深入贯彻“四个坚持”维护开放环境下的网络安全

党的十八大以来，党中央高度重视网络安全工作，进行了一系列重要的顶层设计与战略布局，推动我国网络安全工作取得历史性成就。当前，我们进入新的历史时期，以数字化、网络化、智能化为特征的第四次工业革命孕育兴起，政治经济、国际局势等均进入历史变革期，网络安全工作也迎来了新的问题和挑战。2019年9月16日，国家网络安全宣传周在天津开幕，习近平总书记作出重要指示，强调国家网络安全工作要做到“四个坚持”，为新时代网络安全工作提供了根本遵循。

中国电子信息产业发展研究院
王闯 吴志刚

- 网络安全国家标准数量持续增加，标准建设进入快速发展期。截至目前，全国信安标委累计发布网络安全国家标准数量322个（现行标准291个）。
- 2018年我国网络安全市场规模达495.2亿元，增速20.9%。随着数字经济的发展，网络安全投入将持续增加，2021年我国网络安全市场将达到926.8亿元。
- 网络安全一直是资本关注的焦点，投融资金额和交易数量逐年上涨，2018年国内网络安全领域企业总融资金额达72.1亿元。

我国网络安全工作成效显著

党的十八大以来，国家网络安全顶层设计不断完善，基础工作扎实推进，人才培养取得突破，产业能力快速提升，国际影响力持续增强，网络安全工作成效显著。

（一）顶层设计不断完善

一是网络安全法制体系不断健全。2017年6月1日，《网络安全法》正式施行，为我国网络安全工作提供了法律依据和保障，配套法律法规制定工作快速推进，《关键信息基础设施安全保护条例》《网络安全漏洞管理规定》等相继公开征求意见。二是网络安全战略规划陆续出台。《国家网络空间安全战略》《网络空间国际合作战略》等明确了我国网络安全发展的战略方针和任务，以及国际合作的系列主张和立场。三是网络安全标准体系加速建立。网络安全国家标准数量持续增加，标准建设进入快速发展期。截至目前，全国信安标委累计发布网络安全国家标准数量322个（现行标准291个），其中2012年以来新发布的232个。

（二）基础工作扎实推进

一是关键信息基础设施保护工作深入开展。国家网信办、工信部、公安部和相关行业部门积极推进关键信息基础设施保护工作，于2016年7月组织开展了首次全国范围的关键信息基础设施网络安全检查工作。二是个人信息保护工作取得明确成效。2019年以来，国家网信办、工信部、公安部、市场监管总局开展APP违法违规收集使用个人信息专项治理，对存在严重问题的APP采取约谈、公开曝光、下架等处罚措施。三是全民网络安全意识明显提升。2016年，国家网信办、教育部、工信部、公安部等六部门联合印发方案，明确每年9月统一举办国家网络安全宣传周，采取各种形式的活动增强广大网民的网络安全意识，提升基本防护技能。

（三）人才培养取得突破

一是网络安全学科建设取得进展。自2015年国家设立“网络空间安全”一级学科以来，全国160余所高校开设信息安全或网络空间安全专业，40余所高校成立网络空间安全学院。二是校企联合培养新模式基本形成。全国近半数高校开展校企合作育才实践，如北航、北邮、哈工大等多所高校分别与网络安全企业等成立联合实验室，提升学生的网络安全实战能力。三是社会培训体系建设取得成效。企业逐步加强人才实训基地建设，开展从业人员在职培训，国内主流的安全人才培训企业都在实战训练、攻防演练等方面加以布局。

（四）产业能力快速提升

一是网络安全市场规模快速增长。赛迪数据显示，2018年我国网络安全市场规模达495.2亿元，增速20.9%。随着数字经济的发展，网络安全投入将持续增加，2021年我国网络安全市场将达到926.8亿元。二是网络安全集聚效应初显。工信部和北京市共同打造的国家网络安全产业园区于1月份正式揭牌，预计到2020年将带动北京市网络安全产业规模超过1000亿元，拉动GDP增长超过3300亿元。三是网络安全资本市场持续活跃。网络安全一直是资本关注的焦点，投融资金额和交易数量逐年上涨，2018年国内网络安全领域企业总融资金额达72.1亿元。

