科技日报
■责编 陈 莹 2018年3月7日 星期三

网络安全 国之命脉

中国科学院云计算产业技术创新与育成中心主任 季统凯

当今社会，随着互联网、云计算、大数据、智能制造等新兴领域技术的创新与发展，互联网逐渐成为人类社会的基础设施，对人类社会的进步和发展产生了广泛而深远的影响，渗透到了政治、经济、文化、娱乐、大众媒介和人际社交等各个方面。互联网彻底颠覆国民生活方式的同时，网络信息安全问题日益凸显，信息安全是国家的核心命脉，直接影响国家的安全利益和经济利益。可以毫不夸张地说，网络安全，国之命脉！

如何在飞速发展的互联网技术方面，掌握国家安全话语权？如何才能摆脱网络核心关键技术受制于人的窘境？如何真正做到等保核心系统的自主、可控，等保服务的快捷、迅速、持续服务模式，从而真正成为世界科技强国和经济强国？

这是新时代给我们提出的历史使命。

网络信息的安全基石

云计算、大数据服务设施是网络信息的主要承载和运行平台，也是互联网的重要基础设施。当前，确保云计算服务平台的自主、安全、可信和高效利用是维护网络信息安全，有效利用网络空间的核心关键。为响应和落实国家网络和信息安全总体战略，中科院云计算中心联合国云科技股份有限公司（简称“国云科技”）自主研发国内首个自主知识产权的云计算平台——G-Cloud云操作系统，共同打造中国自主、安全、可信的基础设施和云服务平台，G-Cloud云操作系统也是国内首个通过国家信息安全评测中心最高安全级别认证（EAL3+）的云操作系统，拥有公安部信息系统安全等保四级认证，也是工信部认证的基于安全可控优秀云计算解决方案，技术服务指标达到了国内领先水平。为我国网络信息安全建设奠定了基石。

G-Cloud云服务是面向政府IDC数据中心、电子政务、企业机房云化需求研发的云操作系统，该产品可确保其上运行的应用系统安全稳定，并提高信息安全防护能力，这也使得我国在全球性的信息基础领域更具话语权，国云科技以云计算操作系统为核心技术，积极参与服务国家战略和国民经济的发展。

责无旁贷的时代使命

成立于2010年4月的国云科技股份有限公司，是国内最早一批专注于云计算、大数据核心技术研发和产业化的公司，是国内信息技术服务业首批获得《企业知识产权管理规范》认证企业之一。国云科技始终以中国领先的云计算与大数据全面解决方案及服务供应商为目标，自2010年起，国云科技提前布局，整合资源，面向国民教育、电子政务、应急指挥、遥感云等领域的智慧城市及互联网应用，提供体系化的信息安全整体解决方案和产品支撑，形成了以云计算、大数据、孵化培育、基金投资的产业集群。

国云科技依托信息安全领域的丰富经验和技术积累，打造自主、安全、可信的云计算、大数据服务平台，创造云计算、大数据创新融合的新局面，带动地方云计算、大数据应用创新与发展。国云科技秉承自主创新原则，积极研发网络基础设施的核心软件，维护国家信息网络空间安全，努力打造成为国家网络信息安全的坚强后盾，这是国云科技初衷、责任和义务，也是国云科技服务国家信息安全战略的历史使命和担当。

不可逆转的大势所趋

互联网时代，云计算与大数据为政府机构决策提供科学的信息分析支撑，为传统产业提供前所未有的海量数据。国云科技响应国家号召，积极在全国开展推广信息化项目应用，先后在广东、海南、安徽、江西、内蒙古等地设立了分支机构，以东莞制造业名城为阵地带动江西上饶、内蒙古呼和浩特、安徽宣城、湖南株洲等区域特色发展，构建协同有序、优势互补、科学高效的区域协同创新体系。

