DOI 10.15302/J-SSCAE-2021.02.015

国外工业互联网安全产业布局及启示研究

李阳春[1]，王海龙[1]，李欲晓[1]，陈磊[2]，李幼平[3]

（1. 中国网络空间研究院，北京 100191；2. 中国工程院战略咨询中心，北京 100088；
3. 东南大学计算机科学与工程学院，南京 211189）

摘要：工业互联网安全产业是工业互联网健康发展的重要基础支撑，发达国家和地区在这一产业的布局已相对完善。我国在建设制造强国、网络强国、数字中国的宏观需求下，亟需科学优化工业互联网安全产业布局。本文运用文献调研和情报分析相结合的研究方法，研判了工业互联网安全产业的发展需求，围绕政策引导、企业创新、协同发展、资本整合、联盟生态等方面深入剖析了美国、德国、英国、日本等发达国家工业互联网安全产业的布局现状；评估分析了国际发展趋势，阐述了我国在政策标准、技术产品、市场空间、投资融资、区域布局方面的发展现状和面临的挑战。研究建议，借鉴他国有益经验、结合我国发展实际，充分发挥体制机制优势，统筹安全产业均衡发展；坚持自主创新，打造具有国际竞争力的优势产品；健全安全标准体系，积极引领国际规则制定；加强对中小企业政策和资金的扶持力度，激发创新活力；构建多链环协同发展生态，促进形成国际国内双循环格局。

关键词：工业互联网安全；工业互联网安全产业；产业布局；均衡发展；自主创新

中图分类号：TP393　　**文献标识码：**A

Layout of Foreign Industrial Internet Security Industry and Its Enlightenment to China

Li Yangchun[1], Wang Hailong[1], Li Yuxiao[1], Chen Lei[2], Li Youping[3]

(1. Chinese Academy of Cyberspace Studies, Beijing 100010, China; 2. Center for Strategic Studies, Chinese Academy of Engineering, Beijing 100088, China; 3. School of Computer Science and Engineering, Southeast University, Nanjing 211189, China)

Abstract: The industrial Internet security industry is crucial for the healthy development of industrial Internet. The layout of this industry in developed countries and regions is relatively perfect. To strengthen the manufacturing, cyberspace, and digital sectors, the layout of this industry in China needs to be optimized. This study investigates the development demands for the industrial Internet security industry using literature research and intelligence analysis. Subsequently, the current status of industrial Internet security industry layout in the United States, Germany, the United Kingdom, Japan, and other developed countries is studied from the aspects of policy guidance, enterprise innovation, collaborative development, capital integration, and alliance ecology. Based on this, the international development trend is analyzed. Meanwhile, the current status and challenges faced by China are discussed in terms of policy and standard, technology and product, market space, investment and financing, and regional layout. The study points out that the optimization of China's industrial Internet security industry layout should draw on the useful experience of other countries and consider China's development reality. It is suggested that China should maximize the advantages of its system and mechanism to coordinate the development of the security industry; adhere to independent innovation to create an internationally competitive brand; improve the security standards system to actively lead the international rule making; strengthen the policy and financial support for

收稿日期：2021-01-15；**修回日期：**2021-03-14

通讯作者：王海龙，中国网络空间研究院高级工程师，研究方向为网络与信息安全、工业互联网安全；E-mail: whl2000721@126.com

资助项目：中国工程院咨询项目“新一代工业互联网安全技术发展战略研究”(2020-XZ-02)

本刊网址：www.engineering.org.cn/ch/journal/sscae

small- and medium-sized enterprises to stimulate their innovation vitality; and build a collaborative development ecology to create an international and domestic dual circulation development pattern.

Keywords: industrial Internet security; industrial Internet security industry; industrial layout; balanced development; independent innovation

一、前言

当前，全球新一轮科技革命和产业变革加速拓展、深入推进，以云计算、大数据、第五代移动通信（5G）、人工智能（AI）、物联网为代表的新一代信息技术正迅速向能源、电力、通信、化工、航空、航天、机械设备、汽车制造等领域渗透。工业互联网是第四次工业革命的关键支撑和竞争焦点，以核心综合基础设施的形态，通过“人、机、物、数、用”的安全互联和融合，提升工业领域的数字化、网络化、智能化水平，构建全要素、全产业链、全价值链的新型生产制造和服务体系，成为推动数字经济与实体经济深度融合的关键路径，同时成为全球主要经济体经济高质量发展的共同选择[1]。

工业互联网的内涵和外延不断拓展，传统封闭的工业制造环境被打破，内生安全与外部风险交织并存，工业互联网安全问题日益复杂化，给现有的安全防护体系、产品技术架构和应对解决方案带来了颠覆性的挑战。世界主要国家和地区高度重视工业互联网安全，积极采取相关措施，优化和完善工业互联网安全产业的发展环境。我国拥有全球门类最为齐全的工业体系，近年来在工业领域的数字化方面转型迅速。借鉴各工业互联网强国的发展经验和成功模式，分析我国相关产业存在的风险与威胁，对解决当前我国面临的工业互联网安全困境，建立适应我国网络空间治理特色的工业互联网安全产业体系，推进制造强国、网络强国、数字中国战略建设，具有重要的现实意义和深远的历史意义。

