

中国工程院院士邬贺铨：

工业互联网安全挑战不是静止的 搭建安全保障体系势在必行

本报记者 徐恒

工业互联网安全工作 永远在路上

邬贺铨认为，工业互联网的安全需要通过IT与OT融合来保障，要善于运用大数据、人工智能和区块链等技术来助力工业互联网安全的保障。同时，工业互联网的安全需要管理与技术并重，企业的安全要与行业的安全和社会的安全实现威胁情报共享与协同联动。只要行业重视、技术采用得当，工业互联网的安全还是可控的，但安全挑战不是静止的，工业互联网的安全工作永远在路上。邬贺铨建议，搭建工业互联网安全保障体系，其中涵盖企业平台、省级平台和国家平台三个级别。

据介绍，工业互联网涵盖物联网通信/传感网、工业以太网/时延敏感网络、企业内网和外网等多个网络，安全更复杂、形势更严峻。

“5G、物联网、大数据、云计算和人工智能技术在工业互联网的应用，推动了企业数字化转型，但也带来安全领域新的挑战，工业互联网的安全形势较消费互联网更严峻。”6月21日，中国工程院院士邬贺铨在2019中国工业信息安全大会上表示。

工业互联网涉及的大量的传感器、物联网终端、边缘计算、数字孪生、工业软件等都存在被黑客攻击的风险。

三点措施

保障工业互联网安全

对此，邬贺铨提出了一些对策。一是可以利用大数据技术发现工业互联网威胁隐患。系统利用大数据技术可以根据用户上网的操作习惯，检测用户的异常行为，及时发现用户偏离日常行为所隐藏的潜在危险。基于大数据挖掘技术发现大量新的网站攻击

特征，溯源定位攻击源，将威胁发现范围扩展到包括数据资产、软件资产、实物资产、人员资产、服务资产和其他为业务提供支持的无形资产。另外，大数据技术还特别适合用作高级持续性威胁（APT）的检测和取证。

“工业企业应全面掌握工业资产、工业网络安全威胁、工业生产异常和故障，才能解决资产数量、类型、分布不清楚，设备断线、设备停机、异常操作难定位的安全问题。”邬贺铨表示。

二是利用AI提高处理信息安全的效率。“AI的典型作用是代替人类做大量重复的劳动，利用AI技术一分钟就能完成一个信息

安全分析师一年分析数据和代码的工作。AI对网络安全的直接贡献是提高了处理效率。”邬贺铨表示。

据介绍，AI可对网络流量内外所包含的无数元数据所存在的成千上万个关联进行分析，实现对网络流量异常检测。AI技术可将包括企业运营日志数据和外部威胁情报服务在内的多个信息源整合分析，具备处理上百万数据点以及生成预测的能力，获得最准确的网络风险评估。大量伪装成可执行文件（.exe）、PDF文档和微软Office文档的恶意软件是“钓鱼攻击”和僵尸网络最常见的攻击渠道，AI技术可用来侦测可疑文件。

三是实时威胁情报共享机制可保障工业互联网的安全。企业除了要在内部建立IT与OT统一的安全团队和企业安全运营中心外，还要与上下游合作伙伴实现威胁情报共享和安全防护协同联动机制，同时还要从政府方面获得安全态势感知信息。

SAP全球CEO孟鼎铭：

云之后的下一个 趋势是体验经济

目前，全球经济发展充满了诸多不确定性，逆全球化趋势抬头，在这样的背景下企业该如何完善全球产业链、进行全球化的布局？最近，云计算领域发生了很多大的并购案，接下来云计算产业发展会有哪些趋势性的改变值得我们关注？SAP全球CEO孟鼎铭（Bill McDermott）6月20日参加在北京举行的“全球首席执行官委员会”第七届圆桌峰会，在此期间接受了《中国电子报》等8家中国媒体的采访，透露了诸多他执掌SAP公司期间大并购的关键细节、对全球经济的判断以及云计算产业趋势分析。