在服务国民经济的主战场上，推动当地政府打造云计算和大数据产业集群，驱动地方信息产业创新发展。围绕江西上饶充分发挥大数据研究院的优势，打造长江三角洲一带的大数据创新引擎和产业融合创新中心；围绕安徽合肥区域优势，推动该地区数字经济的产业应用与创新；围绕内蒙古自治区云计算与大数据标准化技术委员会的成立，双方共同打造大数据产业生态系统，加快呼市云计算、大数据应用落地；围绕株洲高端制造行业，与当地政府打造“互联网+”产业园，最终形成以东莞辐射全国的信息产业创新格局，提升各地信息化产业的发展，构建信息安全开放共赢生态链。

国云科技致力于打造中国自主、安全、可信的云计算、大数据产品，面对日益严峻的信息安全问题，充分发挥自主创新的核心竞争优势，坚守网络国门！

（季统凯，国云科技股份有限公司董事长，中国信息化专家委员会专家，中国云计算专家委员会委员，中国大数据专家委员会委员，国家“万人计划”科技创业领军人才，是我国云计算领域的先行者和实践者。）

季统凯（左一）向参观领导介绍自主云计算平台。

■院士点评

院士李国杰

中科院云计算中心是中国科学院唯一以云计算、大数据为核心研发、产业育成的新型研发机构，承担起国家网络信息安全，特别是国家政务的网信安全，都是无可替代的时代使命。“十年磨一剑”，经过十年刻苦攻关与研发，他们终于为国家研发完全自主知识产权的、可与列强争高低的政务云盾牌——G-Cloud云操作系统。

同时，中科院云计算中心是中国科学院与广东省政府、东莞市政府联手打造的一支面向主战场的科技劲旅。中科院云计算中心与国云科技股份有限公司联合在云计算、大数据应用，智慧城市建设，信息安全等领域为国家战略和地方经济发展做出了突出贡献。

目前，我国网络与信息安全产业在政策、环境技术标准企业发展等方面仍面临巨大的问题和挑战。在国家信息安全建设上，首先要加强安全产业政策引导和优化产业生态环境；其次，加强基础安全技术能力攻关和金融扶持及人才培养；与此同时，还要加强面向云计算、大数据、智能制造等新兴领域的安全技术的研发应用，培养自主知识产权的产品品牌；最后，要打造自主的“高精尖”的技术产品布局，开展新技术新业态安全前瞻研究，占领信息产业新高地。

（李国杰，中国工程院院士、第三世界科学院院士、中科院计算所首席科学家、中国科学院云计算中心“广东省云计算产业国际创新团队”带头人。）

铸造国家政务安全的云盾牌

左朝胜 马军峰 徐晓颖 高建远

近几年，国内外频繁爆发的信息安全泄露事件，让人们对网络安全的关注日益强烈。尤其是信息泄露已从个人家庭、社会企业、事业单位逐渐渗入到国家政府部门及相关组织的云化系统和业务，这导致的后果和危害将更加严重。在这种形势下，借助一种达到国家网络安全等级保护标准（简称“等保”），并且快捷、高效、低成本的提供一站式、可定制的信息安全服务，无疑成为政务云的一块首选安全盾牌。

针对这一问题，中科院云计算中心的几位年轻专家分别就国家安全政策、防御措施、解决方式等几个方面阐述了各自的观点。

陈强：“黑手”已触国家机器

从2017年“永恒之蓝”勒索病毒席卷全球的医院、学校和政府机构，到2018年初的“英特尔CPU漏洞事件”，从洲际酒店用户信用卡金融信息泄露、德勤邮件受攻击，到美国约2亿选民个人信息泄露、我国12306官方网站出现安全漏洞……一系列信息安全事件揭示出黑客们的目光已经不再局限于一般的行业企业、社会机构，而是开始逐渐触及国家政府机构甚至最高级别的领导组织，直接威胁到国家战略层面的安全问题。

