清华经管学院 Tsinghua SEM | CIDG Center for Internet Development and Governance 互联网发展与治理研究中心

百度安全 有AI更安全

中国网络安全现状研究报告

（2018）

清华大学经济管理学院互联网发展与治理研究中心　百度安全

2018 年 9 月

本研究由清华大学经济管理学院互联网发展与治理研究中心主任陈煜波教授领导的研究团队与百度安全合作完成，特别感谢百度公司在数据、案例方面给予的大力支持，感谢国家自然科学基金（71532006，71325005）、国家万人计划青年拔尖人才项目以及教育部人文社会科学重点研究基地项目（16JJD630006）的资助。

获取电子版请联系 cidg@sem.tsinghua.edu.cn

9/2018

目　　录

1 引言

近几年，随着移动互联网、大数据、云计算、人工智能等新一代信息技术的快速发展，围绕网络和数据的服务与应用呈现爆发式增长，丰富的应用场景下暴露出越来越多的网络安全风险和问题，并在全球范围内产生广泛而深远的影响，例如近几年频繁发生的勒索病毒攻击、跨国电信诈骗、数据泄露、网络暴力等事件，给各国的互联网发展与治理带来巨大的挑战。

从概念上来看，“网络安全”所涵盖的内容和范畴越来越大，从过去简单的上网和网络传输方面的安全问题扩展到整个“网络空间”的安全问题。国际电信联盟将网络安全定义为：“网络安全是集合工具、政策、安全概念、安全保障、指南、风险管理方法、行动、培训、实践案例、技术等内容的一整套安全管理体系，用于保护网络环境、组织以及用户的资产。组织和用户的资产包括连接的计算机设备、人员、基础设施、应用程序、网络服务、电信系统以及网络环境中传输和/或存储的信息[1]”。这个定义将网络安全视为一个生态系统，生态系统的良好运行需要来自技术、法律、政策、组织机构、技能、合作等多方面的保证，这一理念已经在许多国家得到认可和传播。国外近几年除了推动网络安全的立法和政策，也在推进网络安全的保险服务，保险行业需要对网络安全的概念和范畴进行更明确的限定，例如知名国际保险行业智库日内瓦协会(The Geneva Association)将网络安全定义为“在使用信息通信技术过程中产生的危及数据和服务机密性、可用性和完整性的任何风险[2]”。保险行业更加关注数据和服务的安全问题，在实际操作层面，保险公司会确定一系列网络安全事件，并及时更新事件类型和安全风险的场景。我国在 2017 年 6 月 1 日正式实施的《中华人民共和国网络安全法》中也对网络安全赋予了更加明确的定义，“网络安全是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、

[1] 参考国际电信联盟官方网站，https://www.itu.int/en/ITU-/studygroups/com17/Pages/cybersecurity.aspx

[2] The Geneva Association (2016), *Ten Key Questions on Cyber Risk and Cyber Risk Insurance*, The Geneva Association, Zurich.

保密性、可用性的能力”，其中网络数据的安全问题成为一项重要内容。在实际应用层面，我国也是从网络安全事件类型的角度出发，制定一系列政策、标准、条例、指南等对不同的网络安全问题进行防范、处置和应对。目前，不论是政府、企业还是相关行业协会等机构都在积极推动网络安全治理能力的提升和网络安全生态的完善，但在具体实践中也面临着诸多方面的挑战。

政府层面，过去三年推动了一系列网络安全管理的法律法规、标准和政策的落地。2015 年 7 月 1 日，《国家安全法》公布施行，其中首次以法律形式提出“维护国家网络空间主权”，并明确提出国家建设网络与信息安全保障体系。2015 年 7 月 6 日，《中国人民共和国网络安全法（草案）》发布，于 2017 年 6 月 1 日正式实施。过去三年间先后提出或颁布了多个配套法律法规和规范性文件，包括《网络空间国际合作战略》、《国家网络安全应急预案》、《网络产品和服务安全审查办法》、《网络关键设备和网络安全专用产品目录》、《公共互联网网络安全威胁监测与处置办法》、《公共互联网网络安全突发事件应急预案》、《个人信息和重要数据出境安全评估办法》、《关键信息基础设施安全保护条例》等等。这些法律法规和政策的落地极大地促进了我国网络空间法制体系的建设和完善，在保护网络空间主权、防范公共互联网风险、规范企业网络服务和保护个人数据与隐私方面形成了良好的指导作用，不过还需要通过较长时期的实践检验，才能在整个网络安全生态中营造出有效的规制作用。

企业层面，一方面企业正在积极提高自身网络安全防护能力和行业协作，例如 2015 年 6 月 19 日，国内 32 家单位在北京共同签署了《中国互联网协会漏洞信息披露和处置自律公约》，这是首次以行业自律的方式共同规范漏洞信息的接收、处置和发布的行为。就当前发展阶段来看，近几年来企业对自身网络安全防护能力越来越重视，特别是对数据资产保护的重要性有了很强的意识，但是不同行业企业的网络安全防护能力差异很大，特别是一些依靠新兴数字技术快速发展起来的小微企业、初创企业，由于资本和能力的限制，自身网络安全能力建设水平较低，存在很大的网络安全风险。另一方面，企业也积极加强对客户隐私数据的保护和合规使用，特

别是在欧盟的《通用数据保护条例》(The General Data Protection Regulation, GDPR）和《中华人民共和国网络安全法》落地实施后，对个人数据和隐私的保护有了更加严格的要求，企业尤其是跨国企业针对客户数据的收集、存储、使用等方面建立了严格的规范和准则，但就实施初期来看数据滥用、数据泄露的问题依然突出。

整体来说，当前我国的网络安全生态系统尚处于发展初期，相关技术、法律、政策、组织机构、技能、合作等内容正在逐步建立和完善，且处于快速发展的阶段。与其他国家相比，我国在过去十年经历了移动互联网和新兴数字技术的飞速发展，应用场景纷繁复杂，在诸多行业引发了深刻的数字化变革。在这样的背景下，我国面临的网络安全问题具有诸多独特性，下文将从机构和个人两个角度出发，梳理我国的重点网络安全议题，进而分析我国网络安全的整体现状，并对重点行业的网络安全现状和发展方向进行了详细的分析和阐述。

2 中国重点网络安全议题

2.1 机构相关重点网络安全议题

本章从机构和个人两个角度梳理我国当前的网络安全重点议题及案例，机构主要包括政府和企业，目前围绕这些议题正在形成一个越来越完善的网络安全生态系统。

（1）网站和系统安全

a. 恶意网页/恶意内容的情况

从恶意程序的类别来看，目前恶意程序主要包括恶意木马和僵尸网络两大类。其中恶意木马包括远程控制木马、僵尸网络木马、流量劫持木马、下载者木马、窃密或盗号木马等，僵尸网络则包括 IRC 协议僵尸网络、HTTP 协议僵尸网络和其他协议僵尸网络。如图 1 所示，目前我国计算机感染恶意程序的前三种类型为：远程控制木马、僵尸网络木马和流量劫持木马。仅 2017 年，这三种恶意程序感染计算机超过 1000 万台[3]。

[3]数据来源：《2017 年我国互联网网络安全态势综述》

在感染恶意程序而生成的僵尸网络中，规模在 100 台以上的僵尸网络数量达到 3143 台，中小型规模僵尸网络（5000 台以下）占比为 89.8%。从网络安全治理角度来看，近三年以来位于我国境内的僵尸网络数量逐年保持稳步下降趋势[4]。

