数字时代——保障安全，促进发展

中国发展高层论坛二〇一七白皮书

万事达卡

mastercard
万事达卡

摘要

数字技术助推中国的经济增长与发展。但人们也担忧，在数字经济走进千家万户、中小企业之时，网络安全却有失控之虞。在物联网等数字技术大规模应用领域，网络安全的风险尤为突出。未来中国的繁荣有赖于能否采取有力措施保障公民及中小企业的网络安全。

我们分析了欧盟、德国、加拿大等经济体相关举措后，发现对网络安全提出具体的指导细则，特别是对中小企业是必要的。汽车行业发展的历史说明，如果想有效确保行业安全，那么针对物联网等广泛应用技术的安全性标准必须简单易用，并要嵌入到产品设计环节中。同样地，众多产业联盟之所以能够成功，得益于其致力于打造开放、灵活和支持互联互通的标准。

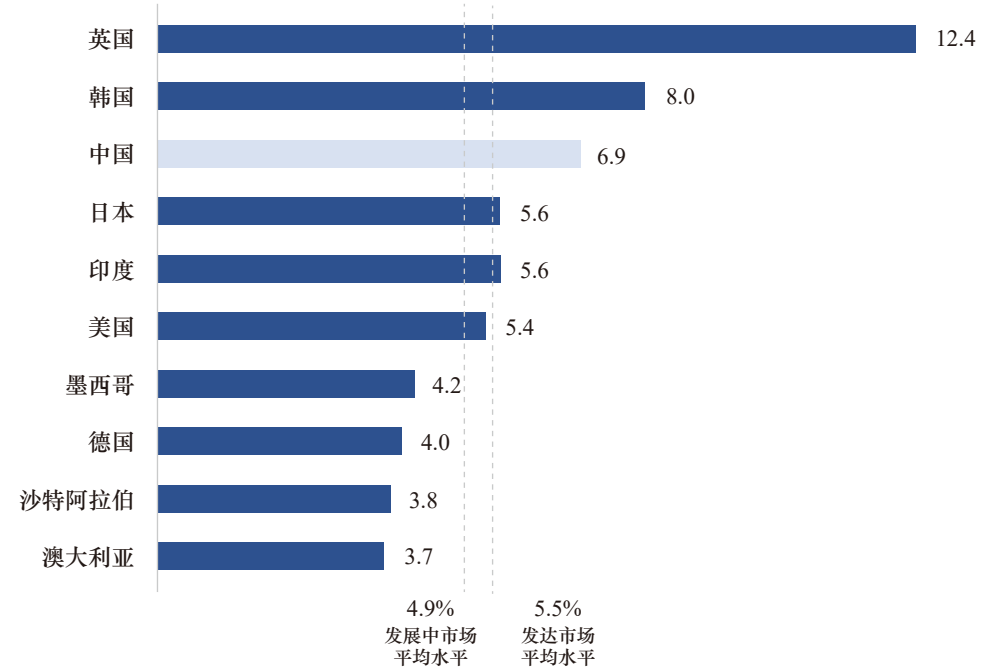
中国新近出台的《网络安全法》就重要的安全问题提出了原则性意见。为进一步保障网络安全，应该在如下领域提出更为具体的细则：一是数据安全与身份认证标准，尤其是在物联网领域；二是个人及中小企业网络安全能力建设。同时，中国的网络安全政策框架应采用通用标准，确保互联互通，并倡导多方协作，充分发挥私营领域的主观能动性。

一、数字革命推动经济的长期稳定发展

1. 中国正处在数字革命前沿

自古以来，中国就是举世闻名的信息技术领导者。在古腾堡发明活字印刷术的400年前，中国就已出现活字印刷书籍。在历史的长河中，技术创新和知识共享一直扮演着重要的角色，而在当今尤为如此。在眼下这股数字革命浪潮中，中国再一次走在了技术革命的前沿。按照公司市值计算，全球15大互联网巨头中有4家都来自中国。[1]目前，中国网民数量已达7.31亿，其中95.1%都在使用移动互联设备。[2]到2020年，中国消费者的个人消费将达到6.5万亿美元的规模，而其中网络消费将占到24%。[3]目前，中国网络经济占GDP比重已超过发达国家的平均水平。【图1】

图1：网络经济占GDP比重（2016年）



来源：麦肯锡全球研究所分析报告

中国已经为未来的发展未雨绸缪。2015年，中国的机器人相关专利申请量已占全球申请总量的35%。[4]到2035年，中国数字经济将创造4.15亿个就业岗位，技术占GDP的比例将提高至48%。[5]

此外，预计中国还将在全球物联网部署方面发挥重大影响力。预计到2020年，全球互联设备数量将突破300亿。[6]而目前，中国的移动互联设备总量已经位居世界第一。[7]到2020年，中国物联网市场规模预计将达3,610亿美元。[8]尽管从近期来看，物联网设备用户大多是企业和政府机构，但随着物联网应用的进一步普及，小型企业和普通消费者也将成为主力。对于中国广大消费者来说，互联设备将成为日常生活的一部分，并将通过微信等社交平台形成全新的人际沟通模式。更重要的是，未来将有越来越多的物联网设备将在中国制造。