中科院云计算中心陈强博士介绍说，在政治安全上，信息化发达国家很容易通过非法或肆意篡改信息等干预内政方式对信息欠发达的国家行使信息霸权，通过信息传递、传播和扩散对一个国家的舆论构成压力和威胁。在经济安全上，目前我国银行系统信息化程度是比较高的，金融业的特点就是网络化、信息化，这个特点极易成为不法分子的攻击目标。国内外，与经济和金融相关的网络攻击事件有很多惨痛的教训。在社会稳定上，由于现代信息网络是现代社会的一个基础设施，任何一个类似银行、电力等关键基础设施或者重要的应用系统出问题，都会直接影响到社会的稳定。在军事国防上更是如此，信息化武装下的作战部队，如果所使用的数字化武器等出现问题，造成的后果将会直接危及国家和人民的安全。

陈强博士认为，“随着信息化的飞速发展和普及，信息基础设施已经成为核心业务和关键活动的重要载体，绝大部分关系我国经济和安全命脉的重要行业和关键领域，已经建立覆盖全国、触及全球的信息基础设施。这些信息基础设施往往对一个行业的正常、稳定运行具有战略性作用，不但涉及大量行业重要数据和信息，更是行业体系中重要的系统节点，同时具有一定社会稳定的代表意义。这些系统一旦被攻击或破坏，不但会影响重要行业的运作，对石油、化工、核电站等行业还会造成巨大的安全隐患或事件，对社会稳定、国家安全产生巨大影响和严重后果。”

涂旭平：国产安全认证产品当为首选

随着政府各部门以及部分重要领域对自主可控软件的需求不断增加，近年来，围绕发展自主可控、安全可信的国产软硬件如雨后春笋般不断涌现。据了解，目前，在中央80多个部委中，几乎都在使用国产自主研发的操作系统。

国家法律制度也为国产安全技术和产品提供政策环境。2017年11月通过的《网络安全法》明确指出：“国务院和省、自治区、直辖市人民政府应当统筹规划加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

此外，政府采购也采取措施支持自主核心技术产品。广东省电子政务建设就提出要优先采用国产软件产品和服务，并优先选用可支持Linux操作系统的跨平台应用软件产品。利用财政性资金建设的信息化工程，用于购买软件产品和服务的资金原则上不得低于总投资的30%。

“近年来，政府也在多个场合明确表示，支持自主品牌软件的发展，自主品牌软件的技术也已经有了很大提升。政府采购自主品牌软件具有非常重要的示范作用。虽然政府采购量相对普通市场较少，但政府使用自主品牌软件，代表了一种肯定和导向，能够带动更多采购人采购自主品牌软件。”中科院云计算中心涂旭平博士介绍说，在当前的经济环境下，政府采购向自主品牌软件的倾斜意义更大。

在他看来，全国各地的政务云、金融云、教育云等建设如火如荼，越来越多的云计算系统承担着重要的基础性服务。在高速发展的同时，安全隐患和威胁也如影随形，如：不安全接口、服务中断、越权、滥用与误操作、共享技术漏洞和信息残留等问题时刻影响着政务云系统和业务的安全。作为云计算的核心，云操作系统坚持采用自主品牌产品对信息安全也具有很大的意义。“除了采用自主品牌软件产品之外，政务云信息系统应具备什么样的安全防护措施，如何通过等级保护测评工作去检查和验证安全措施的合规性和有效性，已经成为政务云建设者、运营者、监管者以及使用者所关心的重要问题。”

自2009年以来，公安部持续开展等级保护测评体系建设工作。随着互联网的快速发展以及CDN行业的蓬勃发展，围绕这些领域的等保认证也被列上日程。其中，公安部推行的国家信息安全等级保护认证，是目前国家最高级别的平台安全认证。信息安全保护等级共分为五级，等级越高，意味着安全保护能力越强。