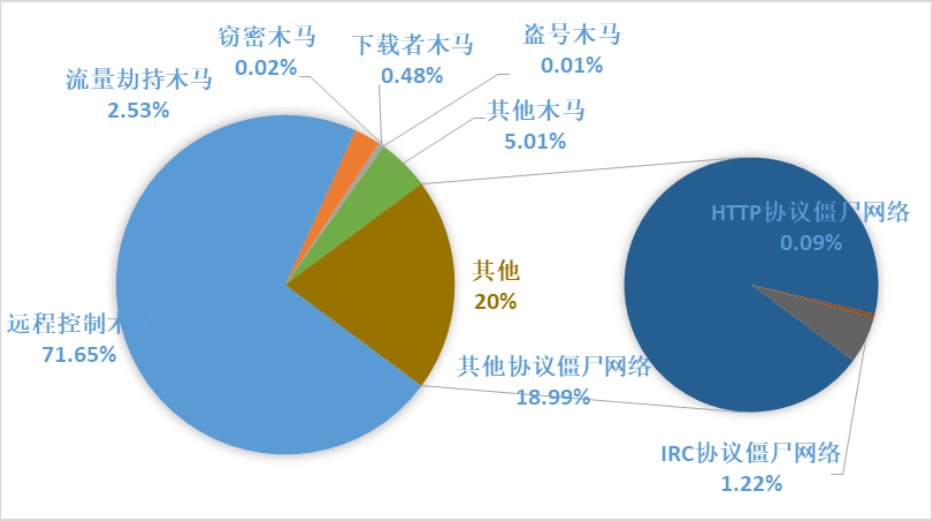

图 1 2017 年我国计算机感染恶意程序类型及分布

b. 安全漏洞

根据国家信息安全漏洞共享平台（CNVD）收录的漏洞统计结果来看，2015 年到 2017 年新增安全漏洞数据年均增长超过 20%，呈现出较快增长的趋势[5]。这些安全漏洞的增长给个人和机构网络安全带来了较为严重的安全隐患。

依据安全漏洞的影响，安全漏洞方面的网络安全问题可以分为：应用程序漏洞、WEB 应用漏洞、操作系统漏洞、网络设备漏洞、安全产品漏洞和数据库漏洞；其中，网络设备包括路由器和交换机等，安全产品包括防火墙和入侵检测系统等。通过对安全漏洞影响类型的统计发现，排名前三的分别为应用程序漏洞、网络设备漏洞和 WEB 应用漏洞[6]。

随着移动互联网的发展，安全漏洞也逐步开始从 PC 端向移动端转变。2013 年，我国移动端安全漏洞收录子库不到 300 个；2017 年，我国移动端安全漏洞收录子库

[4] 数据来源：国家计算机网络应急技术处理协调中心，《2017 年我国互联网网络安全态势综述》

[5] 数据来源：http://www.cnvd.org.cn/

[6] 数据来源：《2018 年 CNVD 漏洞周报第 32 期》http://www.cnvd.org.cn/webinfo/show/4631

超过 2000 个。仅 2017 年，移动互联网子漏洞库收录数量比 2016 年增长幅度达到 105%。此外，电信行业、电子政务和工业控制系统具有大幅度的上升。

c. 网站环境/安全

机构网页环境主要包含面临三种恶意网页导致的安全隐患：网页仿冒、网站后门和网页篡改。根据国家互联网应急中心（CNCERT）监测统计结果，三种恶意网页数量分别约为 4.9 万、5.5 万和 2.4 万，2017 年网页仿冒数量较 2016 年下降 72.5%，境内 IP 地址对境内网站植入后门所占比例大幅下降，但网页篡改的数量增长 20%，其中针对政府网页的篡改数量涨幅超过 30%。

从恶意网页的来源看，境外 IP 对境内网页的仿冒是网页仿冒的主要来源，占网页仿冒总数量的 88.2%，其中主要来源地为中国香港和美国；在网站后门方面，境内 IP 对境内网站植入后门占比 52.7%，对境内网站植入后门的境外 IP 前三个来源地为美国、中国香港和俄罗斯。

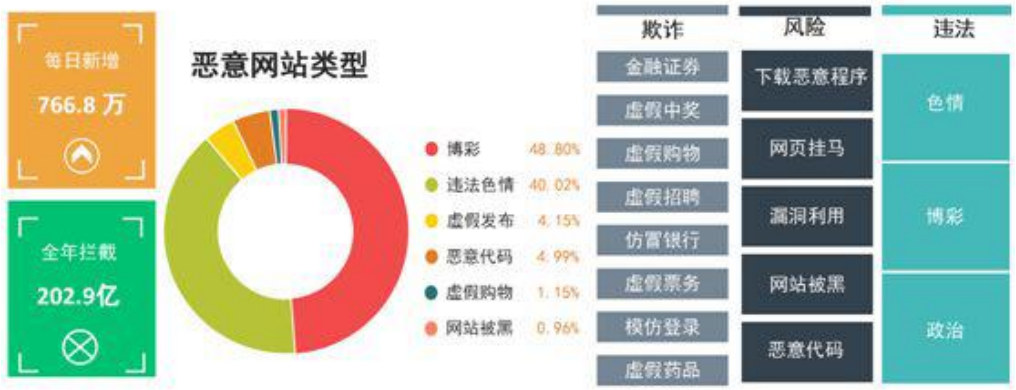

图 2 2017 年恶意网址类型

从恶意网页的内容看，我国恶意网页主要以博彩和违法色情为主，占恶意网页比例约为 90%（图 2）。根据百度安全发布的《2017 年网址安全治理数据》，虚假发布、恶意代码、虚假购物和网站被黑也是其他主要的恶意网站。这些恶意网站会导致网站存在下载恶意程序、网页挂马、网站被黑、恶意代码或漏洞被利用的风险。

d. 攻击风险

针对机构的网络攻击行为中，针对网络数据中心（Internet Data Center，以下简称 IDC）的网络攻击尤其明显，常见的攻击类型主要包括 DDoS 攻击和黑产攻击。以《2017 年度 DDoS 攻击报告》为例， 2017 年，我国 IDC 机房遭受攻击较为频繁，日均达到 1050 起攻击事件，其中 100Gbps 以下的攻击事件占比 90%（如图 3 所示）。

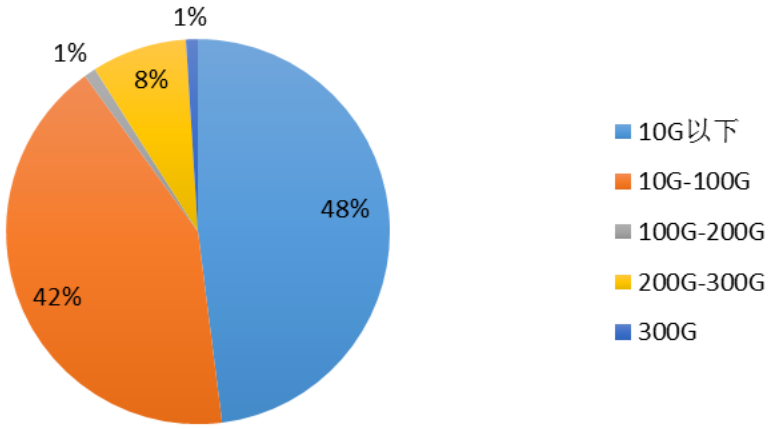

图 3 DDoS 规模占比

根据《2017 年度 DDoS 攻击报告》，游戏行业、互联网金融、电子商务是重点被攻击的行业，其中游戏是最容易被攻击的行业，短时间（30 分钟）内持续攻击占比 50%以上。在黑产攻击中，黑客通常会选择在企业发展的重要时间节点针对企业发起攻击，已达到勒索的目的。比如，当企业发布融资信息、发布新产品、大型促销活动时，通过对企业展开网络攻击获利。

（2）关键基础设施安全

关键基础设施的网络安全主要包含公众类、民生类和基础生产类关键基础设施的网络安全。关键基础设施的网络安全问题与政府、企事业单位以及公众的生产、生活息息相关，企业和政府的正常运转也需要关键基础设施的支撑。公众服务类基础设施网络安全包括政府部门、企事业单位和大型新闻门户的网站安全，这类关键基础设备直接关系到政府、企事业单位和社会治安的正常运行。民生类关键设施网络安全涉及金融企业和机构、电子政府系统以及其他公共服务类基础设施不受到恶意程序攻击、数据不泄露等。这类关键基础设施直接关系到人民的工作和生活，一

