当前移动电子政务的安全保密问题

● 陈 龙 / 扬州市邗江区保密局

据统计，2016年我国338个城市电子政务发展指数平均值为46.59，大部分城市已具备了基础在线服务能力[1]；《2016联合国电子政务调查报告》显示，我国的电子政务发展指数国际排名第63位[2]，同比稳步上升，充分说明我国电子政务发展取得长足的进步，但与发达国家相比仍存差距；2016年，我国使用移动设备上网的人群占比已提升至92.5%[3]，网民上网的方式逐步向移动端集中，移动设备的更新换代、移动网络的迅猛发展，给电子政务发展带来了新的契机。作为传统电子政务的外延，移动电子政务这种新兴的模式正改变着政府人员的办公方式，成为各地提升电子政务服务水平的一个有力切入点。然而，我们也要看到，由于移动电子政务具有一定的安全局限性且办公人员安全素养尚有待提高，当前移动电子政务的安全保密问题仍然比较突出。

移动电子政务存在的安全保密问题

首先，对移动电子政务安全形势认识不到位。有的移动电子政务集政务公开、公文交换、行政审批、视频会议等功能于一体，功能可谓很强大，使用可谓很方便，但办公人员对于移动电子政务可以实现什么功能、能够传输哪类信息、可以运行于何种网络环境尚缺乏清晰认识。例如，有的将带有“内部资料、注意保密”的文件上传到服务器，有的甚至将敏感事件的现场视频通过移动电子政务进行传输。与此同时，用户对移动电子政务安全认识存在偏差，尤其是对于所传输的文字及图片、音频、视频该不该进行保密审查、怎么审查不能做到心中有数。因此，移动电子政务信息安全面临许多潜在风险。

其次，移动电子政务自身存在的安全局限性。相较于传统电子政务，移动电子政务灵活、便捷、智能的优势使其大有取代传统电子政务的趋势，但在现有技术条件下，移动电子政务平台的安全局限也是显而易见的。一是移动终端的“先天”安全局限性。虽然用户可以随时随地通过移动终端电子政务平台实现在线办公，在带来便捷的同时，这也是一把双刃剑，因为移动网络和发布信息的低可控性加大了监管的难度。特别是对属于个人私有财产的移动终端如何进行监管以及对存储、处理过一定数量工作信息的被淘汰终端如何处置，都是移动电子政务推广之后迫切需要解决的问题。二是终端操作系统的不安全性。无论是Android还是iOS都频繁被曝出存在漏洞，而这些漏洞也给恶意软件以可乘之机。诺基亚公司最新公布的“威胁情报报告”（Threat Intelligence Report）显示，2016年的全球恶意软件感染率同比增长400%，其中85%为移动终端感染[4]，由此看出当前移动网络环境并不安全。有一些用户为了追求用户体验，通过Root或越狱的方法获得最高的系统权限，极大地破坏了系统原有的封闭性和稳定性，降低了系统的安全性。三是移动网络存在安全风险。当前，移动电子政务主要通过无线通信技术（Wi-Fi）或蜂窝移动通信技术（3G、4G）来实现网络通信，无论是何种数据网络，都存在着如中间人嗅探或钓鱼网站诈骗等安全风险，同时未经加密的数据在

传输过程中也容易被窃取或篡改。特别是Wi-Fi技术，由于未使用跳频技术或自身缺少有线网线的物理结构保护，虽然采用了WPA/WPA2加密算法，但由于现有的WPS应用可能存在漏洞，使路由器的接入密码和后台管理密码有暴露的可能，Wi-Fi的安全仍受到威胁。