2. 数字经济对中国经济再平衡至关重要

中国经济再平衡旨在促进经济更快、更持续、更具包容性地发展。为此，中国需要刺激国内个人消费、积极引导创新、鼓励更多个人和企业加入到正规经济行列。数字经济在建立消费主导、创新和包容性经济增长模式方面发挥着核心作用。

消费增长与服务业发展息息相关，而数字渠道可为服务的提供和使用带来诸多便利。同时，创新也取决于互联互通的水平，这亦是数字平台的标志特征。对个人及中小企业来说，数字技术也是促进包容性发展的重要推动力。

据麦肯锡预测，到2025年，互联网对中国劳动生产率增长的贡献将高达22%。[9]一言蔽之，中国对数字经济的把握将决定其未来经济增长与发展。

3. 中小企业将成为数字经济的重要参与者

中国的中小企业对GDP的贡献约为60%，因此，中小企业的参与对数字经济的发展至关重要。[10]同样在世界其它国家，中小企业也发挥着同等重要的作用。例如在美国申请专利数量较多的企业中，中小企业的人均专利申请数量要比大型企业多16倍。[11]而德国的中小企业可谓欧洲的创新脊梁，在2008至2010年期间，54%的德国中小企业向市场推出了创新产品或工艺。[12]

对于中小企业来说，数字技术的应用将为其带来以下三点优势：

- 第一，数字技术助力中小企业拓展市场。如今，越来越多的中国消费者选择网上购物，超过3.6亿的购物者参与国际电子商务交易。[13]目前，全球已有超过1,000万家中型企业入驻阿里巴巴，以及5,000多万中小企业注册Facebook账户。[14]

- 第二，云计算的出现让中小企业得以通过更低的成本获取更先进的技术，如存储、处理、网络及越来越多的人工智能（AI）工具。

- 第三，数字技术促进了产品和服务的个性化发展。个性化将变得越来越重要。尽管数字平台为中国的中小企业及更广泛的实体经济带来的影响整体上是积极的，但同时也给企业带来了全新的竞争压力，特别是出售大众化产品的微型企业。现在，即便规模再小的企业，都会选择出售定制化程度更高的服务，以期取得比较优势。

中小企业能否快速、安全地把握数字技术带来的优势将直接影响到中国经济和创新潜力的发挥。

二、新技术带来新隐患

尽管数字化转型具有非常显著的益处，但人们对于数据及个人信息安全也愈发担忧。

1. 个人及中小企业有更高的风险

中国的个人用户及中小企业通常缺乏必要的知识和资源来管理数字技术带来的风险。因此，他们极易成为风险薄弱环节，给其自身，乃至更广泛的网络和供应链造成不利影响。

此类安全隐患已引发重大损失。从2014至2015年，黑客窃取的个人身份信息已超过9亿条。[15]小型企业的安全形势也很严峻。2015年，全球范围内近一半的恶意网络攻击针对的是员工不足250人的小型企业。[16]

数字技术的安全威胁往往源于人为错误，其中企业电子邮件诈骗就是一个最好的案例。由于客户与供应商之间多借助电子邮件进行沟通，这就为黑客攻击提供了便利。黑客可以假冒供应商，要求客户按照发票付款或将款项转至新账户。

- 每年，英国中小企业因票据诈骗损失超过110亿美元，即平均每家中小企业损失约2,000美元。在受访的1,000家英国企业中，在过去一年中近一半收到过假冒或可疑的票据。[17]

- 近期，奥地利一家大型航空零件制造商因电子邮件诈骗损失4,200多万美元。[18]

中国用户也已成为网络攻击对象：

- 中国银监会最近点名批评了多家金融机构监管不力，存在员工出售个人信息的违规行为。[19]

- 中国人民银行副行长范一飞指出，电信网络欺诈已逐渐成为身份信息盗窃案件的重要渠道，因此需要建立起协同联动的政府响应机制。[20]

2. 物联网带来独特挑战

物联网设备的普及给数据和个人信息安全带来诸多严峻挑战，这已超越传统台式计算机和笔记本电脑的安全风险。鉴于中国在未来物联网发展中扮演的重要角色，中国应密切关注物联网行业的益处及相关风险。

互联设备创造的价值将大多源于对其所生成数据的分析。而未来物联网中的数据也将达到令人震惊的规模。一个智能家庭每周可产生10亿字节的数据，而一台互联汽车每小时可产生250亿字节的数据。[21,22]一座普通的风力发电厂每秒可生成15万个数据点。[23]

物联网不仅可以创建数据，还会形成不计其数的接入点，增加互联设备遭遇非法访问或控制的风险。10年前，一家普通大型企业通常拥有约5万个设备终端，如联网的计算机和销售终端。而到2020年，拥有涵盖数千万终端的网络将成为常态。