旦受到网络安全的威胁，会带来严重的影响。基础生产类关键设备的网络安全则涉及到能源、交通、电视广播以及数据中心等。

（3）机构数据安全

根据 Chief Risk Officers 论坛的定义，机构数据安全议题主要包括数据保密性、数据完整性和数据可获得性[7]。

数据保密性主要涉及机密数据泄露的问题（通常也称为“数据泄露”），这也是机构数据安全最常见的网络安全事件。2016 年 CRO 论坛将数据保密性事件分为两类[8]：1）涉及本机构的数据泄露（例如财务数据，商业秘密或知识产权）；2）涉及第三方机构数据泄露的事件（例如客户的个人信息）。数据泄露可能导致不同类型的损失，包括数据和软件损失、事件响应成本、监管和法律辩护费用、罚款和处罚等。

数据完整性主要是涉及损坏或加密自身或第三方数据的相关议题。数据完整性在实践中，主要有两种形式：1）由于软件错误而删除或损坏自己或第三方数据；2）由勒索软件入侵导致的自身或第三方数据被加密。

数据可获得性是指数据托管机构能否把自身或第三方数据提供给其他相关机构和个人的议题。与机构被动数据泄露不一样，数据可获得性的问题是数据托管机构主动把关键或者敏感信息提供给其他机构和个人。尽管该过程中会对相关信息进行脱敏处理，但也会因为侵犯用户隐私给企业声誉带来损害。

（4）物联网安全

智能设备的网络安全所涉及的范围较广，与恶意程序和安全漏洞等网络安全议题存在较大重复的地方。一方面，恶意程序以及由此引发的变种会破坏智能设备、导致数据泄露、引发恶意攻击等；由于智能设备结构复杂、产品更新快、全天在线、感染后不易被发现，也更加容易遭到攻击。另一方面，智能设备由于与其他设备联系密切，无论是自身的安全漏洞还是与其连接设备的安全漏洞都容易被利用和攻击。

[7] 资料来源《Enhancing the Role of Insurance in Cyber Risk Management，2017》

[8] 资料来源《Emerging Risks Initiative Risk Radar Update，2016》

工业互联网安全的议题主要涉及针对工业控制系统和设备的恶意嗅探事件和工业控制系统及设备本身存在安全漏洞隐患。根据 CNCERT 和 CNVD 的数据统计，仅 2017 年有超过 200 万起境外 IP 对我国的工业互联网设备进行嗅探，而且目前我国有超过 200 个存在严重漏洞隐患的工业互联网设备。一旦这些漏洞隐患被黑客攻击或者利用，就会造成停产，敏感信息泄露等严重的经济和安全问题。

（5）云安全

随着越来越多的工作转移到云端，云计算已经成为应用、服务和基础设施交付主流，各类机构对云安全的担忧成为云计算进步的阻碍之一，因此需要为云计算设计专门的安全管理和控制解决方案，以防范数据泄露并促进云计算的发展。基础架构安全和持续保护是机构云安全的关键要素。对于用户而言，云安全的主要威胁是数据隐私侵犯、数据丢失、和保密违规。

（6）人工智能（AI）安全

人工智能（AI）将是下一次工业革命，各行各业都在积极拥抱 AI。现在，越来越多的会议签到、人脸设别、智慧家居、智能音响、无人驾驶等 AI 应用正在逐渐渗透到我们的日常生活。遗憾的是，AI 不可避免的存在安全方面的局限性，在渗透到各行各业的同时，也将会带来很大的安全隐患。AI 的安全问题大概分为三方面：一是 AI 算法，AI 模型自身的安全问题；二是 AI 软件系统、框架、软件实现等附带的安全漏洞；三是 AI 技术被恶意利用，导致各种安全问题的加剧。

2.2 个人相关重点网络安全议题

（1）个人数据与隐私保护

相比机构网络安全的种类复杂和结果严重，与个人网络安全直接相关的议题是个人数据和隐私保护。随着大数据时代与信息经济的到来，数据的经济价值不断上升，网络攻击者开始通过多种渠道和方式获取个人敏感数据，进而造成数据泄露。一旦个人数据泄露发生，往往所涉及到的人数较多，且泄露的数据一般较为敏感。更为关键的是，近年来个人数据泄露的重大事件数量逐年升高，且在 2017 年泄露的数据总量创历史新高。

以 2017 年 3 月公布的一起数据泄露事件为例，攻击者通过入侵社交、游戏、视频直播和电子商务等多家互联网公司服务器，从中非法窃取并倒卖用户账号、密码、身份证信息、电话号码、物流地址等敏感公民个人信息，涉及数据量达到 50 亿条；更利用从窃取到的各类注册信息，复制用户银行卡，实施盗刷银行卡等违法犯罪活动。

在当前个人用户越来越注重个人信息安全，并意识到个人数据和信息泄露随时都可能导致个人人身和财产损失的情况下，个人用户对用户网络安全特别是个人数据和隐私保护的要求也越来越高。

（2）恶意程序

针对个人恶意程序的议题，往往需要将恶意程序与网络黑产结合在一起讨论。网络黑产通过社交工具或者短信传播仿冒的钓鱼网站，引诱用户点击访问钓鱼网站，从而获取到用户的敏感信息。网络黑产通过虚假和欺诈等不良信息、挂马和恶意链接或者黑链和恶意劫持，伪造个人用户需要点击浏览的网站，形成对个人用户的恶意程序。恶意程序对个人用户会造成应用威胁、服务威胁、用户数据窃取和敏感信息泄露等问题。

（3）安全漏洞

与机构安全漏洞相比，个人安全漏洞主要涉及个人应用软件和个人设备的安全漏洞。个人应用软件的安全漏洞主要涵盖 Google、Oracle、Microsoft、IBM、Cisco、Apple、WordPress、Adobe、HUAWEI、ImageMagick、Linux 等软件商的产品。个人设备方面，主要包括家用路由器和网络摄像头等可能存在的设备权限绕过、远程代码执行和弱口令等方面的安全漏洞。

（4）黑产威胁

网络安全对于个人用户直接的结果就是黑产威胁，黑产窃取用户隐私，进行非法经营活动，威胁用户相关安全。《百度 2016 年安全报告》指出，自 2016 年起，较多用户手机号码、QQ 号码等隐私信息在浏览网页过程中遭泄漏，黑产利用运营商系

统漏洞，非法获取公民手机号，将信息转卖给医院、教育培训、金融机构等用作所谓的“精准营销”。

该类黑产窃取用户隐私行为，不仅侵犯了大量网民的隐私，也对搜索服务提供商的声誉造成了极大的伤害。《百度 2017 年安全报告》指出，2017 年，百度安全在全网安全检测、网络犯罪研究、攻击溯源、黑产追踪等方面开展了大量工作，对公安机关打击网络犯罪提供了坚实的技术支持。2017 年 12 月，百度安全配合公安部门开展 “滤网行动”，助北京市公安局海淀分局破获了国内首例新型侵犯用户个人隐私的黑产团伙——“手机访客营销”黑产，抓获了犯罪团伙数十人。

除此之外，从 2013 年起，基于伪基站的各类型诈骗案件频发，此类团伙使用非法的无线电设备，在银行、商场等人流密集的地方冒用国家权威部门、运营商、银行、房东等，向一定半径范围内的手机用户发送诈骗短信，导致大量不明真相的网民上当受骗，钱财损失。为了帮助网民解决短信可信的问题，百度安全在百度手机卫士上推出伪基站短信拦截功能，依托于《一种伪基站的识别方法和装置》专利技术和海量的用户，累计为网民拦截了数十亿条伪基站短信，保护了网民的财产和信息安全。

在服务于网民的同时，百度安全也向全国各地公安机关免费开放实时的伪基站短信、位置数据，近年来，已协助公安机关抓捕伪基站诈骗犯罪嫌疑人上千人。

3 重点行业网络安全现状和发展方向

3.1 金融

3.1.1 现状

自 2013 年互联网金融行业开始兴起，传统金融业务网络化、大数据金融、区块链、第三方支付、众筹平台、P2P 网贷及第三方金融平台等互联网金融模式都得以发展，我国互联网金融用户的数量也逐年持续扩大。金融行业作为对安全性及稳定性要求极高的行业，同时也面临着网络安全的难题，如大规模 DDoS 攻击等威胁。

