工业数据：黑客盯上的又一块“肥肉”

近年来，工业数据平台被曝出的漏洞日益增多，且大量集中在装备制造、交通、能源等重要领域。一些黑客正是利用这些漏洞，窃取了大量的工业信息。

包括克莱斯勒、福特、特斯拉等全球100家车企的超过47000个机密文件遭外泄，这一被媒体称为迄今为止最严重的工业数据“车祸”于近日发生。

据报道，数据泄露的源头指向了这些车厂共同的服务器提供商Level One Robotics and Controls（以下简称Level One），泄露的数据包括产品设计原理图、装配线原理图、工厂平面图、采购合同等敏感信息。

“这只是全球近年来频发的工业信息安全事故的缩影。”北京理工大学网络攻防对抗技术研究所所长闫怀志表示，从全球发展趋势来看，工业互联网和工业数据日益成为黑客攻击的重点目标。

那么，到底谁是这次工业数据泄露事件的罪魁祸首呢？我们又该如何有效防止类似事件的发生呢？

访问不设限酿“车祸” 平台漏洞是祸首

“车祸”主角Level One是一家数据管理平台公司，它主要提供基于客户原始数据的定制化服务。

“Level One在使用远程数据同步工具rsync处理数据时，备份服务器没有限制使用者的IP地址，并且未设置身份验证等用户访问权限，因此任何人都能直接通过rsync访问备份服务器，这是导致事故发生的主要原因。”宝沃汽车（上海）有限公司总工程师刘凯说，“由于业务扩展需要，如今越来越多的第三方公司获得了车企的访问权限，车企数据泄露的风险也就随之增加。”

在闫怀志看来，数据平台存在的漏洞是导致此次事件发生的根本原因。“近年来，工业数据平台被曝出的漏洞日益增多，尤其是工业控制系统内的安全漏洞层出不穷，且大量集中在装备制造、交通、能源等重要领域，严重威胁国家信息基础设施安全。一些黑客正是利用这些漏洞，窃取了大量的工业敏感信息。”闫怀志说。

自2015年以来，全球每年发生的工业信息安全事件接近300起，工业领域已成为网络攻击“重灾区”。

国家工业信息安全发展研究中心监测数据结果显示，我国3000余个暴露在互联网上的工业控制系统，95%以上都存在漏洞，可轻易被远程控制，约20%的重要工控系统可被远程入侵并完全接管。

“目前很多工业系统和设备没有防护软件，也未安装杀毒系统，一旦上了网就基本处于‘裸奔’状态。”一位业内人士表示，目前我国一些通信、能源、水利、电力等关键基础设施存在着较大的安全风险，而入侵和控制工业信息系统也已成为商业上打压竞争对手的不法手段。

企业安全意识薄弱 相关人才储备匮乏

“目前，我国很多地区、部门、工业企业对工业数据安全重视不够，重发展轻安全，不重视漏洞、修复不及时等现象普遍存在。”闫怀志说。

据360补天漏洞响应平台统计，在其涵盖的工业相关信息系统漏洞中，25.6%的漏洞未进行修复，一些漏洞的平均修复时间长达数月之久。

我国对工业信息领域安全的认识还处在初级阶段。2017年5月“WannaCry”勒索病毒事件暴发，微软在当年就发布了相应的安全漏洞补丁，但我国很多单位未及时打补丁，导致近30万台主机和电脑被感染。

直到今年，360公司还能监测到每天有近千台电脑感染此勒索病毒。

在企业中，因私人行为导致设备感染病毒的情况也较为多见。例如，个人通过工控设备违规上网，或是厂商的维护人员电脑感染病毒后造成设备系统全网感染等。

此外，我国工业企业目前的防护技术还较为落后。国家工业信息安全发展研究中心通过安全监测发现，工业企业信息安全应急备灾手段不足，约70%的被调查企业缺少完善的应急备灾体系。