（五）国际影响力持续增强

一是形成有中国特色的网络空间话语体系。我国积极推动构建多边、民主、透明的国际互联网治理体系，主张世界各国应互相尊重网络空间主权，在应对网络空间安全威胁方面平等合作、互利共赢。二是加快提升国际互联网治理参与度。我国积极宣传互联网治理理念，倡导构建网络空间命运共同体，并取得积极成效，如在联合国网络犯罪政府专家组第四次会议上，中国代表团提出的尊重网络主权等理念和主张被纳入会议最终报告。三是积极打造国际互联网治理交流平台。自2014年以来，世界互联网大会已成功举行5届，集聚全球网络安全机构和专家，成功打造为宣传中国互联网治理理念的交流平台。

新时代网络安全工作面临的新问题新挑战

随着数字化、网络化、智能化的深入融合发展，政治经济社会数字化转型趋势明显，网络安全工作面临诸多新问题新挑战，集中表现为以下四大矛盾。

（一）丰富多彩的互联网应用与快速增加的网络违法犯罪行为之间的矛盾

当前，各类互联网应用不断涌现，给广大人民群众的工作生活带来提供了便利，但同时出现大量网络诈骗、网络攻击、数据窃取等违法犯罪行为，严重侵犯了个人合法权益。一是个人数据泄露数量和规模大幅上升，据统计，2019年上半年4000起数据泄露事件共暴露41亿条数据。二是各类网络诈骗带来的损失快速增加，据统计，2018年网络诈骗人均损失约2.5万元，较2019年增长近70%。三是企业非法获取和滥用个人数据的行为不断增多，如AI换脸软件“ZAO”通过霸王条款侵犯隐私，大数据信贷风控企业利用爬虫技术违规获取个人隐私，商家利用大数据技术杀熟等。与此同时，由于执法力量有限、技术取证和主体定位难度大等因素，网络犯罪受害者难以有效维权，如网上被骗超过3000元才会立案，即使立案破案率也很低（据统计不到5%）。

（二）日益增长的网络安全需求与相对不足的网络安全保障能力之间的矛盾

随着网络安全威胁风险不断加剧，全民网络安全意识不断提升，网络安全需求快速增加，但网络安全保障能力仍存在较大缺失。一是网络安全人才储备不足。当前，网络安全人才培养速度远跟不上快速发展的网络安全市场，市场缺口达到90%以上。据统计，2020年中国网络安全人才需求量将达到160万人，但每年网络安全专业毕业生人数仅为1万人。二是网络安全技术能力不足。我国网络安全核心技术仍面临受制于人的问题，在网络攻防技术发展日新月异的今天，我国应对网络安全威胁的能力仍相结较弱，如尚不具备发现信息技术产品安全漏洞和后门的监测分析技术，缺乏能够定位网络攻击源头的攻击溯源技术。

（三）快速迭代的新技术应用与相对滞后的网络安全管理之间的矛盾

当前，人工智能、5G等新技术层出不穷，在应用推进过程中往往会引入新的网络安全问题，给管理部门带来较大的挑战，难以及时有效地进行管理，存在较大的安全隐患。一是人工智能安全问题凸显。人工智能越来越多地被攻击者利用，从而降低了攻击成本，提高了攻击速度和效率，引发了新的网络安全风险。同时，人工智能技术本身也存在安全隐患，如黑客可通过改变数据分布生成恶意对抗样本，向人工智能系统发起“投毒攻击”。二是基于5G的移动互联网应用安全风险成为关注焦点。2019年6月，5G商用牌照正式发放，将加速推动更多行业的数字化转型，有力支撑数字经济蓬勃发展。但同时，5G本身潜在的安全问题也将逐步暴露，基于5G应用将面临新的安全风险。

