探寻“安全、高效的未来互联网”

“2017年网络安全技术高峰论坛”在上海举行

国家网络安全宣传周 China Cybersecurity Week

本报讯　（首席记者　潘高峰）由中央网信办和上海市人民政府指导、上海网信办主办的“2017年网络安全技术高峰论坛”主论坛18日在上海举行。来自国内外的知名企业高管和专家学者围绕“安全、高效的未来互联网”“网络空间安全理念”“新兴技术形势下的网络空间安全新挑战”等议题展开研讨和交流。

记者从会上了解到，中国工程院院士方滨兴、中国科学院院士何积丰、中国科学院院士潘建伟、奇虎360总裁周鸿祎、中国移动副总经理李正茂，以及美国战略和国际问题研究中心网络安全专家詹姆斯·安得烈·刘易斯、诺基亚总裁李思拓、美国电话电报公司（AT&T）高级副总裁莫·卡提拜赫、卡巴斯基实验室首席专家谢尔盖·诺维科夫、美国东西方研究所高级副总裁布鲁斯·麦康纳等国内外知名企业高管和学者，在论坛上结合目前网络安全技术发展现状和存在的问题，从安全理念、新一代互联网、关键信息基础设施保护、个人信息保护等方面发表了自己的真知灼见。

中央网信办副主任杨小伟在会上表示，网络信息技术革命和产业变革正在孕育兴起，科技创新呈现出新的发展态势和特征，对整个经济社会发展的融合、渗透、驱动作用日趋明显，深刻改变着人们的生产生活方式，带来的网络安全风险和挑战也不断增大。网络攻击、网络窃密、网络欺诈、侵害公民个人信息等现象频发，网络安全已成为事关经济社会发展、国家长治久安和人民群众福祉的重大战略问题。

杨小伟说，要立足开放环境维护网络安全，维护网络安全要正确处理开放和自主的关系，树立全球视野和开放心态，在坚持自主创新的基础上，学习借鉴国际先进经验和技术成果，最大程度利用网络空间发展潜力，借助“他山之石”提升我国网络安全发展水平。通过积极有效的国际交流、合作、互动，建立多边、民主、透明的国际互联网治理体系，共同构建和平、安全、开放、合作、有序的网络空间，携手构建网络空间命运共同体。

同时，推动网络安全技术创新和前瞻布局。互联网领域发展变化非常快，新技术、新应用带来的新问题、新挑战层出不穷。要加强技术创新，密切跟踪技术发展演进，同步做好安全防护。在物联网安全、区块链安全、人工智能安全、5G安全等方面加大研究力度，提早谋划，预先布局，有效防范不断变化的安全风险。

杨小伟说，网络空间的竞争，归根到底是人才的竞争，加强网络安全学院、专业、学科建设，支持高校、企业及社会开展网络安全教育培训，通过多种方式大力培养网络安全人才；加快网络安全人才与创新基地建设，形成网络安全人才培养、技术创新、产业发展的良好生态，为维护网络安全提供有力智力支撑、人才保证和产业“要加强网络安全人才培养”。

上海市委常委、宣传部部长董云虎在会上表示，随着网络信息技术的不断创新，互联网对整个经济社会发展的融合、渗透、驱动作用日益明显，带来的风险挑战也不断增大。网络安全牵一发而动全身，已经成为基础性、全局性国家安全问题，成为国家非传统安全领域的重中之重。核心技术是网络安全最大的“命门”，我们要维护网络安全，必须打好核心技术攻坚战，强化关键信息基础设施安全保护、提升态势感知和应急处理能力、加强数据安全和个人信息保护，确保技术先进、攻防兼备、治网权尽在掌握、网络安全坚不可摧。

据悉，19日至20日，高峰论坛还将分别举办“关键信息基础设施安全”“提升网民网络素养　共建清朗网络空间”“网络安全态势感知”“网络·劳动·安全——移动互联时代的挑战与责任”“大数据安全与个人信息保护”“网络安全技术标准”等六个主题分论坛。

网络安全关键靠人　人工智能或有隐患

“这并非危言耸听，自从手机歇菜后，我的物联网烤箱就关不掉了……满园糊味关不住……”昨天下午举行的2017国家网络安全宣传周网络安全技术高峰论坛上，诺基亚公司董事长、芬安全公司董事长兼创始人李思拓在大屏幕上展示的一段文字引来一片笑声。笑声也引发思考。高科技、智能化是不是就意味着更安全？与会专家们认为，有时恰恰相反：物联网的智能，意味着更易受攻击，人工智能更是“亦矛亦盾”。如何应对新技术给网络安全带来的挑战？昨天，各方专家纷纷发表见解。

新技术是一把“双刃剑”

“互联网技术是很多人眼中的新经济增长点。”何积丰院士昨天指出，根据2017年公布的新兴技术成熟度曲线显示，人工智能、沉浸式体验、数字化平台是人们期望最大的新增长点。

但何积丰用“亦盾亦矛”“内忧外患”来形容人工智能。从积极方面来看，人工智能可以构建防御体系，运用态势感知、追根溯源等手段实现主动防御。然而，一旦人工智能被运用到攻击性武器上，它也能轻易攻破个人设置的安全密码，获取大量个人信息。

具体到现实生活中，人工智能一方面面临着诸如无人机乱飞、黑飞，自动驾驶汽车程序失控等内部问题；另一方面，也存在着被恐怖分子、黑客组织等外部力量劫持利用，从而被当作攻击性武器的可能。“如果恐怖分子劫持一架无人机，会对城市安全造成巨大的威胁。”