已有的相关研究集中在对国内外工业互联网安全技术发展现状及面临安全风险的分析[2~8]，侧重从美国工业互联网、德国工业 4.0 等单项规划方面分析相关安全举措对我国的启示[9~14]；针对多个国家和地区安全产业布局的系统化分析和横向比较研究相对缺乏。为此，本文在文献调研、专家研讨与项目研究的基础上，以国外工业互联网安全产业布局为切入点，研判工业互联网安全产业的发展需求，深入剖析诸多发达国家工业互联网安全产业布局的现状和特点；通过横向比较，评估分析国际发展趋势，结合对我国基本情况和面临挑战的统筹思考，提出优化我国工业互联网安全产业布局的对策建议。

二、工业互联网安全产业发展需求

（一）国家竞争需求

近年来，国际社会发展失衡、失序情况频有发生，大国博弈、新型冠状病毒肺炎疫情等加剧了这种状态。工业互联网已经成为少数发达国家利用网络攻击遏制别国发展、胁迫他国服从的重要手段，给国际正常秩序以及国家的安全稳定、经济发展、居民生活造成了严重威胁和巨大损失。例如，2018 年美国 4 家天然气输气管道公司的客户通信系统受到网络攻击，造成系统关闭数小时；2019 年，挪威海德鲁公司（Norsk Hydro）遭遇网络攻击导致生产中断、工厂关闭；2020 年，委内瑞拉国家电网干线遭到攻击，致使全国大规模停电；新型冠状病毒肺炎疫情暴发以来，仅 2020 年上半年发现的针对我国工业互联网的恶意网络攻击行为就高达 1.356×10^7 次，涉及企业达 2039 家[15]。亟需加快发展工业互联网安全产业，形成有效可靠的安全防护与保障能力，为国家间的合作与竞争提供基础支撑。

（二）技术融合需求

工业互联网建设在广度和深度上不断拓展，打通了企业内外网，实现了信息技术（IT）与运营技术（OT）的融合，使得封闭专用、隐患未知的工业控制系统（ICS）风险暴露面大幅扩展；加之 IT 系统存在的自身安全不确定性及其与 ICS 互联互通的融合性问题，进一步增加了工业互联网面临网络攻击威胁的概率。2020 年 2 月，工控安全企业德拉戈斯公司（Dragos）在发布的报告中指出，2019 年披

露的 438 个漏洞，77% 的漏洞位于 ICS 网络深处的系统，50% 以上的漏洞可能导致系统丧失可见性（无法监视或读取系统状态）或失去控制（无法修改系统状态）[16]。惟有夯实工业互联网安全产业基础，加强技术融合，才能为突破上述安全技术难题提供必要保障。

（三）市场拓展需求

2019 年，全球工业信息安全市场规模达到了 164.01 亿美元，到 2026 年市场规模将达到 297.6 亿美元；2019 年，全球 OT 安全开支费用约为 3.8 亿美元（年增长率为 52%），到 2025 年全球 OT 安全市场规模可达 35.31 亿美元 [17]。随着工业互联网设备数量的快速增加、安全隐患的不断暴露，对安全防护解决方案的需求也将激增。未来，工业互联网安全产品和服务市场有望成为增速最快的细分领域，带动整个网络安全产业的发展，拓展更为广阔的市场空间。

三、国外工业互联网安全产业的布局现状

美国、德国、英国等工业强国在工业互联网安全领域的产业优势明显；中国、日本、韩国等国家的信息化、工业化进程加快，对工业信息安全领域的投入也随之加大。本文主要从以下 5 个方面对全球主要国家和地区的工业互联网安全产业布局发展现状和特点进行梳理分析。

（一）制定安全战略政策，引领产业发展

1. 美国

美国为赢得制造业全球竞争优势，在 2011 年正式启动“先进制造伙伴计划（AMP）”，推动政府、学术界、产业界形成合力，共同投资新一代信息技术以制造高水准的美国产品，确保在全球制造业发展中的领导地位。2018 年 10 月，美国在“先进制造国家战略计划”的基础上，推出“美国先进制造领导力战略”，将制造业网络安全作为战略实施的重要着力点和产业布局方向，出台了一系列安全政策与标准规范以保障工业互联网产业安全有序发展。2018 年 11 月，美国成立网络安全和基础设施安全局（CISA），负责网络和基础设施的安全，并将工控安全列为优先事项。CISA、能源部等政府机构注重与产业界的合作，加强工业、能源等领域的信息安全保障建设。同时，美国持续开展工业互联网安全领域的立法工作，为安全产业发展提供法律支撑；仅在 2019 年就通过了《物联网设备安全法案》《保障能源基础设施法》《利用网络安全技术保护电网资源法案》《供应链网络安全风险管理指南》[18]，全面保障物联网、能源、电力、医疗等关键基础设施的信息安全。