（四）蓬勃发展的数字经济与复杂多变的网络安全国际形势之间的矛盾

当前，数字经济快速发展，已经成为我国经济发展的主导力量，也是经济全球化发展的重要推动力量，但网络空间局势不断恶化，逆全球化思潮有所抬头，将给数字经济快速健康发展造成阻碍。一是网络战风险进一步加大。2019年9月，俄罗斯总统特别代表表示，网络对抗持续上升，如不能找到有效方法，全球网络战即将爆发。2019年以来，委内瑞拉电网遭受网络攻击大面积瘫痪、美国在俄罗斯电网预置可大规模破坏的恶意代码、美国对伊朗发动网络攻击削弱其袭击油轮能力等事件频发，网络战一触即发。二是国际ICT供应链安全风险加大。美国持续使用切断供应链的手段打压我信息技术企业，如华为被迫逐步更换其手机和PC产品的芯片及操作系统，并放弃使用国际主流的EDA工具。若贸易保护主义和逆全球化进一步蔓延，将给数字经济发展带来严重障碍。

新时代如何做好网络安全工作

网络时代便捷和风险同在，面对新的网络安全风险和挑战，我们要深入贯彻落实“四个坚持”，着力维护开放环境下的网络安全，让广大人民群众共享技术发展的红利。

（一）“要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益”

一是强化网络执法力度。针对关乎人民群众切身利益的网络犯罪行为，加大执法力度，将打击网络诈骗、违规收集个人信息等专项行动常态化，切实保障个人合法权益。二是创新网络治理模式。打通普通民众网上维权的渠道，充分依托民众的力量提高网络治理效率，如可通过建立网络办案平台，支持小额网络诈骗案件处理、网上举证等，逐步增加普通民众和企业等的参与度。三是保障民众数据权益。大量政务数据、公共数据源于广大人民群众，应进一步规范相关数据开发利用的程序，引导数据合理合规使用，保障广大人民群众的知情权、选择权和受益权。四是提升民众网络安全意识。以国家网络安全宣传周为基础，组织开展多种形式的宣传、教育和培训工作，增强普通民众保护自身合法网络权益的意识，提高网络防护技能。

（二）“要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态”

一是强化网络安全人才培养。继续完善网络安全一级学科和专业建设，鼓励学校通过联合办学等形式培养实战性网络安全人才，支持社会化网络安全人才培养模式，着力培养急需的网络安全人才。二是着力推动核心技术突破。鼓励和引导研究机构和网络安全企业开展基础前沿技术研究，特别要加大核心短板技术的研发投入，加快核心技术成果产业化的步伐，快速提升我国网络安全保障能力。三是加快提升网络安全产业支撑能力。制定出台促进网络安全产业发展的政策文件，强化网络安全技术产业统筹规划和整体布局，扎实推进国家网络安全产业园区建设，培育一批具有国际竞争力的网络安全企业。

（三）“要坚持促进发展和依法管理相统一，既大力培育人工智能、物联网、下一代通信网络等新技术新应用，又积极利用法律法规和标准规范引导新技术应用”

一是跟踪研究新技术应用安全风险。建立新技术应用安全评估制度，依托权威第三方评测机构，密切跟踪和分析新技术应用的安全风险，组织研究应对措施，为及时制定相应的管理规则提供支撑。二是加强新技术安全管理。针对新技术快速迭代的现状，推动建立新技术应用动态管理机制，将市场上涌现出来的典型新技术应用列入动态观察名单，形成应急响应机制，实现安全风险可控。三是引导新技术安全应用。通过开展试点示范等形式，鼓励和引导企业探索新技术安全应用的场景和模式，加强应用安全相关标准规范的研制工作，规范和指导企业做好新技术应用安全工作。

（四）“要坚持安全可控和开放创新并重，立足于开放环境维护网络安全，加强国际交流合作，提升广大人民群众在网络空间的获得感、幸福感、安全感”

一是严守网络安全底线。加快出台关键信息基础设施保护、网络安全审查、数据安全管理等法律法规，逐步健全网络数据安全标准体系，依法依规做好网络安全管理工作，有效防范和应对不断变化的安全风险。二是引导企业开放创新。鼓励和支持企业提升自主创新能力，充分利用全球资源，打造核心技术生态体系，通过开展信息技术产品安全可控评估测试，提高应用单位ICT供应链安全水平，安全可控地使用世界范围内的先进信息技术产品。三是加强国际交流合作。发挥政府、国际组织、企业、科研院所等各方作用，充分利用联合国、ITU、金砖国家等多边平台，积极宣传推广我国互联网治理理念，弥合国际网络空间分歧，反对霸权主义、保护主义，推动构建和平、安全、开放、合作、有序的网络空间。

