【网络治理专题】

# 新型网络安全风险的管控技术与对策

陈 伟,张 平,戴 华,张 伟,杨 庚
(南京邮电大学 计算机学院、软件学院、网络空间安全学院,江苏 南京 210023)

**摘 要**:随着"新技术、新产业、新业态、新模式"为代表的"四新经济"的发展,新型网络犯罪开始出现,主要有网络诈骗、网络黄赌毒、暗网、非法虚拟货币等。新型网络安全风险具有海量多元化、隐蔽虚拟化、异构复杂化、信息智能化的特征,打击难度大。针对新风险,首先应注重前沿技术方向,其次应注意如何从法律、教育、社会动员等多方面进行协同监管,再次应以安全风险中的数据资产为核心,从技术和对策两个方面加强大数据安全和隐私保护,最后还要注意面向新型网络安全风险的基础设施构建,改变被动的防御形势,构建积极主动的安全保障体系。

**关键词**:网络安全风险;新业态;隐私保护;监管技术
**中图分类号**:TN915.07 **文章编号**:1673-5420(2021)04-0001-10

## 引 言

随着高新技术的飞速发展,我国的社会经济转型呈现出以科技化带动产业化的特点,由此出现了以"新技术、新产业、新业态、新模式"为代表的"四新经济"的发展。新业态是指基于不同产业的组合、企业内部价值链和外部产业链环节的分化、融合、行业跨界整合,以及嫁接信息及互联网技术所形成的新型企业、商业乃至产业的组织形态[1]。而新技术、新产业和新模式是推动新业态产生和发展的三大重要因素。新业态不仅促

**收稿日期**:2021-05-24 **本刊网址**:http://nysk.njupt.edu.cn
**作者简介**:陈 伟,教授,博士,研究方向:网络安全。
**基金项目**:国家重点研发计划"智慧城市网络安全综合防控关键技术及系统"(2019YFB2101704);国家自然科学基金面上项目"面向云环境大数据处理的差分隐私保护理论与关键技术研究"(61972209);国家自然科学基金面上项目"面向外包云环境的安全排序检索关键技术研究"(61872197);国家自然科学基金青年科学基金项目"可调认证加密方案的设计与分析"(61902195)

进了国民经济的快速发展,而且促进了新一轮科技革命和产业变革的加速演进,使得依赖于云计算、移动互联网、物联网、工控系统、大数据、区块链、人工智能等核心技术的“四新经济”方兴未艾。越来越多的重要信息系统将承载起与国家安全、经济发展、社会进步、人民幸福等密切相关的核心业务。

“四新经济”的发展也带来了新型的网络安全风险。例如,在新冠肺炎疫情防控期间,居家政策使得众多活动都基于网络,导致基于新型冠状病毒信息的网络诈骗事件和网络攻击事件频发。2020年4月,中国互联网络信息中心(CNNIC)发布的第45次《中国互联网络发展状况统计报告》显示:截至2020年3月,我国网民规模为9.04亿,其中43.6%的网民表示过去半年在上网过程中遭遇过网络安全问题。2019年的网络安全事件数量相比2018年有较大增长,特别是被植入后门的网站数量达84 850个,较2018年的23 608个增长了259.4%[2]。

(一)新型网络安全风险

新型网络安全风险是在基于云计算、移动互联网、物联网、工控系统、大数据、区块链、人工智能等核心技术的“四新经济”中产生的。新型网络犯罪主要有:

1.网络诈骗。网络诈骗是利用互联网实施的一种诈骗,大多通过伪造身份对用户实施诈骗。近年来,不法分子利用大数据技术寻找目标人群,使用人工智能技术伪造身份或编造虚假信息,犯罪成功率明显提高。

2.网络传销。网络传销是一种以互联网平台为载体的新型传销方式,具有欺骗性强、隐蔽性强、传播速度快、涉案范围广的特点[3]。网络传销的手段多种多样,最常见的是利用互联网发布一些所谓的“宣传文本”,而传销组织的文本与正常公司的文本是有差异的。

3.网络贩毒。网络贩毒是利用网络的隐蔽性、便捷性、虚拟性、取证难等特点实施的毒品犯罪。多通过暗网运作,买卖双方都不知晓当事人的身份,一旦交易完成便不再有任何联系。

