十二届全国人大五次会议
全国政协十二届五次会议

两会 2017/ 特别策划 TEBIECEHUA

赢在未来 10

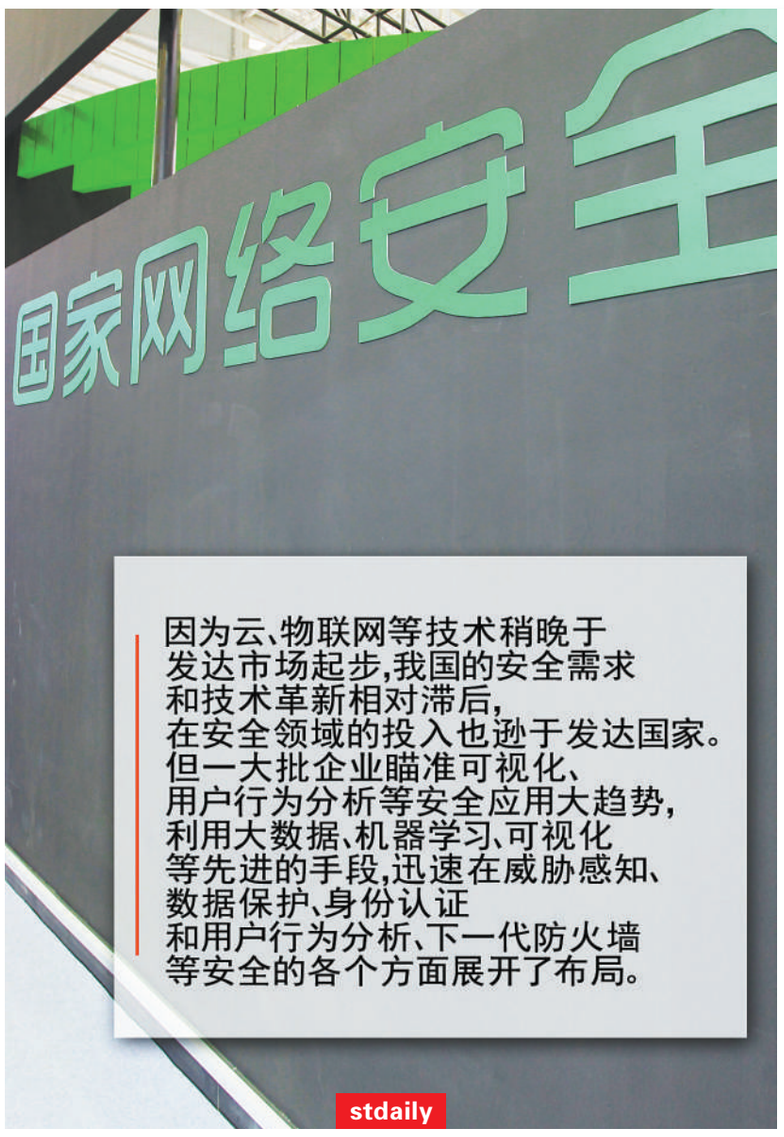
当国家针对网络安全的种种布局和举措成为街谈巷议的话题，相关政策的层层加持就如同一颗石子投入水中，在我国安全市场荡起涟漪，引发了新一波创业潮。国内安全企业数量出现爆发增长，并覆盖数据安全、应用安全、抗DDoS等各领域。

从立法推动到科技政策落地，网络安全市场有望以超预期的速度加快推进，未来三到五年行业复合增速将达到25%—30%，一个万亿级的市场正待打开。

今年1月，科技部部长万钢在2017年全国科技工作会议上指出，“科技创新2030—重大项目”将尽快编制完成实施方案。国家网络空间安全作为六个重大科技项目之一被列入其中，吹响了网络安全科技创新的总号角。

网络安全：2020年万亿市场有望打开

本报记者 刘 艳



安全可控 怎么强调都不过分

并非耸人听闻，复杂的技术组合下的攻击行为已铺天盖地的拉响了“安全警报”，网络安全和信息化日益成为我国安全领域牵一发而动全身的重要因素。

中科曙光网络安全产品事业部总经理刘立对科技日报记者说：“该怎样和你描述当前严峻的网络安全形势？从公开数据看，中国被控制的僵尸服务器或设备已超过几千万台，我们所遭受的攻击每年都在增长。”

就如同思科安全研究部门发布的《思科2017年年度网络安全报告》描述的那样，攻击者与防御者之间不断上演着没有休止的拉锯战，攻击者试图获得更多行动时间，防御者则奋力消除攻击者试图利用的机会。