2. 欧盟

欧盟注重加强网络安全资源整合，促进产业多方协作。欧盟网络与信息安全局（ENISA）发布的《工业 4.0 网络安全挑战和建议》[19]，提出了工业物联网安全面临的 7 项主要挑战，据此指导工业信息安全建设，为欧盟工业 4.0 发展奠定基础。欧盟成立了工控安全应急响应组，负责信息收集与共享、各类工控安全事件响应分析、行业安全态势分析、协调实施关键基础设施保护计划等工作；发布了《保护信息时代社会安全战略》《国家网络安全策略——为加强网络空间安全的国家努力设定线路》《欧盟网络安全战略》《关键基础设施保护计划》《网络和信息系统安全指令》《通用数据保护条例》等战略文件和法律法规 [2]。

德国作为传统制造业强国，在国家层面大力推进“工业 4.0”战略，期望通过数字化、网络化、智能化手段来提高工业效率，巩固在全球制造业中的龙头地位。2015 年，德国政府牵头，联合相关协会、企业启动建设升级版工业 4.0 平台，将数据安全作为五大主题之一；先后发布了《工业 4.0 安全指南》《工业 4.0 中的 IT 安全》《跨企业安全通信》《安全身份标识》等指导性文件 [20,21]，提出了以网络物理系统平台为核心的分层次安全管理思路。德国联邦信息安全局（BSI）出台了《2019 年工业控制系统安全面临的十大威胁和反制措施》等多份工控安全实施建议文件，具体指导企业做好工业信息安全防护工作。

3. 日本

2016 年，日本提出了以 AI 技术为基础、以提供个性化产品和服务为核心的“超智能社会 5.0”概念，“互联工业”是其中的重要组成部分；同年成立工业网络安全促进机构（ICPA），专门抵御关键基础设施的网络攻击。2019 年 4 月，日本依托经济产业省（METI）发布了《网络 / 物理安全对策框架》

及其配套的一系列行动计划，用于确保新型供应链的整体安全，全面梳理产业所需的安全对策。同时，日本积极实施供应链网络安全强化、网络安全经营强化、安全人才培养、安全业务生态系统建设等配套行动计划。

4. 韩国

2019 年，韩国颁布《国家网络安全基本规划》，要求增强网络修复和存活能力，指导改善信息通信网络和信息基础设施的安全环境，加大对新一代安全基础设施的研发和推广力度，有效提升关键基础设施的安全性。同时，韩国政府提出加大人才培养计划，组织开展研发活动，构建创新安全产业生态圈。

（二）参与安全市场竞争，保持合作主体多元化

市场需求催生更多企业参与到工业互联网安全产业，参与主体不仅包括自动化企业和传统安全企业，还包括一批新崛起的工业互联网安全初创企业。美国、德国、英国、日本等国家的相关企业通过收购、合作以及开拓网络安全业务等举措纷纷加入市场竞争。

自动化企业（如西门子股份公司、通用电气公司、霍尼韦尔国际公司、施耐德电气有限公司等）依托原有的工业市场基础，通过收购网络安全厂商、与网络安全厂商建立合作伙伴关系、组建专业团队开发安全产品等方式，一方面加强了自身产品、设备等的网络安全保障，提高了产品和服务的可信水平，另一方面对外提供工业互联网安全产品和服务，开拓了工业安全市场。

传统网络安全企业具有安全技术优势，拥有开拓工业互联网安全产品、服务的丰富经验；缺少对工业互联环境的了解，导致功能安全和信息安全难以融合，产品无法满足工业企业的安全需求。为此，通过收购或合作的方式，发挥各自优势，解决工业信息安全保障的瓶颈问题。

以克拉罗蒂公司（Claroty）、Dragos 公司、希美公司（Nozomi）等为代表的工业互联网安全初创企业，拥有可以引领工业互联网安全产业发展的创新性技术，具备网络安全和工业控制的双重优势；虽然在规模上远不能与业内巨头企业相比较，但作为独立的工业互联网安全供应商已逐渐引起资本市场的关注。自 2011 年起，230 多家本土或外国机构对 165 家以色列网络技术初创企业进行了投资 [22]。2020 年 6 月，美国微软公司以 1.65 亿美元收购了以色列工业网络安全初创企业 CyberX 公司 [23]。

（三）推动中小企业发展，形成安全保障合力

日本为推动工厂智能化以及物联网在制造业中的应用，通过建立“智能制造声援团”对中小企业提供技术、工具、人员等方面的支持；在推动标准国际化、发展面向制造的网络安全、培养数字化人才、加大研发投入等方面进行了积极引导。

韩国制定了“制造业创新 3.0”战略，从政策、资金、技术等方面扶持制造领域的中小企业发展。一方面，加大资金扶持力度，为中小型企业提供利率优惠政策和便捷的贷款服务，激励其专注研发安全产品；另一方面，鼓励大型企业与中小企业共享技术研发成果，形成工业互联网企业协同发展的良好局面。

德国为提高中小企业的研发能力，部署开展了专门针对中小企业与研究机构合作的项目。德国的研发机构通常拥有不同测试环境，中小企业通过合作不仅可以得到软硬件支持和技术帮助，还能加强企业员工在相关专业方面的培训。中小企业还可以从政府获得直接资助，相关研究方向有生产自动化、智能传感器等。