随着区块链技术的飞速发展，虚拟货币及大量虚拟货币交易平台也进入大众视线，成为公众热议话题。然而交易平台的安全性并非稳若金汤，根据360网络安全响应中心发布的《区块链技术安全讨论》中统计，从2014年至今，单纯由于交易所安全性导致的直接损失就达1.8亿美元之多。而据网络安全公司Carbon Black的调查数据显示，仅2018年上半年，就有价值约11亿美元的数字加密货币被盗。以比特币为例，由于其具有去中心化结构，用户通过一个公开的地址和密钥来宣示所有权。而当黑客攻击交易所并取得密钥，也由于区块链具有的交易记录不可篡改特性，而不可能通过修改区块链记录来拿回比特币。

另一方面，P2P网贷自2013年进入野蛮生长期，大量P2P平台涌现。根据国家互联网金融安全技术专家委员会发布的《2018年上半年P2P发展监测报告》[9]统计显示，截至2018年6月30日，国内共有2835家P2P平台在运营。但由于我国现阶段还缺乏成熟的信用评分体系，很难判断借款人资质，导致P2P平台与业务的安全性缺乏保障，甚至出现一些如e租宝与钱宝网的“庞氏骗局”平台。2017年7月到2018年6月，我国新增P2P平台141家，消亡1407家。仅今年上半年，新增P2P平台36家，消亡721家，消亡平台数远高于新增平台数，表明我国P2P网贷已经从野蛮生长期进入淘汰期。

3.1.2 相关案例

2014年2月，钰诚集团收购了金易融网络科技有限公司运营的网络平台，并于7月推出了改造后的平台“e租宝”，以“互联网金融+融资租赁”的名号上线运营。“e租宝”称其经营模式是由其集团下属的融资租赁公司与项目公司签订协议，在平台上以债权转让的形式发标融资。等资金到位，项目公司向租赁公司支付租金，租赁公司则向投资人支付收益和本金。一般情况下融资租赁公司赚取项目利差，而平台赚取中介费，但“e租宝”上显示的95%的项目都是假的。“e租宝”用少量资金向企业购买信息，并把企业信息制成虚假的项目在平台上线。“1元起投，随时赎回，

[9] http://news.ifeng.com/a/20170619/51276146_0.shtml

高收益低风险。”是“e 租宝”广为人所知的宣传口号，其推出的产品，预期年化收益率皆远高于一般银行理财产品的收益率，成为了吸引投资者上当的陷阱。同时，“e 租宝”进行了轰炸式的广告投放，电视广告更是覆盖中央卫视、湖南卫视等国家级、省级电视台。在多方的手段之下，自 2014 年 7 月上线至 2015 年 12 月被查封，“e 租宝”实际吸收资金 500 余亿元，涉及投资人约 90 万名，成为中国的“庞氏骗局”。2016 年 1 月，“e 租宝”相关涉案人员被批准逮捕，最终 111 人入狱，罚款超 20 亿。

3.1.3 发展方向

由于金融行业的特殊性，互联网金融在网站及数据安全方面一直较为稳健。但自 2008 年全球金融危机以来，金融环境不断变化，监管难度日益增加，现有的监管模式已不能完全满足新形势的发展，各国都在积极探寻新的监管与合规方法。监管科技（Reg Tech）应运而生，成为美国、英国等多国政府解决互联网金融安全问题的新思路。近年来，美国的货币监理署、消费者金融保护局、金融业监管局等金融监管部门均鼓励监管科技的大力发展。2017 年 4 月，英国金融行为监管局发布了《2017/18 年度商业计划》(Business Plan 2017/18)。同月，英国财政部发布了《监管创新计划》(Regulatory Innovation Plan)。两份文件皆提出要大力开发及运用监管科技，并对英国监管科技的发展进行布局。

2015 年 3 月，第十二届全国人大三次会议召开。李克强总理在《政府工作报告》中明确指出要“促进互联网金融健康发展”。2017 年 5 月，中国人民银行成立了金融科技委员会，并提出“要强化监管科技,积极利用大数据、人工智能、云计算等技术丰富金融监管手段，提升跨行业、跨市场交叉性金融风险的甄别、防范和化解能力”。17 年 6 月，中国人民银行发布《中国金融业信息技术“十三五展规划》。其中指出监管科技在中国金融监管中取得了丰硕成果。在“十三五”规划中，监管科技将继续作为重点任务全力推进，深入研究云计算、应用程序编程接口(APII)、分布式账本技术(DLT)、密码技术、大数据、人工智能等新技术和新工具，并将其应用于互联网金融监管。

3.2 制造

3.2.1 现状

根据 International Data Corporation (IDC)的研究报告，2017 年全球安全相关的硬件、软件和服务收入支出约 817 美元，2020 年将接近 1050 亿美元。可见在物联网大潮的影响下，全球都在重视网络安全的问题。随着中国智能制造大幕的开启，制造业控制系统网络安全和物联网安全被提升到一个新的高度。黑客可能仅仅通过一个鼠标，石油、核电、化工、电力这些系统就会直接处于瘫痪状态，随时能危及人民生命和国家安全的“命脉”。随着物联网在工业环境使用范围越来越广，其安全手段已经无法满足智能制造背景下工业物联网安全发展的需求。需要国家相关部门负责牵头制定“工控网络监测”、“工控漏洞挖掘”、“智慧城市安全”、“数控安全”等多项企业标准、行业标准和国家标准。

2017 年下半年以来，随着 IPv6、5G、工业互联网等多项前沿科技政策的推出，2018 年相关试点工作的推进，大幅推进了物联网的普及和快速发展。2017 年，物联网设备 IP 地址达 2.7 万个，CNVD 收录的物联网安全设备数量比上年增长 1.2 倍。由于制造上安防能力不足和行业监管尚未完善，物联网安防威胁问题越来越引起关注，对用户的个人隐私、资金财产乃至人身安全造成极大伤害，亟待可实施的防护解决方案。

3.2.2 相关案例

2016 年，Mirai 僵尸网络的肆虐给人们留下了深刻的印象，但是物联网设备的安全仍然很少有人提及。无论是个人还是企业网络，物联网设备都在遭受严重威胁。比如，Reaper 正以比 Mirai 更大的规模“抓肉鸡”。2017 年，Reaper 僵尸网络病毒每天感染 10000 台 IoT 设备，中国设备感染数量排名第一。Reaper 僵尸网络病毒是基于 Mirai IoT 蠕虫病毒而扩展，目前有 9 个不同的包，它们针对的是制造的设备漏洞，诸如 d-link、Netgear、Linksys、AVTech、Vacron、JAWS 和 GoAhead，通过多种途径，攻击者将僵尸程序传播到互联网，并感染大批在线主机，通过控制信道，这些主机可以接收到攻击者指令，从而形成具有规模的僵尸网络。

3.2.3 发展方向

2016 年，Mirai 恶意软件控制了数十万台物联网设备，并发起了一场规模最大的、极具破坏性的网络攻击。这些攻击产生的根源在于物联网制造商只关注设备的功能，忽视了投入资金进行网络安全的防护。

由于物联网安全标准迟迟没有建立，厂商和行业在安全标准上很难取得进展。物联网 IoT 带来如下新的挑战：1）增加的隐私问题经常让人感到困惑；2）平台安全的局限性使得基本的安全控制面临挑战；3）普遍存在的移动性使得追踪和资产管理面临挑战；4）设备的数量巨大使得常规的更新和维护操作面临挑战；5）基于云的操作使得边界安全不太有效。因此，物联网业界的相关人士，也发出了需要政府牵头制定安全标准的呼吁。

物联网制造主要发展方向关注两大方面问题：一是关注智能制造设备功能和工业互联网体系建设。二是关注安全问题，同时加快建立相关企业标准、行业标准和国家标准。既要关注制造设备问题，更要关注物联网安全和漏洞问题。根据《2017 年我国互联网网络安全态势综述》报告数据，根据 CNCERT 监测，2017 年我国联网工控系统和设备的恶意嗅探事件共发生 245 万件，比上年增长了 178.4%。境内工 4772 个联网工控系统或设备型号、参数等数据信息遭到泄露，涉及西门子（36.5%）、施耐德（3.4%）、磨莎（34.2%）等多家厂商的产品。2017 年在 CNVD 工业控制系统中，新增高危漏洞有 207 个。