这样的局面之下，“安全可控”怎么强调都不过分。

“如果无法对网络空间实现安全可控，就如同在别人的地基上盖房子，它所带来的一系列潜在安全风险，将使国家网络安全无从谈起。”曙光公司总裁历军在接受科技日报记者采访时表示，虽然我国的网络安全产业仍处于比较薄弱的发展中状态，相当一部分的核心技术尚受制于人，核心设备不能完全实现安全可控，行业国产化有待提高。但为了不将产业链的“命门”交于别人手中，大力推动国产软硬件产品的研发，培育一批具综合能力较强的龙头企业，壮大自主品牌，带动全社会应对网络威胁的能力是一条可行之路。

历军说：“可以预见的是，为真正实现网络治理的国产化，相关企业将该更加重视网络安全方面的人才培养，通过安全可信的网络产品，结合云计算、大数据、物联网等各类重要的信息技术和应用，从产业链的源头为网络安全提供保障。”

“国家网络安全列入‘科技创新2030—重大项目’，虽然要实现‘发展涵盖信息和网络两个层面的网络空间安全技术体系，提升信息保护、网络防御等技术能力’这个大目标还需多管齐下，但这种政策的落地行为对我们是非常大的激励。”志翔科技CEO蒋天仪对科技日报记者说：“因为云、物联网等技术稍晚于发达市场起步，我国的安全需求和技术革新相对滞后，在安全领域的投入也逊于发达国家。但一大批企业瞄准可视化、用户行为分析等安全应用大趋势，利用大数据、机器学习、可视化等先进的手段，迅速在威胁感知、数据保护、身份认证和用户行为分析、下一代防火墙等安全的各个方面展开布局。”

从“有边界”到“无边界”理念的转变

在网络安全发展的历史中，以入侵检测、防火墙及反病毒为代表的“边界安全产品”一直占据着主导地位，这些产品设计的基础理念是：企业边界的外部是危险的，充斥着病毒、木马等各种安全威胁，安全产品就像在企业的边界网关处加上各种各样的“锁”，将危险挡在企业门外。

令人烦恼的是，美国CSI/FBI的调查显示，80%的安全威胁来自企业内部员工或外包人员有意无意的违规行为。随着万物互联时代的开启，“边界安全产品”对内部威胁的预知与防范越来越力不从心，“上锁”不再是有效的安全保障。但是，据蒋天仪介绍，当前的国内安全市场上，传统的“边界安全产品”占据着80%以上的份额。

当我们还在用“堵”的方式进行被动式防御时，国外的网络安全逻辑框架已从单纯的边界防护上升到整个网络空间的防护，形成以“察知”为核心的网络空间管防控系统化的方案。在这个“无边界世界”里，基于用户行为分析、大数据业务风控、可视化等技术的“察知”成为安全防护的关键，网络安全向更快（机器学习、人工智能、自动化）、更准（行为识别、可视化）等方向加速演进。

事实上，RSA总裁Amit Yoran在RSA大会上发表“睡者醒来”的主题演讲时就强调，传统的网络安全防御技术已无法抗衡新的安全威胁，以防火墙为代表的被动防御策略是失败的，产业需要变革。利用大数据技术、人工智能和技术学习等新技术，让安全看得见，对未知威胁检测、可视化、分析和处置响应成为网络安全行业新的发展方向。

虽然国内大部分安全厂商还在“防和堵”套路上摸爬滚打，但主打内容识别的天空卫士、关注新型攻击检测的默安科技、定位网络空间数据安全与大数据风险管控的志翔科技等企业和他们的创新产品已开始崭露头角，并向国际领先技术与产品看齐，将网络安全向看得见的方向推进，将网络安全的防护从有边界拓向无边界。

蒋天仪对科技日报记者说：“网络技术的革新带来信息安全的新需求，和国家战略对网络空间安全的重视与投入，为我国安全市场迎来爆发创造了条件。近两年，围绕这个方向的国内优秀的安全团队与创新产品不断涌现，围绕用户行为分析、安全可视化、大数据风控等方向的安全创新技术，或将催生新的安全独角兽企业。”

技术防护网保障个人信息安全

也就一年多的时间，所有的人仿佛瞬间就明白了，国家网络安全不止是“上层建筑”或安全厂商“游说、圈地”的高冷词汇，它与民众安全不可分。尤其是“徐玉玉案”等几起网络电信诈骗案酿成的悲剧，更加剧了公众对网上安全的深度担忧。犯罪分子精心研发设计的一系列新型高危网络骗术，已使很多传统的防骗知识和防骗意识都显得过时。

在十二届全国人大五次会议于3月4日举行的新闻发布会上，个人信息泄露及保护等问题被再次提及后，汕头大学国际互联网研究院院长、互联网实验室主任方兴东表示，如果《网络安全法》将实施重点转向着眼于广大网民利益，尤其目前最灾难深重、人人备受其害的个人信息保护，将善莫大焉。

事实上，不仅《网络安全法》明确了网络空间主权的原则和网络产品和服务提供者、网络运营者的安全义务，具体确定了个人信息保护的基本规则。我国已在多项法律法规中关注并强调对个人信息的保护，在政策层面将个人信息安全上升至国家战略的高度。