防护技术之外，我国在工业信息领域的核心产品自主可控度也较低。

国家工业信息安全产业发展联盟发布的《2017年工业信息安全态势白皮书》显示，国产数据库仅占据7%的低端市场，大量工控系统由外国厂商提供运行维护。我国部分企业不具备自主维护能力，而且缺乏对外国产品和服务的监管。

同时，人才匮乏也是导致工业信息安全技术薄弱的原因之一。“公共信息安全人才需掌握自动化和网络安全两个学科的知识和技能，这类人才缺口巨大。但目前在高校中尚没有设立工业信息安全领域硕士、博士的培养方向，工业信息安全从业人员几乎都是在实践中学习。”闫怀志说。

筑防线需多方合力 可借鉴欧盟做法

“工业大数据的共享是工业互联网应用的基础和灵魂，而工业数据安全及隐私保护又是一切应用的前提。”闫怀志建议，要想给工业信息构筑起一道“防线”，首先企业应树立信息安全与隐私保护意识。

闫怀志介绍，传统IT网络中的隐私规范，主要应用“告知与许可”原则，由信息所有者自行决定可否、如何且由谁来处理或利用其信息，信息隐私保护的责任方为信息所有者。在工业大数据和工业互联网领域，工业数据需要被多次使用，传统的“告知与许可”隐私保护机制不具备现实可行性，工业数据信息隐私保护的责任将由数据使用方来承担。这种方式下可采用的保护手段包括数据分类分级和数据脱敏等。

此外，掌握大量工业信息的数据平台也应肩负起管理的责任。“此前我国网络安全与信息平台监管主体不清晰，多头监管问题突出，信息系统平台安全监管不力甚至监管缺失的情况时有发生，特别是在工业互联网和工业数据安全保护方面表现得更为突出。”闫怀志表示，“平台应不断完善数据隐私保护以及网络安全策略，成立数据安全与隐私保护的专门负责机构或组织。”

360集团董事长兼CEO周鸿祎也强调了漏洞管理的问题。他认为，应建立漏洞管理全流程监督处罚制度，制定覆盖网络安全漏洞的发现、审核、披露、通报、修复、追责等全流程管理细则，强制要求漏洞必须及时修复，对漏洞修复时间以及违规处罚措施予以明确规定。此外，应建立监督检查机制和力量，及时发现未及时修复漏洞，追究相关单位和责任人责任。

中国政法大学法学院大数据和人工智能法律研究中心主任汪庆华教授则从立法角度给出了建议。我国在网络安全和信息保护方面的立法呈现出分散式立法、多头式监管的特点。目前，我国已经初步建立起了以《网络安全法》为中心的分散式信息保护和数据安全方面的法律体系，未来还需进一步加强相关立法工作。

在政府监管方面上，闫怀志认为，我国可参考借鉴欧盟出台《通用数据保护条例》（GDPR）的做法，提高对信息非法获取的惩戒力度。

“GDPR是与当前网络空间现状最为契合的数据保护条例，要求手握数据的企业和机构设立专门的数据保护官员来负责数据管理。我国也可适当借鉴，要求企业和机构设立类似职位。此外，GDPR不仅倒逼中国企业更加重视数据安全和隐私保护，而且也为中国数据安全工作提供了一种思路——中国也可以制定类似条例来维护我国企业和公民个人的数据安全，防止国内外机构非法滥用。特别是在工业互联网和工业数据安全保护方面，有针对性的制度已成为燃眉之急。”闫怀志说。（于紫月）

数字经济与工业制造融合，还有这些难题待解

网上购物、扫码支付、网上政务……这些数字经济在商贸、物流、交通、金融、社会服务等领域的应用已为人们熟悉，不过，中科院院士怀进鹏表示，数字经济在中国发展的主要着力点应该转到与实体经济的融合发展方面，特别是集中到与制造业的融合发展上来，不断地从消费型互联网经济进入制造业实体数字经济。

