跨国网络巨头独占先机 中国云平台谋求自主可控

“云”时代网络安全的中国突围

刘洪强

互联网新闻研究中心于5月26日发表的《美国全球监听行动记录》指出，美国曾秘密侵入雅虎、谷歌在各国数据中心之间的主要通信网络，窃取了数以亿计的用户信息。这也说明，近年来兴起的“云计算”在给人们带来巨大便利的同时，也存在着不容忽视的安全隐患。

1 云计算是一把双刃剑

正如业内专家所指出的，作为一种崭新的互联网模式，云计算将会是新一代也是今后很长时间的基本模式，自问世起，便受到了人们的广泛关注。云计算以现有的分布式网络为基础，用户数据的存储和运算都是在“云”上完成的，鲜明地体现了“网络便是计算机”的理念。

云计算的出现和广泛应用，不仅降低了运算成本，还极大地改变了用户以桌面为核心的使用习惯，并改变了信息获取和知识传播的方式，给人们带来了前所未有的便利。从某种程度上说，“云”时代的到来，不亚于一场革命。

“云计算掀起了一场新的互联网革命，云计算通过集中供应的模式，打破了地域和时空的限制，真正形成了信息化。通过云计算，人们可以大大提高运算效率，从而把时间和精力更有效地投入到主要工作中。”业内专家如是说。

与此同时，云计算也潜藏着一定的安全风险。甚至可以说，安全性和隐私问题已经成为困扰云计算进一步发展的一个重要瓶颈。由于数据的处理和存储都在远程的云端上完成，用户因而也容易遭受到拒绝服务攻击、中间人攻击、网络嗅探、端口扫描等多种方式的攻击。在其面临严重的网络攻击时，用户会面临数据丢失和隐私泄露等风险，乃至于威胁到社会稳定和国家安全。

中国工程院院士邬贺铨指出：“云计算也有大量的安全问题，云计算逻辑上的集中容易成为攻击目标，而云储存虚拟化和物理上分布及异构化，缺乏物理安全边界。用户数据管理权与所有权分离，则使得数据面临泄露和篡改的风险。云存储面向端用户的应用程序也存在安全漏洞。”

实际上，国外不少知名互联网公司的云平台自运行以来已经发生了多次故障。此外，由于云平台上数据高度集中，其遭受攻击的风险以及遭受攻击后面临的损失也较以往呈几何级数增加。凡此种种，都增加了云安全防护的难度，也说明云安全已经成为顺利推进云计算所不容忽视的一个问题。

2 美第四空间一家独大

美国是云计算概念和技术的先行者，早在2006年，美国互联网巨头谷歌就正式提出了“云”的概念。此后，亚马逊、微软、英特尔、IBM等互联网巨头先后跟进，随后这场“云”潮流在短时间内便风靡全球。

随着计算机网络的兴起，网络空间已经成为继领土、领海和领空之后的第四空间，网络空间安全也称为国家安全的重要组成部分。有鉴于此，美国等发达国家开始积极部署，力图掌握制高点。美国为了巩固其网络霸权，一方面加强相关方面的安全防范工作，另一方面也通过其国内公司积极部署全球范围内的“云计算”架构。

早在2003年，美国总统布什就出台了《美国保护网络空间国家战略》；2009年6月，美国正式组建网络战司令部。美国目前实际上控制着全球互联网。

正如邬贺铨院士指出的，全球13个根域名服务器中除了英国、瑞典和日本各有1个之外，其余10个都在美国。而签署和发放根服务器的互联网域名与号码分配机构（ICANN）实际上是由美国控制的。尽管越来越多国家提出美国应该将互联网管理权尽快移交给国际组织管理。尽管相关各方也就此进行了多次的博弈，但美国一直拒绝将互联网管理权移交联合国。

与此同时，美国还依托国内网络巨头掌握了对全球信息的绝对控制权，并垄断和控制了云计算的发展趋势。由于云计算需要很高的技术门槛，因而全球真正有实力研发和提供云计算服务的公司只有微软、谷歌、思科、IBM等少数互联网巨头。微软还计划联合其他巨头组成“云计算联盟”。此外，英国和韩国近年也加紧推动各自国内云计算部署。