根据《2017 年我国互联网网络安全态势综述》报告数据，在对电力、燃气、供暖、煤炭、水务、智能楼宇六个重点行业安全检测时，发现严重漏洞隐患案例超过 200 例。这些漏洞要是被黑客恶意利用，将造成相关系统的瘫痪和个人信息数据的泄露。例如，全国物联网电梯云平台开展网络安全专项检查，发现 30 个平台存在严重安全隐患，包括党政军的涉密单位。为此，需要智慧电梯利用云平台以及大数据处理分析技术，能够按周期进行安全情况评分，并计算出安全隐患百分比，降低危险系数。

3.3 消费

3.3.1 现状

随着我国新一代信息技术的发展及消费需求的不断升级，互联网消费开始对传统的实体消费逐步渗透。自 2014 年起，大量互联网电商进入消费金融领域，我国开启了互联网消费金融时代。比起实体消费，互联网消费拥有更广泛、更精准的客户覆盖面，使客户突破地域限制，更快捷、方便地参与消费，从而创造更多的消费需求。同时，随着移动互联网与共享经济商业模式的发展，互联网消费的商业模式正在进行进一步升级，包括共享经济的深耕、内容与商品的结合、零售渠道去边界等。

伴随着“京东白条”、“蚂蚁花呗”、“天猫分期”等业务的推出，各类网贷平台及支付征信机构也通过小贷、分期类产品进入互联网消费金融领域，支付安全成为关注焦点。而共享经济在出行、住宿、租赁等行业的渗透，也使得个人信息安全成为热议话题，个人信息被泄露的新闻也屡见不鲜。虽然国家自 2013 年 9 月公布了《电信和互联网用户个人信息保护规定》，规范了互联网信息服务过程中收集、使用用户个人信息的活动，但从现状来看，惩罚力度不够明显。近日，中国青年报社会调查中心联合问卷网对 2002 名受访者进行的一项调查显示，有 75.9% 的受访者遇到过 App 账号难以注销的情况，有 62.9% 的受访者担心 App 账号注销难会导致账号被盗用。虽然对软件运营商而言，设置账号注销通道并不困难，但由于很多软件商旨在通过注册的形式获取用户数据，并将数据转手卖出来获取额外收益，所以他们并不希望用户注销账户。类似的个人信息泄露事件会给消费者造成种种困扰与不便，甚至带来网络安全隐患和人身安全隐患。

3.3.2 相关案例

近年来互联网/电商行业“泄密”事件频频出现，典型类型包括：用户银行账户遭盗刷、企业员工内外勾结泄露客户信息、第三方支付机构漏洞致用户信息泄露等、酒店住宿信息泄密、社交网络技术漏洞导致用户个人信息泄露等。

以 2017 年 3 月公布的一起数据泄露事件为例，某电商企业工作人员长期与盗卖个人信息的犯罪团队合作，将从所供职公司盗取的个人信息数据进行交换，并通过

各种方式在互联网上贩卖。该团伙通过入侵电子商务等多家互联网公司服务器，从中非法窃取并倒卖用户账号、密码、身份证信息、电话号码、物流地址等敏感公民个人信息，涉及数据量达到 50 亿条；更利用从窃取到的各类注册信息，复制用户银行卡，实施盗刷银行卡等违法犯罪活动。

另外， 2018 年 3 月一家名为 Cambridge Analytica 的数据分析公司通过一个应用程序收集了 5000 万 Facebook 用户的个人信息，该应用程序详细描述了用户的个性、社交网络以及在平台上的参与度。经过 Facebook 确认，其平台上的 8700 万名用户的数据已经遭到泄露。6 月 27 日，安全研究员 Inti De Ceukelaire 透露了另一个名为 Nametests.com 的应用程序，它已经暴露了超过 1.2 亿用户的信息。

3.3.3 发展方向

由于移动互联网消费及共享经济在我国仍处在飞速发展阶段，国家相应的监管机制及平台信任体系还在完善之中，各项法令法规也逐步配套出台。2017 年 6 月 1 日起正式实施的《中华人民共和国网络信息安全法》第二十二条明文规定，网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意。第四十四条规定，任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。2017 年 7 月 3 日，国家发改委、中央网信办、工信部、人社部、税务总局、工商总局、质检总局、国家统计局印发《关于促进分享经济发展的指导性意见》，强调要依法严厉打击泄露和滥用用户个人信息等损害消费者权益的行为，加强对分享经济发展涉及的专利、版权、商标等知识产权的保护、创造、运用和服务。今年 5 月 1 日开始正式实施的《信息安全技术个人信息安全规范》中，也对个人信息以及个人敏感信息的范围加以界定，进而明确提出了开展个人信息处理活动中个人信息控制者应当遵循的基本原则和安全要求，包括：1）权责一致；2）目的明确；3）选择同意；4）最少够用；5）公开透明；6）确保安全；以及 7）主体参与等等。未来随着互联网消费行业法律制度与监管机制的完善，信征体系的加快建立，互联网消费金融会在准入门槛、资产质量、资产规模、资金情况、

信息使用等方面得到更加有效的监管，同时更加注重个人信息安全，妥善保管客户个人信息资料与交易信息状况，切实保证信息安全。

3.4 安防

3.4.1 现状

现今的安防行业已经深入到家庭、店铺、银行、城市建设、政府部门等生活中的方方面面，很多人为了方便和根据自己的习惯，采用自己的身份证、出生日期、邮箱等作为密码，这样给了黑客盗取银行密码、机密文件有了可成之机，安防产品、安防行业、安防信息安全的重要性不言而喻。近些年个人信息泄露事件层出不穷，据《中国网民权益保护调查报告（2015）》数据显示，有 63.4%的网民个人网上活动信息被泄露过，78.2%的网民个人身份信息被泄露过，82.3%的网民亲身感受到了个人信息泄露对日常生活造成的影响。个人信息的泄露给人民生活带来极大的不便和隐患，安防监控和相关的安防产品在信息安全问题越来越备受关注，越来越凸显重要性。如何确保信息系统的安全已成为全社会关注的问题。根据清华大学经济管理学院互联网发展和治理研究中心《人工智能驱动的中国经济数字化转型——中国人工智能社会认知与应用需求研究》报告，安防行业结合硬件和人工智能算法，可催生多样化的人工智能应用场景。安防领域的智能摄像头、门禁系统都是有效地人工智能应用场景。物联网行业催生的各类智慧城市形态也都是人工智能未来广阔的应用空间。物联网和人工智能为安防安全提供了最佳的途径，以防个人信息和隐私信息收到侵害和损失。

3.4.2 相关案例

央视的一项大调查显示[10]，大量家庭摄像头遭入侵扫描软件轻松获取 IP 地址。有的卖家公然贩卖这些能够攻破摄像头 IP 地址的扫描软件，只要将被破解的 IP 地址甚至公开叫卖涉“年轻女性”、“夫妻生活”等标签的大量摄像头 IP 账号。只要将被破解的 IP 地址输入播放软件，就可以实现偷窥，不被觉察。根据国家法律规定，截

[10] http://news.ifeng.com/a/20170619/51276146_0.shtml

取家庭摄像头中的性行为进行展示、制作、传播达到一定数量就构成传播淫秽物品罪，如果传播者因此牟利并达到一定数量将构成传播淫秽物品牟利罪。

3.4.3 发展方向

随着安防监控的大力普及，视频监控走向网络化、高清化和智能化，尤其是近年来以云计算、大数据为代表的视频监控技术深度应用，使得视频监控行业与 IT 行业的界限越发模糊，IT 化浪潮正在席卷整个安防行业，个人信息的大量泄露给我们的金融资产安防工作带来极大隐患。信息安全问题也越来越受到包括安防在内的各行业的重视，作为“安防产品”亦不例外，产品的信息安全，在产品的安全设计、检测机制、安全防护等方面都起到了重要作用。安防产品要考虑用户身份安全、共享业务安全和用户数据安全问题。