最后，移动电子政务技防能力的欠缺。当前，移动电子政务重应用、轻防护的情况比较普遍，若没有必要的技术防范手段，仅拓展功能，会持续增加安全保密风险。由于移动电子政务平台建设的低门槛情况比较突出，建设单位普遍对技术防护重视不够，一些单位借助了微信群进行“在线办公”，这其中存在很大的安全风险，因此亟须针对移动电子政务制定统一规范的安全技术防范标准。又由于当前对于互联网涉密（敏感）信息的管理主要通过关键字筛选加人工筛查的方式，但政务信息数据量庞大，筛选效率低、管理效果尚不理想。同时，随着移动网络的发展，移动电子政务的信息载体已由传统文字发展到今天的图片、视频、音频等多种形式，对于这部分信息的管理尚缺乏行之有效的技术手段。

针对当前移动电子政务发展过程中比较突出的安全保密问题，笔者认为，既不能轻视也不必恐慌，这是新兴事物发展的必然过程，只要我们积极应对，就能变被动为主动，推进移动电子政务的健康发展。

相关防范措施

明确移动电子政务属性

在现有技术条件下，非涉密网络的安全性明显低于涉密网络，移动网络的安全性明显低于有线网络。因此，在移动网络安全防护能力未有明显提升的情况下，应明确移动电子政务的非涉密属性，只能用于处理非涉密信息。

提高办公人员的安全保密素养

一是加强安全保密教育。开展经常性的安全保密教育，组织学习保密法律法规，特别是互联网、信息系统、信息设备安全保密管理相关规定，加强保密技术防范常识教育。要求工作人员不得在移动终端上存储、处理涉密（敏感）信息，引导办公人员养成良好的上网习惯，例如，不随意连接公共场所Wi-Fi热点，定期进行系统升级和病毒查杀。一旦发现终端存在安全风险，立即与系统管理员联系，锁定系统账号，尽可能减少损失。

二是加强保密管理。认真贯彻保密法律法规和《信息安全等级保护管理办法》《信息安全等级保护定级指南》《电子政务保密管理指南》等规定，切实加强移动电子政务平台的信息安全等级保护工作，不能简单地将其作为现有电子政务平台的外延或子系统进行管理；认真落实《政府信息公开条例》，切实加强信息公开保密审查工作，结合移动电子政务的特征，采取切实有效的审查方式、审查程序，确保“先审查，后公开”“涉密信息不上网，上网信息不涉密”；结合《“互联网+政务服务”技术体系建设指南》和地方实际，切实推动移动电子政务技术体系建设。

三是加强数据管理。各级政务服务系统的数据库管理系统要做好数据库自身的安全配置，登录账户要专人专管，口令要实现数字和字母符号混合设置并定期更换，且不得与其他平台口令和私人口令相同，防止外网和内网用户直接访问或恶意攻击。要定期做好本地重要数据备份和异地的远程数据备份。备份恢复工作要专人负责、责任到人。

完善移动电子政务安全保密机制

针对当前移动电子政务快速发展的实际情况，建议加快建立健全安全保密防范机制，主动应对潜在的安全风险。

一是完善移动电子政务网络安全保密标准。针对移动电子政务呈现的新特点，在不同的安全域边界部署防火墙系统，在上下级网络边界

部署VPN虚拟专用网关设备，可在核心交换区部署IPS入侵防御系统，在相应的设备上根据自身网络结构配置相应的安全策略，保障必要的数据和服务交换安全。建立健全更有针对性的安全保密技术标准，提高准入门槛，对于接入认证、访问授权、防病毒、防入侵、防篡改、防抵赖验证、防泄露等方面提出更为明确的要求，对于涉及社会保障、医疗卫生、文体教育等重要领域，提出更加严格的技术要求和管理标准。

二是加强移动电子政务终端安全保密管理。制定移动电子政务终端管理办法，根据移动电子政务平台和终端自身的安全防护等级，对其所处理的政务敏感度提出明确要求，严禁非涉密设备存储、处理涉密信息，禁止低防护等级设备存储、处理高敏感度信息，同时对移动终端网络连接方式、移动电子政务应用程序上线流程进行规范，对拟淘汰终端提出技术处理要求，以防范信息泄露。