面对这一前景，尽管人们期待互联网成为一个真正的开放的空间，但由于极高的技术和资金门槛，云计算也日渐被美国等少数国家高度集中和垄断。正如《美国全球监听行动记录》所显示的，美国不单在战时对于敌国的网络封锁可以说是毫不含糊，而斯诺登事件更是说明即使在和平时期、即使对盟友，美国相关机构在对其监控中也毫无道义可言。如果未来全球的个人数据高度集中在美国公司的云计算中心，这对广大发展中国家来说并非幸事，其信息化建设的步伐将越来越受制于国际互联网巨头所制定的标准和游戏规则。

3 中国式突围任重道远

随着跨国巨头在云计算领域咄咄逼人的“圈地运动”和某些国家在云计算领域的加紧布局，一场没有硝烟的战争就此展开。如果我们不具备“自主可控”的云计算能力，那么我们将不得不借助于相关跨国巨头的云计算中心进行存储和计算数据，这将对中国的网络国家安全构成严峻挑战。

工业和信息化部总工程师张峰在近日召开的2014年中国计算机网络安全年会上说：“2014年是我国接入国际互联网20周年，如今我国已成为名副其实的网络大国。然而，互联网的发展也给经济社会带来一系列挑战，网络安全问题日益复杂，云平台、社交网络、移动互联网等新技术新业务快速发展，不断带来新的安全风险。”

尽管与美国相比，中国目前云计算基础较为薄弱，许多研究都还处在起步阶段，一些应用技术也还不成熟，而中国信息安全产业还处在重重包围之中，但“云”的理念已经弥漫各行各业，并迸发出无限的生机和活力。

正如北京天融信科技股份有限公司总裁于海波所说：“只有关键基础设施的软硬件上自主可控了，才称得上安全。20年的中国信息产业的发展，已经取得了巨大成就，比如中国安全厂商在防火墙、防入侵、防病毒这3个安全的体系关键产品或者核心产品上已经处于市场的主导地位。”

“云计算”的战争刚刚拉开序幕，如果我们能够抓住机会，在新一轮信息变革中赢得主动权，缩小与发达国家的差异，乃至于实现超越。反之，就有可能被“云计算”主导的新信息化时代所抛弃，进一步拉大差距。

尤为重要的是，经过多年信息化建设，我国信息化基础设施已经达到了相当的规模和水平，而且拥有全球最广阔的市场，如果充分发挥集中力量办大事的制度优势，就完全有可能成功建设出我国自主可控的云计算平台。

中国工程院院士倪光南说：“在这新一轮技术变革中，中国具有人才和市场优势，中国可以凭此达到其他很多发展中国家所无法实现的突破和超越。”

链接1

云计算

近年来云计算这一概念频繁出现在互联网以及媒体上。云计算是基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源。云是网络、互联网的一种比喻说法。过去在图中往往用云来表示电信网，后来也用来表示互联网和底层基础设施的抽象。目前社会上对于云计算还没有确切、统一的定义。一般认为，云计算是一种新兴的共享基础架构的方法，是此前网络领域几项重要理念与技术——分布式处理、并行处理和网格计算的发展，或者说是这些计算机科学概念的商业实现。推动它发展的是各类设备互联、实时数据流以及信息搜索、开放协作、社会网络和移动商务等Web 2.0应用的急剧增长；同时，数字元器件性能的大幅提升及价格下降带来的全社会计算机拥有量的大规模增长，既刺激了对于大规模资源进行统一管理的云计算的需求，也成为支持它发展的物质基础。

云计算的根本特点，是它发展起来一种智能算法，可以动态管理几十万台、几百万台甚至几千万台计算机资源所具有的总处理能力，并按需分配给全球用户，使他们可以在此之上构建稳定而快速的存储以及其他网络服务，而所有数据处理都是远程的，用户无须知道资料存储在哪里，也无须知道计算在哪里进行。云计算被视为科学技术领域的又一次革命。

链接2

云安全

云安全是继“云计算”之后出现的“云”技术的重要应用，是网络时代信息安全的最新体现。云安全是我国企业创造的概念。它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到云端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。云安全技术应用后，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理。云安全已经在反病毒软件中取得了广泛的应用，发挥了良好的效果。

计算机网络安全年会召开

本报汕头5月28日电 2014年中国计算机网络安全年会（第11届）28日在广东省汕头市召开。年会由国家计算机网络应急技术处理协调中心主办，历经11年发展，目前已成为网络安全领域交流的重要平台。来自政府和重要信息系统部门、行业企业、高校和科研院所等单位的代表共600余人参加了本次会议。会上还举行了汕头大数据产业发展咨询专家聘请仪式。