对此，在近日由中国科协、工业和信息化部、全国工商联、重庆市人民政府联合举办的数字经济百人会上，来自国内外科技、产业及相关领域的专家学者和企业家们针对数字经济与工业制造融合的难题展开了深度讨论。

大数据支撑能力仍显不足

“数字经济，是新一代信息技术与实体经济深度融合产生的新的经济形态。”工信部原部长、中国数字经济百人会顾问李毅中说，当前，数字经济首先在商贸、物流、金融、社会服务等领域取得了成功，但在工业制造业领域，深度融合显得难度很大。

李毅中认为，首先是大数据支撑能力还不足，需要加强自主创新。目前，中国的不少核心技术、关键技术还受制于人，产品结构处于中低端的格局没有根本改变。因此要强化攻关，尽快地突破。同时，一些企业还没有建立数字化转型意识，大数据应用深度不够，需要加强引导和支持。

李毅中表示，如何保护商业秘密也是一大难题。数据的高度集中也意味着风险的集聚，如果发生问题甚至会涉及到国家安全。他建议要研究如何保障工业控制系统的安全，在健全网络信息安全的同时健全法规、法律，制定细则、办法和司法解释。还应该促进行业自律，对违法行为强化惩戒。

推动信息技术与实体经济深度融合

“中国目前数字化竞争力度还低于国家竞争力在世界上的排名。”中国工程院院士、中国互联网协会理事长、中国电子学会名誉副理事长邬贺铨对比了世界上不同组织对数字经济的发展情况后表示，目前，中国面向消费的数字化转型走在前列，但经济领域的数字化转型仍然滞后。

对于数字经济的发展，我国投入和产出增长较快，但软环境还有不少差距，需要进一步推动信息技术与实体经济的深度融合。

“创新特别是核心技术的创新将决定数字中国发展的未来之路。”邬贺铨表示，财富500强的榜上企业要花20年才能达到10亿美元的市值，但是中国的类似企业平均只要4～6年就能达到市值10亿美元。美国的企业主要是靠技术创新，中国的企业则主要是双元模式创新，两者之间差别很大。

专家介绍，双元创新理论将创新分为开发式创新和探索式创新。开发式创新是指现有知识的利用、现有技术的完善与现有产品性能的改进，一般具有渐进性；而探索式创新是指新知识的探索、新技术的开发、全新产品的设计，一般具有突破性。有效的创新需要平衡开发式创新和探索式创新，即“双元”均衡创新。专家表示，双元模式创新在很大程度上促成了中国企业的快速发展。

阿里巴巴集团副总裁刘松认为，下一个10年信息技术不再是为了解决生活和社会的问题，而是创造智能化的经济。

工业互联网发展应符合软件规律

对于传统企业如何破解行业重构困局，德勤全球副主席、德勤中国主席蔡永忠表示，数字化时代，企业特别是传统企业，要在劳动力结构、商业模式、产业链上下游关系等方面，积极运用新技术手段。

不过，他并不认同企业在数字变革过程当中“数字化万能”“移动端能解决所有的问题”的思维。他建议行业变革中，企业转型的策略要随着不同情况改变，从大处着想，小处着手，快速推进，才可以在数字经济下完成变革。

“当我们还在争论工业互联网是姓工业还是姓互联网时，国外提出首先它是一个软件。”全球领先的企业应用软件解决方案供应商思爱普（SAP）副总裁兼首席数字官彭俊松则表示，从全球角度看，无论是传统工业领域还是整个企业的应用市场，工业互联网的竞争焦点最终将会集中在基于公有云的软件即服务（SaaS）系统上。对此，不应该把工业互联网和传统的信息化建设完全割裂开来，而是应该借数字化的浪潮将两者融合。（雍黎 王珂）

华为麒麟980创下6个全球第一 手机终端AI应用的竞速赛

近日，在2018德国IFA展会上，华为消费者BG CEO余承东以“奇点将至”之名，正式发布了麒麟980。作为全球首款量产的7nm手机芯片、双NPU加持，麒麟980共拿下全球六项第一，相比上一代旗舰——10nm工艺制程的麒麟970，980性能提升约20%，能效提升约40%，逻辑电路密度提升60%，即原来的1.6倍。

