

# 筑盾工业互联网安全 护航高质量发展大计

## —《加强工业互联网安全工作的指导意见》系列解读之二



中国电子技术标准化研究院副院长 杨建军

伴随着互联网、大数据、人工智能与实体经济的深度融合,以工业互联网为典型代表的新一轮科技革命正不断重构产业发展格局。工业互联网继承了传统互联网的实体低成本连接、信息高效率流通等特点,同时又在体系结构、传输内容、网络边缘等方面具有自身特色,承载着助力制造业高质量发展、经济社会创新发展的新使命,是推动“制造强国”和“网络强国”建设的关键支撑。但同时我们也应清醒地认识到,目前其发展仍处于探索过程中,还有很多不成熟、不完善之处,其中网络安全问题便是面临的新挑战之一。传统互联网安全保障体系已难以完全应对新时代需求,亟需从制度机制、技术手段、数据保护和产业发展等方面入手,加快构建涵盖设备安全、控制安全、网络安全、平台安全和数据安全的工业互联网多层次安全保障体系,为“两个强国”战略实施提供坚实保障。

工业互联网具有传统信息系统和工业控制系统的双重属性,在其快速发展推进过程中,面临各种叠加安全风险的威胁。

## 网络安全保障能力建设迫在眉睫

工业互联网具有传统信息系统和工业控制系统的双重属性,在其快速发展推进过程中,面临各种叠加安全风险的威胁。当前工业互联网安全保障能力建设还存在一些突出问题,主要表现在:一是工业互联网安全技术手段不足。早期的工业控制系统在相对独立的网络环境下运行,产线规划只考虑功能性和稳定性,对网络安全性要求较低。随着工业设备联网数量越来越多,通过互联网对工业控制系统实施攻击的可能性越来越高,传统工业控制系统和新兴工业互联网平台安全

技术手段不足的短板越来越凸显。二是工业互联网安全责任落实尚不够明确。工业互联网覆盖行业广泛、平台种类繁多、服务类型丰富、涉及企业众多,目前尚未完全落实主管部门、平台企业和工业企业等的责任分工。主管部门应履行安全监督管理职责,平台企业应明确在工业互联网安全保障方面的责任和义务,工业企业应明确关键设备和数据资产,并在接入平台前开展安全风险测评。三是工业互联网安全管理制度缺失。当前我国陆续出台《关于深化“互联网+先进制

造业”发展工业互联网的指导意见》《工业互联网发展行动计划(2018—2020年)》等文件,为工业互联网发展提供顶层政策指导,但工业互联网企业在实际开展平台安全设计、建设、运维等活动中,仍然存在安全管理活动缺乏统筹规划、相关部门组织间协调不畅、安全管理制度建设严重滞后等问题。四是工业互联网安全标准体系亟需完善。目前,我国网络安全标准体系已较为成熟,但针对工业互联网安全的专门的标准体系尚待完善,已立项研制《信息安全技术 工业

《指导意见》不仅是工业互联网安全工作的纲领性指引,更是强化安全保障体系建设、各部门协同发力的重要举措。

## 加快构建层次化的安全保障体系

日前,工业和信息化部联合教育部、人力资源和社会保障部、生态环境部、国家卫生健康委员会、应急管理部、国有资产监督管理委员会、国家市场监督管理总局、国家能源局、国防科技工业局等十部委共同印发了《关于加强工业互联网安全工作的指导意见》(以下简称《指导意见》),明确提出了构建工业互联网安全保障体系的总体要求、主要任务以及保障措施,指出要按照《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》有关要求,围绕设备、控制、网络、平台、数据安全,落实企业主体责任、政府监管责任,健全制度机制,建设技术手段,促进产业发展,强化人才培养,构建责任清晰、制度健全、技术先进的工业互联网安全保障体系。《指导意见》不仅是工业互联网安全工作的纲领性指引,更是强化

安全保障体系建设、各部门协同发力的重要举措,为切实推进当前工业互联网安全工作指明了方向。

在制度机制方面,我们应加强顶层设计,出台工业互联网安全指导性文件,建立健全监督检查、信息共享和通报、应急处置等工业互联网安全管理制度,明确企业主体安全责任;建立分类分级管理机制,制定工业互联网行业企业分类分级指南,对重点企业实施差异化管理;发挥标准规范引导作用,编制工业互联网安全标准体系建设指南,加快制定设备、平台、数据等层面亟需的工业互联网安全标准;针对工业互联网平台企业、工业生产企业、工业APP和联网设备开展安全能力评估和认证,探索构建工业互联网设备、网络和平台的安全评估认证体系。