美国重点加强对中小企业劳动力的教育培训。2019 年，美国国防部为数字化制造（MxD）拨款 1000 万美元，对服务水平低下的中小制造商进行培训，加强财务模型和易用工具的使用，创建更具弹性的工业体系。具体业务包括：推行网络安全工具试点计划；实施就业分类 2.0 计划，帮助员工深入分析特定工作角色；开展数字能力工作坊，促进识别数字计划；提供技术实习机会；开展工业物联网培训，推动中小企业加快物联网制造。

（四）加大投融资力度，强化基础创新

近年来，工业互联网安全初创企业受到资本市场和网络安全企业的青睐。2017—2019 年，来自美国、以色列、法国等工业互联网安全企业的融资金额超过 3.4 亿美元 [17,21]。美国不断加大对工业

信息安全领域的资金投入，在 2020 年联邦预算中，用于网络安全的预算约为 110 亿美元；美国国土安全部在工控安全方面的预算主要用于加强工控安全培训、恶意软件分析、工控系统脆弱性分析、事件响应以及新兴行业和细分领域的安全评估；美国能源部在网络安全、能源安全和应急响应等方面新增了 1.56 亿美元的预算，用于提升美国电网安全和弹性的早期研究项目。2019 年 2 月，欧盟宣布在“地平线 2020”计划中投入 6350 万欧元，启动网络安全能力建设计划，为工业领域网络安全发展提供支撑 [17]。

（五）产业联盟推进标准化建设，构建国际工业互联网安全发展生态

美国工业互联网联盟（IIC）、美国国家标准与技术研究院（NIST）、德国电工电子与信息技术标准化委员会（DKE）、日本工业价值链促进会（IVI）等产业联盟组织均在积极布局和推进工业互联网安全标准化工作 [6]。

IIC 在 2016 年发布了工业互联网安全架构（IISF），旨在规范企业在安全防护领域的规划和实践；先后发布《工业互联网安全成熟度模型：从业者指南》《端点安全最佳实践》《数据保护最佳实践》《在实践中管理和评估工业物联网（IIoT）可信度》等一系列与安全相关的文件内容 [18]，为工业互联网安全研究和实践提供指导；不断加强与国际标准化组织、开源组织、标准研制部门的协同合作，推动研究成果转为统一标准。NIST 发布了《制造业与工业控制系统安全保障能力评估》《工业控制系统安全指南》等，力求引领工业控制系统安全标准的制定。

德国 DKE 发布《德国工业 4.0 标准化路线图》，全面布局工业 4.0 的标准化工作。在德国政府的支持下，德国工程院、弗劳恩霍夫协会、西门子公司等共同组建了“工业 4.0 平台”，围绕工业 4.0 的安全、架构、路线图等关键方向，加速推进德国工业产业布局；将安全作为落实工业 4.0 的三大重要主题之一，针对设备、系统安全的加固与增强，发布了《工业 4.0 中的 IT 安全》；针对架构、标准、安全、测试床等关键共性问题，加速与 IIC 的技术协同和产业协作。

日本成立 IVI，以企业联合体牵头的方式，打造开放安全的制造业生态体系；发布了《日本互联工业价值链的战略实施框架》，提出了新一代工业互联网参考架构，成为指导日本产业界发展工业互联网的顶层框架。

综上所述，美国、德国、英国、日本、韩国等发达国家根据本国工业水平和信息技术发展现状，在布局工业互联网安全产业时各有侧重（见表 1）。①在政策制定方面，以美国、德国为代表的发达国家或地区占据了主导地位。美国互联网技术优势明显，通过不断强化工业互联网安全的相关立法，加强对产业发展的法律保障和战略指导。德国作为工业 4.0 的发起方，更加注重工业信息安全的管理体系建设，以政府为主导，统筹布局工控安全建设。相比之下，其他国家现阶段更为聚焦工业互联网的发展，专门针对工业互联网安全产业的政策较为薄弱。②在企业发展方面，美国将工业互联网安全作为传统安全企业和工业企业发展的重要方向，德国、英国等国家的制造企业通过收购、合作等方式推动工业企业网络安全业务发展。③在对中小企业扶持方面，日本和韩国的资金投入力度相对更大，通过对中小企业的投入来激励其提升创新能力、快速发展状大。④在资金投入方面，美国、欧盟在工业信

表 1　主要国家工业互联网安全产业布局比较

国家	政策标准制定完备度	领军企业国际竞争力	对中小企业扶持力度	资金投入力度	产业联盟全球影响力
美国	高	高	高	高	高
德国	高	高	高	高	高
法国	中	高	中	低	低
英国	中	低	中	低	低
日本	中	中	高	中	中
韩国	低	低	高	低	低