本报记者 李佳师

全球化

是唯一成功路径

中美贸易摩擦带来了诸多经济不确定性，逆全球化有抬头趋势，在这样的背景下，企业应该怎么样布局，是收缩还是继续扩张？

孟鼎铭表示，全球化是最好的一条道路，这些年全球化取得了非常大的成绩，而今天出现贸易摩擦带来的艰难他并不意外。“我认为所有的挑战都有可能转化为机遇，中美两大经济体有非常多的理由携手合作，而合作很重要的一点是信任。我相信中美之间也不再需要太多的时间谈判和交流，一方面全世界都在看着，另一方面全世界需要中美最终能够携手合作。因为未来的大势是合作创新，合作创新不仅对于中美两国重要，对于全世界都一样重要。”孟鼎铭说。

孟鼎铭进一步表示，逆全球化是一种严重低效做法，所带来的挑战包括了供应链错位，重新布局供应链，时间和成本都将大大增加。比如有的企业原来整个生产链条都可以在中国完成，现在为了向美国市场出口，不得不将生产任务拆分到世界不同的地区去，再组合起来，最后再向美国市场出口。

下一个趋势

是体验经济

目前，IT产业进入了云计算时代，在这一轮转型中，所有及时踏上云计算这辆“战车”的公司大都转型成功，SAP也是企业级IT企业中及时向云转型成功的企业之一。孟鼎铭2010年就任SAP公司CEO，这几年他一共操刀了SAP公司700多亿美元的并购，那么他是在什么时间点意识到SAP必须转型，又是在什么时间节点明确了云是转型方向的呢？最近，云计算领域发生了很多大的并购案，从技术革新的角度看，云计算之后的下一个浪潮会是什么？

孟鼎铭透露，2010年他被任命为公司的联席CEO，而当时的SAP是全球应用和分析工具市场的领军者，全球应用和分析工具市场当时的市场规模是1100亿美元，SAP即便是做到了极致也可以看到市场的天花板就是1100亿美元，没有更多的空间。“而当时我判断未来发展有三个趋势：云计算、智能移动终端和大数据。

如果进入这个市场，我们将能够翻几番，市场规模是4500亿美元。于是我们决定转向这个市场，并购这个领域中最好的云计算资产，而且是在其他人还没有意识到的时候，快速完成这些收购。”孟鼎铭说。

其后SAP推出了HANA内存数据平台，把ERP和S/4HANA进行了整合，开始了云端基础架构的补充，全面迈向云的世界。

关于云最近发生了很多大的并购案，而事实上这样的并购不会停止，因为孟鼎铭认为，云计算是21世纪最主要的计算方式。不同的行业、不同的公司面对的环境不一样，公司规模、类型不一样，上云过程中的复杂性、难度也不一样，所以需要各种各样的

云，对于云的需求和消费方式也不一样，所以要按用户喜欢的时间、喜欢的方式给用户提供云，云的世界会变、创新也会变，并购还会继续不断发生。

“而在我看来，不管是上云还是不上云，其实这都不是本质，也不是核心，这个世界的核芯是创新，而云是高效、低成本创新的平台。”孟鼎铭说，“因为云一方面使企业创新的成本大大降低，另一方面使创新的周期大大缩短。”

而云之后的下一个浪潮，应该是体验经济。孟鼎铭认为，目前世界上有80%的CEO认为他们所做的工作是让客户满意，但其实只有8%的客户认为得到了满意的服务，而这其中的差距就是1.6万亿美元的商机，客户体验经济的市值达到1.6万亿美元。所以，未来所有的信息技术的变革都将是朝着创造更好的体验经济这个方向进行演变。为此，SAP推出了Qualtrics解决方案，它是面向体验经济的解决方案。

中小企业

有强烈长大渴望

目前，中国经济遇到一些波折，比如房地产、汽车等这些市场出现不同程度的下滑趋势，孟鼎铭如何看待中国经济未来的发展？给中国企业哪些建议？SAP在中国的发展，下一步会做哪些调整？又会即将进入中国的其他外企哪些建议？

