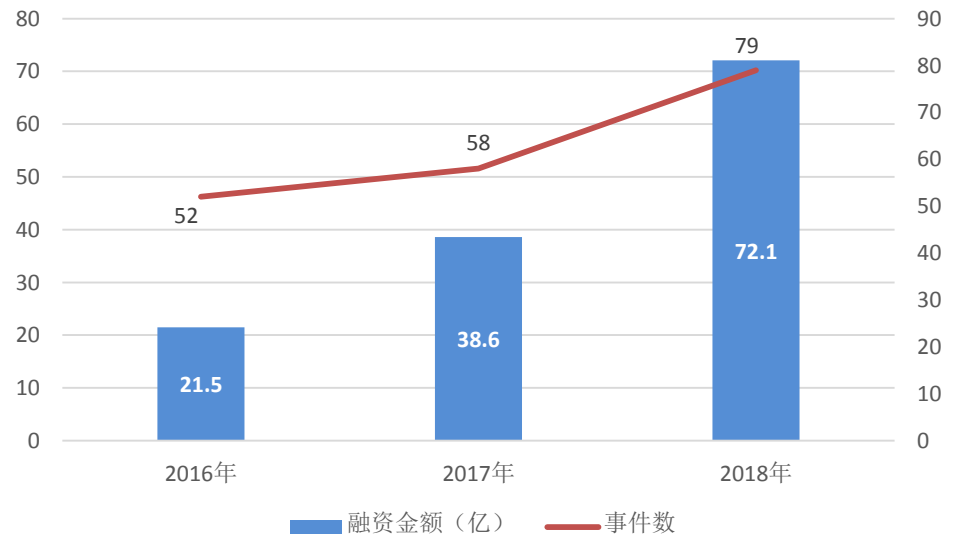
二、中国安全产业现状

（一）安全产业规模持续增长，各方积极协同合作，总体趋势稳定

1. 安全产业联盟发挥积极作用，网络安全市场投融资持续火热。

一是 IT 厂商、网络安全企业等加强安全联盟建设，打造协同联动的网络安全防御生态。如:2018 年，华为联合天融信、微步在线等从厂商成立网络安全联盟，通过整合联盟伙伴的优势产品，实现协同联动构建防御体系；同时，腾讯携手卫士通等上市公司，成立 P16 上市企业协作共同体，在应对网络安全威胁、核心技术突破、推动网络安全产业发展等方面发挥重要作用。**二是** 2018 年，中国投融资金额和交易数量都大幅上涨，而单笔融资金额也不断上涨。亿级融资 20 起，千万级融资 44 起，百万级融资 2 起，市场热度持续高涨。

图 1 2016-2018 年中国网络安全初创公司融资态势



数据来源：2019 中国网络安全发展白皮书

2. 政府出台政策大力扶持安全产业，优化生态建设。

2019 年 6 月，《国家网络安全产业发展规划》正式发布,工业和信息化部与北京市人民政府决定建设国家网络安全产业园区。此次规划是继等保 2.0 之后又一网络安全领域国家顶层规划政策,是对网络安全的国家战略地位进一步肯定。根据规划,到 2020 年,依托产业园带动北京市网络安全产业规模超过 1000 亿元，是对未来信息安全产业的发展有巨大的指引意义。同时，天津宾汉信息安全产业园迎来了首批企业入驻。在政策持续利好下，2017 年我国网络安全产业规模约为 453 亿元，增长 28%，2018 年达到 545 亿元，增长 20.4%。连续 4 年，我国网络安全产业的年复合增长率都超过 20%[1]，构建了良好的网络安全生态环境。

3. 多措并举促进网络安全人才培养，提供有力安全支撑。

一是在政策支持方面，自六部委联合发布《关于加强网络安全学科建设和人才培养的意见》后，各地政府纷纷出台相关网络安全人才建设政策，如武汉政府出台《关于支持国家网络安全人才与创新基地发展若干政策的通知》、成都市政府出台《信息安全专项资金补贴》等用于网络安全人才培养等资金支持；**二是**在人才培养、选拔方面，党政机关、事业单位和相关企业开展网络安全技能培训，提升网络安全从业人员的技术水平。同时，全国各地开展网络安全

