数字时代需筑牢工控系统“安全堤”

本报记者 宋婧

近日，一个自称黑暗面（DarkSide）的团体因攻击美国科洛尼尔管道运输公司（Colonial Pipeline），导致美国能源基础设施遭遇了有史以来最具破坏性的网络攻击。美东多州宣布进入紧急状态，在国内掀起了囤油热潮。最终，Colonial Pipeline公司不得不向黑客支付了440万美元赎金。

此后不久，日本科技巨头东芝的一家子公司公开承认受到“DarkSide”勒索软件袭击，超过740GB的数据被窃取，包括护照扫描和其他个人信息。

另据最新消息，美国最大的保险公司之一（CNA Financial Corp.）也因遭遇勒索软件攻击，被迫支付了4000万美元赎金，以重新获得对其网络的控制权。该公司已确认这起攻击的实施者是一个名为Phoenix的组织。

自2010年伊朗“震网”事件爆发以来，世界范围内针对工业信息系统的网络攻击事件愈演愈烈。关系到国家关键基础设施建设、国防安全和经济安全的工控系统已成为网络攻击重点目标。面对数字时代新形势，应该如何筑牢工控系统的安全堤坝？在近日召开的2021第四届工业安全大会上，来自各行各业的专家对此进行了深入探讨。

可信计算提高工控安全“免疫力”

为了安全，必须从逻辑正确验证、计算体系结构和计算模式等方面进行科学计算创新。

一直以来，国家工控系统网络安全都是一场没有硝烟的战争。“考虑到工控系统的脆弱性和工业应用场景的特殊性，传统网络安全防护手段已经难以满足工业控制系统安全需求。”宁波和利时信息安全研究院有限公司方案总监穆雷霆指出。

中国工程院院士沈昌祥介绍称，由于人们对IT的认知逻辑的局限性，不能穷尽所有组合，只能局限于完成计算任务去设计IT系统，必然存在逻辑不全的缺陷，从而难以应对人为利用缺陷进行的攻击。因此，为了安全必须从逻辑正确验证、计算体系结构和计算模式等方面进行科学计算创新，以解决逻辑缺陷被攻击者所利用的问题，形成攻防矛盾的统一体。确保为完成计算任务的逻辑组合不被篡改和破坏，实现正确计算，这就是主动免疫防御。可信计算为构建主动免疫防御架构提供了技术支撑。

可信计算是指计算运算的同时进行安全防护，全程可测可控，不被干扰，是一种运算和防护并存的主动免疫的新计算模式，以密码为基因，实施身份识别、状态度量、保密存储等功能。它可以及时识别“自己”和“非己”成分，从而破坏与排斥进入机体的有害物质，相当于为计算机信息系统培育了免疫能力。

穆雷霆称：“工业网络安全应基于可信计算等主动防御技术，通过控制系统内嵌可信计算防护体系，可实现主动识别、主动度量和主动保护功能，增强自身防护能力。”

“网络空间已经成为继陆、海、空、天之后的第五大主权领域空间。没有网络安全就没有国家安全，安全是发展的前提。”沈昌祥指出，“网络空间安全是计算科学问题，是体系结构问题，也是计算模式问题。经过长期攻关应用，我国形成了自主创新安全可信体系，完备的可信计算3.0产品链，将形成巨大的新型产业空间。”

风险评估是安全状态的试金石

风险评估工作需要在网络安全法律法规和标准要求下，根据工业控制系统实际特点，针对性开展评估工作。

根据工控典型风险评估案例分析，工控系统目前面临十大主要安全风险，涉及网络架构、工控协议、安全基线、安全漏洞、威胁感知、人员机构、安全管理、接入管理、物理环境、运维记录等多个方面。工控系统安全不仅需要核心技术支撑，还需进一步加强安全防护能力建设，风险评估首当其冲。

国家信息技术安全研究中心牵头、参与了核电网络安全大检查、某大型枢纽网络安全验收、工业互联网分类分级试点、车联网网络安全检测评估、数控机床网络安全检查等几十项专项任务。通过对核电领域DCS系统、油气管道SCADA系统、智能制造DNC系统的对比分析发现，各类系统基本都会存在服务器机房或控制器节点位置等物理环节风险。部分安全防护意识较差的机构，未将工控系统纳入企业网络安全管理体系或网络安全防护规划建设中，且未设专门人员负责工控网络安全。此外，数据安全与技术防护方面也存在欠缺。

为此，国家信息技术安全研究中心总工程师王宏指出，工业控制系统涉及领域广、业务场景丰富，系统类型差异巨大，因此，风险评估工作需要在网络安全法律法规和标准要求下，根据工业控制系统实际特点，针对性开展评估工作。同时，要将目标系统模拟仿真环境测试与实际系统评估相结合，将未知漏洞挖掘与已知漏洞对标两种检测途径相结合，加强评测环境选择合理性。另外，要加强技术手段选择的有效性，基于多种手段开展综合评估，保障评估的有效性与完整性。

“网络安全本质上是动态的平衡，没有百分百的安全，也没有一步到位的解决方案，它永远在路上。风险评估是安全状态的试金石，只有不断发现目标系统的安全风险，才能促进系统网络安全防护良性循环。”王宏谈道。