我国的电信运营商也已为企业数据和客户个人信息安全构建了一个体制和技术先进的立体防护网。

据中国移动新闻处介绍，中国移动已拉起了一个涉及安全策略、安全管理、安全技术、安全运营、合规评测、服务支撑的大数据安全保障体系框架。在这个体系之下，特别强调：严控数据对外开放过程中的安全风险，确保敏感数据不出网、不出境，不在网外留存；完善数据安全内控，确保大数据资源的全生命周期安全管理；保护用户隐私信息，确保数据开放前的用户明确授权；确保大数据安全防护能力同步规划、建设、运营；确保数据安全事件的应急响应及快速处置。

对涉及用户敏感信息的关键操作，采取“关键操作、多人完成、分权制衡”的原则，用操作与授权分离、敏感信息模糊化等手段，确保所有敏感操作都有严格的控制，并对全部运维操作实行全面审计。这个防护手段被业内称为“金库模式”，已成为中国移动主导完成的9项行业标准之一。

不仅如此，中国移动还主导完成了7项国际标准，参与了全国信安标委4项前沿技术标准的制定，为运营商开展国际和行业合作治理提供了有力的技术支撑。

主　　编　林莉君
副 主 编　滕继濮
责任编辑　姜晨怡

听TA说

我们的快乐很简单

刘立 博士 中科曙光网络安全产品事业部总经理

科研的历程谈不上快乐，也许用艰辛来描述更准确。很多时候，我们这些人在外人眼里是“黑与白”间的模糊，可是，出发点和动机决定了我们所扮演的角色。

自2008年博士毕业后从中科院计算所来到曙光，就一直摸爬滚打在“网络安全”这个以吃苦耐劳、善打硬仗和攻坚战、关键时刻顶得上去的团队，有时候也会问自己，身体的疲惫和超强的压力之下，心情的愉悦究竟来自于什么？

读了这么多年书，学了这么多的技术，就一定要让它转化为成果和价值，这是技术人员的普世价值观和能始终如一钻进枯燥的产品研发的最大动力吧？当然，曙光这些年在自主可控和相关安全领域，倾注了非常多的心血，为“数据中国”保驾护航已成为曙光各条战线团队的行为准则，与此同时，公司也给了科研人员非常不错的待遇和尊重，使我们这个本就很有凝聚力的团队更具战斗力。

然而，那种美剧常展现的嘻嘻哈哈就突破了某个技术难题的场景，不是我们的研发氛围。我们的研发过程很严肃，更不指望“一帆风顺”。无论是项目的按期或提前交付，还是通过一些异常苛刻的入围测试，常会遇到种种难以预测和想象的困难，当克服“苦难”成为一种常态，那些太多值得骄傲的事情似乎也变得理所当然。

只是，每当产品研发成功并真正应用到国家大项目建设之中时，看着咧着大嘴乐的团队成员，那些艰难至催人崩溃的攻坚场景就会一幕幕在我头脑中回放，他们的快乐真的很简单。

有时我们经常会被问到一些有趣的问题，比如，你们是不是黑客呀？你们的工作场景是不是满屏滚代码呀？

怎么回答这些问题，往往成为我们快乐的“谈资”。实际上，那些满屏东西不停地滚很多时候是出于影视效果的需要，在实际工作中去编译去跑程序也会出现这种情况，而一些如帮助找回密码的简单的民用的软件工具采用“暴力破解”的方法不停地去试各种可能时，也会看到数字不停地变。但是，当前个人安全领域暴露出来的黑客拿到用户信息去“撞库”时，却不一定像影视效果展现的这么炫。

从某种角度讲，我们这些从事安全工作的人就是要识别攻击并反击，虽然从技术和行为上来讲与“黑客”没有太多的区别，但是，关键看你的目的是否用到正途。

黑科技

天盾平台与伪基站杀手

本报记者 刘 艳

围绕网络信息安全热点、焦点问题，中国移动等电信运营商也在积极提升并利用其丰富的大数据防御能力、云计算等新技术，使通讯信息诈骗治理实现了全程技术管控。

据中国移动新闻处介绍，中国移动自主研发的“天盾”反欺诈系统平台，已在浙江开展试点，实现了对国际、网间、网内诈骗电话的精准拦截和受害人群的事中提醒。仅2016年8—10月，即与公安部门联动阻止诈骗案件2203起，挽回群众经济损失1770余万元。

另据了解，中国移动在业内首创的“伪基站杀手”工具，已可精准发现“伪基站”并自动对其反制，有效解决了“伪基站”危害大、抓捕难的问题。截至目前，中国移动已配合执法机关侦破“伪基站”案件6771例，缴获设备7474套，抓获犯罪嫌疑人9182名。