在技术手段方面,应加快建设国家、省、企业三级协同的工业互联网

安全技术保障体系,包括国家工业互联网安全技术保障平台、安全基础设施库和安全测试验证环境等共性支撑基础,提升工业互联网安全综合管理和保障能力;针对标识解析系统、工业互联网平台、工业控制系统、工业大数据等方面的安全需求,要加强攻击防护、漏洞挖掘、态势感知、安全审计、可信芯片等关键技术及安全产品的研发攻关力度,强化设备、控制系统、网络设施、平台和工业APP等安全保障,建立与产业发展相匹配的核心安全技术能力。在数据保护方面,应规划建立工业互联网全产业链数据安全管理,明确数据收集、存储、处理、转移、删除等全生命周期各环节的安全保护要求,提升企业在数据防窃密、防篡改和数据备份等方面的安全防护能力,鼓励商用密码应用于工业互联网数据保护工作;建立工

业互联网数据分级分类管理制度,形成数据流动管理机制,明确数据留存、数据泄露通报要求,加强工业互联网重要数据安全监测和管理,有效提升工业整体性数据安全能力,在实践中逐步形成健全的数据安全保护体系。

在产业发展方面,应整合行业资源,依托国家级、省级网络安全产业园等形式,发挥市场主体作用,打造产学研用协同创新发展平台,培育一批具有核心竞争力的工业互联网安全企业,形成工业互联网安全对外展示和市场服务能力。针对汽车、电子、航空航天、船舶、能源等重点领域,研发创新实用的安全产品并形成整体安全解决方案,组织开展工业互联网安全试点示范,遴选优秀安全解决方案和最佳实践,并加以应用推广,提升行业整体安全保障服务能力。

建议从“放管服”改革、标准化服务、保障措施落实、明确安全责任等方面综合施策,加快提升我国工业互联网安全保障能力水平。

## 全面落实工业互联网安全各项任务部署

根据《指导意见》的总体部署要求,结合当前我国工业互联网安全现状,建议从“放管服”改革、标准化服务、保障措施落实、明确安全责任、强化人才培养等方面综合施策,加快提升我国工业互联网安全保障能力水平:

一是落实“放管服”改革,激发企业自主安全意识,去行政化管理,以标准化服务提供安全保障。深刻总结网络安全监管行政命令模式的不足与弊端,切实以深化“放管服”改革思想为实践指导,激发企业做好工业互联网安全工作的自主意识,围绕工业互联网的安全防

护、检测、响应、恢复、预警、追踪、测评、认定等实际市场需求,建设完善管理机制,形成对应的技术标准、实施指南、示范案例,为产业界提供包括标识解析系统安全、终端安全、边界安全、平台安全、数据安全、工业云安全在内的标准化、体系化服务支撑。

二是强化网络安全保障“全国一盘棋”的整体观思想认识,落实保障措施及安全责任,力戒“形式主义”防护。借鉴传统互联网安全治理经验,统筹好生态环境、卫生健康、能源、国防科工、应急管理等部门职责分工,

在各行业、各领域、各地区内各司其职、协同配合,做好指导与监管工作,各级监督检查要能够真正发现问题、查清问题,切实帮助企业进行整改,提升安全保障硬实力;同时,企业自身要提升思想认识,切实将工业互联网安全防护措施部署到位,将安全责任合理的落实到人,优化安全管理结构及技术方案,避免安全防护手段流于“形式化”“走过场”。

三是加快从建设规划、运维保障、监督检查三个方面同步强化人才培养工作,实现安全工作“提质增效”。在网络安全领域,我国一

百度近期宣布战略投资大连东软控股有限公司(以下简称“东软控股”),投资金额总计14.43亿元,双方达成战略合作伙伴关系,将在智慧城市、智能教育、智能医疗等关键领域推进产业智能化变革,同时,百度CTO王海峰将出任东软控股董事。而在此前的3月1日,百度宣布以5.5亿元收购汉得信息5.26%的股权,两家达成战略协议,共同拓展工业制造、金融、教育、医疗等领域的机会,具体落地的是百度2B的核心业务——百度ABC智能云。百度为何注资东软、汉得?东软、汉得之后,百度还有可能再投资谁?未来百度的2B之路会怎么走?

## AI工业化渐行渐近 百度2B之路怎么走

本报记者 李佳师

### 为何撒钱东软和汉得?

为什么是东软和汉得?资料显示,汉得信息成立于1996年,是首家以ERP咨询实施为主的A股上市公司,定位为“数字化生态综合服务商”,已为3000多家企业提供信息化服务,在制造业、金融、贸易、电子商务、房地产等沉淀有大量客户。汉得拥有超过7000名专业咨询人员,并在日本、新加坡、美国等设有子公司。而东软控股是一家专注于信息技术、医疗健康和教育培训的高科技投资与管理企业,是东软集团、东软教育科技、东软医疗、东软熙康、东软望海等公司的主要投资者,布局涉及医疗健康及社会保障、智能汽车互联、智慧城市、企业互联、医疗设备、云医院、教育事业等多个行业。