建立健全移动电子政务服务安全保障体系

随着信息技术的发展，信息由单一的结构化数据转变为复杂的非结构化数据，对于信息采集、分析、监控、预警提出更高的要求，因此要切实提升安全保密技术防范能力。

在终端安全方面，建议用户启用指纹、人脸、虹膜等身份识别技术，完善身份识别系统；通过安装的终端安全应用产品，实现远程数据擦除，对非法的网络链接、恶意信息、钓鱼Wi-Fi进行提示、警告和屏蔽。

在用户安全方面，按照“后台实名、前台自愿”的原则，对于移动电子政务用户进行基于移动电话号码等真实身份信息认证，默认采用身份证号码登录，或已绑定手机号码登录。登录过程中，应采用短信验证、口令等方式提高安全性；建立系统日志，实现用户操作的全程可追溯；对重要数据实行服务器端存储、处理策略，规范用户在终端进行数据存储和处理行为，加强移动电子政务用户权限管理，拒绝未经授权访问。

在网络安全方面，推广用户身份绑定、数字证书，强化接入认证管理；规范网关、防火墙等安全设备，安全卫士、杀毒软件等安全软件的配备，并做好设备及软件的升级更新工作，有效防范各种病毒入侵、恶意攻击；在重要政务平台推广VPN加密通信技术，防范重要信息泄露。

在平台监管方面，严格落实《移动互联网应用程序信息服务管理规定》，切实加强对应用程序、应用程序提供者以及应用商店的监督管理执法工作，同时要加快部署具备实时比对、自动筛选功能的互联网信息管理系统，加强对微信、微博等自通信媒体的规范与管理，提升对违法违规信息发布的发现、处置能力。END

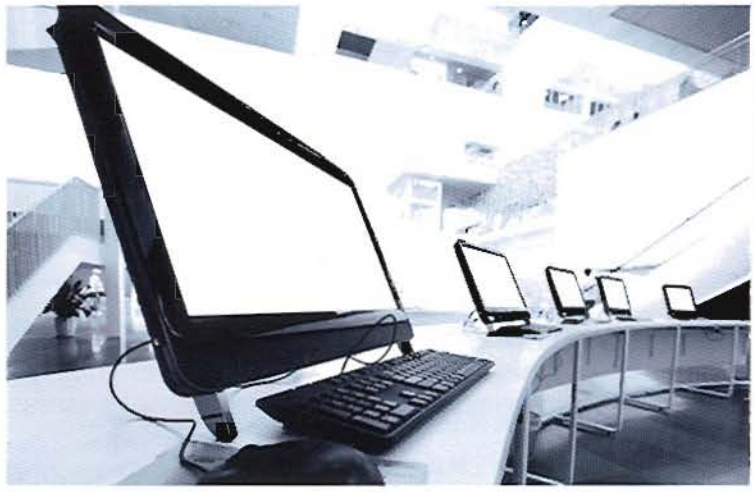
参考文献：

[1] 2016中国城市电子政务调查报告在京发布[EB/OL].(2016-8-22)[2017-4-25].http://news.china.com.cn/2016-08/02/content_39005954.htm.

[2] 《2016联合国电子政务调查报告》发布[EB/OL].(2016-7-31)[2017-4-25].http://mt.sohu.com/20160731/n461898396.shtml.