也就是说，随着接入点的增多，敏感信息泄露风险也随之加大。此外，为了妥善管理物联网应用引发的网络流量，需要全新的基础设施。但是，并非所有企业和消费者都能清楚了解这种新的基础设施，同时这些基础设施间也不见得能够彼此兼容。而保障物联网设备的安全要比保障家用电脑的安全更为复杂，这无异于雪上加霜。尤其对于廉价设备而言，在售出设备后，再想升级软件或安装补丁实非易事。

尽管物联网技术尚处于起步阶段，但已经引发的形形色色的风险案例说明，该技术可为个人乃至整个生态系统带来严重的安全风险。

物联网可能带来严重的人身安全风险

安全研究人员表示，从互联汽车到智能医疗设备，任何互联设备都有可能遭到黑客攻击。研究人员通过一系列实验证实，这些攻击有能力破坏互联汽车的传动系统、发动机和刹车系统，甚至针对高速公路上行驶的汽车。研究人员对多种不同车型的研究结果证实这种危险的广泛性以及后果的严重性。此外，实验表明，心脏起搏器和药物输注泵等医疗设备也能遭到严重入侵，说明互联设备可能为人类带来致命的风险。[24]

物联网对整个生态系统的风险

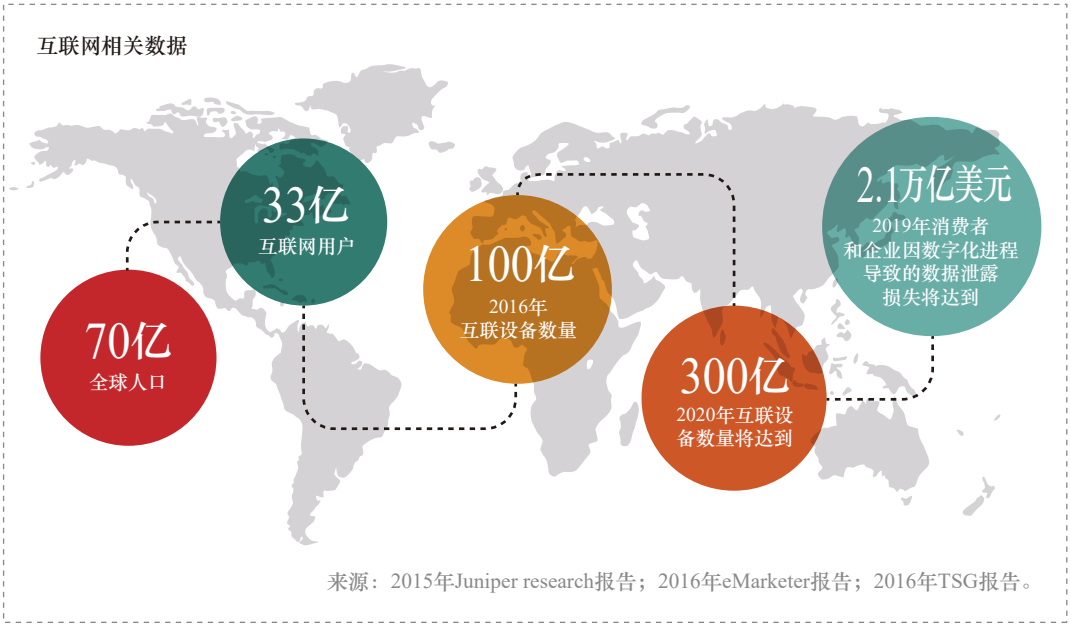
随着互联设备的大量涌现，相关风险可能扩展至更广泛的生态系统，如分布式拒绝服务（DDoS）攻击等。

- 2013年，中国国家顶级域名“.cn”曾遭受大规模DDoS网络攻击，持续时间长达数小时。[25]

- 2016年上半年，平均每周会发生近12.5万起DDoS攻击事件[26]。2016年，黑客们通过数千台互联设备对域名提供商Dyn发动攻击，导致该公司服务器瘫痪。这也成为有史以来最大规模的DDoS攻击事件，破坏程度超过以往两倍，这也导致Twitter、Netflix、GitHub和Spotify等主流网站中断服务或无法登陆达数小时之久。[27]黑客之所以能够入侵物联网设备，主要是因为设备用户未重设默认密码。[28]

随着消费者和企业的数字化程度逐渐加深，预计到2019年因数据泄漏而造成的损失可达到2.1万亿美元。【图2】

图2：物联网相关数据



三、富有活力的数字经济需要建立综合性的多层次安全保障体系

全国人大常委会表决通过了新的《网络安全法》，计划于2017年6月1日起施行。这部法律为确保中国数字经济的健康发展提出了重要的安全议题。

但在保护个人和中小企业的利益上，尚有更多工作要做。只有网络安全得到保障，个人和中小企业才能完全信任数字经济，并愿意参与其中。**一旦失去公众的信任，数字经济的繁荣也就无从谈起**。