网络安全策略结构示意图 来源：《解放军报》

应对网络安全挑战

张峰

我国网络发展面临一系列挑战，其中，网络安全问题日益复杂突出，最近发生的微软停止对XP系统升级服务等事件，不断给我们敲响了警钟。而随着新业务、新技术快速发展，网络安全风险，特别是信息泄露风险有进一步加大趋势。目前，社交网络成为黑客攻击的新途径，移动支付安全和移动终端安全成为新挑战，这损害了广大网民的利益，对经济社会发展和国家安全造成了严重威胁。

没有网络安全就没有国家安全，网络安全和信息化是“一体两翼”，必须要统一谋划，统一部署，统一推进，统一实施。我们必须从保护国家安全，维护公众利益，促进信息化发展的高度充分认识做好网络安全的重要性和紧迫性。在党中央和国务院的部署下，近年来，工业和信息化部按照依法管理确保安全的方针，深入推进网络安全防护体系的建设，不断完善建立网络安全标准规范和机制，加强网络安全应急管理，加大互联网管理的力度，取得了积极的进展。

在当前环境下，为进一步推进国家网络安全工作，笔者认为应该加大以下四个方面的工作。

一是积极强化网络安全措施。下一代互联网、云计算、物联网和大数据等新技术的运用带来了新的网络安全风险，相关信息服务部门特别是电信企业、网络运营部门等应当积极负起责任，确保网络安全保障各项制度措施落实到位，加强关键设备采购安全，加强网络系统的安全防护，及时发现并消除重大安全隐患，不断提高关键信息技术设施的攻击能力。

二是增强组织创新能力，提高安全部署，要以企业为主体，推动信息技术特别是网络安全技术的进步和产业化。加强关键核心技术的协同和创新应用能力，不断丰富互联网信息服务，促进技术和业务模式创新，满足我国社会公众多样化的信息需求等网络安全核心技术能力，完善网络安全评估方法。

三是健全网络安全协调机制，加强国内信息安全和服务各界的合作。打造安全的网络环境需要政府和各界集团共同努力与配合，提高防范的意识，协同采取安全保障措施。网络安全厂商在信息安全中承担重要而独特的作用，因此，它们要切实承担起社会责任，与国家加强协作配合，建立健全反应灵敏的网络处理方式，提高应急效率，打造我国漏洞隐患排查和网络安全事件应急响应为一体的多方联动的防御和处理体系。

四是加强国际合作，努力提高我国在网络中的话语权。维护国际网络安全，构建更好的网络国际空间秩序，需要各国家和地区的通力合作。近年来，工业和信息化部与有关部门一起积极参与和推动建立了联合国、上合组织等政府间国际组织的网络合作机制，指导国内相关单位加强了与国际标准化组织等相关组织的合作。这些工作为我国参与互联网国际治理和增强国际网络治理话语权奠定了坚实基础。

（作者为工业和信息化部总工程师。此稿根据其在2014年中国计算机网络安全年会上的演讲编辑整理）

青年科技人才获机遇

本报北京5月28日电（记者**郝青**）5月28日，2014年全球研究理事会（GRC）全体大会在京闭幕，来自40余个国家的70多家科学机构代表110余人参加了本次会议。会议深入研讨了青年科研人才培养议题，并通过了青年人才培养原则和行动声明。

“没有全球的开放交流，科学难有巨大成就；没有青年人的后来居上，科学难有辉煌未来。”此次会议围绕青年人才培养进行了充分的研讨，旨在交流经验，相互学习借鉴，完善支持机制。

作为本次大会的一个重要成果，全球研究理事会发布了关于支持青年人才培养的原则和行动声明。声明提出，人才是科技创新过程中最关键的因素，青年人才培养关系到人类科学事业的未来，需要全球科技界的共同努力。全球研究理事会的参与者应积极思考未来几十年需要发展哪些类型的技能和培训；如何推进与履行社会责任相关的研究以及面对变化的全球社会、文化、政治、经济和环境背景，研究应如何做出贡献并随之转型。

广告处 电话 65369288 传真：（8610）65003109 总编室 65369316 经营部门 65369405 发行部 65369319 零售周一至周四1元/份 周五1.5元/份 周六1元/份 国内定价全年280.80元 国内统一刊号：CN11-0066 广告许可证：京朝工商广字0153号