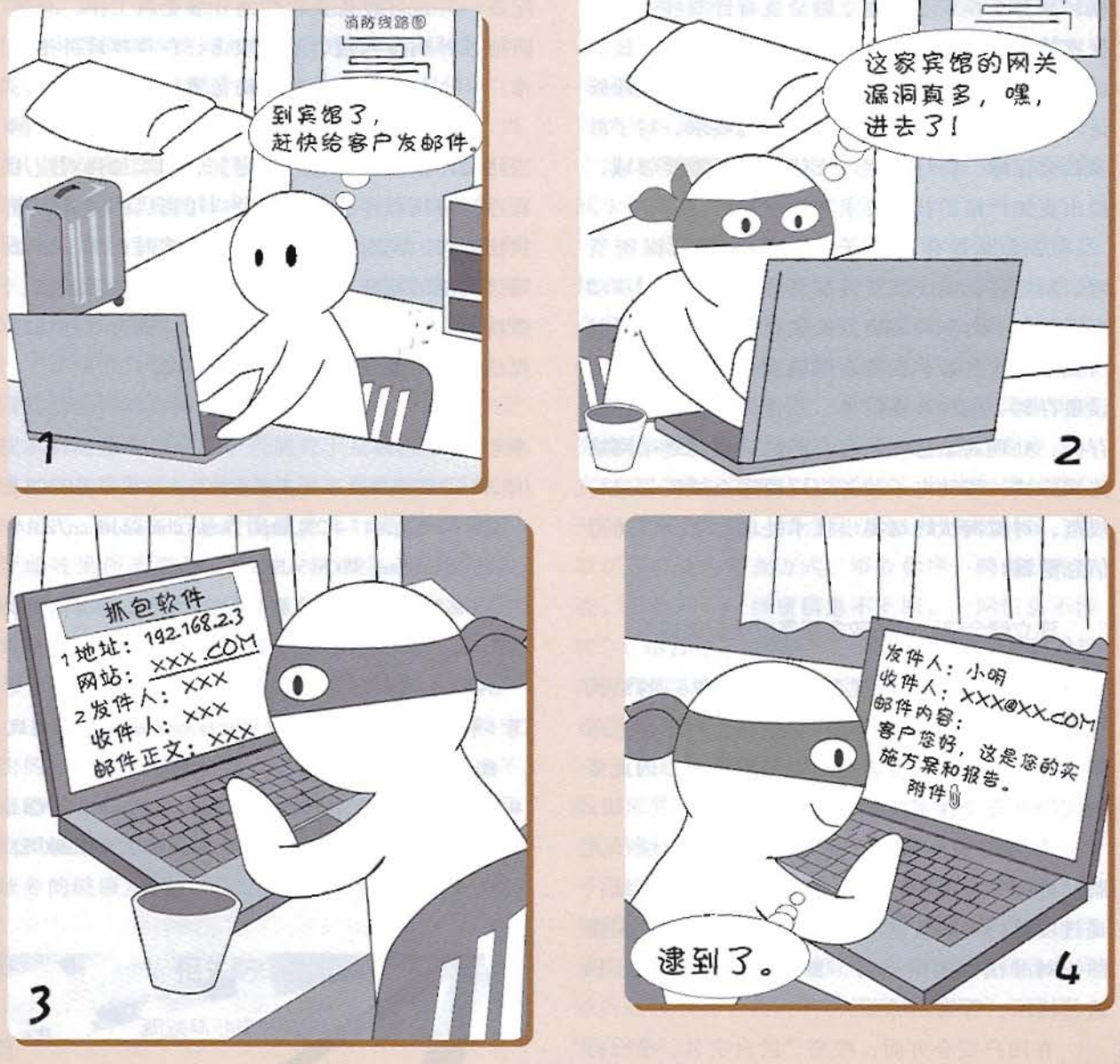
[3] 《中国互联网络发展状况统计报告》发布[J]. 新闻战线,2016,(17):146.

[4] 2016恶意软件感染率增长400%安卓成重灾区[EB/OL].(2017-3-28)[2017-4-25].http://soft.yesky.com/223/113890723.shtml.