众所周知，传统芯片遵循摩尔定律，以提升单位面积内晶体管的数量，来提升芯片的性能。工艺提升，于企业而言，芯片的制造成本更低；于用户而言，芯片体积减小、功耗更少。

而目前芯片制造工艺普遍停留在10nm，7nm工艺则一度被称为“最逼近硅基半导体工艺的物理极限”。因而，麒麟980的7nm工艺，则是走在了手机芯片的前沿。

AI方案各家着眼点不同

手机上的终端AI应用于2017年由苹果及华为带起一波浪潮，二者几乎同时在其主打方案——苹果A11 Bionic与麒麟970中引入了NPU硬件神经计算网路单元，大幅加速终端与边缘AI计算落地时程。

同时期的其他方案供应商，多半只能通过软件来模拟AI功能，这导致一来计算性能不足，使得AI场景在应用时明显会感觉到迟滞，无法随心所欲；二来，AI计算包含了复杂的数学与逻辑计算，需要处理大量的数据，因此缺乏硬件设计的方案在功耗及发热等层面的表现亦更为疲弱；最后，如果是以丢回云端处理再回传结果的做法，除了迟延性的问题，云端存储个人数据所建立的学习模型，又可能牵涉到个人数据隐私疑虑。也因此，诸如苹果或华为的本地端AI方案也就成为手机AI发展主流。

以硬件NPU而言，A11Bionic的神经网络专用加速模块比较特殊，目前只用在了Face ID人脸解锁上，没有开放给第三方。而华为的NPU则是支持了标准AI框架，并且对第三方开发者开放，由此所衍生的整体生态效应非常具有想象空间，也可看出华为极力打造自有AI生态的强烈企图心。

即将在2018下半年推出的新款手机方案中，硬件AI计算单元基本上已经是必备要件，这主要归功于苹果和华为带动的潮流效应，而可以预期的是，苹果与华为也必定会在此处持续加强，以延续先前的优势。但联发科等追随者也不甘示弱，AI计算单元成为其主流芯片方案中的标配功能。联发科将采用与高通同样的GPU与DSP混合计算，这种设计虽然弹性高，但能耗表现并不漂亮，而高通则传言未来将全面走向硬件AI计算设计。

手机成为全能接口：他傻瓜你聪明背后隐藏庞大商机

为什么要重视AI在手机上的发展？各家厂商或方案公司之所以争先恐后要推出相关产品，主要就是因为手机是作为日常陪伴用户时间最长的消费类电子产品，其上捆绑的应用已经成为用户黏着性最高的商业接口，不论是游戏，或者是智能语音服务，其对接的是庞大无比的商机，任何对此趋势有基本认知的厂商都不会轻易放过这块市场大饼。

这些所谓的AI功能，其目的之一就是为了带给消费者更便利的日常生活，尽量用最少的程序就可以完成最大多数的工作步骤，很多关键问题的判断就是交由AI来处理。换言之，通过AI辅助，麻烦琐碎的工作都交由手机来代劳，使用者只要动动手，甚至连动手都不用，动口就好。

然而AI并不是先天就什么都懂，它必须通过训练才能获得处理这些工作流程的“知识”，在主流的AI神经网络框架中，我们可以通过对庞大样本的观察与学习，训练出可解决特定应用问题的模型。而这也是包含华为在内的各大手机厂商所努力的方向。