之前的安全措施通常更多强调的是检测与响应。这次情况有所变化，因为仅靠检测与响应已远远不够。在当今的数字时代，更需要采取保护措施。为了增强消费者对中国下一阶段经济增长的信心，中国应在网络安全保障的工具、程序及流程方面采取更多措施。为此，万事达卡就以下四个方面提出建议：

1. 电子身份认证的标准；
2. 数据安全的标准；
3. 提高用户网络安全意识；
4. 帮助企业构建网络安全保障能力。

支撑网络安全的四大支柱

1. 电子身份认证标准

如果说数字经济是经济再平衡的主要动力，那么电子身份验证是数字经济成功的基础。无论企业服务还是政府服务，人们都需要通过电子身份验证。在数字经济时代，之前毫无关联的实体建立联系，如跨境交易，因此基于电子身份的交易量也与日俱增。[29]简单易用的数字身份解决方案会提升用户体验，从而推动更多用户使用数字化产品和服务。

电子身份不仅可无缝获取服务，而且与信息安全密切相关。电子身份盗用是网络诈骗的主要途径之一，美国过去六年里发生的绝大多数重大欺诈事件都由电子身份盗用引起。[30]现有的电子身份管理方法对于数字经济而言是远远不够的，我们亟需采用安全和易于使用的数字身份证书。

除了推动在更大范围内使用电子身份证书，中国应制定有关个人及设备的身份验证的标准。采用强大的身份验证方法，比如指纹识别或脸部识别技术，或更为基础性的措施（如一次性密码验证），可防止2015年美国境内发生的几乎63%的网络入侵事件。[31]网络安全政策得到完善的关键就在于可靠的身份验证。

（1）利用生物识别验证个人身份

从推广安全和简便的身份验证解决方案中，中国的网络安全将获益颇丰。此类解决方案不仅能解决问题，而且易于使用。生物特征识别技术使用户无需记忆复杂的密码即可确认真实身份，让用户免去复杂操作的麻烦，实现便利与安全合一。

我们建议，只要条件允许就应使用双重因素身份验证。这种方式在账户登录时增加了第二层身份验证，要求用户只有具备以下三类证明中的两类时，才能登陆账户。

- 用户知道的信息，例如个人识别码（PIN）、密码或图案密码
- 用户拥有的物品，例如银行卡、电话或智能手表
- 用户自身的特征，例如指纹或声音等生物特征

在推动更严格的身份验证方面，中国应鼓励采用开源标准，如在消费者应用领域的“线上快速身份认证联盟”（FIDO）的相关标准和在企业应用领域的Kerberos标准。这些标准采用符合行业标准的公共密钥密码技术，支持多种设备上持续、可靠地进行身份验证。例如，FIDO标准可支持在移动平台上实现多因素身份验证。微软的Windows 10和多家全球性金融机构均已将FIDO技术运用于个人银行业务。

案例研究：基于生物识别的身份验证

我们的下一代解决方案——万事达卡移动身份识别（Identity Check Mobile）就是万事达卡推出的一种融合当前身份验证方法（指纹和人脸识别）和未来生物识别身份验证方法的跨设备解决方案。通过采用万事达卡移动身份识别技术，金融机构就不必再让用户接受多重身份验证。这项技术还可免去生成和记住静态密码的麻烦。这项技术无论在现在，还是未来，都提供了一种更加安全、简单和一致的用户体验，从而帮助发卡银行提升运营效率。

（2）使用“设备身份”验证设备

正如用户需要了解自己在网上的交流对象的身份一样，用户也需要了解与自己通信的设备的身份。随着消费类物联网设备日益普及，对设备进行身份验证也变得十分必要。利用公共密钥密码技术，在用户已注册设备和有效验证平台之间交换公钥和私钥，即可实现设备的身份验证。将消费者生物识别验证、设备身份验证及设备密码技术相结合，就能增强多因素身份验证这一全球标准的安全性。对于医疗健康等敏感的物联网设备，应使用双因素身份验证方法。

2. 数据安全标准

中国应采用通用的数据安全标准，以确保无论物联网数据处在何处，均可通过加密或标记等方式得到保护。无论是在数据生成、传输、存储或处理过程，数据均需要得到保护，对此行业组织及政府机构已达成共识。[32]强大的数据安全措施和设备身份验证技术的结合，可能确保数据受到加密保护并且真实可靠，并确保通信过程的安全性。

数据安全也高度依赖于管理物联网设备的软件和应用程序。在大多数已知的物联网安全事件中，漏洞往往出现在应用层。因此，中国的网络安全战略应强调物联网应用的安全性，并要求物联网设备自动接收软件更新，包括安全补丁。[33]

mastercard
万事达卡

中国《网络安全法》第十五条指出，支持相关行业组织参与网络安全国家和行业标准的制定。国际上由行业联盟出面解决共同关心的安全和互联互通等问题的案例包括：工业互联网联盟（IIC）、AllSeen联盟和开放互联联盟（OIC）。AllSeen联盟和开放互联联盟（OIC）重点关注物联网软件层面相关标准的制定，而工业互联网联盟（IIC）则致力于推广可靠的工业物联网应用。

