网络安全发展综述

魏亮　田慧蓉

（中国信息通信研究院，北京 100191）

摘要：当前，网络安全已成为国家安全重要基石。自“十三五”以来，我国在完善网络安全政策体系、提升网络安全技术水平、推动产业数字化安全和数字产业化安全发展等方面取得卓越成效。在百年变局与全球新冠肺炎疫情交织叠加的变革关键期，做大做强数字经济、全面强化网络安全意义深远。展望“十四五”，我国将主动把握网络空间发展未来趋势，从前瞻谋划布局、防护演进升级、产业链可控强化、安全产业发展壮大等各方面提升网络安全综合保障能力，大力推动数字经济安全、高质量发展。通过对当前数字经济发展和国内外安全形势进行研判，梳理和展望我国网络安全发展成效及未来趋势。

关键词：网络安全；网络空间安全；数据安全；安全产业

中图分类号：TP393.2；TP393.08　　**文献标识码：**A

引用格式：魏亮，田慧蓉. 网络安全发展综述[J]. 信息通信技术与政策，2021，47(8)：17-23.

doi：10.12267/j.issn.2096-5931.2021.08.003

0　引言

当今世界正经历百年未有之大变局，新一轮科技革命和产业变革加速演进，习近平总书记强调，数字经济成为全球未来的发展方向，要大力发展数字经济，加快推进数字产业化、产业数字化，推动数字经济和实体经济深度融合[1]。随着数字经济重要性、活跃度的不断提升，网络安全对数字经济健康发展的作用也不断凸显，已成为重塑国际战略格局、抢占国际竞争至高点、争夺发展主动权的战略要素。近年来，我国网络安全发展取得显著成效，但也面临新问题、新挑战。在当前数字经济大发展和国内外安全形势胶着时期，本文对我国网络安全发展成效及未来趋势进行了系统的梳理和展望。

1　我国网络安全发展现状

“十三五”以来，我国网络安全发展成效显著，网络安全水平不断提升。2021 年 3 月，国务院发布《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》[2]，进一步强调统筹发展和安全，健全网络安全政策法规体系，提升网络安全防护能力，健全数据要素市场规则，加快推动网络安全等数字新兴产业，强化网络安全产业综合竞争力和人才培养，营造安全的数字生态。

1.1　政策法规和管理体系逐步完善

我国不断强化网络安全顶层设计，从国家全局出发做出长远部署和谋划，在数据安全、关键信息基础设施安全、新兴领域安全、产业安全等领域出台了多项法律政策，逐步形成自上而下的政策法规和安全管理体系。

在顶层立法方面，自我国第一部网络安全领域基础性法律《中华人民共和国网络安全法》（简称《网络安全法》）出台后，《中华人民共和国密码法》《中华人民共和国数据安全法》（简称《数据安全法》）相继出台，《电信法》立法进程也在不断推进，形成了网络空间安全管理的基本法律遵循，为各行业网络安全、数据安全监管提供了法律依据，有力支撑数字化经济的安全、有序发展。

在配套制度方面,各领域政策法规逐步出台,强化网络安全监管力度。关键信息基础设施专项安全条例即将出台,网络安全审查办法正结合《数据安全法》进行修订,着重增加对企业国外上市的数据安全监管。工业和信息化部、国家互联网信息办公室、公安部联合发布《网络产品安全漏洞管理规定》,网络安全产业发展行动计划有序推进,行业领域安全管理和服务政策不断细化,推动安全工作各项措施落地实施。

在安全标准方面,已形成国家、行业、团体标准协同工作机制。目前,网络安全相关标准共300余项[3]。网络安全标准已成为规范安全管理和推动技术要求落地的重要手段,有效地促进了网络安全发展,同时也为国际标准制定合作提供基础。

1.2 网络基础设施安全防护体系持续演化升级

随着全球威胁形势加剧,网络基础设施已成为主要攻防阵地,是各国网络安全防护重中之重。电信和互联网等传统网络基础设施具有双重身份,既是独立的基础设施主体,亦是金融、交通等其他领域重要信息系统、核心关键业务的重要支撑载体,承担着为各行各业安全稳定运行保驾护航的职责。随着国家提出加快建设5G网络、数据中心等新基建重要战略,网络基础设施的内涵与外延不断拓展,逐步成为推动数字产业化、产业数字化的根基,其战略性、基础性、全局性地位全面凸显。