息安全方面的投入持续增加。⑤ 在产业联盟方面，美国、德国成立了专门的工业互联网产业联盟，成员众多、国际合作广泛，具有一定的世界影响力和话语权。

四、国外工业互联网安全产业的发展趋势

（一）政府将加强主导地位

面对地缘政治冲突、科技领域竞争、制造产业转移等严峻复杂的国际形势，尤其工业互联网安全已经成为影响国家安全的重要因素，各国政府将制定实施一系列战略政策和相关标准，发挥产业主导地位，积极抢占工业互联网安全产业高地，确保自身国际地位和全球经济话语权。

（二）相关企业将全面渗透

无论是以互联网为代表的跨国科技企业，还是以制造业为代表的传统大型企业，都认识到在消费互联网向产业互联网转型过程中工业互联网安全的广阔市场前景；通过收购、并购、投资等渠道加快进入工业互联网安全产业，进一步整合创新资源和集成产品服务。同时，工业互联网安全产业的不断发展也为中小企业创造了相对有利的发展机遇和创新条件。

（三）跨界融合将更加显著

一方面，工业互联网是随着 5G、AI、物联网等新兴技术发展而来的，工业互联网安全产业的发展既要解决这些新技术带来的安全问题，也要充分利用新技术应对安全挑战，因而各种技术的融合将进一步加速安全产业的创新发展；另一方面，工业互联网将与能源、电力、交通、航空、航天等重要应用领域不断深化结合，针对特定行业的技术、产品、服务以及新兴企业会不断涌现。

（四）安全标准将趋于统一

数字时代的工业全球化愈加明显，数据和服务的流动将成为工业能力的重要体现。为解决网络信息安全、信息技术和制造技术等因原理、接口、数据结构不同而产生的融合困难，统一的安全标准将是工业互联网实现服务世界能力的前提和保障。因此，涉及构建、开发、集成、运行等环节的统一国际安全标准框架将成为关键的解决方案。

五、我国工业互联网安全产业的现状梳理

（一）加强顶层设计，指引产业发展

我国工业互联网安全政策和标准日益完善，垂直行业工业信息安全建设提速，工业企业安全意识全面增强，工业信息安全保障技术水平显著提升，推动了工业互联网安全产业的全面发展。2017 年，国务院印发《关于深化“互联网 + 先进制造业”发展工业互联网的指导意见》，明确要求提升安全防护能力，建立数据安全防护体系，推动安全技术手段建设。2019 年，我国工业信息安全产业规模保持快速发展势头，产业规模达到 38.3 亿元，较 2018 年增长了 51.62% [17]。2020 年，我国工业信息安全主管部门和行业监管部门密集出台了《关于推动工业互联网加快发展的通知》《“工业互联网 + 安全生产”行动计划（2021—2023 年）》等多项与工业互联网安全相关的政策，指导工业互联网安全保障工作的具体实施。

（二）促进技术产品创新，壮大产业规模

工业互联网安全产品体系正在逐步完善，以边界防护、终端防护、监测审计为代表的安全产品种类增多、功能性能增强，基于 AI、大数据、商用密码的安全新产品也在加快研发 [24]。我国工业互联网安全产业的市场主体主要包括大型自动化企业、传统综合网络安全企业、专注工控安全的初创安全企业。在工业自动化领域，青岛海天炜业过程控制技术股份有限公司、北京力控元通科技有限公司、和利时科技集团有限公司等企业，在 2009 年前后就将业务延伸到工业互联网安全领域，开展工业互联网安全技术产品的研发与应用推广。近年来，众多专注工业互联网安全领域的初创企业涌现，如北京威努特技术有限公司、长扬科技（北京）有限公司、北京安点科技有限责任公司等；凭借网络安全和工业控制方面所具有的人才优势，以工业互联网安全为主要业务方向，在能源、制造、化工等领域开拓国际客户，通过技术创新引领整个行业的发展趋势。

（三）丰富应用场景，积极拓展市场

工业互联网平台已成为工业企业构建网络化协

同、规模化定制、服务型制造等新模式、新业态、新动能的重要支撑，工业互联网安全的产业市场正在从防护、管理等产品型向评估、培训等服务型转变。目前，工业互联网安全解决方案已在能源、电力、制造业、交通、石油石化、航空、航天、核工业等领域得到广泛应用。各行业在工业互联网信息安全方面的投入也在逐年增长，市场规模逐步扩大，如 2021 年我国工业互联网安全市场规模预计为 228 亿元 [25]。

（四）加大投融资力度，提升产业竞争力

工业互联网产业政策频出利好，网络安全的社会关注度持续上升，相关企业和投资机构不断加大对工业互联网安全市场的投融资力度。例如，奇安信科技集团股份有限公司、启明星辰信息技术集团股份有限公司、北京六方云科技有限公司等企业不断加大投入，积极推进工业互联网安全技术研发和突破。截至 2020 年上半年，我国在工业互联网方面的投融资规模累计达 15 亿元，其中工业互联网安全、数据安全、云安全等方向成为市场投融资热点 [15]。