贯标是工控安全政策标准落地、落实的基础，旨在为工控安全防护领域提供技术、标准、人才等方面支撑。中国电子技术标准化研究院高级工程师李琳指出，要进一步提升工业企业工业控制系统信息安全防护水平，服务制造业高质量发展，应该在学习借鉴两化融合贯标、数据管理能力成熟度评估等先进经验基础上，以贯标为抓手，推动工业企业工业信息安全防护工作的开展。

工业互联网数据安全亟待加强

进入数字时代，工业互联网数据成为提升制造业生产力、竞争力、创新力的关键要素。

进入数字时代，工业互联网数据日益成为提升制造业生产力、竞争力、创新力的关键要素。然而，在互联开放的环境下，网络攻击路径增多、难度降低，这导致数据安全风险进一步加剧。与此同时，新一代信息技术的广泛应用与渗透，带来了包括深度伪造、数据污染等在内的全新的数据安全风险。从数据采集、数据传输、数据存储、数据使用的全生命周期各个环节来看，工业数据安全风险无处不在。

如何加强互联网数据安全防护？国家工业信息安全发展研究中心标准质量处处长陈雪鸿认为，工业互联网数据进行分类分级防护刻不容缓。应从工业互联网数据全生命周期各环节，细化防护方位及内容，从工业互联网数据分类分级、通用安全、一级数据安全、二级数据安全、三级数据安全等方面的不同防护要求进行治理。

“未来是高度数字化的数字孪生世界，网络安全风险遍布数字化所有场景。”360政企安全集团助理总裁兼工业安全事业部总经理李航谈道，“传统安全思路还停留在碎片化产品层面。我们应以工业数据为核心、资产为基础，通过‘白+黑’的技术手段，打造工业安全‘三位一体’的纵深安全运营防护体系。”

美国历史学家克拉克教授曾经说过：“人类历史上只发生过一件事情，那就是工业革命。”现如今，中国已经到了从要素密集型、规模型的重工业，向智能化、信息化、服务化的高端制造、智能制造转型的新阶段，工业安全成为一个绕不过去的重要话题。数字时代新形势下，应该如何筑牢工业控制系统“安全堤”？长路虽漫漫，但未来仍可期。

我国泛工业领域数字化转型发展潜力巨大

电气电子工程师学会（IEEE）院士
傲林科技董事长 刘震

数据显示，2020年我国数字经济规模达到39.2万亿元，占GDP比重为38.6%；数字经济增速达到GDP增速3倍以上，成为稳定经济增长的关键动力。有数据显示，2020年，数字经济进一步发展，我国数字经济规模占GDP比重已近四成，对GDP贡献率近七成，预计2021年将进一步增至47.56亿元。在此背景下，数字化转型成为各大产业的发展之重。在这个过程中，数据智能、工业互联网在其中充当着什么样的角色？会遇到哪些具体的挑战与机遇？数字经济未来的发展潜力有多大？

2021年将是“数智化时代”元年

中国数字经济的发展潜力巨大。首先，中国现在的数字经济占GDP的比例与欧美先进国家相比还有很大距离。目前我们是36%~40%，而英、德、美等欧美国家已经达到60%。其次，我国的GDP组成中，金融、IT以及零售行业数字化程度比较高。零售行业占GDP大概2%左右，但其中就涌现出了像阿里、京东这些巨头。但泛工业占GDP的比例是52%，这52%尚处在实现数字化转型早期，可见数字经济发展空间非常巨大。

埃森哲《2020中国企业数字转型指数研究》显示，85%的受访企业高管表示，希望能够在一年内看到数字化转型的效果，43%的企业希望在6个月就能够看到数字化转型的效果。而两年前IDC针对中国1000强企业做的一个调研显示，有50%以上的企业表示数字化转型是他们的重要战略。可见整个市场对数字化转型已经有一个很好的认知。

国资委在2020年下发《关于加快推进国有企业数字化转型工作的通知》，专门鼓励央企、国企带头做数字化转型。工业和信息化部也在今年1月印发了《工业互联网创新发展行动计划（2021—2023年）》，要求所有的企业加强工业互联网的建设，特别是加强其中的数字化管理。

因此，从市场和政策两个层面来看，2021年将是“数智化时代”的元年。

工业互联网建设从数字化到“数智化”

数字化转型主要包括两大部分。第一是业务数字化。也就是说在业务中把数据抽取出来，然后通过数据的整合来做分析，对整个业务有所洞察，业务的数字化要通过工业互联网来做。第二是数字业务化。这需要借助数据智能的技术。数据智能指的是人工智能和大数据的融合，也就是用大数据把人工智能的算法模型与应用范围做得更好。首先要把抽取出来的数据建成模型，建模后进行模拟仿真，做预测、优化，使得决策者能够通过数据作更准确的、更好的、更靠前的决策。