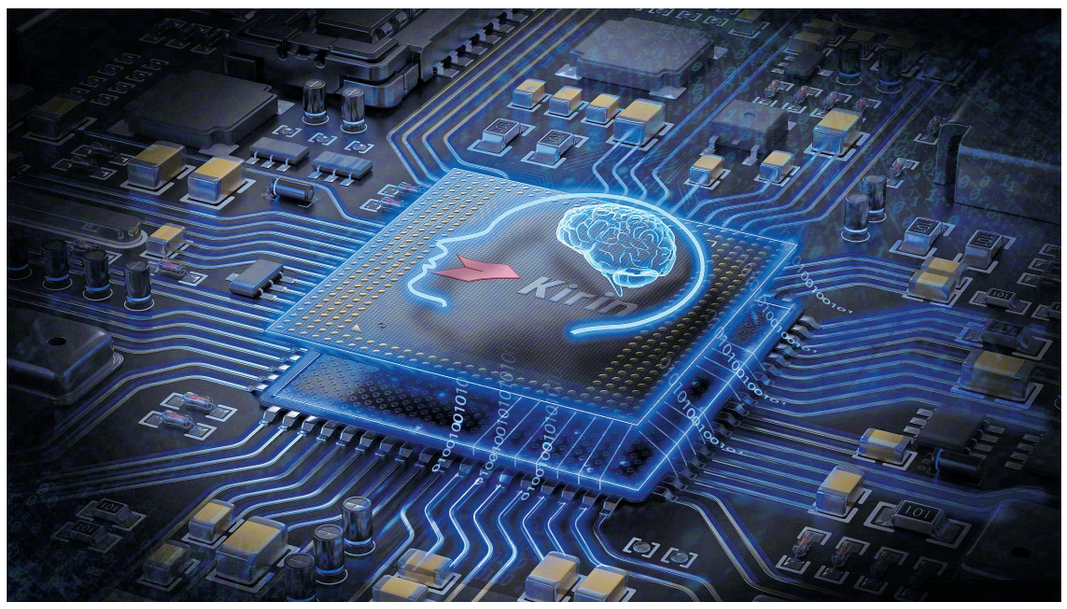
即将引入硬件NPU的高通

作为全球最大的手机方案供应商，高通过去通过Hexagon与GPU、CPU协同工作，达成对主流AI框架的计算加速能力，虽然在效率上还是明显落后苹果与华为的硬件方案，但总是给市场一个交代。

然而，异构计算（Heterogeneous computing）虽然弹性高，且可以有效利用芯片中的不同类型计算架构，但目前AI计算方案讲求的是更高的能效表现，而在手机等移动终端上，更显重要，虽然高通的异构计算已经属于相当高效的技术，但仍与ASIC有一定的落差，也因此，在使用针对AI加速框架进行性能的评比应用时，高通很明显要落后采用硬件NPU的竞争对手，未来如果AI模型往更复杂的方向发展，或者是同时需要执行多种AI服务，那么在发展空间上就可能会明显不如竞争对手了。

不过，高通也不是不知应变，根据市场传闻，其在下一代中高端方案骁龙700系列中，将引入硬件NPU设计，而如果成真，其下一代高端方案，也就是骁龙855，也将可能沿用同样的方式。

而目前高通也引进了包含商汤等多家AI算法设计公司所设计出来的应用框架，想要快速冲刺相关市场，不过高通目前的AI性能还有相当大的改善空间，如果要负载更复杂、多元的AI计算，恐怕还是要等到下一世代的AI设计问世。高通将在12月正式发布新一代的高端AI手机方案，按照往例，明年初就可以见到实际终端产品。



三星：走出自己的路

三星作为全球最大的手机厂商，其势力涵盖终端、消费、云端服务、半导体制造与设计等领域，而其中，手机市场是其最重视的一块，而为了推动其手机市场的布局，三星过去亦步亦趋的追随包含苹果与高通的步伐，并将学习到的设计精髓转化为自有的方案设计。

目前三星主要的芯片来源包含了自行设计的Exynos系列、高通的骁龙系列、联发科的低端MT系列，以及展讯的SC系列，市场从最高端，到最低等级，以及可能会被我们直接当作电子垃圾的产品，几乎都有覆盖。