(1)网络安全防护体系不断完善。在《网络安全法》等国家法律法规的指引下,电信和互联网行业网络安全防护体系不断完善,已形成覆盖管理制度、标准规范、技术手段、综合保障等多维度以及网络安全事前、事中、事后全流程的国家安全综合防御体系。在此基础上,正逐步强化国家关键信息基础设施安全防护能力,重点加强风险评估、监测预警、信息通报和应急处置等相关工作,同时推进与国家网络安全审查工作机制的协同联动。

(2)面向融合业务特性的安全能力持续创新升级。随着国家新基建战略落地,5G+人工智能、5G+大数据等新应用、新场景的涌现,面向融合特性的新型基础设施业务安全需求应运而生。完备高效、智能演进、自主可靠的网络安全基础设施建设逐步推进,网络安全能力成熟度评价、先进技术应用试点示范等促进网络安全能力持续提升,着力面向自适应安全、主动防御、智能对抗等高端能力等重点方向攻关。

1.3 数据安全治理体系初步建立

全球数字经济发展进入加速活跃期,数据量呈几何级数增长,数据价值和地位不断提升,数据已成为国家基础战略资源和重要生产要素。与此同时,数据安全问题也日益凸显,影响范围从个人、企业辐射到产业甚至国家。从国内视角看,数据作为新型生产要素将加速数据流动,呈现出规模更大、领域更广泛、技术更复杂的特征,显著增加了数据触点和暴露面,数据安全风险由原有静态存储环节向数据全生命周期迅速延展。从国际视角看,数据作为战略资源引发各国激烈争夺,各国争相布局和引领数据安全规则体系,强化数据资源掌控。加之基于数据的深度挖掘能力不断提升,融合应用领域持续扩展,数据跨境流动的安全风险影响日趋泛化,甚至危害国家安全。

近年来,我国高度重视数据安全工作,数据安全立法进程不断提速,同时各部门基于自身职能积极强化数据安全监管,数据安全保护日趋完善。在国家层面,《数据安全法》作为数据安全领域的基本法,明确了分行业监管模式以及数据安全管理制度框架。在地方层面,多地都在积极开展数据安全政策先行先试,例如贵州、上海、深圳等地聚焦数据权属、开放共享、数据交易等重点问题探索制定相关立法。在行业层面,金融、医疗、通信等数字化程度较高、数据较为敏感的行业已先行开展数据安全管理实践,积极出台行业数据安全管理制度标准,为企业提供有效指引。此外,网信、公安、工信等相关部门围绕APP违法违规收集使用个人信息、摄像头偷窥、黑产等重点领域持续加大数据安全重点问题的监督执法力度。

1.4 产业数字化安全体系布局和应用深耕加速

产业数字化是数字经济的重要构成、关键驱动和创新动能,重点包含传统产业数字技术应用以及衍生的融合型新模式、新业态。《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》提出“加快数字化发展”[2],以数字化转型驱动生产方式、生活方式和治理方式变革。以工业互联网、车

联网等为代表的产业数字化转型和深层次拓展持续加速,安全体系化布局逐步形成。

(1)在工业互联网方面。近年来,我国工业互联网发展逐渐进入深耕落地阶段,安全管理和技术支撑体系不断发展完善。一是政策标准体系基本形成,工业和信息化部等 10 部门联合印发的《加强工业互联网安全工作的指导意见》明确了工作体系和推进方向[4],工业互联网企业网络安全分类分级管理试点工作在天津、吉林、上海等 15 个省市有序开展,30 余项安全标准立项研制并加快在航天、装备、能源等领域的试验验证。二是技术保障能力不断增强,工业互联网国家、省、企业三级安全监测服务体系已建成,产业链上下游、大中小企业协同创新,攻关培育了数据流动监测、工业互联网时序安全网关等一批关键核心技术和防护产品。三是产业生态繁荣创新发展。以工业互联网产业联盟等协会联盟为平台的产业链、创新链协同能力不断增强,涌现出一批面向工业互联网安全综合服务、测试验证、安全众测等的公共服务平台,智慧矿井、自动驾驶等典型场景的安全解决方案和试点示范不断复制推广,工业互联网安全大赛持续开展,初步形成“赛、训、职、教”为一体的安全人才培育新模式。

(2)在车联网方面。车联网安全体系化布局加速推进,在工作机制上,国家制造强国建设领导小组下设车联网产业发展专项委员会,建立了部际协同工作机制,工业和信息化部发布《车联网(智能网联汽车)网络安全管理工作的通知(征求意见稿)》[5],安全管理体系初步建立。在技术标准上,20 余项车联网安全标准立项研制和落地实施,车联网身份认证和安全信任试点有序开展,汽车安全网关、车载防火墙等技术产品和服务创新稳步推进,车联网安全检测评估工作、安全保障能力建设持续开展。