[1]数据来源：2018 年网络安全产业白皮书

竞赛，2018 年 8 月中科院信工所、清华大学、百度等单位联合协办"网鼎杯"网络安全大赛，大赛共吸引 7000 多支战队，21000 多名选手参赛，通过网络安全攻防对抗，选拔出色的网络安全人才加以重点培养，为网络安全产业发展提供高质量战队。

（二）积极落实"一带一路"倡议，强化多边交流，把握国际网络安全市场拓展新机遇

1. 建立中国与东盟国家网络安全领域合作平台，加强多边交流。

建设中国-东盟信息港，其建立的 5 大平台：基础建设平台、技术合作平台、经贸服务平台、信息共享平台、人文交流平台促进区域内网络安全产业的多边发展与合作，并提出建设网络安全事件共同响应机制等；同时，2018 年中国-东盟环境信息共享平台也正式启动、由中国和东盟成员国共同建设、维护、使用，共享环境信息和数据。建立平台旨在促进中国和东盟之间环境信息的互联互通，提高环境信息和数据收集、整理、分析、加工和应用的能力，提高环境管理和规范化水平，促进区域绿色和可持续发展[2]。

2. 建立与东盟国家良好伙伴关系，积极布局海外网络安全市场。

目前国际市场空间广阔，老挝、巴基斯坦、中东地区的网络安全市场具有较大的挖掘潜力。启明星辰持续强化国际化产品能力开展，通过具有国际竞争力的部分优势产品，加速建立和完善海外营销和服务网络；深信服设立了美国、新加坡、马来西亚、迪拜等七大境外直属分支，业务遍布全球 16 个国家及地区；美亚柏科面向"一带一路"有关国家提供网络安全领域专业服务，并且推广了其

具有优势的网络安全技术产品，率先占领海外市场。同时南宁、厦门、杭州、济南等城市皆参与了中国-东盟智慧城市建设。智慧城市的共建拓展了国际市场，成为宣传网络安全产业重要性、推动产业体系化的良好机会。

3.借力“一带一路”，进一步增强国际影响力与认可度

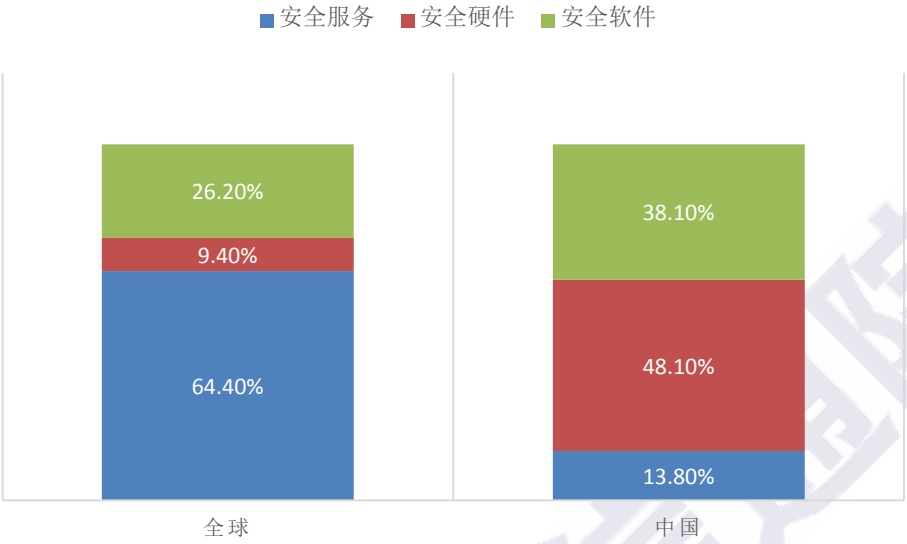
一是我国积极利用好各类双边与多边机制相关网络治理平台，适时开放并举办“一带一路”网络空间治理论坛等活动，加强“一带一路”沿线国家网络空间治理合作，增强国际影响力。**二是**安天、奇虎 360、安恒信息、Nexusguard（耐誉斯凯）、瀚思、绿盟、深信服、微步在线等 8 家企业入围 2018 年国际网络安全创新 500 强榜单，较 2015 年增加 100%。在漏洞挖掘、攻防竞赛、技术认证、标准制定等领域,虽然我国与欧美国家技术水平还有一定差距，但是我国安全企业的参与度、认可度在逐步提升。