从近年来屡屡发生的安全事件可以看出，安防行业已经成为黑客们新的攻击目标。现今的安防行业已经深入到家庭、店铺、银行、城市建设、政府部门等生活中的方方面面，黑客利用互联网环境下的安防设备，植入病毒脚本文件，将这些设备变成为病毒源，再去攻击其它网络设备，甚至侵入一些国家重要部门，如公安、金融、交通等部门，盗取银行帐号、机密文件等信息。因此安防网络信息安全的重要性不言而喻。

基于安防网络安全存在的新问题，物联网和人工智能的相关产品将成为新的方向。例如人脸识别技术产品为护航个人信息安全和隐私安全提供新的方向和路径。基于深度学习算法的人脸识别技术和产品也日臻成熟，因其用户体验好、安全系数高的实用特性，商业应用场景不断被挖掘，市场需求持续扩大。“人脸识别就像是一个随身携带的 U 盾一样，它不会替代密码，而是在你的密码、信息泄露的时候能够多一道安全保证”，人工智能技术和人脸识别技术形成的产品能够让每个手机、每个 VTM、每个一体机都能像有人值守一样认真审核以保护信息安全。同时这项技术可应用在金融行业、社保、酒店、教育、公安等多个领域。可见，人脸识别技术在账户信息安全体系构建中发挥出越来越大的作用。

3.5 医疗

3.5.1 现状

随着互联网、大数据、云计算技术飞速发展，互联网医疗也代表了医疗行业全新的发展方向。以互联网连接医院、医生、病人、制药公司及保险公司，将诊断、治疗、康复、健康管理等过程相结合，由此得以优化看病流程，积累并利用医疗数据，同时更加合理的配置医疗资源。

互联网医疗在我国已经历了两个阶段。第一阶段是发展信息化医疗，医院致力于管理、业务功能等系统的整合与信息化。随着移动互联网的发展，远程医疗、移动医疗、医疗大数据挖掘等新型模式的出现标志着互联网医疗逐渐进入第二阶段，呈现出多元化的局面。在未来，互联网医院、智慧医疗将是我国互联网医疗的发展方向。

我国互联网医疗行业发展迅猛，但新型技术的应用也带来新的安全风险。医疗行业作为关乎社会民生的重要行业，健康数据是具有极高价值的商品。但一般医疗机构往往使用易被攻击者利用的端口和服务器，如 web 服务器、DNS 服务器、mail 服务器等等。有些医疗机构使用的嵌入式系统由于制造方式的问题，即便发现漏洞也难以打上补丁。同时，许多医疗机构对服务器及系统的最基本安全防护的认识也严重不足，缺少日常定时维护的意识。在世界范围内，勒索软件、盗窃病人数据、内部威胁、网络钓鱼、以及 Cryptojacking 成为了互联网医疗最严重的五大安全威胁。

3.5.2 相关案例

根据 HIPPA Journal 的调查数据显示，自 2015 年来，每年医疗数据泄露事件的数量呈逐年上升趋势，医疗信息泄露事件的累计影响人数也呈现爆发式增长。2015 年 2 月，美国第二大医疗保险公司 Anthem 宣布公司被黑客盗取了超过 8000 万客户的个人信息，包括了客户的家庭住址、社保号，及个人收入信息等。此次泄露成为美国有史以来最严重的医疗信息泄露事件。

2018 年 8 月， MongoDB 数据库的信息在网上被曝光，这些数据包括了公民的姓名、性别、年龄、家庭住址、保险信息、以及疾病状况。虽然相关医疗机构 Hova 已

经开始采取措施来保护数据库的安全，但已有200万墨西哥公民的医疗保健数据被泄露。

3.5.3 发展方向

2014 年，国家卫计委首次将医疗数据资源整合提升为国家战略规划及“46312”工程。2016 年 6 月 21 日，国务院办公厅颁布了《关于促进和规范健康医疗大数据应用发展的指导意见》，将医疗大数据正式纳入了国家发展战略，并对夯实健康医疗大数据应用基础、全面深化健康医疗大数据应用、规范和推动“互联网+健康医疗”服务、加强保障体系建设等重点任务做出了指导。相关政策相继出台，电子档案、电子病历等数据库已逐步建立并完善。随着互联网医疗的发展，公民的全生命周期数据的保密将成为互联网医疗的核心安全问题。医疗行业需做到快速响应网络攻击，快速识别风险、及时修补漏洞，同时医疗行业内部正在逐步开展网络安全意识培训，完善系统安全防范机制，以期提高互联网医疗安全。

3.6 汽车

3.6.1 现状

随着信息技术、物联网与汽车产业的不断融合，汽车网络互联和智能化已成为汽车产业发展的必然趋势。同时，以信息篡改、病毒入侵、恶意代码植入等手段对联网汽车进行网络攻击而引发的汽车网络安全问题也越发严峻。

随着汽车拥有量的上升，对汽车网络安全等问题也日益显著。车联网[11]作为信息化与工业化深度融合的重要领域，对促进汽车、交通、信息通信产业的融合和升级，以及相关产业生态和价值链体系的重塑具有重要意义。伴随车联网智能化和网联化进程的不断推进，车联网网络安全事件不时出现，用户生命财产安全受到威胁，车联网安全已成为关系到车联网能否快速发展的重要因素。当前，正处于车联网发展关键时期，结合国际网络安全整体形势，强化车联网网络安全保障已成为当务之急。

[11] 车联网指借助新一代信息和通信技术，实现车内、车与人、车与车、车与路、车与服务平台的全方位网络连接，提升汽车智能化水平和自动驾驶能力，构建汽车和交通服务新业态，从而提高交通效率，改善汽车驾乘感受，为用户提供智能、舒适、安全、节能、高效的综合服务。车联网是物联网在网络安全领域的具体应用。

根据中国信息通信研究院《车联网网络安全白皮书 2017》报告，从防护对象看，汽车网络安全主要以下五大方面：智能网络汽车安全、移动智能终端安全、车辆网服务平台安全、通信安全、数据安全和隐私保护。汽车网络安全现状和问题主要聚焦在以下四个方面。一是网络安全事件显现， 车联网网络攻击风险加剧，用户生命财产安全受到威胁。目前，已出现针对车联网的网络攻击事件，部分案例中攻击者可控制汽车动力系统，导致驾驶者的生命安全遭到威胁。二是汽车网络安全问题多样复杂，车联网产业链长、防护环节众多。三是安全企业、整车厂商加快安全布局，但尚未深入合作。目前，国内以比亚迪、上汽等为代表的整车厂商已开始车联网网络安全工作部署，企业内部初步形成了跨部门的合作机制，不断加强车联网全生命周期各环节的网络安全管理。但整体来看，整车厂商和安全企业的合作以服务采购和黑盒测试为主，双方深度合作进行安全方案设计和安全方案评估的案例有限。四是车联网安全发展势头良好，但速度较慢。

当前车联网发展迅速，车联网安全问题得到相关业界和政府管理部门的重视。相关的政策和标准正在积极推进中，车联网的安全发展局面逐渐形成，但现有车辆的安全技术在过渡中，部分车辆网的安全发展需要时间，存量汽车的淘汰周期较长，网络安全能力尚无成熟的解决方案。

3.6.2 相关案例

根据中国信息通信研究院《车联网网络安全白皮书 2017》报告，2015 年，克莱斯勒的 Jeep 车型被国外的安全专家入侵，利用系统漏洞，远程控制汽车的多媒体系统，攻击 V850 控制器，对其进行修改，获取远程向 CAN 总线发送指令的权限，达到远程控制动力系统和刹车系统的目的，即在用户不知情的情况下降低汽车的行驶速度、关闭汽车引擎、突然制动或者让制动失灵。2016 年，同款 Jeep 车型在被物理接触的情况下，被攻击者通过接口注入指令，控制车辆的动力系统，可操控方向盘和刹车系统，严重威胁驾驶员人身安全。另外，黑客可以通过破解车联网远程控制账户，使得车主个人信息和财产安全受到威胁。2016 年，来自挪威安全公司的专家在入侵用户手机的情况下，获取特斯拉账户用户名和密码，通过登录特斯拉车联网