1.5 5G、人工智能等新技术产业化安全防护体系初步形成

5G、人工智能作为新一代科技革命和产业变革的代表性、引领性技术,是实现万物互联、助力经济社会转型升级的重要驱动力量。伴随着新技术产业化的加速推进,新技术产业化安全防护体系初步形成。

(1)在 5G 融合应用安全方面。我国正处于 5G 规模化应用的关键时期,5G 与工业、能源、交通等垂直领域深度融合带来了“通用安全”向“按需安全”的挑战,受到产业各方高度关切。在顶层规划方面,我国相继发布《5G 安全报告》《5G 应用“扬帆”行动计划》等指导性文件,建立健全 5G 安全标准框架和评测体系,积极倡导开放合作的 5G 安全理念,为产业链各环节规划、部署和运行 5G 网络提供技术指引。在技术手段方面,一方面,产业界逐渐凝聚共识,聚焦切片安全隔离和防护、边缘安全服务等 5G 安全关键问题,5G 安全技术、产品与服务逐步落地;另一方面,全行业积极探索 5G 安全最佳实践,“5G+电网”等融合应用安全解决方案加速研制,5G 行业应用端到端安全防护体系逐步形成。

(2)在人工智能安全方面。人脸识别、深度伪造、自动驾驶等热点应用所带来的用户隐私侵犯、生命财产安全问题受到公众广泛关注。我国积极推进人工智能安全治理工作,形成政府部门、行业组织和企业单位多方主体参与的协同共治格局。在管理机制方面,人工智能安全治理逐步从伦理原则软性约束向法律法规、技术标准等硬性规范转变,并在热点应用领域开展安全监管实践;在技术手段方面,人工智能安全攻防、安全检测技术已成为当前研究热点,不断取得创新突破,人工智能安全评估和防护体系初步构建。

1.6 网络安全综合治理成效明显

随着网络在社会生产、生活各方面的全面渗透,网络空间日益成为现实社会的映射,并与现实社会形成广泛的互动,对现实社会带来了深刻的影响,网络空间安全治理成为国家治理的重要内容。2016 年,百度竞价排名引起的魏则西医疗诈骗事件[6]、个人信息泄露导致的徐玉玉电信诈骗案件[7]等,引发全社会对网络空间安全尤其是电信网络诈骗的广泛关注。党中央、国务院坚守人民立场,响应群众关切,高度重视打击治理电信网络诈骗违法犯罪工作,公安部、工业和信息化部等多部门联动,持续开展治理专项行动,治理工作取得阶段性明显成效。

(1)法律体系逐步完善。2015 年,《刑法修正案(九)》规定明晰“帮信罪”的处罚准则;此后,最高人民法院、最高人民检察院等部门先后发布了系列解释和

案件处理意见,逐渐完善电信网络诈骗治理法律规范体系,进一步加强了惩治电信网络诈骗犯罪的力度,对其上下游关联犯罪实行了全链条、全方位的打击。

(2)精准治理能力不断提升。从工业和信息化部组织建立全国诈骗电话防范系统,到信息通信行业反诈大平台的建立,再到12381涉诈预警劝阻短信系统的启动,目前已基本实现对涉案号码、域名、互联网账号以及涉诈电话、短信等"一键下发,全网生效"的快速处置能力,实现了对潜在受害用户的主动监测与精准预警。

(3)协同联动机制不断健全。工业和信息化部与公安部建立"总对总"工作机制,在手段建设、信息查询、线索研判、联合执法等方面完善工作流程,加强工作协同。各单位各部门主动作为、综合施策,组织建设了企业信息联网核查系统,建立涉诈线索联合研判、协同处置机制,组织开展系列联合宣导工作,提高全民反诈意识,共筑全民防诈反诈的防护网。

1.7 网络安全产业发展持续向好

在我国相关政策、资金的扶持下,网络安全产业蓬勃发展,网络安全规模、企业水平、技术手段不断升级。

(1)我国产业规模呈现持续高速增长态势,网络安全投入显著提升。根据中国信息通信研究院测算[8],2020年我国网络安全产业规模超过1700亿元,较2019年增速超过9%。我国网络安全投入占信息化投入的比重接近2%,近5年复合增长率达到约14%。

(2)安全企业稳步发展,市场活力不断涌现[9]。一方面,我国网络安全企业营收水平和盈利能力逐步增强。2020年,20家典型上市企业平均营收规模、净利润、研发投入较2019年相比增速超过15%,其中3家上市企业营业收入突破30亿元。另一方面,网络安全融资并购活动持续活跃。据不完全统计,2020年我国网络安全领域共发生融资活动超过70起,涉及金额近80亿元,融资活跃度较2019年有所提升。此外,安全企业、重要行业厂商、大型国企均通过收购新兴企业、投资独角兽企业、组建安全子公司等方式,深度布局安全市场。