（三）我国安全产业结构、技术实力和应用创新与全球产业存在差距，有待进一步提升

1.相比全球产业发展,我国产业结构存在“重产品轻服务”现象

根据 Gartner 统计数据，全球网络信息市场产品以安全服务为主，2018 年安全服务市场份额占网络信息安全市场的 64.4%;相比全球市场,我国网络安全市场结构则呈现了完全不同的情况，2018 年我国网络信息安全硬件市场份额最大，占 48.1%，而安全服务市场份额仅占 13.8%。存在着“重产品轻服务”和“重硬件轻软件”的结构性失衡问题。

2018 年全球/中国网络安全产业市场份额占比



数据来源：iiMedia Research 艾媒咨询

2. 我国网络安全技术水平滞后于发达国家，影响安全产业发展

我国经过几年快速发展，虽已成为网络大国,但在网络安全技术水平方面仍落后于发达国家。以美国为例，美国在网络安全各领域具有较强的实力。**一方面**，其拥有众多掌控核心技术的基础安全产业，如思科、微软、甲骨文、英特尔、苹果、谷歌等一系列掌控核心技术的产业巨头。**另一方面**，美国形成了综合解决网络安全问题的 IT 安全产业，涵盖了赛门铁克等综合性网络安全企业以及 FireEye、Palantir 等具体领域的专业化企业。这些企业综合各方力量全面推动美国网络安全产业发展。而我国在基础性底层技术、颠覆性非对称技术等创新缺乏，网络安全的核心技术研发相对滞后，使得我国在信息技术产业的发展上独立性不足。如在 APT 研究领域，美国在全世界都处于遥遥领先的地位，而我国在 APT 攻击检测和防

御方面，我国技术实力较弱，不能及时发现 APT 攻击，无法对其分析取证，难以掌握整个攻击过程，并缺乏有效的反击手段。

3.我国产业需求和创新力有待提升，细分领域发展水平不均

据 2018 年《全球网络安全企业竞争力研究报告》显示，全球范围内网络安全百强企业中，美国企业 55 家，独占半壁江山，并在 top10 中美国企业占 8 个。我国 17 家企业入榜，虽名列第二，但与美国处于绝对优势的地位相比，我国网络安全产业在市场需求和产业创新能力角度来说对于美国相对落后。**一方面，**网络安全产业无论在研发投入还是增长规模上仍有很大发展空间，产业发展迫切。**另一方面，**从报告总体看来，美国网络安全产业发展均衡,各个细分领域均有成绩突出的企业。相比之下，我国企业在高端威胁防护、应用安全，检测响应等细分领域发展水平不均，有待进一步提升。

三、东盟安全产业现状

（一）各成员国网络安全需求不同，网络安全产业发展不均

1.东盟安全产业发展空间较大，各成员国安全需求不断提高

一是东盟各成员国间安全产业规模差异较大。据统计，东盟国家人口约 6.2 亿，网民规模总数达到 2.6 亿，拥有世界上增速最快的互联网市场。随着需求不断增加，互联网用户规模持续扩大。然而由于经济发展不均衡，东盟各国之间的安全产业发展水平差异大，包括新加坡在内的成熟亚太地区网络安全产业规模近 90 亿美元，而新兴亚太地区 2019 年预计产业规模仅 50 万美元，远远低于全球平

均水平，网络安全产业在新型亚太地区仍属于需求蓝海，市场有待拓宽和发展。**二是大部分成员国网络安全需求日趋旺盛。**新加坡拥有完善网络安全体系，在联合国专门机构国际电信联盟（ITU）发布的《全球网络安全指数》（GCI）的报告中位列全球第六（图 1），因此对高技术的引进、国际合作需求较高。近年来，东盟的发展中国家也积极完善网络安全顶层设计。泰国参与网络安全政策制定，在第 59 届 APEC 会议上提出 APEC 数字经济安全框架；印尼为加强网络安全建设，目前正在加紧制定《个人信息保护法》和《网络安全弹性法》。马来西亚、越南也纷纷更新网络安全战略，加快发展步伐。然而，东盟少数不发达国家如：老挝、柬埔寨、缅甸由于目前对基础设施的需求较大，对网络安全的需求相对较少，因此尚未制定国家级的网络安全战略，也缺乏关键领域网络安全政策，导致安全水平较低。