信息安全意识漫谈——邮件安全篇

◆ 传输加密



◆ 案例解析：

一些公共网络的安全性较差，黑客很容易入侵到其网关设备并监控网络流量。如果收发邮件时没有采取加密手段，黑客很容易抓到数据包后还原出邮件正文和附件。

◆ 安全建议：

- 收发含有敏感信息的邮件时要确保传输通道是加密的。
- WEB邮箱的传输是否加密要看URL是HTTP还是HTTPS，若是HTTPS则说明是加密传输。
- 邮件客户端的加密设置一般为在发送和接收服务器设置处勾选SSL。

下期将为您继续介绍邮件安全相关的信息安全常识，希望您继续关注！ END （绿盟科技供稿）

信息安全小百科

云存储与信息安全

现在，人们都喜欢使用服务商提供的云存储功能，将照片、通信录、非涉密工作资料等数据上传到网盘、大容量邮箱等云端进行保存，可随时随地通过PC，手机、平板等移动智能终端登录账户，输入口令，进行下载、查看和分享。这种云存储功能使用方便、快捷，既可承担数据备份功能，又能对数据进行云端备份，防止智能终端丢失而造成的重要电子数据丢失，给人们的日常工作与生活带来极大的便利。

云存储

云存储（Cloud Storage）是在云计算概念上延伸和发展出来的新概念，是一种新兴网络存储技术。云存储概念和云计算类似，是通过集群应用、网格技术或分布式文件系统等功能，将网络中大量不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统，具有保证数据安全、节约存储空间等优势。

云存储系统是一个多存储设备、多应用、多服务协同工作的集合体，任何单一的存储系统都不是云存储。云存储系统指的不仅仅是存储，更多的是应用和服务。应用云存储技术，可将所有的存储资源整合到一起，实现自动化和智能化管理，在一定程度上解决了存储空间的浪费问题，提高了存储空间的利用率，降低了运营成本，同时具备负载均衡、故障冗余功能。

云存储与信息安全

近期，美国国家标准技术研究院（NIST）发布了SP.800-184《网络安全事件恢复指南》，旨在帮助各类组织机构制订并实施恢复计划，以应对随时可能出现的各类网络攻击活动。该指南对云存储的发展提出了明确的路线，指出了包括数据备份、灾难恢复、应急预案等在内的数据恢复规划。

由此可见，云存储在为大家提供便利的同时也存在一定的安全风险。例如，苹果的iCloud曾遭非法攻击，导致大批好莱坞女星私照流出。归结起来，导致云存储信息泄露的原因主要有以下3点：一是存储账户和密码被非法盗取、破解，二是存储和传输数据过程中没有加密或简单加密，三是云服务商遭受攻击。

那么，在日常工作生活中我们该如何防范可能发生的数据泄露风险呢？一是不往云端上传敏感信息，如工作秘密、个人隐私、银行卡信息等。这些敏感信息可备份在U盘、光盘等与外界有物理隔离的介质上。二是保护好账户名和密码。设置较为复杂的账户和密码，并妥善保管。三是对网盘内容进行加密。目前，大多数云存储网盘都提供文件加密功能，登录网盘后，需输入密码才能查看文件。四是尽量不要选择自动备份功能。很多手机服务商都为用户提供可自动将手机照片、通信录、数据等定期备份至云端的功能选择，这项功能易造成隐私信息的误上传。END

（康双勇/国家保密科技测评中心）

（栏目编辑：郝君婷）

两高“释法”为公民个人信息护航

5月9日，最高人民法院与最高人民检察院联合发布《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下称《解释》）及相关典型案例，该《解释》自2017年6月1日起施行。据悉，这是首次针对侵犯个人信息犯罪的定罪量刑明确标准，此举再度引起社会对个人信息安全的关注。本次两高《解释》明确了“公民个人信息”范围，划定了“情节严重”标准，明确规定严打信息公司“内鬼”等，这些将对打击侵犯个人信息犯罪提供了可操作性依据。