孟鼎铭认为，中国经济一定会继续保持增长，虽然增速有所放缓，但是现在仍在6.5%或者6%，即便假设有一天降到5%，中国也仍然是世界上特大型经济体中增长最快的。

过去，中国经济在规模化、高增长、高质量发展上取得了全球瞩目的成绩，接下来中国应该将发展体验经济作为着力点，而且不仅是大企业可以做到，中小企业也都能做到，只要关注消费者的体验和需求，所有的企业都有能力有机会做到。孟鼎铭表示：“如果中国能够把自己从一个高质量、高速度、大规模的制造大国转化为一个体验经济的大国，那产生的效果将是令人震撼的。”

明年是SAP进入中国的第25个年头，SAP公司不久前宣布了在中国的新一轮“中国加速计划”，这一新的五年计划涵盖了一系列战略举措，包括培育新型生态系统、深耕中小企业市场，以及加大人才和设施投入等。孟鼎铭透露，SAP在中国的投资计划不会改变，而且将进一步加大，接下来的3年时间里SAP将在中国的农村市场培训5万名创业者。

“中国的中小企业都有快速增长为大型企业的渴望，这就是很大的创新机会，我希望帮助他们把自己的创新理念扩展到全国，甚至是全球市场。”孟鼎铭说。

他同时透露了上午出席“全球首席执行官委员会”第七届圆桌峰会的感受，中国释放出还将进一步扩大开放的信号。对于即将进入中国的其他国外企业，他的建议是：“最重要的要建立起信任，并保持耐心，始终关注客户满意度以及客户的体验。最好的销售就是市场对你的信任，一个满意的客户会给你带来你想要的市场机会，对此你要充满信心，并保持耐心。”

奇安信集团副总裁左英男：

工业主机和工业大数据 是工业互联网安全两大核心

本报记者 徐恒

工业互联网信息安全防护与消费互联网有哪些异同？左英男认为，工业互联网80%的网络攻击手段和防护方法与消费互联网大同小异，但剩下的20%则需要针对工业不同的场景进行个性化防护。毕竟工业门类众多，工业场景各不相同，而这20%非常关键，需要投入巨大精力进行研究。

当前，很多工业企业看到工业互联网带来的好处，但网络安全问题是工业企业在接触并应用工业互联网技术时关注的焦点。而对于工业互联网网络安全，左英男认为，企业关心的问题主要聚集在两个方面：一方面，工业互联网与外网连接后，如何保障网络安全不被黑客攻击从而保障安全生产的顺利进行。另一方面，随着企业上云走向深入，当数据上云并通过工业互联网向上下游供应链开放后，如何保障工业大数据的安全。

从工业主机 安全防护开始

工业主机主要指生产管理层和过程监控层的电脑设备，它们

“新一代IT技术与传统工业OT技术的深度融合造就了工业互联网，而IT与OT的深度融合不仅拓展了网络安全的外延，也改变了其内涵。”近日，奇安信集团副总裁左英男在2019年中国工业信息安全大会上表示。据介绍，“工业安全+互联网安全”让工业互联网相较于消费互联网而言，其安全问题变得更为复杂。

被称为是信息世界通往物理世界的“大门”。

“工业主机的生命周期往往比较长，操作系统老旧，存在大量漏洞，并且由于工业生产连续性的特点，工业主机很难定期升级补丁，因此工业主机已成为各类网络攻击和安全事件的首要攻击目标。”左英男表示。

根据该公司应急响应处置的工业企业网络攻击事件发现，汽车生产、智能制造、能源电力、烟草等行业发生的数起工业安全事件，大多数攻击或影响的是工业主机，导致工业主机蓝屏死机，无法执行正常的生产作业流程，最终造成停产事件，给企业造成直接经济损失。