图 1 2018 年全球网络安全指数（GCI）排名

国家	排名
新加坡	6
马来西亚	8
泰国	35
印度尼西亚	41
越南	50
菲律宾	58
文莱	64
老挝	120
缅甸	128
柬埔寨	131

数据来源：《全球网络安全指数》调查报告

2. 东盟安全产业发展不均，区域产业促进机制较为灵活机动

一是安全产业发展受复杂的外部环境影响。由于东盟各成员国网络发展程度参差不齐，受政治、经济、文化价值观等因素影响，各国之间在技术、执行、政策和法律方面存在一定差异，在共同讨论网络安全标准规范时，会有意地回避复杂的政治安全问题等各种因素，在网络安全方面需求不高的落后地区不能积极响应政策的变化，加大了安全产业的发展差距。**二是东盟网络安全产业促进机制实施方式较为机动。**为在复杂环境下保证安全产业的有序发展，东盟尊重成员国的互联网主权，通常采用非正式的制度安排，采取声明、宣言、总体规划和行动计划等较灵活的制度形式。此外，东盟网络安全相关政策更趋向于主动遵循而非强制执行，更多考虑各国情况，以建议性政策为主，通过设立跨国犯罪、技术合作、社会安全、多边对话与合作四大机制讨论网络安全问题，以制定更易遵守的安全准测，共同推进安全产业合作。

（二）政府积极调整政策，改善安全产业发展环境

1. 制定安全产业政策规划，推动政企合作实现共同发展

一是更新完善网络安全策略以促进安全产业发展。各国积极举办东盟会议，制定安全领域新标准。第 32 届东盟峰会通过了《关于网络安全合作的声明》，要求协调网络安全政策，确定东盟网络空间国家行为自愿规范清单，在会上，印尼总统倡议加快推进东盟国家加强网络安全合作，重点提出了安全企业所存在的数据泄露等安全问题。马来西亚、泰国也在 2019 年纷纷制定了新的网络安全策略，点明了推动网络安全产业发展的意愿，大力推动企业活力和人才培

育体系，以适应新的网络安全环境。此外，缅甸也在信息技术和网络安全部（ITCSD）下设了国家网络安全中心，为安全产业发展打造安全、可靠的网络环境。**二是加强政企合作以助力网络安全双赢战略。**东盟国家强调政府与企业、公民社会在网络安全领域合作的重要性，为加强合作关系，各国代表提出保障政府与行业中关键信息基础设施弹性、激励企业提高网络安全标准等建议。其中，新加坡2016 年出台的《网络安全法案》就强调了在多个方面协调私营企业、非政府部门参与到网络空间治理中，并在网络安全研究计划中大力推动政府机构和私人企业、大学、研究所、科学院的联合研究与开发工作，把握政企合作机遇共同推动网络安全产业发展。

2. 遵循国家网络安全研发规划，形成良好网络安全生态系统

一是积极推动网络安全专业人才队伍建设。新加坡在《网络安全战略》中形成了完善的人才培育体系，将发展充满活力的生态系统作为新加坡网络安全战略的四大支柱之一[2]。2016 年新加坡政府拨款巨资推出“网络安全技术及伙伴计划”[4]，吸引国际顶尖网络科技企业进入新加坡市场、帮助本地企业研发开拓全球市场的方案，培养更多的网络安全科研人才。马来西亚网络安全平台“亚洲网络安全交易所”也通过了网络安全加速器计划，旨在增强网络安全新人才队伍力量，助力安全产业生态建设。**二是不断为网络安全产业发展寻求最新解决方案。**新加坡推出“安全加速器计划”，支持企业家促进网络安全生态创新发展。该计划为初创企业提供免费的工

[2] 四大支柱：通过网络安全法建立弹性基础架构、创建安全网络空间、发展充满活力的生态系统、加强国际伙伴关系

作空间、测试设施、区域市场和企业支持服务，并向企业家或研究人员提供训练营，用于测试理论和商业可行性。新加坡网络安全局（CSA）每年举行一次网络安全行业创新呼吁活动，邀请网络安全行业提出应对挑战方案，并鼓励终端用户超越现有解决方案，着眼于能够满足长期需求的创新解决方案。此外，马来西亚也建立了一套网络安全行业发展计划，包括赋权产业合作、创新、能力建设三个方面，涵盖了行业实践分享、地方解决方案展示、行业人才培训等部分，促进网络安全行业与生态系统发展。