支付卡行业（PCI）委员会负责制定世界各地支付卡需达到的最低安全标准。它为行业联盟提供了一个很好的范例。

案例研究：行业合力推动全球标准

为协调和简化商户执行各个银行卡组织标准的义务，万事达卡联合其它主要卡组织在全球范围内要求商户执行《支付卡行业数据安全标准（PCI DSS）》，从而确保所有商家都能遵守最低的安全要求，同时优化它们的体验。与以往标准相比，PCI标准带来的最大不同在于能够简化商家的安全措施。在PCI委员会成立前，各家卡组织都有自己的安全体系和评估程序。

PCI DSS的主要目的是，通过防范、检测可能引发账号数据泄露（ADC）的潜在破坏或入侵，并采取措施，降低支付卡数据被窃取的风险。PCI DSS目前已发布了九部安全标准和实施这些标准所需的50多个指导文件和必备工具，规定了在支付交易过程中商家、服务提供商、软件开发商、应用程序及设备制造商应遵从的要求，包括资格评估、自评问卷、培训、教育及产品认证项目。

PCI DSS的宗旨在于保护支付卡数据免受违法行为威胁，将各种规模商家面临的数据泄露风险降至最低。PCI DSS是集全球行业和供应商的十年努力而形成的稳定的技术标准，在支付行业以外也被经常提为先进的安全标准。

物联网标准的制定可遵循“设计环节就要确保安全”的原则：中国的网络安全政策应将上述数据安全及身份验证原则在物联网设备设计环节和上市之前就作为强制要求，中国的网络安全将受益匪浅。如此，安全就不是“马后炮”，而会成为产品自

身的一部分。正如本文前面所述，已有攻击者利用默认密码和不可更改的硬证书等物联网设备的设计漏洞，造成了严重的损失。总之，我们的目的就是将安全保障机制像汽车上的安全带和安全气囊，融入物联网设备之中。

案例研究："设计环节确保安全"原则在技术中的应用

早在1908年，汽车就已在美国得到普及。但是，直到20世纪60年代中期，人们才开始重视汽车安全问题，并开始齐心协力地改善汽车安全。当时，汽车在美国人的生活中至关重要（不久后物联网设备也会如此），但在汽车发明后的五十年间，却一直存在着巨大的但可被解决的安全漏洞。当安全带、限速及安全气囊等简单措施未被推行之时，道路上发生了上万起严重的本可避免的伤亡事故。1973年，美国的车祸死亡概率每10万人中有26人遇难。次年，美国在更大范围内展开了强制要求限速和使用安全带。2015年，车祸死亡概率降至每10万人中有11人遇难，即便同期上路行驶的车辆有明显增加。[34]

3. 提高消费者网络安全意识

人的行为往往会成为确保数据安全或个人信息安全的决定性因素。实际上，无论是联合国的政府专家工作组（GGE），欧盟、德国、美国和加拿大等经济体拟定的国际性、地区性和本国内的体系，都强调提高公众网络安全意识的重要性。例如加拿大最近发布"网络安全新举措"强调亟待采取行动的三大领域之一就包括"加大力度提高公众对网络安全威胁的认识，让每个加拿大公民和企业学会如何保护自我。"[35]

除了提高公众网络安全意识外，中国网络安全体系还可支持标准的数字产品标签和评级体系，此举将让更多的消费者购买安全的设备，从而为物联网设备制造商增加安全防护功能提供激励。

网络安全宣传活动：在建立标准的标签及评级体系前，中国可采取繁简结合形式，大力开展公众网络安全意识宣传活动，提升公众网络安全意识活动目的有二：（1）鼓励用户更改默认密码，并选择适当的安全设置；（2）确保用户了解使用互联设备可能带来的潜在安全风险。

设备安全风险标签及评级：最终解决方案是设计一套由以下两部分组成的体系：（1）标准标签：告知人们与产品相关的网络安全风险及安全使用指南；（2）评级体系：依据第三方的独立评估结果，确定产品的安全等级。我们建议采用分层评级体系，这会激励物联网设备制造商提高标准，超越最低标准要求。在此，可借鉴食品包装上营养标签体系的做法，也可参考根据电量使用情况对电器进行能效评级体系。

4. 帮助企业构建网络安全保障能力

人才教育：随着数字经济的蓬勃，更多工作岗位要求人们至少具备一定程度的网络安全知识。中国需要为现有的劳动力大军提供在职培训，更要加强具备丰富经验的网络安全专业人才储备。中国政府和企业可共同努力，加强高校层面网络安全研究项目和奖学金设置，并将网络安全基础知识纳入中小学教育课程之中。上至高级主管和政府官员，下至年轻学生，都应具备基础的网络安全知识。

中国每年都会举办“国家网络安全宣传周”活动[36]，并设立了3亿人民币的网络安全基金，为专门从事网络安全的专家和教师提供财政资助。[37]