左英男表示，工业互联网安全应从工业主机安全防护开始，在利用白名单技术进行病毒拦截的基础上，提供“入口、运行、扩散”三

层关卡拦截，进行全方位病毒拦截。同时，在无需打补丁、关端口的前提下，通过“漏洞利用分析—流量解析对比—可疑攻击阻断”引擎可以有效对病毒进行超前防御。

与此同时，左英男补充道，在防护工业主机的同时，还要研究针对工业底层也就是现场控制层如PLC的安全防护，以防范于未然。

工业大数据安全 风险不容忽视

数据是企业的资产，代表着核心竞争力。数据的安全对工业企业生存发展而言至关重要。近几年，随着工业互联网的发展，企业上云的步伐加快，数据上云成为大势所趋，数据也开始在不同的平台间持续流动，工业大数据的开放、共

享、流动创造了更大价值的同时，也加剧了安全风险。数据的安全问题在某种程度上阻碍了很多工业企业去拥抱工业互联网的步伐，这些企业担心一旦数据上云，数据的知识产权、工艺配方面面临严峻的安全问题。

对于工业大数据的安全防护，左英男认为，工业大数据安全风险管理的核心目标是“看得见、控得住、管得好”，需要摸清数据资产、梳理数据使用、管控数据风险、强化安全运营，构建数据全生命周期的安全治理体系。

据介绍，在以工业云平台和大数据平台为特征的新技术环境下，需要构建全新的安全架构去解决工业大数据的访问控制问题，其关键手段就是构建基于“零信任”的动态可信安全访问平台。在工业大数据安全防护的应用场景下，首先需要梳理工业大数据中心的暴露面，然后部署相应的产品组件，形成动态的虚拟身份边界，使得工业大数据中心不再对外暴露任何物理的网络边界，有效管控内外部用户和终端设备、工厂内部的工业主机和边缘计算网关、工厂外部的工业互联网平台数据共享API调用等访问主体对工业大数据的访问行为，从而保护工业大数据的安全。

英特尔One API 简化跨不同计算架构应用程序开发

本报讯 近日，在伦敦举行的英特尔软件技术日上，英特尔的工程技术人员介绍了软件项目“One API”的最新进展。该项目旨在提供一个统一的编程模型，以简化跨不同计算架构的应用程序开发工作。

英特尔副总裁兼计算性能及开发者产品部总经理Bill Savage介绍说：“One API项目将为开发者带来一套能提供一个统一编程模型的工具。针对跨多种架构的工作负载，这个模型简化了相关的开发工作。英特尔广泛的计算产品组合目前已经包含专用加速器，我们提供的软件解决方案将帮助开发者们充分释放硬件性能。”

英特尔将在2019年第四季度发布一个One API开发者测试版本，并披露更多项目相关细节。

东方通与中电建设等 签署应急产业战略合作协议

本报讯 近日，北京东方通科技股份有限公司（简称“东方通”）、中电系统建设工程有限公司（简称“中电建设”）和中电福富信息科技有限公司（简称“中电福富”）在京签署应急产业战略合作协议，推动“智慧应急”建设。根据协议，三方将围绕应急产业体系建设、技术创新及市场开拓等全面深入合作，共同构建更智能、更高效、更安全的应急系统，提供应急大数据融合、感知网络及智能化系统建设。

东方通黄永军董事长表示，东方通将充分挖掘业务板块协同效应，依托多年的行业积累和技术创新等资源优势，以优秀的数据交

平台及应急通信系统为基础，联合中电建设和中电福富，打造“智能+”应急系统，为应急管理部门提供可靠的数据融合及智能应急业务系统。中电建设董事长马卫华表示，将根据自身在工程领域的业务优势和技术积累，与合作伙伴共同推动应急产业工程业务的开展，为建设全面支撑具有系统化、扁平化、立体化、智能化、人性化等特征，与大国应急管理能力相适应的中国现代应急管理体系而贡献力量。中电福富相关负责人表示，公司紧跟国家应急产业规划，以基础性、全局性、战略性的信息化应急管理建设为抓手，推动全国应急管理信息化跨越式发展。

（徐文）