（三）与域外大国密切合作，不断提升安全防护能力

1.积极推动国际合作，提高安全应急响应能力

一是与西方大国合作获得援助与技术能力指导。东盟积极与美国进行合作，近年来美国参加了东盟部长会议、东盟地区论坛和东盟峰会等，推动东盟网络安全框架协议的制定，强化安全产业政策指导。为发展东盟技术援助计划，新加坡网络安全局还同美国政府签署了意向声明（DOI），其中包括了东盟网络能力计划（ACCP）与美国“数字连接和网络安全伙伴关系”提案的内容，旨在加强人才储蓄与产业活力。东盟还与欧盟保持良好交流，汲取欧盟向东盟提供的网络安全防御经验，通过提高安全防御技术水平，拉动安全产业发展。**二是通过网络安全演习加强政企应急响应合作。**东盟国家通过组织网络安全应急演练提高政府、安全企业及各机构面对突发网络安全事件的分析、应急和处置能力。老挝每年参加东盟-日本的网络安全演习，加强信息共享和协调合作，提高各参与演练的安全

企业的网络安全意识和防护能力。2019 年 9 月，来自中国、印度、韩国、日本和澳大利亚的五个伙伴国共同参与了新加坡网络安全局主办的第 14 届东盟计算机应急响应小组事故演习，检验了应急响应技术和能力，增强了政府与安全企业共同保障网络安全的协作。

2. 借助平台优势深化合作，建立安全产业联盟

一是促进网络规范与安全产业的交流培训。东盟与中国进行合作，构筑中国-东盟区域“信息高速公路”，打造一系列信息交流平台，定期开展专业网络安全培训，提高相关安全企业与人员的技术知识储备。其中，泰国积极举办 2019 泰国物联网产业峰会，与华为进行深入交流；泰国数字经济促进局还与中国启迪之星共同制定了中泰数字孵化器计划。此外，东盟与澳大利亚成立东盟-澳大利亚特别峰会，在会上提出了加强网络安全集体应变能力的建议；与日本、韩国就网络安全企业间的合作问题积极开展对话，以寻求更多的安全企业合作机遇，为产业发展提供新动能。**二是通过联盟等形式鼓励国内外企业共同发展。**新加坡于 2016 年启动网络安全联盟，包括新加坡电信有限公司、新加坡奥兰国际有限公司、普华永道、毕马威等企业，促进研究并有效转化研发成果到行业应用中。2019 年 9 月，中国—东盟信息港数字经济产业联盟在广西南宁正式启动，包含中国信息通信研究院、数字广西集团、柬埔寨皇家集团、缅甸 Myan Tel 控股有限公司、马来西亚 red ONE、等 51 家中国与东盟国家相关政府机构、国际组织、企业和科研机构等，旨在合作打造开

放型合作平台，在云计算、大数据、物联网等方面开展联合研发、注重人才培养和产业服务，共享研究成果[5]。

四、中国-东盟合作面临的问题与机遇

当前，中国与东盟网络安全产业国际合作面临的挑战与机遇并存。就挑战来看，两国合作面临外部环境复杂、内部条件有限、技术及产业布局差异等问题。就机遇而言，“一带一路”倡议为双方安全产业合作、开展务实项目提供了巨大的空间。

（一）我国与东盟合作面临复杂环境，网络安全产业合作发展长期以来受到限制

1.国际利益纷争影响安全产业合作发展

一是大国博弈对我国与东盟的合作形成压力。发达国家通过与东盟合作提升自身国际影响力，如：2019 年美国科技巨头包括亚马逊、苹果、谷歌、微软、Netfilx 和高通联合访问了越南科技部，在电子商务和工业 4.0 领域，如物联网、人工智能、大数据和 5G 方面加强与越南的合作。日本与东盟不仅在预知网络攻击和病毒预警系统开发方面展开技术合作，还在 2018 年建立了东盟-日本网络中心（AJCCBC），并承诺提供 500 万美元的资金支持安全机构人员的培训。由此可见，各大国争先与东盟在网络产业和网络技术的能力、网络安全教育和科研的能力方面加强合作，在无形中也对中国与东盟的网络安全各领域合作施加了压力。**二是西方大国依靠技术优势获得了先发市场优势。**欧盟国家网络安全技术较强，安全产品在全球范围内占有较大市场，如：美国 Paloalto、Fortinet 和英国