全球智能硬件创新酝酿变局

（上接第1版）

也是在很多年前，萨提亚就敢揣着装满微软应用的苹果手机iPhone，公开亮相于对手Salesfoce的销售会议上。在一切皆服务的云时代，服务才是核心，背后集成了敌人还是友人并不重要，“没有自我包袱才会拥有更大空间”，所以萨提亚把微软带到了云时代，带到了全球市值第一的位置。

现在，萨提亚要把微软从云时代带到“生产力”时代。在这次纽约的发布会上，萨提亚在6分钟、不到700字的演讲中给出了微软硬件的新定义，上半场定位“消费类”，下半场聚焦“生产力”。他给出了微软硬件下一个创新定律：一是把计算机嵌入到每一个地方和每一件事中，人是设备体验的中心。二是设备要在形态和功能上进行创新。所以，微软做出了二合一的Surface、“像画布一样”的计算机Surface Studio，以及连接物理与虚拟的混合现实HoloLens等。三是不局限于创造某一个体验和设备，而是跨越所有的设备，并且包括使用所有自然的交互方式，无论是墨水、触摸，还是语音、手势。

基于这个硬件创新的三定律，我们就能够理解为什么微软不再纠结于用谁的操作系统，为什么在手机市场都已经如此炙热的背景下，仍要再次重返。因为作为生产力的工具在“任何形态、任何场景都缺一不可”。占领每一段时间、每一个场景、每一个产品的形态，会成为“生产力”维度下的硬件厂商必争之地，在电脑、平板、手机、混合现实之后，还有哪个形态被遗漏，还有哪个形态没有被创造出来，都有可能是微软的“下一个”。

微软联合高通进行芯片定制是第二个“槽点”。一直以来，微软的芯片合作伙伴都主要是英特尔，少许采用AMD，而现在加入了高通。这次微软基于ARM架构联合高通定制了一款名为SQ1的高通衍生芯片，这颗芯片将装在新款Surface Pro X中，按照微软给出的说法，这款笔记本能够让笔记本电脑拥有像手机一样的“全天的电池寿命”。性能和功耗是移动智能终端厂商之间永远的“奥运”焦点，谁能够在更低的功耗实现更高的性能，谁就是赢家，这是笔记本、手机等厂商间没有终点的竞赛。

这颗名为“SQ1”定制的芯片，有几个关键点：一是微软自主开发、基于ARM架构、高通骁龙深度参与。二是微软和高通重新设计了GPU，达到2 teraflopss算力。结果是“该产品每瓦的性能是Surface Pro 6的3倍”。这透露出微软未来在芯片道路上新的动向：软硬件深度定制，甚至走向完全芯片自研。

一直以来，软硬件深度定制带来最佳效应似乎都只有苹果为之。但其实微软从萨提亚开始，芯片定制路线就已经就揭开了序幕，在十年前微软基于云开始尝试采用FPGA进行深度定制，以期在云上获得超越亚马逊的更强大性能，对这点微软研究院的工程师道格·伯格曾透露过有关信息。在2017年7月，微软宣布将进行应用于HoloLens混合现实头盔上的芯片研发，也是在2017年萨提亚曾表示他的头等大事是要将微软在云上的强大人工智能能力，移植到手持和头戴设备上。现在这种“移植”的路线正在变得越来越清晰。

在人工智能时代，每一种计算设备、每一种场景下的智能获得，都有着深深的“算法+芯片”的烙印，也正因为如此，包括苹果、谷歌、微软等业界巨头都加入了造“芯”的战壕，由此来获得更高效的软硬集成效应。当我们看到苹果5G因为移动缺“芯”而变得被动，从而大动干戈地招兵买马进行芯片布局，我们就不难理解微软未来有可能在芯片上的进一步布局。今天我们看到微软的移动设备端的芯片还主要是自研体系、由高通等芯片巨头进行定制，在未来，微软很有可能走上部分芯片完全自研的道路。

由此带来的另外一个敏感问题是微软与英特尔的关系，尽管目前看英特尔依然是微软笔记本等移动设备的最主要供应商，而在5G时代到来，越来越多元的移动设备形态下，或许微软与高通会走得越来越近。