（http://www.it.people.com.cn）

中国成立“类脑国家工程实验室”借鉴人脑攻关人工智能

我国类脑智能技术及应用国家工程实验室日前在合肥成立，将借鉴人脑机制攻关人工智能技术，推进类脑神经芯片、类脑智能机器人等新兴产业发展。今年1月，国家发改委批复中国科学技术大学牵头承建“类脑智能技术及应用国家工程实验室”，共建单位包括复旦大学、中科院沈阳自动化所、中科院微电子所和百度公司，共同建设类脑智能技术应用研究平台，支撑开展类脑认知与神经计算、类脑芯片与系统、类脑智能机器人等技术的研发与工程化。目前，类脑智能的发展面临三大瓶颈，即脑机理认知不清楚、类脑计算模型和算法不精确、计算架构和能力受制约，类脑实验室将围绕这三大瓶颈展开攻关。

（http://www.it.people.com.cn）

科技部发布先进制造技术领域科技创新专项规划

为明确“十三五”先进制造技术领域科技创新的总体思路、发展目标、重点任务和实施保障，推动先进制造技术领域创新能力提升，科技部组织制定了《“十三五”先进制造技术领域科技创新专项规划》（简称《专项规划》）。《专项规划》明确，“十三五”期间，我国先进制造领域重点从“系统集成、智能装备、制造基础和先进制造科技创新示范工程”4个层面，围绕3D打印、激光制造、智能机器人等13个主要方向开展重点任务部署。《专项规划》要求，在“十三五”期间在战略布局上要瞄准国际制造业发展的最前沿，力争率先突破，构筑先发优势。依托新兴信息技术，建立健全制造业的创新发展模式，形成网络协同制造创新服务体系，提高市场竞争力。

（http://www.it.people.com.cn）

27.7%

全球首个“关键信息基础设施网络安全状况分析报告”于近日发布，指出在针对关键信息基础设施领域的攻击中，敏感信息泄露事件占比最高，达27.7%。

60多年

美国国家安全局（NSA）前雇员斯诺登提供最新爆料，日本从1950年代就开始与NSA秘密合作，对周边国家和中东地区实施监控，至今已60多年。

5万

360网络安全研究院近日发布报告，率先披露了一个名为http81的新型IoT僵尸网络。监测数据显示，该僵尸网络在中国已感染控制超5万台网络摄像头。

中国科学家在量子计算机研发方面取得系列突破

日前，中国科学技术大学潘建伟教授及其同事陆朝阳教授、朱晓波教授等，联合浙江大学王浩华教授研究组，在基于光子和超导体系的量子计算机研究方面取得了系列突破性进展。5月3日，该研究团队正式发布了这一系列研究成果。潘建伟在现场宣布，在光学体系，研究团队在去年首次实现十光子纠缠操纵的基础上，利用高品质量子点单光子源构建了世界首台超越早期经典计算机的光量子计算机。在超导体系，研究团队打破了之前由谷歌、美国国家航空航天局（NASA）和加州大学圣塔芭芭拉分校（UCSB）公开报道的9个超导量子比特的操纵，实现了目前世界上最大数目（10个）超导量子比特的纠缠，并在超导量子处理器上实现了快速求解线性方程组的量子算法。

（http://www.cac.gov.cn）

我国5G第二阶段技术试验预计年底完成

工信部信息通信发展司司长闻库近日在国新办新闻发布会上表示，我国5G技术研发已进入第二阶段试验，该阶段试验更加注重技术方案的集成度和可实现性，预计到今年底完成。据了解，目前我国已在北京怀柔规划了5G试验外场，并加快了5G频率的规划。闻库提到，未来要重点开展面向移动互联网、低时延高可靠和低功耗大连接这三大5G典型场景相关技术方案的研发与试验，并将引入国内外芯片和仪表厂商，共同推动5G产业链成熟，推动形成全球统一的5G标准。

（http://www.cac.gov.cn）

人工智能“情感交互”标准有望推出

日前，中国科研团队提出有关“情感交互”的标准获得正式立项，由此再次打开了人们对于人工智能的种种幻想。情感交互已成为人工智能领域中的热点方向，其目的就是让人机交互变得更加自然。但是，目前人机交互界面中情感交互信息的处理方式多种多样、情感描述方式，情感数据获取和处理过程，情感表达方式等均缺乏统一的标准。王宏安还告诉记者，该标准不仅是中国在“用户界面”领域第一个立项的国际标准项目，也是国际“用户界面”分委会第一个关于情感计算的标准项目，可以说填补了国内外该领域标准的空白。