Sophos 安全公司占领了全球近 70%的市场。由于东盟本土安全厂商较少，先发市场优势使美国在东盟国家也占据了较大的市场份额，东盟诸多防火墙、云计算、安全服务、应用管理等产品来自于欧美国家。中国的安全技术相对较落后于欧美国家，缺少可以引领市场的创新技术，无法突破利益格局，在市场竞争方面未能占有优势。

2. 东盟内部发展条件欠缺导致合作内容深度受限

一是东盟环境复杂导致合作内容不深入。东盟各成员国在经济、政治、文化、宗教等方面特点显著，双边关系错综复杂，我国在与东盟国家合作时，对于采取的合作方式、涉及的合作内容都应根据国家特点所决定。互联网自由、数据隐私保护、数据跨境等问题易与东盟国家产生分歧，因此，大部分情况下，我国与东盟关注于空间治理的规范，并采取培训交流的合作方式，但此类适用性的合作内容及方式涉及层面较浅，对于推动我国安全产业的国际化发展效力欠佳。**二是语言成为发展交流突出障碍。**东盟将英语作为工作交流的官方语言，然而各成员国都拥有自己的语言体系，多数国家网络安全人员的英语语言水平能力不足，导致双方无法深入交流。语言障碍不仅存在于东盟各成员国之间，中国与东盟的合作也存在相同问题，在参加对外交流合作会议时，简单的翻译无法使双方得到足够的理解，导致讨论内容深度有限。

3. 中国与东盟网络安全技术能力不对称

一是中国安全技术对外输出受限。我国受东盟复杂环境影响，我国因缺少调研、资金、专业人才等原因，导致技术的转出方和需

求方存在着信息不对称问题。在搜集资料和数据时，因东盟十国语言体系复杂不易处理，难以统计东盟网络安全相关隐形技术的需求，无法掌握安全产业市场最新的动态发展，造成了两国技术能力不对称的现象。**二是需求差异影响中国安全产品进一步打开东盟市场。**东盟实力较弱的国家与我国有约 3 至 5 年的发展差异，对网络安全产业投入较少，网络安全产品进出口量大大低于其他国家，导致我国的新产品和新技术也无法及时与其进行交流，无法进一步开拓国际市场。如：2017 年缅甸 ICT 产品进出口总占比仅为 3.7%和 0.2%，比中国 ICT 产品进口占比 22.7%和出口占比 27.1%少了约 10 倍左右[3]。

4. 国际产业对接缺少统筹规划与政策指导

一是中国与东盟国家安全产业合作体系不完善。中国与东盟国家内部都面对不完善的产业体系与结构。在全球产业加速升级的过程中，我国缺乏与东盟建立优势互补的产业链以及企业间横向合作组成的联营体，在引进东盟国家资本时，对产业层次高、网络安全技术先进的产业和资本的引进较少，无法填补我国产业空白区，如：我安全企业集中在防火墙、入侵检测、入侵防御等单点技术产品上，而综合性网络安全技术发展水平却仍低于欧美等西方国家。**二是缺乏对外政策指导我国企业在东盟的发展布局。**中国与东盟的安全合作面临政策落地、法律监管、文化差异等问题，缺乏安全产业发展的针对性政策性指导。中国在 2017 年举办的“中国-东盟基础设施合作论坛”上也提出，为实现在东盟的业务拓展，还需进一步出台

[3] 数据来源于中国信息通信研究院

相关政策指导各企业制定东盟市场战略，以实现资源在东盟各国之间的有效流动和配置。同时，还应加强技术研发、人才培训方面政策的针对性，加快制定切实可行的合作路线与规划。