（五）深化区域布局，促进产业平衡

我国主要经济区域根据自身工业和网络安全产业发展条件，出台了相应的发展规划和政策，引导工业互联网安全产业的区域布局：京津冀地区通过突破平台安全核心技术，形成区域协同发展示范效应；长江三角洲地区通过搭建安全创新功能型平台，建设世界级先进制造业集群；粤港澳大湾区通过打造平台安全保障和服务体系，解决新型基础设施建设的安全问题；长江中上游地区（武汉市、成都市、贵州省）通过提高安全技术基础支撑能力，促进传统工业转型升级；东北地区通过重点领域应用试点示范，加强新型产业体系的安全保障；西北地区通过打造安全企业和安全生态，为优势产业发展提供服务保障。

也要注意到，现阶段我国工业互联网安全产业的发展仍处于起步期，产业布局尚不完善，面临着诸多严峻挑战：统筹协调能力不足，政策体系尚不健全，区域、行业、企业间发展不均衡现象普遍存在；核心技术受制于人，技术自主化程度较低，功能安全和信息安全的融合欠缺；安全标准体系尚未建立，重点行业领域布局不到位，工业互联网设备和安全产品在通信协议、配套规范等方面未统一；资金、设备等资源要素保障能力缺乏，专业人才缺失严重，中小企业发展动力不足；产业生态尚待完善，工业企业对安全理念的认识不充分，安全产品设计与生产实际结合不密切，尚未形成协同发展合力。

六、国外工业互联网安全产业发展对我国的启示

发达国家和地区积极推进工业互联网安全产业的顶层设计与应用实践，对我国落实工业互联网安全规划部署具有良好的借鉴价值。“十四五”时期是我国深入实施工业互联网创新发展战略的关键期、工业互联网建设的快速成长期，为了科学高效地应对困难挑战，本文从以下 5 个方面提出科学优化布局我国工业互联网安全产业发展的建议。

（一）发挥制度优势，统筹均衡发展

充分发挥我国集中力量办大事的体制机制优势，形成工业互联网安全产业的发展合力。建议完善适应安全产业发展的政策体系，解决相关领域融合渗透面临的政策和制度瓶颈，秉承创新、自主可控的发展思路，营造更加良好的发展环境；加强各类资源统筹协调，在不同区域、行业、企业间促进安全产业均衡发展，形成东西部协调、南北方平衡、全国各区域优化发展的产业布局；构建形成兜底线、防风险的安全监管体系，制定负面清单、权力清单、责任清单，着重构建工业数据安全责任体系，推动形成支持工业互联网发展的包容性监管环境；全面提升工业企业的安全防护意识，加强工业互联网安全共建共练、联防联控。

（二）坚持自主创新，打造优势产品

借鉴和吸收国外工业互联网安全技术和产业创新理念，避免照抄照搬他国技术体系和运营模式。建议以构建国家战略科技力量需求为导向，推动建设工业互联网安全国家重点实验室、国家工程研究中心、国家技术创新中心等创新载体，打造支撑工业互联网安全高水平创新的基础设施和平台环境；

加快推进设备安全、网络安全、控制安全、应用安全、数据安全等关键核心技术和基础理论的创新突破，充分利用卫星物联网、北斗卫星导航系统等新一代技术装备，辅助提升工业互联网安全防护能力；自主研制具有国际竞争力的安全新技术、新产品、新服务，加强自主成果应用和推广；鼓励并支持工业企业和安全企业开展需求对接，强化技术交流和优势互补，不断提升各方在安全技术、产品和服务上的合作契合度，联合开展关键技术难点攻关，加快工程化产业化突破，研究推出适合不同应用场景的安全防护解决方案；支持通过众测众研等方式聚集社会力量，创新网络攻击防护、漏洞挖掘等安全技术。

（三）健全标准体系，引领国际规则

借鉴发达国家的有益经验，健全工业互联网垂直应用行业安全标准规范，超前布局能源、电力、交通、航空、航天等重点领域安全标准的研究制定。建议构建涵盖各部委、省市、企业，多方协同的工业互联网安全服务和保障支撑平台，统筹总体系统架构建设，建立全国统一的系统准入标准与接口，制定安全融合应用系列指南；建立并不断完善国家级工业互联网安全基础信息资源库，涵盖工业互联网所需的资产目录、通信协议、安全漏洞、恶意代码、工业安全防御处置建议策略等，同时构建信息情报资源共享机制和共享激励机制；加快《统一内容标签格式规范》（GB/T35304—2017）等已有国家标准的应用推广；围绕工业互联网设备、控制、网络（含标识解析系统）、平台、数据等方面安全需求，加快研究制定安全防护、测试、评估等国家和行业安全标准，建设安全技术与标准试验验证环境；在制定工业互联网安全标准时，应遵循国际惯例，衔接好其他国际标准，采取更加开放的态度，欢迎国外企业或专家参与；鼓励更多中国专家承担相关国际标准组织的职务和任务，大力支持专业机构、工业企业、安全企业等积极参与国际标准制定，推动工业互联网安全标准高水平“走出去”。