4.网络赌博和色情。这是网络黑产中对普通人影响较多的一种。在支付行业监测、监管加强的情况下,网络赌博和色情产业通过虚构交易背景、虚设支付场景,使用非法支付结算服务。这不仅会使人民的财产受到损失,而且会对社会金融稳定产生不利影响。

5.暗网。暗网是一种存在于地下网络中的分散性匿名网络,通过百度等搜索引擎无法查到,只能通过特殊加密匿名软件才能访问。其匿踪性导致政府部门难以进行有效监管,暗网上毒品交易、儿童色情制品交易等非法活动猖獗。

6.非法虚拟货币。虚拟货币是在网络虚拟环境下生成的一种数字货币,它基于密码算法、区块链等技术,不依赖于各国央行的发行监管,具有匿名性、去中心化、可兑换性

和可信赖性等诸多特点。虚拟货币是暗网交易的重要工具,例如勒索病毒要求支付赎金的唯一方式就是使用比特币。还有一些犯罪分子借虚拟货币组织传销,捏造虚拟货币的营销概念,发行虚拟货币,许诺不切实际的超高回报以引诱普通大众投资。

新型网络安全风险带来了新的挑战。传统网络安全可以通过划分安全域和确定网络边界实现。但在基于云计算、移动互联网、物联网、工控系统等的新业态下,网络的边界可以虚拟化迁移和动态化调整,无法直接通过物理区域进行分隔。例如,云计算平台在传统 IT 技术的基础上,部署增加了虚拟化层,具有按需分配和弹性调配等特点[4]。因此,需要进一步分析新型网络安全风险的特征,运用最新的技术,从而制定高效的安全防护方案[5-6]。

(二)新型网络安全风险的特征

新型网络安全风险的特征,具体表现为:

1.规模大、多元化。各类同构和异构数据被广泛收集、存储、分析和应用,数据日益成为重要战略资源和新生产要素。信息系统和平台呈现出存储数据规模巨大、数据类型多样、数据产生速度快、数据价值高等特点,这些有价值的数据将会成为不法分子违法犯罪的目标,大数据时代下数据安全问题将更加凸显。

2.隐蔽性、虚拟化。在互联网、云平台场景下,信息虚拟化在促进“四新经济”发展的同时,也使网络安全风险更隐蔽。如以互联网平台为载体的网络传销、网络贩毒、虚拟货币、勒索病毒等,由于其隐蔽性强、传播速度快、虚拟化、取证难、涉案范围广、匿名性等,使不法分子有可乘之机。

3.异构性、复杂化。互联网、工业互联网、物联网等已经成为“新基础设施”。新基础设施下的网络环境日益复杂和异构化,虽然可以根据用户、业务需求,为其提供个性化服务,但是各种网络攻击手段的与日俱增,使安全的需要在异构网络的各个关键环节日益增加。

4.信息化、智能化。人工智能技术的革新促进了“四新经济”的发展,使传统网络安全风险与新型网络安全风险相互交织。信息化、智能化技术是一把双刃剑,既带来了新的网络安全风险,导致新的智能化网络攻击手段增多,又推动形成了新的网络安全治理手段。

## 一、新型网络风险监管

新业态环境下的网络安全风险具有海量多元化、隐蔽虚拟化、异构复杂化、信息智

能化的特征,因此打击网络犯罪的难度很大。针对新型网络安全风险,只有从政策、法律、技术等多方面进行监管[7-8],才能维护数据安全,保护个人隐私。下面分别从监管技术和监管对策两个方面进行阐述。

(一)监管技术

1.异常行为检测技术。通过对用户行为的关键信息进行分析,从中发现是否有违反安全策略的行为或存在攻击的迹象。对用户行为数据进行采集后,采用决策树、神经网络、关联规则、支持向量机、CNN 等算法训练模型等进行检测[9-10]。

2.敏感文本分类和识别技术。文本分类和识别的实质就是利用文本数据中所包含的一些信息训练文本分类模型,区分正常文本信息与异常文本内容。网络传销最常见的是利用互联网发布一些所谓的“宣传文本”。而传销组织的文本与正常公司的文本是有差异的。因此,可以通过文本向量化、分类、识别等技术来识别网络传销组织[11-13]。