等级保护级别的认定为政务云安全提供了可以参考的重要测评机制，让一切不安全因素无所遁形。然而，等保工作具有持续性的特点，随着应用系统的升级和等保制度的改进，等保工作会经历螺旋上升的周期性过程，新的应用系统上线、在原有等保级别基础上升级、等保制度的修订以及等保认证的周期性审核都需要对应用系统进行等保测评，面对政务云平台上成千上万的安全测评应用，以及每年需要重复审核的流程，一个能够整套批量等保认证的产品极大地提高了效率和成本。

杨松：“进不来、拿不走、看不懂、改不了、赖不掉”

等级保护制度是国家主管部门对政府、金融、能源等行业重要信息系统进行安全监管的一个重要手段。国云科技股份有限公司（简称“国云科技”）高级工程师杨松总监介绍说：“传统信息安全等级保护测评的模式主要依赖硬件设备满足技术层面的要求，如果一个应用系统要顺利通过等级保护三级测评，那么其需要配置防火墙、堡垒机、审计设备、入侵防护、流量清洗等安全设备才能符合要求，这对传统的IT基础设施建设模式是一个很大的挑战，采购大量的设备需要经历复杂的采购流程和花费大量的资金；另外，传统模式主要依赖于人工收集文档记录的方式满足管理层面的要求，需要投入大量的人力，是一种低效的工作方式。”

与其他同类的安全云服务相比较，国云科技的等保云服务是一个使用云计算技术解决信息安全问题的快速、高效、低成本的方案。使用该服务的应用系统无需进行技术改造，即可满足网络等级保护标准在技术层面和管理层面的要求，包括技术层面的物理安全、网络安全、主机安全、应用安全和数据安全，以及管理层面的安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理。杨松总监介绍说：“满足等保要求所需要的设备以软件的方式存在于云计算平台上，应用系统可按需快速获得需要定制化的安全设备，既节省了时间，又节约了成本。另外，等保云服务通过统一的管理中心集中收集各种运行记录，测评机构通过管理中心就能获取各种过程记录，大大提升了测评工作的效率。”

接着，他向笔者讲述了一个项目经历。“在2017年9月完成开发和调试的东莞市电子政务工程的网格化管理系统及基础数据库平台是该市电子政务工程的核心业务系统，承载着该市电子政务系统基础要素、后台管理、指挥调度中心、社区综合业务、部门综合业务、代办管理业务以及基础数据服务，具有非常重要的作用，在上线前必须通过等级保护三级认证。测评机构经过第一次测评结果不予通过，一共发出70个技术整改建议和48个管理整改建议，同时通过扫描发现6个网页安全高危漏洞和66个端口高危安全漏洞。系统上线在即，项目经理需要在短时间内尽快解决诸多问题、通过评测，且不能追加过多的项目经费，但涉及到设备设施条件整改的，无疑不是一笔小数目，难度很高。然而，在使用国云科技的等保云服务20天以后，测评机构进行了第二次测评，结果显示所有问题都已经解决，两个应用系统得以顺利通过等保测评并成功上线。”

据Gartner预测，到2022年每家公司将会花50%的金钱去修复IoT所造成的安全危害。杨松总监说：“今天我们要考虑的应该是风险跟信任度，不仅仅是安全，安全已经是基本盘。面对各种不同的突发安全事件，我们讲风险，讲可信，讲如何用DevSecOps的理念把安全做进去，目的都是建立持续渐进性的风险跟信任机制，用安全技术不断地去实现云计算的安全可控。”

等保云就是通过自下而上层层标记控制的主动防御可信安全体系，自上而下的N+1漏洞防护，自左而右的“进不来、拿不走、看不懂、改不了、赖不掉”的纵深防御强制访问控制，根据安全标记和策略进行白名单机制控制，只有策略允许的才能运行，从而防止病毒、木马的执行，0day漏洞的出现，保护敏感文件，即使遭受攻击，域控制也可以缩小攻击所带来的危害。此外，等保云还提供一套先进的运维安全管控与审计解决方案，帮助用户转变传统IT安全运维被动响应的模式，建立面向用户集中、主动的运维安全管控模式，降低人为安全风险，满足合规要求，保障企业效益。