（四）加大扶持力度，激发中小企业发展活力

建议重视和鼓励工业和安全领域中小企业改革创新，提升经营能力和管理水平，加大对中小企业的政策和资金的扶持力度；支持中小企业开展基础研究和科技创新，参与关键核心技术研发和国家重大科技项目攻关；科学规划并加快建设中小企业创新创业基地、企业孵化园、科技孵化器等，促进中小企业产业聚集发展，提高产业集聚度；完善多元化投融资体系和试点应用的试错容错与风险对冲机制，发挥好信托、保险等投资基金作用；加强供应链、产业链上下游协同，发挥好行业“领头羊”角色，经济基础较好区域的龙头企业要先行将安全研究成果进行试点转化并评估效能，通过龙头企业带动配套中小企业的发展；鼓励和支持在相关地区实施帮扶策略，以项目方式为中小企业提供改造升级和创新活动的技术支持、服务转型、技术指导；引导和帮助中小企业配套软硬件设备、培训相关专业人员、引进先进创新成果，逐步培养中小企业核心竞争力，打造各类型企业协同发展的优势格局。

（五）构建协同生态，促进双循环格局形成

加强顶层规划，建立并完善我国工业互联网安全产业体系，引导地方政府、工业企业、科研机构、安全企业等核心参与者在产业体系中找准定位、精准发力、协同发展，共同支撑构建我国工业安全产业生态。建议面向国内外市场和不同领域产业链、供应链，构建统一规划的智能化、协同化、网格化的平台框架，提高安全可控能力；依托产业联盟、高端智库等力量，推动“政产学研用”深度融合，培育一批具有产业整合能力的龙头和特色企业；制定工业互联网安全人才发展规划，建立安全人才库、专家库，创新联合培养机制，挖掘和培养国家和企业亟需的复合型、实战型专有人才；加大对工业互联网安全相关国际赛事的支持和推广力度，创新赛事形式，增强赛事名次的含金量，广泛吸引国外选手和团队参赛；加强国际合作和区域布局，重点衔接“一带一路”倡议，同时深化与先进发达国家互动融合，鼓励并支持工业企业、安全企业进一步提升“走出去”的层次、水平和效益。

参考文献

[1] 徐晓兰. 工业互联网是经济高质量发展重要引擎 [N]. 科技日报, 2019-12-09(01).
Xu X L. Industrial Internet is an important engine of high quality economic development [N]. Science and Technology Daily, 2019-12-09(01).

[2] 张尼, 刘康如, 田志宏, 等. 工业互联网安全进展与趋势 [J]. 广州大学学报(自然科学版), 2019, 18(3): 68–76.
Zhang N, Liu L R, Tian Z H, et al. Progress and trend of industrial Internet security [J]. Journal of Guangzhou University(Natural Science Edition), 2019, 18(3): 68–76.

[3] 康双勇, 胡万里. 工业互联网安全技术研究及我国工业互联网安全产业发展情况分析 [J]. 保密科学技术, 2020 (5): 27–31.
Kang S Y, Hu W L. Research on industrial Internet security technology and analysis on the development of industrial Internet security industry in China [J]. Secrecy Science and Technology, 2020 (5): 27–31.

[4] 王新霞, 李璇, 陈意, 等. 工业互联网安全问题分析及对策建议 [J]. 智能建筑与智慧城市, 2020 (3): 76–77.
Wang X X, Li X, Chen Y, et al. Analysis of industrial Internet security problems and countermeasures [J]. Intelligent Building & Smart City, 2020 (3): 76–77.

[5] 李璇, 王新霞, 陈意. 工业互联网安全关键技术研究 [J]. 智能建筑与智慧城市, 2020 (4): 101–102.
Li X, Wang X X, Chen Y. Research on key technologies of industrial Internet security [J]. Intelligent Building & City Information, 2020 (4): 101–102.

[6] 郑忠斌, 王朝栋. 工业互联网安全技术现状与发展趋势 [J]. 价值工程, 2020, 39(32): 190–191.
Zheng Z B, Wang C D. The situation and development trend of industrial Internet security technology [J]. Value Engineering. 2020, 39(32): 190–191.

[7] 张君, 朱晨鸣, 魏珂悦. 工业互联网安全态势及防护对策研究 [J]. 数字技术与应用, 2020, 38(11): 163–165.
Zhang J, Zhu C M, Wei K Y. Research on industrial Internet security situation and protection countermeasures [J]. Digital Technology and Application, 2020, 38(11): 163–165.

[8] 张飞, 郭子梦, 孙晓辉, 等. 工业互联网安全及评测综述 [J]. 科技视界, 2019 (25): 120–121.
Zhang F, Guo Z M, Sun X H, et al. An overview on industrial Internet security and evaluation [J]. Science & Technology Vision, 2019 (25): 120–121.

[9] 王冲华, 李俊, 陈雪鸿. 工业互联网平台安全防护体系研究 [J]. 信息网络安全, 2019 (9): 6–10.
Wang C H, Li J, Chen X H. Research on industrial Internet platform security protection [J]. Netinfo Security, 2019 (9): 6–10.

[10] 刘晓曼, 董悦, 张瑜, 等.《工业互联网安全成熟度模型: 从业者指南》对我国的启示 [J]. 信息通信技术与政策, 2020 (2): 57–60.
Liu X M, Dong Y, Zhang Y, et al. *The IoT security maturity model practitioner's guide* and its enlightment for China [J]. Information and Communications Technology and Policy, 2020 (2): 57–60.