（二）“一带一路”倡议带来国际合作新机遇，中国和东盟安全产业合作迎来发展期

1. “一带一路”倡议为中国与东盟安全产业发展增添动力

一是带来了产业发展新机遇。2019 年 6 月，国家工业信息安全发展研究中心举办了“中国-东盟工业大数据应用与产业安全发展论坛”，东盟各成员国与中国达成了强化推动中国与东盟国家在共性技术、产品、应用的互联互通合作的共识。9 月，中国还与东盟开展了电子商务论坛，不断寻求电子商务合作共商新机遇，如：菲律宾目前有 3775 万电子商务用户，电商正处高速发展阶段，成为诸多国际企业重点布局的新兴市场。[6]我国可抓住这个机遇，进一步推动共同推动中菲两国包括电子商务在内的数字经济发展。 **二是拓展了两国安全产业合作范畴。**“一带一路”倡议将中国与东盟国家各自的发展战略对接起来，通过多种不同层次的高层领导人会晤机制，如：“10+3”、“10+1”、12 个部长级会议机制、以及 5 个工作对话机制等，推动双方对各类网络安全议题进行讨论，使得中国与东盟的合作不仅限于电子商务、网络犯罪等单个领域，还逐渐拓展到了安全技术、人才培养、产业合作实践等方面。

2. 我国发展成功经验和先期合作成效拓展了未来合作空间

一是我国网络安全发展历程对东盟国家借鉴意义较强。虽然中国安全产业发展起步晚于欧美国家，但我国为加快推动安全产业发展，制定了一系列战略规划和工作计划，如：建立信息安全标准化委员会，编制多项安全设备的技术要求和安全服务要求的行业标准和规范，为促进安全产业发展奠定良好的基础。这些努力使得中国安全产业规模迅速扩大，步伐更加快速、稳健，对发展中国家具有较强的借鉴作用，提高了东盟与我国合作的积极性，加深了两国安全产业的沟通交流。**二是中国与东盟务实合作成效开始凸显。**近年来，中国与东盟持续深化务实合作。我国深信服、绿盟等安全企业与当地政府、运营商、IDC 达成了伙伴关系，不断优化合作模式，通过提供综合服务平台传递安全技能与发展经验，为未来进一步强化共性技术、产品、应用的互联互通合作打下了基础，推进了威胁预警情报共享平台、共建智慧城市等实质性合作项目的开展，推动了双方安全产业发展共同走向市场化、专业化、国际化。

五、启示与建议

（一）缩小网络基础设施安全技术鸿沟，改善东盟国家合作底层环境

1. 加强关键信息基础设施安全防护水平

掌握相关网络信息技术是进行国际网络安全合作的前提，拥有更加先进网络信息技术的国家在国际网络安全合作中的领导作用会更为凸显。因此，我国应**一方面，高度重视网络安全防护技术研发。**加大对关键信息基础设施防护、网络安全保护等技术等的投资与研

发，建立网络信息技术创新体系，争取占领网络技术的制高点。打破发达国家对网络安全技术的垄断，促进与东盟国家的技术交流，争取在国际网络安全合作中获得更多的话语权。**另一方面，缩小“技术鸿沟”提升合作竞争力**。利用自身掌握的网络技术生产相应的网络硬件设备和软件设备，缩小与发达国家的“技术鸿沟”，提高我国网络安全核心竞争力。加强与东盟国家在技术支持、政策制定、产业发展方面的沟通交流，进一步深化与东盟国家网络安全方面的合作。

2. **多维度、多层次改善东盟各国间安全发展水平差距**

我国应充分利用自身的技术、经济、政治等优势在与东盟国家开展合作中减少东盟各国的网络安全发展水平差距，努力缩小数字鸿沟。**在技术层面**，联合东盟国家中新加坡、马来西亚等网络安全领域较为发达的国家，为其他技术发展相对滞后的东盟成员国提供技术支持，提高东盟整体发展网络安全水平。同时，注重与网络安全领域发展较为领先的东盟国家开展新兴技术方面的交流合作。**在经济层面**，帮助缅甸、柬埔寨等安全水平相对落后国家完善网络基础设施建设，提供必要的网络安全专项扶持资金。**在政治层面**，为东盟国家提供技术、政策研究等专家支持，维护良好的外交关系，为探讨如何深化合作、促进网络安全产业发展奠定基础。

（二）搭建中国-东盟合作机制，引领增进合作的积极性和主动性

1．完善中国东盟合作框架和信息共享机制

建设并完善中国-东盟网络安全合作法律机制。通过国际合作的司法手段打击网络犯罪，深化法律标准和法规实施，保护关键信息基础设施安全。具体内容包括达成网络安全合作基本协议、增强与东盟各成员国网络安全战略合作、健全网络安全合作法律法规和设立专门的网络安全合作法律机构等。**一方面，**统筹完善中国-东盟网络安全合作机制可以集中东盟各成员国在网络安全合作领域所关心的问题，由此形成集中解决网络安全合作方案的平台；**另一方面，**制定中国-东盟网络安全作机制可促进中国与东盟各成员国中相关的职能部门的参与协同，有效推进各东盟成员国在相关网络安全时间中的信息共享与合作。