目前，政务应用基本都要求通过二三级等保，已部署的云平台也在要求范畴内。在政府很多传统应用基本找不到开发商，或者开发商改造需要增加费用的情况下，等保云能够全覆盖、全管理式的帮助云上、云下企业（特别是金融、政府、网约车行业）快速通过公安部要求的《信息系统安全等级保护》测评。可以说，等保云服务在应用系统的等保工作全生命周期中发挥作用：在等保的定级备案阶段，等保云服务为客户提供测评资料的标准参考模板并收集应用系统的基本信息，为定级和测评准备工作提供支持；在等保的测评阶段，等保云服务为客户提供漏洞扫描和脆弱性分析，找出应用系统的不足之处，同时获取各种过程记录，大大提升测评工作效率；在等保的整改阶段，等保云服务为客户提供系统的安全防护服务，确保应用系统满足等保的安全要求；在通过等保认证以后，等保云服务为客户提供应用系统的持续监控和安全审计服务，为应用系统提供持续的安全护航，极大地降低了传统政务应用通过等保认证的难度，提高了效率，节约了成本。

孙傲冰：被动防范应转为主动攻防

2017年6月1日，《中华人民共和国网络安全法》正式实施。其中第二十一条规定，国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

在中科院云计算中心孙傲冰博士看来，“从单纯的重视信息安全、提高安全意识，到主动的有效防范攻击、保障安全，这说明国家再次将信息安全战略升级，抢在问题事故爆发前面采取措施进行有效的防卫，这也给政府的各项云业务提出了更高的要求”。

报告指出，检查中发现各地在贯彻实施“一法一决定”、维护网络安全中，许多关键信息基础设施运营单位对网络安全的重要性认识不到位，认为受到网络攻击只是小概率事件，对可能受到网络攻击的危害性缺乏认知。在信息化方面“重建设、轻安全；重使用、轻防护”，缺乏主动防御意识，不愿在安全防护方面进行必要投入。

孙傲冰博士说，许多行内的权威专家共同认为，“解决网络安全问题应该从计算体系结构和计算模式等方面进行科学技术创新，采取主动免疫防护的措施，使正常的逻辑组合不被破坏。大数据是一个有密码保护的可信计算环境，要有可信边界，要有安全可信的保护，更要有管理中心进行安全管理，相当于监护室一样，发现问题及时处理。构筑这样的安全管理体系，才能应对各种漏洞，这就是一个重要标准。这样能达到攻击者进不去的效果，即便进去了也拿不到东西，尽管拿到了也看不懂，也改不了。”用中国的可信技术，用可信计算构筑网络安全，其中，涉及核心的关键设施就是用自己的创新技术解决安全问题。要从根上解决大数据安全问题，就要构建安全管理支撑下的防御体系。因此，对于政务云平台上的应用来说，更应该具备利用可信计算来主动攻防外来病毒和漏洞侵害的预警机制和系统，并且都应该达到国家的等级保护标准，最大限度的保证政府机构云平台应用的安全性和可靠性。

广东东莞的科技地标——中科院云计算中心大厦

■相关链接

国云科技股份有限公司研发的G-Cloud云操作系统是国内自主知识产权的云计算产品，该产品可确保其上运行的应用系统安全稳定，并提高信息安全防护能力。国云科技的等保云服务是基于G-Cloud云操作系统，针对最新网络安全等级保护标准，为客户提供可满足网络安全等级保护二级、三级要求的信息安全服务，利用云计算快速、低成本的优势，联合各地服务质量优异的咨询和测评机构，为客户提供一站式、可定制的信息安全服务。

本报社址：北京市复兴路15号 邮政编码：100038 查询电话：58884031 总编室：58884048 58884050（传真） 策划运营中心：58884126 广告许可证：018号 本报激光照排 印刷：人民日报印刷厂 每月定价：33.00元 零售：每份2.00元