美国“网络安全教育国家倡议（NICE）网络安全人才框架”规定了几大类的网络安全工作，其中包括30多个专业领域和50多项工作职责。中国可以利用上述人才框架，对当前的网络安全人才培养开展详细评估，找出潜在的差距。

新兴安全解决方案：企业应考虑利用先进的分析工具补充人工能力。无论欺诈者多么高明，他们总会留下数据痕迹。机器学习算法可将这类数据集合起来，就能分析出相关迹象，预测后续骗局。顾名思义，这种算法会随着时间推移而不断自我学习，从而帮助我们比犯罪分子领先一步。我们可以利用此类人工智能（Al）应用软件分析行为数据，更好地保护消费者，又避免过度干扰其生活。有组织的大规模网络攻击呈现出日益增多趋势，利用人工智能解决方案可以帮助我们应对这类攻击衍生的威胁。相关技术也于近期取得了新的进展，使用起来也不再复杂。这意味着，各种规模的企业都可利用强大的人工智能来获得更强的网络安全保障能力。

中国《网络安全法》第十八条指出，国家鼓励开发网络数据安全保护和利用技术，提升网络安全保护水平，科技公司对于助力实现这一目标起着重要作用。

四、和全球标准接轨的重要性

在未来商业环境是可预测的前提下，私营企业必将成为助力中国在上述四个领域取得进步的强大合作伙伴。要想打造更加强大的政企合作关系，中国网络安全框架应遵循三大基本全球准则：（1）遵守相关国际标准；（2）实现全球互联互通；（3）利益相关方广泛合作。

1. 遵守相关国际标准

黑客们发起的网络攻击不分国界。因此，促使各国网络安全要求符合相关国际标准是保障数字生态系统安全的最佳方式。但在缺乏全球统一标准的情况下，国际社会只能选择那些虽成熟但安全性能较弱的技术，从而危害到网络安全。

《网络安全法》在第七条指出了国际合作的重要性。与全球标准的关联性越强，受益就会越多。为此，我们建议中国政府积极采纳并助力完善现有和新兴的全球准则，造福全世界。此举优势明显：首先，推动现有体系的变革要比建立全新体系更容易；其次，在目前的架构中有充足机会来保护现有的成果，并加入新的内容，实现全球领导地位。

中国政府致力于将物联网打造成经济的重要组成部分。为此，中国正积极制订物联网行业国家发展计划，并已投入巨资推动物联网项目。中国还计划成立物联网标准协会，在双边合作、地区和全球层面倡导物联网安全。我们非常赞赏中国在积极参与国际电信联盟（ITU）和联合国政府专家组（GGE）活动中所做的努力。《2015年联合国政府专家组报告》指出，各国应“积极促进跨境合作，应对超越国家界限的重要基础设施隐患。”[38]

中国应在此类跨境合作中发挥更加积极的领导作用，推动形成统一的全球安全标准。《欧盟网络与信息系统安全指令》（NIS指令）及欧盟与中国开展的物联网合作等，无不凸显了参与制定和遵守全球安全标准的重要性。

《中欧物联网标识白皮书》第五章鼓励欧洲和中国共同支持“OneM2M、欧洲电信标准化协会（ETSI）、CEN/ISO、电气和电子工程师协会（IEEE）、国际互联网工程任务组（ITEF）及国际电联电信标准化部门（ITU-T）等国际标准化组织

采取的措施，推动国际化标准的制定。”[39]此外，《欧盟网络与信息系统安全指令》指出，“为了确保能统一应用安全标准，各成员国应鼓励用户遵循相关标准，以确保整个欧盟范围内的网络与信息系统安全。”[40]

2. 实现全球互联互通

物联网40%的潜在价值来源于系统之间的互联互通。[41]互联互通的缺失不仅会造成安全问题，还会影响用户的体验效果。若无法实现互联互通，则每一部家庭智能设备均需安装单独的应用程序。互联互通可允许数据传输至包括硬件、软件及应用程序在内的所有物联网层级，并确保解决方案在各设备间成功运行。

欧盟委员会在《数字化单一市场战略》中强调，要想发挥物联网的全部潜力，必须着力增强物联网行业的互联互通。[42]此外，欧盟和中国物联网咨询专家组也在《中欧物联网标识白皮书》中强调了互联互通和标准化合作的重要性，并指出：“物联网行业亟需出台统一的标准，以便为不同品牌、型号、制造商及行业打造可顺畅沟通、操作及编程的横向平台。由此，无论使用何种设备、软件、界面或数据，均可实现用户、流程和内容之间的连通性。”[43]

案例研究——互联互通的重要性

在信息技术行业发展初期，如果两家机构使用的是不同企业开发的应用程序，那相互发送电子邮件都会很麻烦。随着互联网技术的普及，各公司间收发邮件已经变得非常容易，究其缘由在于所有用户都采用了同样的标准，包括重要协议的开放源代码。各机构并未选择打造自己的专属网络，而是合作构建通用的互联网架构及电子邮件和Web等互联网应用程序。