2. 发挥引领作用推动与东盟安全合作深入发展

中国-东盟网络安全国际合作应坚持主权平等和互利共赢的基本准则，尊重其他国家的网络发展、管理模式等，不干涉别国内政，提高网络安全合作水平，构建网络空间命运共同体。**一是**积极推行我国“互联网+”战略，以网络信息技术创新带动网络贸易的发展，将我国先进网络安全管理经验推广至东盟国家，促进东盟各国内的互联网资源流动与共享[6]。进而实现网络空间的长治久安。**二是**中国应适时地发挥自身在东盟成员国中的影响力，将本国发展战略与东盟的行动框架相结合，实现自身对网络安全防护的诉求。同时，

中国-东盟网络安全合作需在充分尊重对方主权和合作意愿的前提下，通过协调双方的利益预期，增进合作的积极性和主动性，推动网络安全合作的深入发展[8]。

（三）优化安全产业生态环境，提高与东盟国家网络安全产业对接能力

1. 优化并创新网络安全产业生态环境

一是多方推动网络安全产业发展。调动我国网络安企业、网络运营商、高校、科研机构等主体的积极性，打造“政产学研用”一体化网络安全产业发展生态。同时,壮大网络安全产品服务市场，积极与东盟国家通信、能源、金融、交通等重要行业龙头企业开展网络安全合作，促进网络安全产品服务应用普及[9]**二是**强化我国网络安全产业创新。支持相关科研机构、企业对新兴业务技术的研究。建立技术研发、创新服务、产业协同的平台，优化完善网络安全产业环境，形成良好的创新产业生态系统，以推进与东盟国家网络安全产业创新合作。

2. 提升安全产业政策统筹指导和产业对接能力

一是制定中国与东盟国家网络安全产业发展规划。明确我国与东盟国家网络安全产业层次结构、功能定位以及发展重点，分析未来发展趋势，细化安全保障措施。为我国网络安全企业“走出去”、东盟国家的网络安全合作活动提供指导，提升我国企业与东盟网络安全产业对接能力。同时，制定与东盟网络安全市场合作战略，加快打造我国层次鲜明、保障有力的产业梯队。对具有产业整合能力

的安全巨头给予重点支持，发挥产业带动引领作用，实现资源在东盟各国之间的有效流动和配置。**二是**完善人才培养、激励机制，加快人才队伍建设。加强与东盟国家网络安全人才国际交流，对先进的管理经理和技术结合我国国情进行创新和吸收，及时相互了解网络安全发展动态，把握网络信息产业发展新机遇，推进网络信息产业的高效快速发展。

参考文献

[1]《中国网络安全产业白皮书（2018）》信通院 [DB / OL]. 信通院官网，2018-10-25，http://www.caict.ac.cn/kxyj/qwfb/bps/201809/t20180919_185440.htm.

[2]2018 年中国—东盟生态环保合作周系列活动在京举行[DB / OL]. 中国国家生物多样性信息交换所，2018-05-14,

[3]马来西亚“网络安全加速器”计划为当地人才提供 4800 万美元，2019-04-19，http://www.sohu.com/a/309197463_804262.

[4]中国—东盟信息港数字经济产业联盟启动 51 家机构加入,2018-09-13,https://baijiahao.baidu.com/s?id=1611498868379068662&wfr=spider&for=pc.

[6]中国与东盟强化电子商务合作共商新机遇,2019-09-23,http://www.cac.gov.cn/2019-09/23/c_1570766826767249.htm.

[7] 龙转. 国际网络安全合作存在的问题及对策研究[D].湖南师范大学,2017.

[8] 郑怡君,薛志华.中国——东盟网络安全合作及其布局[J].东南亚南亚研究,2017(02):17-23+108.

[9] 《国家网络安全产业发展规划》正式发布[J].自动化博览,2019(07):3.

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191
联系电话：010-62304839
传真：010-62304980
网址：www.caict.ac.cn