目前Exynos 9810是三星的主力自产高端产品，今年的Galaxy S9系列、Note9系列都可见到其身影，其采用的AI计算方式与高通类似，主要是通过DSP、GPU与CPU的协同计算，不过三星有个特殊的做法，那就是视觉相关的处理交由硬件，而非异构计算。

目前的9810采用脱胎自Cortex-A75的M3定制架构，并搭配Cortex-A55作为小核心，而与华为最大的不同是，三星在GPU规模上相当舍得下工本，其Mali-G72核心数量配置高达18个，比麒麟970多出6个，虽然芯片成本会较高，但可以在较低的时钟频率达到更稳定、更好的效能表现，换言之，能效也更好。

而9810中有个VPU计算单元，顾名思义，是用来处理视觉方面的计算工作，这个单元应该是硬件设计，但只能用来处理比较固定的功能，三星也未公开发布任何支持该计算单元的可编程或开发套件框架。

而下一代方案，也就是Exynos 9820，将会采用ARM DynamIQ架构设计，并且将以“2+2+4”三丛集形式打造，其中两组大核将采用三星第四代自主架构“M4”，第二道两组大核则以ARM Cortex-A75构成（也可能以Cortex-A76取代），而小核部分则将以4组ARMCortex-A55构成。

AI部分则将可能维持9810的做法，那就是采用VPU硬件处理单元来处理部分视觉计算工作，并搭配既有的异构计算方式来处理标准AI计算框架，也就是半软半硬的方式。

最后，9810采用的是三星10nm工艺，而9820将可能是三星7nm案首发，但因为三星的7nm采用EUV技术，目前还在调试中，真正量产最快也要今年底或明年初，这也可能让9820成为最晚推出的次世代AI手机芯片方案。

赚走最多钱的手机公司搞AI——苹果

苹果基本的手机芯片布局是每年一款，当然，为了配合如平板电脑或者是手表等其他终端的产品时程，也会在不特定的时间点发布相关方案。而苹果最新的手机芯片是去年发表的A11 Bionic，内建的硬件NPU是最大特色。而苹果在其芯片中往往都使用较少的核心，相较对手都已经走到8核以上，苹果A11还只是个6核产品，但其表现出来的性能数据却远远超越所有竞争对手，其原因包括苹果对其使用的Arm架构深度定制化，并舍得为了特定性能目的来堆加更多晶体管，因此其芯片制造成本往往也都比同时期的手机芯片方案更高。但此策略成功推动手机的销售，并创造更高的获利，因此每一代方案苹果也就更舍得堆料，形成正向发展。

A11使用的是台积电10nm工艺，这也是少数几次没有使用到三星代工工艺的苹果芯片，由于目前苹果的开发套件中，只开放GPU计算能力给开发者，而GPU也负担包括第三方AI应用的训练或推理的工作，对苹果而言，GPU的份量也越来越重要，这也是之所以苹果要推动自有GPU架构的发展。

虽然目前所采用的PowerVR架构在性能与菜单现上相当出色，该公司也愿意配合苹果进行高度定制工作，但这对于苹果而言仍远远不足，而展望未来苹果对其GPU架构的布局，将可能是个结合绘图、计算以及推理、训练的全功能AI优化设计，当然，为了能耗表现，推理工作可能还是维持独立的NPU单元来进行。

而未来A12将会如何？其实在现阶段也只能猜测，唯一能确定的只有使用7nm制造工艺这点。而在架构方面，根据过去的惯例，性能的增长肯定是不能忽略的，毕竟对手也都在积极追赶，今年对手的主流方案都已经在整体性能上有相当大的改善，也拉近了与A11的距离，A12肯定会在CPU与GPU方面进行更深度的改造，不论是增加更多的处理管线，更优化CPU或GPU内部的流水线设计，抑或者粗暴的堆加核心，都是可能的做法。

至于在关键的AI硬件单元方面，除了强化效率以外，也可能就规模方面进行扩展，借以压制华为或高通等即将面世的下一代AI方案。（于平）