（http://www.cac.gov.cn）

（本栏目数据内容摘自相关媒体、网站）

1.51亿

美国国家情报总监办公室最新报告显示，即便国会已出台遏制国安局（NSA）大规模收集电话记录的新法系统，但其仍在2016年收集1.51亿多条电话记录。

8.36亿

工业和信息化部最新发布的通信业经济运行情况显示，我国4G用户总数达到8.14亿户，占移动电话用户总数的比重达到61.1%。

29.2亿

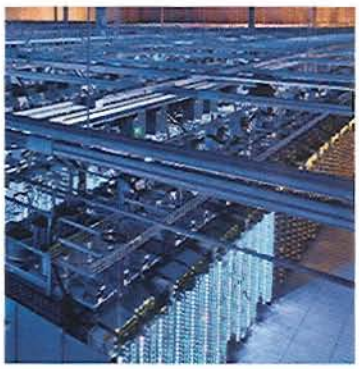
据印度普纳研究机构MarketsandMarkets预测，预计到2022年，全球移动加密市场规模将达到29.2亿美元，在未来5年将增长近3倍。

威 胁

FireEye报告称工业环境存在六大软肋

据报道，FireEye最新的报告盘点了多家工业企业共有的一些软肋，这些企业包括电力公司、石油公司和制造业。报告作者Sean McBride指出了工业领域所使用的多项进程和技术背后的种种问题，这些问题有时候容易被企业所忽略。报告中列举了有关协议、硬件、身份认证、关系、文件完整性和操作系统的6个薄弱点。考虑到许多工业环境中的具体情况，报告所强调的多个问题很难得到解决。考虑到FireEye已经在工业领域投入极大，很多观点极有可能是对几年来出现问题的归纳。

（http://www.ics-cert.org.cn）



Windows操作系统勒索软件Wannacry对我国构成威胁

近日，互联网上出现针对Windows操作系统的勒索软件Wannacry攻击案例。勒索软件利用此前披露的Windows SMB服务漏洞（对应微软漏洞公告：MS17-010）攻击手段，向终端用户进行渗透传播，并向用户勒索比特币或其他价值物。包括高校、能源等重要信息系统在内的多个国内用户受到攻击，已对我国互联网络构成较为严重的安全威胁。

（http://www.cert.org.cn）

英特尔芯片曝远程执行漏洞 影响10年内的企业PC产品

英特尔近日发布消息称，安全研究人员Maksim Malyutin发现一款关键安全漏洞“CVE-2017-5689”，并于今年3月报告了该漏洞。该漏洞允许无特权的攻击者控制这些产品提供的可管理性功能，这影响了使用英特尔AMT、ISM或SBT的企业PC和设备。要获取英特尔补丁关闭该漏洞，机器制造商必须进行固件升级。而这个关键安全漏洞存在数百万的英特尔工作站和服务器芯片中长达9年之久，该漏洞潜在被利用可执行远程控制操作，并通过间谍软件感染系统。

（http://www.secdoctor.com）

数 字

（本栏目数据内容摘自相关媒体、网站）

1000亿

据韩联社报道，全球最大互联网保安企业赛门铁克（Symantec）发布最新报告称，朝鲜网络攻击集团对各银行发起攻击，窃取超1000亿韩元。

5000亿

据5月4日全国电子信息行业工作座谈会消息称，到2018年，我国智能硬件全球市场占有率将超30%，产业规模将超5000亿元。

3万亿

从2017中国智能制造创新发展论坛发布的《智能制造创新基地发展规划（2017-2021）》获悉，到2020年中国智能装备制造产业销售收入将超3万亿元。

（栏目编辑：郝君婷）