3.图片识别和对抗技术。应用图像深度学习等算法,提升色情、暴恐等图片的识别准确率,可以极大地降低人工识别的成本。目前,不法分子用机器学习的对抗技术,通过添加噪点、更改场景、数据压缩等手段进行对抗。人眼可以看见这些图片,但是识别系统可能会被欺骗,相关技术博弈不断升级[14]。

4.网络大数据分析技术。大数据和电子取证技术在网络犯罪案件的处理中起着十分重要的作用,利用云计算、大数据技术拥有的资源共享、分布广泛、存储信息方便等优势可以打击网络犯罪。例如,网络毒品犯罪必然会留下痕迹,可以对这些痕迹进行筛查。在证据收集中,将线上云技术与线下传统的方法结合起来,能够推动数字化背景下的网络贩毒治理。

5.匿名通信追踪技术。目前,学界主要从两个方面进行暗网内容监管的研究:针对暗网的匿名性,提出了利用协议的脆弱性实现对抗和追踪[15];对暗网空间资源的侦测,则可以使用暗网信息采集技术寻找相应的暗网域名、地址和页面数据[16]。

6.虚拟货币监管技术。应当对虚拟货币进行规模化控制,及时控制虚拟货币种类、规模和资金体量,避免未来由虚拟货币的巨大体量带来更复杂的技术监管问题,及早划定实验区规范管理[17]。监管机构不应对虚拟货币一味禁止,避免陷入虚拟货币创造者越来越想逃避监管,而监管者越来越疲于奔命的恶性循环。

(二)监管对策

针对新型网络风险,除了使用技术手段外,还需要从法律、教育、社会动员等多方面进行协同监管。防范新型网络安全风险是全社会的共同责任,需要政府、企事业单位、广大群众参与,共筑网络安全防线。防范新型网络安全风险的监管对策如下:

1.加快网络监管的法治建设。法律是防范和打击新型网络安全风险的最重要手段[8]。近些年来,我国在网络空间安全方面取得了长足进展。我国自 2017 年 6 月 1 日起施行《中华人民共和国网络安全法》(以下简称《网络安全法》),这标志着我国在网络空间安全领域有了基本法,网络空间治理实现了有法可依。然而,这与发达国家相比仍有较大差距。例如,自 2002 年以来,美国已通过了近 50 部与网络空间安全有关的联邦法律。我国需要加快法律上的建设工作,积极借鉴国外经验,结合实际情况及时制定出相应的法律。

2.明确网络安全的主体责任。《网络安全法》对网络安全的主体责任有了新的规定,强调了政府部门在保障网络安全方面的责任,也强调了网络运营服务商的责任。但在一些领域,责任还需进一步明确。例如,有些企业为了短期利益,利用网络犯罪手段进行恶意竞争,但法律却并未认定企业构成犯罪,使这些企业在一定程度上逍遥法外。还有一些发生数据泄露的企业也无需承担相关责任。例如,2018 年华住酒店 2.4 亿条用户开房记录遭泄露,但法律却未明确华住酒店需承担责任,因此,明确责任主体的问题亟需解决。

3.落实网络用户的道德教育,坚持法治与德治相结合。在网络立法、普法之外,提高公民的网络道德意识也十分重要[8]。从个人信息安全的角度出发,公民应该注重个人的信息保护,这有助于改善网络黑产的盛行态势。从预防网络犯罪的角度出发,公民应该做到合法使用计算机网络,在使用互联网时不参与某些非法行为。目前年轻人更倾向于网络犯罪,因此,对青少年进行道德教育,能够很好地预防网络犯罪行为的发生。

4.协调组织个人的合作关系。各级行政机关、互联网企业与社会个人应该相互协作,共同配合是减少网络犯罪行为的有效途径。社会个人在发现网络风险时,可以及时向相关部门举报。政府和企业之间可以形成合作关系,企业可以利用技术手段帮助政府识别风险,并且对犯罪行为进行取证。有些风险还需要世界各国协同规划。例如,针对虚拟货币的监管以及打击虚拟货币带来的犯罪问题,需要世界各国相互合作,协调规划进行更多制度层面的设计。

## 二、大数据安全与隐私保护对策

### (一)新业态环境中的大数据安全

监管新型网络安全风险的核心在于对数据资产的监管。在新业态环境中,互联网技术与各行各业深度融合,各类同构和异构数据被广泛收集、存储、分析和应用。大数据技术的应用和发展为个人和社会带来了便捷,同时也带来了新的风险,数据安全问题