[11] 刘晓曼, 全湘溶, 李姗. 国外工业互联网安全发展概况 [J]. 保密科学技术, 2020 (5): 20–26.
Liu X M, Quan X R, Li S. An overview on the development of foreign industrial Internet security [J]. Secrecy Science and Technology, 2020 (5): 20–26.

[12] 刘晓曼, 靳文京, 李南. 美国工业互联网安全推进情况及对我国的启示 [J]. 信息通信技术与政策, 2019 (8): 81–84.
Liu X M, Jin W J, Li N. The advancement of American industrial Internet security and its enlightenment to China [J]. Information and Communications Technology and Policy, 2019 (8): 81–84.

[13] 傅扬. 国内外工业互联网安全态势和风险分析 [J]. 信息安全研究, 2019, 5(8): 728–733.
Fu Y. Security situation and threats analysis of industrial Internet in China and abroad [J]. Journal of Information Security Research, 2019, 5(8): 728–733.

[14] 肖琳琳. 国内外工业互联网平台对比研究 [J]. 信息通信技术, 2018, 12(3): 27–31.
Xiao L L. A comparative study on the industrial Internet of Things platform at home and abroad [J]. Information and Communications Technologies, 2018, 12(3): 27–31.

[15] 中国信息通信研究院, 工业互联网产业联盟. 2020年上半年工业互联网安全态势报告 [R]. 北京: 中国信息通信研究院, 工业互联网产业联盟, 2020.
China Academy of Information and Communication Technology, Alliance of Industrial Internet. Report on industrial Internet security situation for the first half of 2020 [R]. Beijing: China Academy of Information and Communications Technology, Alliance of Industrial Internet, 2020.

[16] 中国网络空间研究院. 世界互联网发展报告2020 [M]. 北京: 电子工业出版社, 2020.
Chinese Academy of Cyberspace Studies. World Internet development report 2020 [M]. Beijing: Publishing House of Electronics Industry, 2020.

[17] 工业信息安全产业发展联盟. 中国工业信息安全产业发展白皮书（2019—2020）[R]. 北京: 工业信息安全产业发展联盟, 2020.
National Industrial Security Industry Alliance. White paper on the development of China's industrial information security industry (2019—2020) [R]. Beijing: National Industrial Security Industry Alliance, 2020.

[18] 工业互联网产业联盟. 中国工业互联网安全态势报告 (2019) [R]. 北京: 工业互联网产业联盟, 2020.
Alliance of Industrial Internet. China industrial Internet security situation report (2019) [R]. Beijing: Alliance of Industrial Internet, 2020.

[19] European Union Agency for Cybersecurity. Industry 4.0 cybersecurity challenges and recommendations [R/OL]. Brussels: European Union Agency for Cybersecurity, 2019. (2019-05-20) [2021-03-14]. https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations.

[20] 工业互联网产业联盟. 工业互联网平台安全白皮书（2020）[R]. 北京: 工业互联网产业联盟, 2020.
Alliance of Industrial Internet. Industrial Internet platform security white paper (2020) [R]. Beijing: Alliance of Industrial Internet, 2020.

[21] 上海工业控制安全创新科技有限公司, 上海赛博网络安全产业创新研究院. 工业互联网安全白皮书 [R]. 上海: 上海工业控制安全创新科技有限公司, 上海赛博网络安全产业创新研究院, 2019.
Shanghai Trusted Industrial Control Platform Co., Ltd., Cyber Research Institute. White paper on industrial Internet security [R]. Shanghai: Shanghai Trusted Industrial Control Platform Co., Ltd., Cyber Research Institute, 2019.

[22] 灯塔实验室. 网络安全强国——以色列的工控安全之路 [EB/OL]. (2017-01-07) [2021-03-14]. http://plcscan.org/blog/2017/01/development-path-of-ics-cybersecurity-in-israel/.
Beacon Lab. Network security power: Development path of

industrial control safety in Israel [EB/OL]. (2020-06-22) [2021-03-14]. http://plcscan.org/blog/2017/01/development-path-of-ics-cybersecurity-in-israel/.

[23] Official Microsoft Blog. Microsoft acquires CyberX to accelerate and secure customers' IoT deployments [EB/OL]. (2020-06-22) [2021-03-14]. https://blogs.microsoft.com/blog/2020/06/22/microsoft-acquires-cyberx-to-accelerate-and-secure-customers-iot-deployments/.

[24] 工业互联网产业联盟. 工业互联网典型安全解决方案案例汇编V3.0 [R]. 北京: 工业互联网产业联盟, 2020.
Alliance of Industrial Internet. Industrial Internet typical security solutions case collection V3.0 [R]. Beijing: Alliance of Industrial Internet, 2020.

[25] 赛迪顾问股份有限公司. 中国网络安全发展白皮书（2019）[R]. 北京: 赛迪顾问股份有限公司, 2019.
CCID Consulting Co., Ltd. White paper on China's cyber security development (2019) [R]. Beijing: CCID Consulting Co., Ltd., 2019.