服务平台可以随时对车辆进行定位、追踪，并解锁、启动车辆，最终导致车辆被盗，造成用户的财产损失。

3.6.3 发展方向

2017 年 12 月 27 日，工业和信息化部、国家标准化管理委员会联合发布了《国家车联网产业标准体系建设指南（总体要求）（征求意见稿）》（以下简称《建设指南》），明确提出了到 2020 年基本建成国家车联网产业标准体系的目标。根据《建设指南》，作汽车网络安全主要发展方向有：一是加强硬件安全芯片的自主研发和创新。硬件安全芯片为抵御黑客攻击、保障网联汽车安全的的重要载体。当前，相关汽车企业已经研发除了硬件安全相关模块，或者直接采纳诸如 Intel SGX、ARM TrustZone 之类的硬件 TEE（Trusted Execution Environment）方案，将加密算法、访问控制、完整性检查、数字签名嵌入汽车控制系统、以加强 ECU 的安全性、提高安全级别。目前硬件防护能提供的安全功能主要包括：安全引导、安全调试、安全通信、安全存储、完整性监测、信道防护、硬件快速加密、设备识别、消息认证、执行隔离、远程验证等。二是加强软件防护手段。一方面，需要加强软硬件开发阶段的漏洞审计、安全防护、和形式化安全验证；另一方面，需要加强安全 OTA/FOTA 升级功能更新服务和通过热修复技术提升安全修复速度。而对于核心关键模块，最经济有效的根治内存安全漏洞的方法，则是采用 Rust/Go 等内存安全语言重构相关组件。开源社区热度很高的 MesaLock 系列项目便是非常好的实践。这些技术是未来汽车电子快速健康发展的重要基础，是规范车联网电子产品与服务、智能网联汽车、信息通信、智能交通、车辆智能管理发展的关键核心。通过软件实现漏洞快速修复、防御加固、固件加密、通信内容加密、数据存储加密、数字签名加密，防范数据窃听和窃取。众多软件的防护一定程度上增加了攻击者的攻击难度，提升了网络安全的防护水平。

2016 年以来，随着机器学习和人工智能的兴起，AI 在网络安全领域取得一定的成绩，多家科技公司打造了以 AI 为技术基础的安全体系，以便监控、发现和防止黑客入侵。深度学习、计算机视觉、智能语音、自然语言处理等 AI 技术为网络安全提

供了核心技术基础，也为汽车车联网的智能网络汽车安全、移动智能终端安全、车辆网服务平台安全、通信安全、数据安全和隐私保护提供了技术基础。实际应用中，对于人工智能无人驾驶场景，针对人工智能训练集和训练方法的对抗增强也非常重要。厂商应该在训练集里加入对抗样本，提升模型对于这类攻击的鲁棒性；同时，可以采用蒸馏等方案通过前沿的高对抗性训练过程提升模型的防御力。

3.7 人工智能（AI）

3.7.1 现状

人工智能是计算机科学的一个分支，它企图了解智能的实质，并生产出一种新的能以人类智能相似的方式做出反应的智能机器，该领域的研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等。人工智能从诞生以来，理论和技术日益成熟，应用领域也不断扩大，可以设想，未来人工智能带来的科技产品，将会是人类智慧的“容器”。人工智能可以对人的意识、思维信息过程进行模拟。它不是人的智能，但能像人那样思考、也可能超过人的智能。

2018 年上半年，我国人工智能政策不断落地，技术应用商业化进程加快。十八大以来我国的信息化水平大幅提升，互联网用户数量跃居世界第一，信息领域核心技术进步深刻改变了人们生活的诸多方面，而人工智能技术和应用飞速发展，带来更为持久深刻的思维冲击与变革。政策层面，国务院发布的《新一代人工智能发展规划》提出“到 2030 年，使中国成为世界主要人工智能创新中心”。在我国国家战略规划中，人工智能已超越技术概念，上升为国内产业转型升级、国际竞争力提升的发展立足点和新机遇；行业应用层面，巨大的行业应用需求场景、研发能力积累与海量的数据资源、开放的市场宏观环境有机结合，形成了我国人工智能发展的独特优势，依靠应用市场广阔前景，推动技术革新，形成技术和市场共同驱动。预计 2018 年中国人工智能市场规模将达到 238.2 亿元。

3.7.2 相关案例

2016 年以来，随着机器学习和人工智能的兴起，AI 自身的安全问题也逐渐暴露。在 2018 年某信息安全大会的现场，参会的高级安全研究员展示了百度 X 实验室在人

工智能安全和样本对抗领域的最新研究，并做了《给自动驾驶汽车变‘障眼法’魔术》的主题分享。揭示了如何通过对抗机器学习算法和机器学习模型，达到欺骗汽车雷达系统的方法。在分享中，通过对传输给自动驾驶汽车雷达的图片作出特定干扰，就可以让一辆汽车在雷达的“视界”中消失不见，如果这样的场景发生在真实环境中，将带来不可估量的生命财产损失。另外，通过对公路基础设施，比如限速路牌等等，别有用心的处理，对人类而言，其传达的意义没有改变，但在自动驾驶汽车的雷达系统中，就会把“限速”识别为“停车”或者相反。

系统越复杂，就越有可能包含安全隐患。AI 系统的实现复杂性决定了在软件层面 AI 本身也存在一定的安全问题。例如，谷歌的深度学习系统 TensorFlow 就存在一些传统的、基础的网络安全问题，举例来说，通过构造一个特殊的模型文件输入深度学习框架后，就可以控制整个 AI 系统。某个安全研究团队发现了数十个深度学习框架以及库中的软件漏洞，几乎涵盖了计算异常、空指针引出、整数溢出、越界访问等问题，这些漏洞带来的危害可以导致对深度学习应用的拒绝服务攻击、控制流劫持、分类逃逸，以及潜在的数据污染攻击。例如，基于 TensorFlow 的语音识别应用，如果攻击者通过构造语音文件，会导致系统内部循环无法结束，使应用程序长时间占用 CPU 而不返回结果，从而导致拒绝服务攻击。

AI 技术可以给各行各业带来便利，同样也会被黑色产业所利用。某威胁情报中心的数据显示，在一些知名互联网公司开放其图像识别技术后，有大量的黑产从业者利用该技术识别网站注册和身份识别的过程中的图像验证码，从而实现批量注册、刷单等目的。

3.7.3 发展方向

美国政府在“美国产业人工智能”峰会上表示，将允许人工智能在美国不设限制的“自由发展”，以保证美国在人工智能领域的领先地位。与此同时，法国、印度相继宣布国家层面人工智能的战略部署。而早在 2017 年，人工智能已列入我国政府工作报告，成为国家战略性新兴产业发展规划的重点之一。5 月，第一批中小学人工智能课程开展试点，人工智能人才梯队逐渐成型。

据技术研究公司 Venture Scanner 的调查报告显示，截至 2017 年 12 月，全球范围内总计 2075 家与人工智能技术有关公司的融资总额达到了 65 亿美元，这一数据与 2012 年相比增长了足足 10 倍。

人工智能已成为兵家必争之地，预计 2020 年我国人工智能核心产业将突破 220 亿美元的规模。根据 Gartner 2017 年发布的技术成熟度曲线预测，人工智能在未来的 10 年内将成为最具颠覆性的技术，无处不在的“AI+”将会成为主流。

3.8 智能家居

3.8.1 现状

随着人工智能技术的日趋成熟，智能家居生态逐渐完善，智能音箱、智能电视、智能冰箱、智能门锁等产品开始渗透到生活的方方面面。根据 Market and Market 报告显示，智能家居市场规模将现在 2023 年达到 137.91 万亿美元，2017 至 2023 年间的增长率为 13.61%[12]。智能家居广阔的发展前景，吸引了国内外科技互联网公司的纷纷布局。随着各大公司的相继入局，智能家居迎来了高速发展阶段。