工业互联网作为工具，对数字化转型起到至关重要的作用。我们在实践中发现并主攻工业互联网的五大挑战。

第一是数据维度扩大。数字化转型需要把不同数据源的数据都整合在一起，打通数据孤岛。这需要把数据进行统一分析、统一建模。

第二是应用范围越来越广。原来的人工智能基本上就是人脸识别、语音处理、语言的人机对话等，这些几乎是To C的业务。现在我们看到更多的是人工智能在To B领域的应用，这个应用范围就大得多，场景也多得多，涉及各行各业。

第三是人工智能应用深度加大。除了人脸识别、语音识别等认知服务，人工智能还需要进行预测、预警，这就要求数据能够做更深入的分析，要把所有的历史数据进行考量与分析规律。

第四是全局化的优化。原来大家看到更多的是局部优化。针对某一个工艺点、某一个工序、某一个小场景来做应用。对企业来说，现在更重要的是全局化的优化。要把“供产销”的经营铁三角进行协同，更好地提升企业的经营效益。

第五是智能化的系统化。这个数智化系统主要是给决策者做辅助决策用。相当于是给决策者配备了一个大脑，真正做一个企业级的大脑，而且这个企业级大脑要不仅能够管好企业所有的部门、业务与流程，同时要做好上下游协同，能灵活应对外围市场。

工业互联网企业应根据自己的特色找准定位

工业互联网的蓝海中，很多初创企业不断涌现。短短三四年之内就出现了数以百计的初创企业，光是平台级的、具有较强行业和区域影响力的工业互联网企业就有100多家，而且这100多家企业已经连接了7000万台设备，另外还有59万个工业APP出现。这么短的时间内，工业互联网有这么广泛的普及是一个很好的现象。

但正因为是在一个大海里，大家要特别注意，不能迷失方向，每个初创企业都要根据自己的特色找准定位。

这个领域有点像人工智能，就是所有的技术实际上都会有一定的波谷。人工智能在过去的60年里已经出现了两个冬天，工业互联网领域也需要投资者有耐心。工业互联网是一个很好的赛道，但是任重而道远。

在工业企业里，所有的变革都需要耐心，要细细地将产品打磨出来。To C可以通过市场效应瞬间铺开，但是To B需要在行业里细致地做好自己的工作。

同时，也要认识到，工业互联网建设会产生海量数据。一方面，这些数据需要高质量的数据治理；另一方面，数据的安全隐私是一个很重要的问题，从法律角度而言，一些欧美国家有专门的法律法规，中国也有《数据安全法（草案）》，这些法律法规会在数据的安全和保隐私保护上起到很好的作用。

2021年，阿里云打“大数据”+“AI工程化”新牌

本报记者 李佳师

企业数字化转型进入深水区，需要供给侧进一步升级其产品与服务。如果说前几年各云计算厂商的核心是“云”，那么进入2021年，“数”+“智”就成为各家云厂商产品与服务的“主力军”。近日，阿里巴巴副总裁、阿里云计算平台负责人贾扬清在媒体沟通会上表示：“要想真正把数据用起来，需要‘大数据’+‘AI工程化’。”

大数据大家并不陌生，各厂商已经推动数年，而“AI工程化”则是新趋势。去年年底，Gartner将“AI工程化”列为2021年度九大重要战略科技趋势之一。Gartner认为，目前只有53%的项目能够把AI技术转化为生产力。由于缺乏创建和管理生产人工智能管道的工具，AI项目的扩展难度很大。为了将AI转化为生产力，就必须转向人工智能工程化这门专注于各种人工智能操作化和决策模型治理与生命周期管理的学科。

推进AI工程化，目前不同厂商有不同的理解和不同的路径。贾扬清认为，“AI工程化”从供给角度看，它是数据和算力的云原生化；从核心技术角度看，它是调度和编程范式的规模化；从需求或者出口的角度看，它是开发和服务的标准化普惠化。

为此，阿里云机器学习平台PAI构建了灵活、易用和功能丰富的机器学习全栈产品：PAI-Studio（可视化建模平台）、PAI-DSW（云原生交互式建模平台）、PAI-DLC（云原生AI基础平台）、PAI-EAS（云原生弹性推理服务平台）。

对企业来说，工程化已经超越算法，成为AI落地的更大瓶颈。日前，阿里巴巴与清华大学合作发布了超大规模中文多模态预训练千亿参数模型M6。该模型的数据集包含超过1.9TB图像和292GB文本，参数规模达到1000亿，可完成产品描述生成、视觉问答、问答、中国诗歌生成等跨模态任务。目前，M6已经用于业务场景里。“我们希望将M6的场景化服务能力开放给所有企业。”贾扬清表示。

要把AI转化为生产力，不仅要懂AI更要懂行业。阿里云机器学习平台PAI以电商、金融、游戏、直播等业务为起点，在智能推荐、用户增长、金融风控、音视频文本等多模态场景积累了丰富的实战经验，沉淀了大量成熟算法、框架及工程化组件等“原子能力”，帮助开发者及企业客户更快地孵化和构建新场景业务。

“大数据和AI密不可分，结合在一起，更能帮助企业在数字时代从容应对不确定性。”贾扬清表示。从大数据的维度看，经过近20年的发展，大数据已从早期的数据挖掘进化为承载数据分析、数据管理、数据协同功能的综合治理平台。