从这两家企业来看,有两个共性。

其一是有丰富的行业客户行业场景资源。汉得的制造业、金融、贸易、电子商务、房地产与东软的医疗健康及社会保障、智能汽车互联、智慧城市、企业互联、医疗设备、云医院、教育等行业,都是产业互联网时代的市场“富矿区”,都是百度的AI未来想落地产业互联网市场的重点场景。

其二是这两家企业有丰富的行业经验和行业解决方案,能够与百度的AI产品进行快速融合,创造出“智能化”的行业解决方案。比如东软在医疗与教育领域的多年积累创造的解决方案,东软的渠道、医疗IT资源、医疗解决方案与百度的AI能力融合,就有可能创造出智慧医院、智慧教育的解决方案。截至2018年末,累计服务医院客户2500余家,三级医院近500家,社保业务覆盖人群超过7亿人,这些资源是百度迫切需要的。

又比如在工业领域,汉得的行业化、场景化知识以及现场经验孵化出来的大量解决方案,与百度在AI领域的技术能力进行融合,就可以在工业质检领域形成新的解决方案,创造新的商业模式。事实上,机器视觉在制造业有巨大的应用空间。在8月29日百度举行的“ABC SUMMIT 2019百度云智峰会”上,来自江苏常州市的制造业企业精研科技,分享了其利用百度智能云技术打造的智能质检设备,解决了过去主要靠“肉眼+放大镜”来检测的痛点的故事,采用该方案能同时检测6个零件面的33种缺陷,将漏检率控制在0.1%内,设备投资回报率则达到了传统机型的6.5倍。

行业解决方案的AI化有巨大的市场,如果行业方案AI化能够在这两家企业试点成功,那么这些经验可以快速复制到各个行业,快速打开百度的行业市场。而行业解决方案的AI化决不是简单的方案捆绑,其背后有大量的联合研发技术的融合,而且在产品的服务方式、商业模式上也有大量需要探索的地带。也正因为如此,百度才需要选择以注资的方式,成为这两家公司的大股东或董事,以这样的紧密合作方式来获得更高的

话语权,使得行业解决方案的AI化得以顺利落地,形成示范案例快速推广复制。

### 2B转型之路提速

从消费互联网到产业互联网的转型,尽管BAT三家都非常重视AI,但百度是将AI看得最重的公司,所以业界用“押宝AI”来称百百度的转型。如果说前几年百度将AI聚焦在“技术”,经过几年的发展,那么接下来百度的重点必然是AI“落地”。就像李彦宏所言:“在产业智能化大潮来临之际,我们要做的就是扎实地推进人工智能在各产业的渗透”。

9月2日,李彦宏发布内部信宣布进一步升级“云+AI”战略,提高百度智能云的战略地位。自此,百度智能云与CTO体系融合,公司副总裁、百度智能云总经理尹世明携团队向集团首席技术官王海峰汇报。李彦宏在内部信中表示,百度智能云事业群组(ACG)是百度AI产业智能化落地的“排头兵”。这次组织架构的升级,是公司进一步升级“ABC智能云”业务战略的重大举措,有利于加速TG中台战略实施过程中积累的底层技术能力向云输入,更有利加速AI能力的商业化,让技术更直接更有效率地在云平台上支撑业务。

在8月底举行的“ABC SUMMIT 2019百度云智峰会”上,百度智能云发布了AI工业化智能公式,这个公式表明,智能计算和智能应用相互交叉促进,通过智能生态实现指数级的发展,将实现人工智能的工业化。在这次峰会上,百度智能云一口气发布了18大智能计算新产品。

百度副总裁、智能云事业群组总经理尹世明表示,人工智能正在进入工业化进程。而智能应用是AI工业化中的关键因素,从视觉智能、对话智能再到数据智能,当数据可以安全合规且开放融合地跨越边界,将产生更多可以标准化、规模化复制的场景。

百度推进AI工业化,从观察来看,收购和注资拥有多年行业积累和行业资源的IT服务提供商是路径之一。除了东软和汉得,百度应该还会和更多的行业解决方案软件企业联手。

而另一个路径是联手头部客户,探索行业AI解决方案和AI方法论。比如百度智能云联合浦发银行推出了金融领域的“数字人”员工小浦;与重庆市气象局联合打造了“智慧气象”系统,用云+AI让“天气”不再难测;和央视打造了AI编辑部等等。

再有一个路径是以生态的方式加速AI产业化的“枝繁叶茂”。在“ABC SUMMIT 2019百度云智峰会”上百度智能云宣布推出人工智能生态联盟——百度产业智能联盟,并展现面向制造行业的子生态领航俱乐部。目前,百度智能云的产业智能化生态中已经拥有数千个合作伙伴,共同建设产业智能化生态圈。

眼下BAT都在2B的赛道上纷繁狂奔,百度从注资到联手头部用户再到加速生态枝繁叶茂,能否后来居上,超越腾讯与阿里,我们等待时间给出答案。