智能家居系统既能为生活带来便利，也能被黑客利用进行攻击。但目前智能家居行业主要关注算法研究、功能实现等方面，缺乏安全方面的整体考虑，生态环境面临着严峻的威胁。一方面，操作系统碎片化、应用软件设计缺陷等传统安全问题依然存在，比如攻击者可以利用系统漏洞进行设备劫持，控制语音系统，或进行应用恶意代码注入等攻击；另一方面，人工智能技术可被用于黑色产业，比如攻击者可以利用人耳听不到、语音交互系统可以理解的频率声音，向智能家居设备下达指令，进行网购、拨打电话等操作；此外，智能家居很多服务和产品是围绕用户数据或隐私数据建立的，而在数据收集、使用以及传输、公布过程中，都不可避免的存在暴露风险。2016 年，Vormetric 公司调查显示，61%美国人担心自己的智能家居设备，如安保系统、摄像头等会遭受黑客攻击[13]。

12 Smart Home Market by Product (Lighting Control, Security & Access Control, HVAC, Entertainment & Other Control, Home Healthcare, Smart Kitchen, and Home Appliances), Software & Service (Behavioral, Proactive), and Geography - Global Forecast to 2023.

13 [11] http://smarthome.ofweek.com/2016-07/ART-91004-8130-30017447.html

Strategy Analytics 报告显示，2017 年全球智能家居设备销售量为 6.63 亿个，预计 2023 年将增加到 19.4 亿个[14]。智能家居设备数量多，信息传输量大，在互联互通的过程中，安全性问题不可忽视。如果互联互通协议存在漏洞，攻击者可以通过一台设备感染成千上万台设备，进行大规模攻击，对用户甚至国家造成安全威胁。但因为通信标准不统一、不同牌品数据共享困难等问题，当前智能家居难以形成统一的互联互通安全标准。

3.8.2 相关案列

门锁作为家中的第一道屏障，安全性最为重要。但目前智能门锁产业存在技术同质化严重，安全系数参差不齐等问题。2017 年 在某信息安全会议上，百度安全实验室展示了通过逆向工程，分析通信协议，破解一款广泛应用的新型智能门锁的过程。整个过程无需拆解门锁，也无需物理接触。而且，对于一款门锁从一无所知到成功破解，只需要三周的时间。

2017 年 11 月，Gheck Point 研究人员发现 LG 智能家居设备中存在安全漏洞，并将其命名为“Homehack”。利用该漏洞，攻击者可以完全控制一个用户账户，然后进行远程劫持 LG SmarThinQ 智能家居设备的行为，包括冰箱、干衣机、洗碗机、微波炉以及吸尘器机器人等。

2017 年，MWR InfoSecurity 的研究人员发现，Echo 音箱存在与窃听相关的安全漏洞。2018 年 DEF CON26 会议上，腾讯安全团队现场再次破解了 Echo 音箱，攻击者可通过一个开放端口，远程控制 Echo 进行录音，并进行录音文件的网络传输。

2018 年 2 月，美国《消费者安全报告》对智能电视进行了安全审查，发现数百万的智能电视存在安全漏洞，攻击者可以通过这些漏洞操控电视机，播放冒犯性视频，或者安装不需要的应用程序。此外，报告显示 Roku 软件和三星电视提供的第三方应用软件开发接口均存在安全问题，如果用户在与智能电视共享使用 WLAN 的智能手机或个人电脑上访问恶意网站或下载含有恶意代码的 APP，则会使得电视遭受黑客攻击。

14 Strategy Analytics’ Smart Home Strategies service, June 2018.

3.8.3 发展方向

在传统互联网时代，智能终端的安全防护点包括操作系统、应用程序以及用户数据等。智能家居系统引入了人工智能技术，且算法模型依赖于海量的用户训练数据，实现需要互联互通协议。因此，对智能家居设备的安全保护，应在继承传统安全的基础之上，结合人工智能、大数据以及互联互通带来的新安全风险，提出更高级别的要求。

构建智能家居生态安全屏障可从技术研究、标准建设、加强监管等方面出发。技术研究方面，通过将人工智能、区块链等新技术用于安全领域，可以在提升用户体验的同时，提高设备的安全攻防对抗能力。智能家居产品形态多样，成本差距大，建议针对不同的家居品类制定安全标准。但在互联互通方面，应建立统一的安全标准，降低攻击者利用互通协议进行恶意操作的可能性。此外，应切实加强智能家居安全管理，加大对黑产攻击、数据滥用、隐私泄露等行为的惩戒力度。2017 年，工信部发布了《促进新一代人工智能产业发展三年行动计划（2018-2020 年）》，该计划指出，应提升智能家居产品的智能水平、实用性和安全性，建设一批智能家居测试评价、示范应用项目并推广。

智能家居是一个大的生态系统，安全也是复杂多面的，应发挥整个产业链的力量，联合终端厂商、安全厂商和研究机构，通过生态开放、技术共享的力量，保护智能家居生态的安全，最大化避免生态出现安全和隐私灾难。

4 结语

在当前互联网和大数据高速发展的阶段，网络安全涉及到硬件、软件、数据、服务等方方面面的内容，网络安全的防治和治理都不可能只依赖政府或企业单方面的努力，推进政府、企业、行业协会等相关机构的协作非常重要。与此同时，对于不同行业来说，网络安全的重点议题通常有较大差异，相关法律法规和政策的制定应当充分考虑行业特点，提高法规政策的适用性。相应的，不同行业内，企业在网络安全能力建设方面的侧重点也应有所不同，并能够结合行业内的技术发展和新型网络安全问题积极调整自身策略。目前，在我国整个网络安全生态系统中，个人隐

私数据的保护是比较明显的一个短板，虽然在法律层面有了明确的规定和保障，但在实际落地过程中并不理想，政府、企业等机构在收集、储存、使用个人数据时尚未形成严格规范。

未来，随着一些新兴数字技术的发展和应用场景的不断扩大，一些突出的网络安全问题应当受到重点关注，其中最重要的就是物联网和数字货币带来的安全问题。一方面，物联网设备往往缺乏相关的安全措施，而且这些设备大多运行基于 Linux 的操作系统，攻击者利用 Linux 的已知漏洞，能够轻易实施攻击。另一方面，区块链技术尽管不断得到研究、应用，依旧存在着一定的安全局限，对于区块链中的共识算法，是否能实现并保障真正的安全，需要更严格的证明和时间的考验。

关于清华大学经济管理学院互联网发展与治理研究中心

清华大学经济管理学院互联网发展与治理研究中心（Tsinghua SEM Center for Internet Development and Governance, CIDG），成立于 2016 年 4 月，是清华经管学院响应国家网络强国战略，基于学院在互联网经济与管理领域的研究、人才培养优势和国际影响力而成立的。中心以思想引领中国经济数字化转型为使命，整合全球顶级专家资源、充分利用互联网大数据等前沿科技，重点围绕数字经济、全球互联时代的商业创新、中国经济的数字化转型、互联网治理等领域展开研究工作，为提高政府科学决策水平、促进科技与商业创新和公共事业发展提供客观参考建议，为相关行业与企业提供智力支撑，同时建设促进数字经济发展与产业创新的合作平台。

如需获取关于清华经管互联网发展与治理研究中心的更多信息和研究资料，欢迎访问：cidg.sem.tsinghua.edu.cn，或关注我们的官方微信账号：TsinghuaCIDG。

关于百度安全

百度安全是百度公司旗下，以 AI 为核心、大数据为基础打造的领先安全品牌，是百度在互联网安全 18 年最佳实践的总结与提炼。业务由 AI 安全、云安全、移动安全、数据安全、业务安全五大安全解决方案矩阵构成，全面覆盖百度各种复杂业务场景，同时向个人用户和商业伙伴输出领先的安全产品与行业解决方案。

百度安全以技术开源、专利共享、标准驱动为理念，联合互联网公司、安全厂商、终端制造商、高校及科研机构， 共建安全的 AI 时代，让全行业享受更安全的 AI 所来带来的变革。