心脏起搏器也会遭勒索？

诺基亚董事长李思拓举的例子更直截了当：“不远的将来，大家身上带着一个心脏起搏器，而起搏器上收到一个信息，不法分子说我们在每个小时里面有几分钟让你的起搏器停止使用，你要付钱给我们，比如付比特币，不然就持续操纵你的起搏器。这时你该怎么办？”

李思拓认为这并非异想天开，从目前来看，互联互通的技术会越来越廉价，所有制造企业的设备将来都会多多少少去联网，“今天，想要买到一台联网的烤箱还很难，但也许在不久的将来，想要在商店买到一台不能联网的烤箱才困难”。在这样的潮流下，原本不需要联网的制造业企业，也会寻求变化，无论消费者是否真的从中获益，企业都会为自己的新产品接上网络。因此，李思拓认为，解决安全问题，不仅需要加强技术和法律监管，同时也要让普通人能够牢记，“智能也意味着脆弱”。

网络安全关键还是靠人

新技术带来新挑战，但不意味着停步不前才最安全。奇虎360董事长周鸿祎认为，必须在认识危机的同时，认识到网络安全不再是网络层面问题，也不只是查杀病毒或运营渠道的问题，“当今社会已经进入一个大安全时代，应该想想有哪些策略需要调整”。周鸿祎说，今天有个看起来很悲观的观点，就是没有攻不破的网络，任何网络都会攻破，只是时间问题，没有绝对的安全。周鸿祎认为，其实一切是有解的，这个答案就是人。

“所有网络安全里面最薄弱的环节是人，漏洞是人造的，管理问题也是人导致的；但最后解决问题的，不是所谓的软硬件和规定，而是要有专业的、高智商的网络安全专家，要有全社会网络安全知识的普及。”周鸿祎认为，这也契合了网络安全宣传周的主题，就是网络安全靠人民，“我们要发挥中国的人才优势和人口红利，打一场网络安全的人民战争”。

首席记者　**潘高峰**

● 亚信网络空间平安城市指挥中心，通过平台管理实现对城市网络安全的治理和守护　本报记者　刘歆　摄

2017年国家网络安全宣传周博览会探营——

“巧科技”破解盗卡泄密难题

二维码中隐藏木马链接，轻轻一“蹭”就盗走银行卡信息，连上公共wifi都让个人资料瞬间外泄……移动互联网时代，人们日益关注网络安全方面的隐忧。昨天，记者在2017年网络安全博览会暨网络安全成就展上看到，参展企业带来大量安防方案：二维码木马识别技术，信息防泄露保护卡，公民网络电子身份标识eID……

自动识别二维码木马

在阿里巴巴和蚂蚁金服展台前，一个“奇怪”的二维码引起记者注意。仔细一看，这个二维码是由数十个小二维码“拼”成的。蚂蚁金服安全专家王亦菲介绍，这些小二维码全是木马链接。记者打开手机支付宝一扫描，手机上马上跳出“此链接有风险”的提醒，扫码失败。“现在大家都习惯出门、吃饭随时扫一扫，但也有坏人故意在商场等公共区域贴上含钓鱼链接、欺诈木马的二维码，一般用户难以辨别。”蚂蚁金服副总裁芮雄文说，用户通过支付宝APP进行扫码时，支付宝会对二维码链接进行钓鱼和木马检测，当检测到风险时，会弹出“风险提示框”，另外支付宝风控系统会对感染木马设备的用户账号进行保护，并通过数据分析、数据挖掘进行机器学习，自动更新监控策略，提升防御能力。

薄片解决“擦肩盗卡”

随身携带的银行卡，与人“擦肩而过”的工夫，卡内信息竟流入对方手中。展会上，“众人科技”展台的简易“盗刷”演示让人意外。

只见工作人员用一台手机轻轻贴住一张具有闪付功能的银行卡，几秒种后，包括银行卡号、用户身份信息、消费记录等内容都出现在手机上。工作人员介绍，此类具有闪付功能的银行卡，一旦卡号和卡背面的验证码同时泄露，不法分子便可不输入密码就能完成多种类型支付。

作为对策，工作人员展示了防盗刷“神器”——信息防泄露保护卡，只要将这张几毫米厚的卡与银行卡放在一起，便可阻挡所有读卡识别信号。展方表示，希望通过这款产品提升普通市民的安全意识。

eID破解隐私泄露难题

互联网时代，隐私泄漏、身份证冒用等安全问题阻碍了电子政务、电子商务发展。记者在现场了解到，公安部第三研究所针对此类问题，推出了“网络电子身份标识”eID。

“简单来说，eID就是公民在网络上的身份标识。”公安部第三研究所工作人员透露，eID是以密码技术为基础、以智能安全芯片为载体、由“公安部公民网络身份识别系统”签发给公民的网络电子身份标识，能在不泄露身份信息的前提下在线远程识别。eID含有由智能安全芯片内部产生的非对称密钥匙，这个信息在传递过程中是不可逆的，无法被非法读取、复制、篡改或使用。

据介绍，eID已与多家银行签约，发行加载eID的金融IC卡，不动产领域试点也将开始。未来，eID将通过更多种类的银行卡、移动电话SIM卡推广，用户使用搭载eID的银行卡或智能手机时，无须在网上提交自己的个人信息，就能方便进行网上交易。　首席记者　**潘高峰**