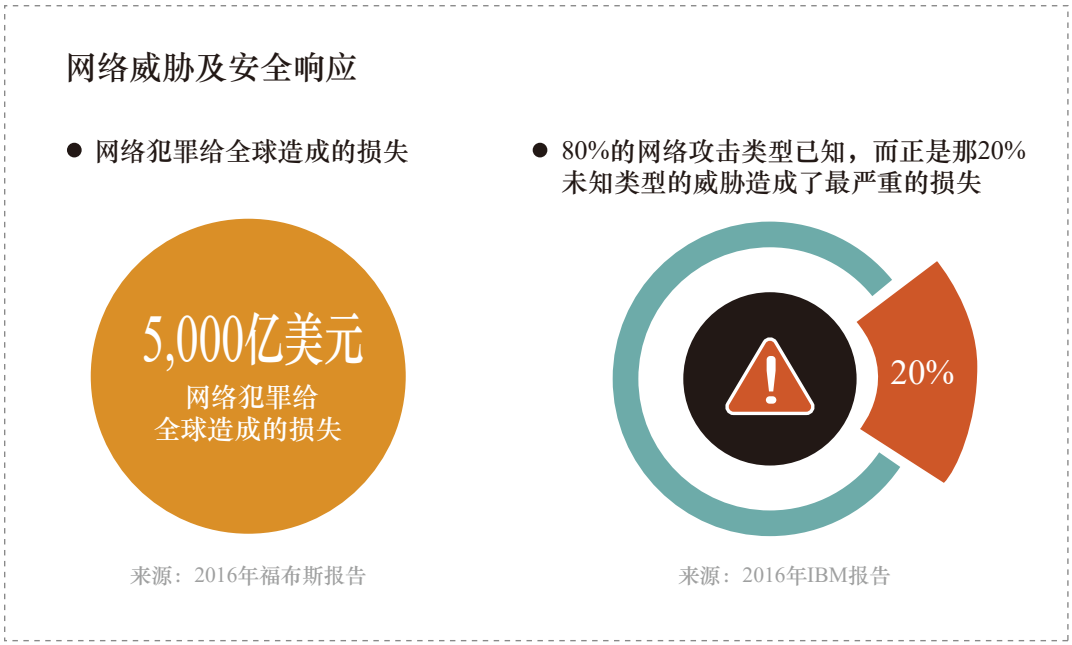
互联网行业所取得的成功，主要归功于那些负责监管标准制定，发布软件开放源码及鼓励公开、协作创新的国际机构。它们带来启示还包括：我们应打造正确的架构，形成统一的开放性标准，建立开放源代码平台，并制定通用的管理流程。

与20世纪90年代初的互联网一样，物联网现在仍处于发展初期。因此，中国以及世界其他各国应该以互联网和连通性的态度，处理数字技术及网络安全问题。

3. 促进利益相关方间的广泛合作

2015年，网络犯罪给全球带来了5,000亿美元的损失，而造成最严重损失的网络攻击占总量的20%，且都属于未知类型的网络攻击。【图3】这些数据表明，各方应积极推动跨领域的知识共享。事实上，只有促进多方合作，才能打造更加安全的网络空间。

图3：网络威胁造成的全球损失及其不可预测性



倘若未能形成统一的响应机制，网络犯罪可能会不断创新，寻找国际安全架构的漏洞。基于此共识，《欧盟网络与信息系统安全指令》提出，要针对重大网络安全事故展开协作，进一步推动成员国的法律和职能的统一。欧盟网络安全政府专家组（中国也是重要参与者）也指出，私营部门与民间团体应积极推动网络安全标准的制定。[44]

五、保障中小企业的安全对于创新和长期发展至关重要

正如很多个人未能充分理解使用互联设备带来的安全问题一样，很多中小企业也未能意识到所面临的风险。在全球范围内，43%的网络攻击是针对中小企业发起的；2016年，50%的小型企业曾发生过数据泄露事件。[45]随着互联设备的不断普及，这些风险也将愈演愈烈。中小企业由于资源和能力有限，始终面临着大量不同类型的网络威胁，使其成为全球网络安全链的薄弱环节。由于网络安全的“木桶效应”，保障“短板”中小企业的安全必须成为重中之重。

《网络安全法》第二十一条强调了实行网络安全等级保护制度的重要性，但如针对中小企业制定单独和具体的指导原则，则会带来更为积极的影响。《欧盟网络与信息系统安全指令》已发布了针对中小企业的信息安全标准。[46]此外，加拿大、美国和德国也出台了针对中小企业的指导文件。这些参考标准和实施指南均有强调，适用于个人的身份认证和培训活动对中小企业也同等重要。这些指导原则还指出，中小企业应通过等级保护制度，利用有限的资源实现既定的安全目标。鉴于中小企业资源有限且面临的网络威胁种类繁多，采取分级保护方法的建议势在必行。