尤为突出和明显[18]。例如,各类购物平台(淘宝、京东等)在为人们生活工作提供方便的同时,不断收集人们的消费数据;各种即时通讯软件(微信、微博等)随时记录人们的聊天数据;医疗系统软件始终存储着病患的医疗信息。这其中的任一环节一旦发生数据安全问题,都有可能产生严重的后果。

事实上,网络诈骗、网络传销等违法犯罪行为,大都是由大数据管理运营不善、存在技术漏洞、配套法律法规缺失等造成的。因此,研发针对大数据安全的前沿技术,制定配套的法律法规,依法严厉打击侵犯公民隐私、损坏数据安全、窃取数据秘密等犯罪活动,提升公民对于个人数据的隐私保护意识,是全方位保障新业态环境健康、稳定、有序的"防护罩"。

(二)大数据隐私保护的对策

大数据隐私保护对策需要从加强研发、制定法律和增强意识三个方面进行:

1.加强大数据安全和隐私保护前沿技术的研发。在新业态环境下,没有先进的、过硬的隐私保护技术,所有的畅想只会沦为一纸空谈。因此,科研人员要不断投入时间和精力研发隐私安全技术,最大限度地保障数据在采集、传输、存储和应用过程中的安全。通常需要解决如下几个关键问题:一是如何选择适当的数据加密机制,在兼顾效率的同时,适应多用户场景的共享使用;二是在数据以加密形态存储的情况下,如何实现对目标数据的精确查找和搜索;三是在确保隐私安全的情况下,如何保证数据的一致性和可用性,保障数据拥有者和使用者的合法权益。当前对上述三个典型问题,提出了各种具有针对性的解决方案,例如,针对多用户共享的广播加密机制[19]、基于属性的加密机制[20]、支持密文检索的可搜索加密机制[21]、支持数据完整性验证和隐私保护的区块链技术[22]、兼顾数据可用性和隐私性的差分隐私保护机制[23]等。

2.制定和完善大数据安全和隐私保护的配套法律法规。面对大数据的技术浪潮以及发展中的数据安全和隐私问题,我国尚未制定成熟且完备的法律体系[24]。一方面,有关数据安全和数据隐私保护,多散见于民法等法律法规中[25],存在法益保护不充分、规制范围较狭窄、法律法规配套不完善等问题。面对不断涌现的大数据安全和隐私泄露问题,亟需制定和完善相应的法律法规,明确个人隐私数据为用户个人所有,收集用户数据的企业必须在用户授权的情况下才能使用隐私数据,并适时告知用户个人数据的使用情况;此外,用户也有权自行删除储存在大数据平台中的隐私数据。对未经授权肆意使用、售卖和泄露用户隐私数据的行为,应视为违法犯罪。另一方面,相关司法机关应规定数据隐私权的界限和范围,明确侵犯数据隐私权的行为特征,并制定针对侵权方的惩罚措施以及被侵权方的补偿规定。

3.增强公民的数据安全和隐私保护意识。大数据时代,仅仅依赖于技术手段和政府立法这类被动式保护机制并不能很好地解决问题,公民需要增强自身的主动式数据安全保护意识和隐私泄露维权意识,从源头上防范数据安全和隐私泄露的发生[26]。首先,在使用各种应用软件时,用户应仔细阅读相关的隐私声明和政策,保证对个人数据的收集方式、流向以及使用目的的知情权;其次,在存在风险的网络环境中,用户应谨慎输入个人信息,保护好各种账户和密码,减少在网络空间中上传和分享私人重要隐私数据;最后,用户应了解有关数据隐私权方面的法律法规,当个人隐私受到侵害时,能够及时留存相关证据,并向相关执法部门举报和投诉,用法律武器保护个人的数据安全和隐私。

## 三、面向新型网络安全风险的基础设施构建

面对新业态、新模式引发的一系列新的安全风险,除了需要在数据安全方面进行隐私保护,更重要的是构建新一代的网络安全基础设施,增强安全风险防范能力,转变网络安全策略,构建积极主动的网络安全保障体系。具体措施包括:

1.建设新一代网络安全基础设施。新一代网络安全基础设施强调对传统安全中身份认证和访问控制的转变。传统的网络边界防护策略,是以网络为中心进行分层防护,一旦内部网络被外部攻击者入侵,内部网络上大量防护微弱、甚至没有防护的数据就会被泄露。新一代网络安全基础设施的典型技术是零信任安全,从传统的以网络为中心转变为以身份为中心进行访问控制。零信任安全架构将网络内部与网络外部一切操作都默认为不可信,这是一种以身份为中心的全域访问控制策略[27],天然地具备内生的安全能力。零信任架构的关键特性包括以身份作为资源请求的基本单位、严格的业务访问授权、持续的信任评估和基于信任等级进行动态访问控制[28]。相对应的,零信任架构需要通过可信代理、动态访问控制引擎、信任评估引擎和身份安全基础设施等逻辑部件来进行构建。

2.增强新型安全防护技术。依靠传统安全产品,很难为新业态下的网络安全提供保障,应积极采用大数据分析、人工智能和云端安全能力等对抗新技术新业态融合所带来的安全问题。新型安全技术包括:使用全新的感知层终端,对感知的海量数据进行特征提取并训练分类算法,构建终端正常行为模型;利用自然语言处理、大数据分析等机器学习方法对海量威胁情报数据抽取实体关系,并利用知识图谱技术将海量威胁情报信息与攻击者基本信息进行结合,构建攻击者的多维度画像;采用人工智能技术,在大量的用户行为样本上抽取关键特征,建立以用户正常行为为基准的行为模型,过滤掉与模

型预测偏离值较大的用户所发起的行为;利用虚拟化技术实现安全资源池,建立虚拟安全设备,确保信息传输和存储的安全性,动态调度安全资源,必要时在数据链路层将内网与外网的链路连接关闭,以防范网络攻击;不断改进数据隐私保护和加密技术,有效保护用户的信息,并防止相关数据和信息被黑客窃取,多次加密内部数据并使用安全密钥管理系统。

3.贯彻按需防护的安全理念。新业态的蓬勃发展使网络安全的内涵外延不断扩大,各类新业态新模式在应用场景、基础设施、业务性质上存在很大差异,需要从通用、全面的安全理念转变为按需防御的安全理念。例如,工业互联网将传统的工控系统、企业信息系统及云服务平台等进行整合,由于不同企业工业场景不同,需要按需将各种平台和系统进行整合、对接。实现按需防御策略,可先将安全需求进行分析与建模,将已有的入侵检测、防火墙、可信计算等安全技术进行封装,构建安全模块部署方便、响应迅速、自动化防御的安全能力体系,针对不同应用场景与需求实现最优的安全解决方案。

## 结 语

新业态促进了国民经济的快速发展,也带来了新的网络安全风险。相比传统网络安全问题,新型网络安全风险具有海量多元化、隐蔽虚拟化、异构复杂化、信息智能化的特征。本文针对新型网络安全风险,从政策、法律、技术等多方面提出监管方法和对策,强调新业态的网络安全需要进行顶层设计,从法律法规、标准体系覆盖上进行持续完善。同时,在这些新技术、新应用领域,鼓励具备相关条件的高校及科研院所对基础、通用的新业态安全技术进行研究,这既需要国家对网络安全基础研究的扶持推动,也需要相关产业企业的携手合作,满足不断变化的场景需求,以应用带动产业发展和技术创新,构建新一代的网络安全基础设施,转变网络安全理念,从根本上保证安全,进一步发展网络治理中国方案[29]。

**参考文献:**

[1] 王丹娜,周汉民.推动中国数字经济安全、高质量发展[J].中国信息安全,2020(5):66-70.

[2] 第45次中国互联网调查报告[EB/OL].[2020-09-10].http://www.cac.gov.cn/2020-04/27/c_1589535470378587.htm.

[3] 叶媛博. 网络传销实证研究及打防对策[J]. 北京警察学院学报, 2018(1):88-93.

[4] 罗原.云计算环境下新型网络安全技术及解决方案[J].电信工程技术与标准化,2019(12):51-56.

[5] GB/T 25070-2019.信息安全技术网络安全等级保护安全设计技术要求[S].2019.

[6] GB/T 28448-2019.信息安全技术网络安全等级保护测评要求[S].2019.

[7] 苏道敬,夏小帆.网络黑灰产的治理困境及法治应对探析[J].法制与经济,2020(5):141-142+147.

[8] 廖继鹏.计算机网络犯罪的防范措施探究[J].法制与经济,2019(5):111-112.

[9] AKILA S, REDDY U S. Cost-sensitive risk induced Bayesian Inference Bagging (RIBIB) for credit card fraud detection[J]. Journal of Computational Science, 2018, 27:247-254.

[10] VARDHANI P R, PRIYADARSHINI Y I, NARASIMHULU Y. CNN data mining algorithm for detecting credit card fraud[M].Singapore:Soft Computing and Medical Bioinformatics. 2019.

[11] 叶媛博.网络传销实证研究及打防对策[J].北京警察学院学报, 2018(1):88-93.

[12] MA C L, XU W Q, LI P J, et al. Distributional representations of words for short text classification [C]//Proceedings of the 1st Workshop on Vector Space Modeling for Natural Language Processing. Stroudsburg:Association for Computational Linguistics,2015:333-338.

[13] DOS S, ZADROZNY B. Learning character-level representations for part-of-speech tagging[C]// Proceedings of the 31st International Conference on Machine Learning. USA: Machine Learning Research Press,2014: 3830-3838.

[14] RUBEN F B. Prior-based probabilistic latent semantic analysis for multimedia retrieval [J]. Multimedia Tools &Applications, 2018(13): 16771-16793.

[15] 郑光.Tor 匿名通信系统的安全性分析与研究[D].上海:上海交通大学,2011.

[16] ILIOU C, KALPAKIS G, TSIKRIKA T, et al. Hybrid focused crawling for homemade explosives discovery on surface and dark web[C]//International Conference on Availability. USA.IEEE, 2016.

[17] CHERTOFF M, SIMON T. The impact of the dark web on internet governance and cyber security [J]. Tourism Tribune, 2015(5):68-77.

[18] 闫晓丽.大数据分析与个人隐私保护[J].中国信息安全, 2014(3):105-107.

[19] 李春花,王桦,张彦哲,等.采用扩展公钥的云存储广播加密优化方法[J].计算机研究与发展,2017(12):2818-2824.

[20] 罗王平,冯朝胜,秦志光,等.一种面向公有云的密文共享方案[J].软件学报,2019(8):2517-2527.

[21] 李西明,陶汝裕,粟晨,等.一种灵活的精度可控的可搜索对称加密方案[J].计算机研究与发展,2020(1):3-16.

[22] 李少卓,王娜,杜学绘.按需披露的区块链隐私保护机制[J].网络与信息安全学报,2020(3):19-29.

[23] 杨旭东,高岭,王海,等.一种面向直方图发布的均衡差分隐私保护方法[J].计算机学报,2020(8):1414-1432.
[24] 陈冉.论大数据背景下隐私权的刑法保护[J].中国刑事法杂志,2017(3):66-87.
[25] 李晓升.大数据时代个人信息安全的刑法立法与完善[J].中国市场,2018(16):185-187.
[26] 王文杰.大数据时代网络信息安全及防护探讨[J].中国管理信息化,2019(12):125-126.
[27] 刘欢,杨帅,刘皓.零信任安全架构及应用研究[J].通信技术,2020(7):1745-1749.
[28] 魏小强.基于零信任的远程办公系统安全模型研究与实现[J].信息安全研究,2020(4):289-295.
[29] 韩瑞霞,徐剑.网络主权视域下当前互联网治理的主要问题、成因及监管对策[J].南京邮电大学学报(社会科学版),2020(5):41-52.

(责任编辑:张秀宁)

# New type network security risk control technology and countermeasures

CHEN Wei, ZHANG Ping, DAI Hua, ZHANG Wei, YANG Geng
(School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

**Abstract**: With the development of the "Four New Economy" represented by "new technologies, new industries, new business formats, and new models", new types of cyber security risks have emerged, including cyber fraud, cyber pornography, gambling, drug, dark web, and illegal virtual currencies. The new type of network security risk has the characteristics of massive diversification, hidden virtualization, heterogeneous complexity, and information intelligence, which is difficult to combat. In view of new risks, we should first pay attention to the direction of cutting-edge technology, then pay attention to how to carry out collaborative supervision from the aspects of law, education and social mobilization. In addition, we should take the data assets in security risks as the core, strengthen big data security and privacy protection from two aspects of technology and countermeasures, and finally pay attention to the construction of infrastructure for new network security risks, change the passive defense situation and build a proactive security system.

**Key words**: network security risk; new business format; privacy protection; supervision technology