中小企业分级保护框架的核心要素

*采用基于风险管理的信息安全保障方法：*中小企业应首先确定所有可能存在风险的数据库、系统、应用程序及设备，并评估风险的严重程度。设备安全取决于多方面因素，包括收集数据的总量和敏感性以及修复安全隐患的成本。中小企业必须及时更新敏感资产和数据相关信息，只有这样，才能透过有限资源最大程度抵御敏感信息最可能面临的危险。[47]

*应用“通过设计确保安全”体系：*与其事后亡羊补牢，中小企业应事先制定相应规划，在组织、产品和服务中部署恰当的工具和协议，如选择更加安全的方案作为物联网设备和软件应用的默认设置。倘若存在重大风险，例如在医疗应用领域，建议对相关产品或服务采用双重因素认证机制。[48]此外，由于基于机器学习的现代诈骗工具已经变得越发常见，中小企业应将这些工具纳入网络安全战略之中。

积极营造网络安全文化：开展员工培训是保障网络安全至关重要的一环。举例来说，要想彻底打击企业电子邮件诈骗，除安装必要的安全软件外，员工也应了解如何识别电子邮件诈骗的端倪。中小企业应考虑任命信息安全官，确保企业具备信息安全和数据保护能力。在这一方面，中国应积极探索并打造适用于小型企业信息安全官的培训方案。[49]

六、总结

中国新近出台的《网络安全法》就数字经济的发展提出了重要的安全议题。我们建议在以下四个方面出台更为详尽的指导意见，以完善网络安全保障：

1. 电子身份认证标准；
2. 数据安全标准；
3. 提高消费者网络安全意识；
4. 企业网络安全保护能力构建。

在商业环境可预测的未来，私营企业必将成为助力中国在上述领域取得进步的强大合作伙伴。要想实现这一目的，中国网络安全框架必须遵循三大关键性全球标准：（1）遵守相关国际标准；（2）实现全球互联互通；（3）促进利益相关方的广泛合作。

mastercard
万事达卡

来源

1 “中国的转型技术”，麦肯锡公司，2015年8月
2 第39次《中国互联网络发展状况统计报告》
3 “改变中国消费市场格局的三股力量”，世界经济论坛，2016年1月
4 “机器人技术崛起引发投资热潮”，《金融时报》，2016年5月3日
5 阿里研究院及波士顿咨询公司研究
6 高德纳公司及朱尼普研究公司调查
7 “中国物联网规模化发展之路”，GSMA报告，2015年7月
8 “工业物联网：大融合”，《经济学家》，2016年7月21日
9 “中国的数字化转型：互联网对生产力与增长的影响”，麦肯锡全球研究院分析报告，2014年7月
10 国际金融公司报告，2012年10月
11 “基于行业及企业规模的小型企业专利分析（2002~2006年）”，美国小企业管理局倡导办公室（2008年）
12 德国联邦经济及科技部
13 “数字全球化，一个全球流动的新时代”，麦肯锡全球研究院分析报告，2016年2月
14 *同上*
15 尼尔森，万事达卡数据
16 赛门铁克报告，2016年
17 “预防发票诈骗，保障企业安全”，《每日电讯报》，2016年5月
18 “你是否正在把公司资金送给诈骗犯？”，BBC，2016年9月
19 中国人民银行：www.pbc.gov.cn
20 *同上*
21 Gigaom文章，2014年7月
22 Quartz文章，2016年
23 “推广工业物联网数据科学”，O'Reilly报告，2017年
24 “物联网是如何被黑客入侵的”，《连线》杂志，2015年
25 战略与国际研究中心报告
26 Tripwire文章，2016年
27 美国网络安全委员会报告
28 ABC新闻文章，2016年
29 “数字身份蓝图”，世界经济论坛，2016年8月
30 美国网络安全委员会报告
31 “数据泄露调查报告”，Verizon，2016年
32 “物联网安全及隐私保护建议”，宽带互联网技术咨询小组，2016年11月
33 “抵御物联网网络威胁，IBM DeveloperWorks最佳实践”
34 美国国家公路交通安全管理局
35 “网络安全新方法”，加拿大政府，2016年
36 湖北省人民政府办公厅
37 《环球时报》文章
38 《2015年决议性报告》，联合国政府专家组
39 《中欧物联网标识白皮书》
40 《欧盟网络与信息系统安全指令》
41 “释放物联网潜力”，麦肯锡全球研究院，2015年7月
42 “推动欧洲物联网发展”，欧洲委员会报告，2016年
43 《中欧物联网标识白皮书》
44 《2015年决议性报告》，联合国政府专家组
45 赛门铁克、Keeper Security及波耐蒙研究所
46 “中小型企业信息安全与隐私保护标准”，欧盟网络与信息安全局，2016年
47 “谨慎连接：巩固物联网安性”，联邦贸易委员会，2016年；“中小型企业信息安全与隐私保护标准”，欧盟网络与信息安全局，2016年；“制定中小型企业网络安全指导”，加拿大政府，2016年
48 *同上*
49 “中小型企业信息安全与隐私保护标准”，欧盟网络与信息安全局，2016年


mastercard
万事达卡