(3)网络安全技术持续演变,安全产品体系逐步完善。在新威胁、新需求的牵引下,传统防火墙、抗DDoS、入侵检测等固化单一形态的安全技术向集流量监测、DDoS防护、威胁处置等全面云化、协同联动的安全即服务方案演变,零信任、隐私计算、拟态防御等新兴安全技术逐步成熟落地。现有网络安全产品从传统网络安全领域延伸到云、大数据、物联网、工业控制、5G等新兴应用场景,覆盖底层基础设施安全至上层应用场景服务安全等多个维度的网络安全产品体系日益完备。

1.8 网络安全人才培养机制日臻完善

我国在网络安全人才发展方面做出一系列重要部署,通过"政、产、学、研"深度融合,网络安全人才建设取得了重要进展。

(1)不断完善网络安全人才培养体系。近年来,网络安全人才培养领域重要政策相继发布,从学科专业建设、人才培养机制、教师队伍建设、促进校企合作等多方面提出网络安全学院学科专业建设方向和人才培养重点,为人才培养提供了有力的政策引导和支撑。

(2)持续促进校企网络安全合作发展。网络安全、互联网等龙头企业深度参与高等院校网络安全人才培养工作,通过共建网络空间安全研究院、制定网络安全人才联合培养计划等手段协同育人,定向培养网络安全人才,形成网络安全人才培养、技术创新、产业发展的良性生态链[10]。

(3)多措并举选拔网络安全人才。鼓励网络安全科研人才参与国际大学的联合研究和国际学术交流活动,提升人才的学术水平和国际交流能力。开展网络安全技术技能大赛、开展攻防演练,选拔优秀的网络安全人才,提升实战能力。

2 "十四五"网络安全发展趋势展望

随着新一轮科技革命和产业革命深化发展,国际网络安全竞争将空前激烈,数字经济和实体经济深度融合背景下网络安全防护要求愈加严苛。对此,我国应准确研判未来网络安全发展的形势并进行超前布局,更好地迎接未来网络安全发展的机遇,应对未来网络安全面临的严峻挑战。

2.1 各国网络空间安全较量愈加激烈,立足高位前瞻谋划成为网络安全发展重中之重

在大国竞争和新冠肺炎疫情叠加的背景下,网络

安全外部形势动荡,网络安全发展机遇与挑战并存。抓住窗口期,抢占发展先机,成为网络安全谋篇布局的重点之一。一方面,全球网络空间博弈持续深化,网络安全成为决定国家核心竞争力的关键要素。站在大国博弈的制高点上看,网络空间作为创新活跃、渗透性强、影响力广的领域,面临全球产业链、供应链分化等新情况,数据跨境流动和新兴技术安全等国际主导权争夺激烈度空前,成为各国间科技竞争角力场。另一方面,世界竞争格局面临重塑,提前布局成为提升我国网络安全综合实力的关键举措。在新冠肺炎疫情的冲击下,全球各国产业、经济重新洗牌,网络安全发展格局面临重塑。我国将紧抓窗口期,站在国家战略高度对网络空间安全进行前瞻性、全局性统筹谋划,深入了解域外大国网络安全战略发展趋势,不断提高网络安全防护技术水平,建立健全新型基础设施网络安全保障体系,构建行业网络安全新发展格局。

2.2 供应链安全上升为国家战略重点,产业链供应链自主可控能力和弹性加快提升

近年来,西方大国频繁出台供应链安全政策,不断收紧供应链安全政策强化管控,将供应链安全作为贸易壁垒并利用优势地位对竞争国家实施“断供”[11],以此保障国家竞争力。我国审时度势,沉着应对国际形势变化。一方面,供应链安全上升为国家战略高度,加强核心技术攻关提升自主可控能力。核心技术受制于人对我国国家安全、网络安全有着巨大潜在风险。未来,我国政策、资金扶持力度持续加大,综合汇集产、学、研力量,核心软硬件国产化创新加快研发。着力突破大数据、工业互联网、人工智能等前沿领域技术瓶颈,优化供应链安全产业结构,有效提升自主创新能力和本质安全水平,打造自主可控、安全可靠的供应链。另一方面,强化网络安全审查,推动国内国际市场双循环有序发展提升供应链弹性。2021 年 7 月 10 日,《网络安全审查办法(修订草案征求意见稿)》发布,将针对企业国外上市行为的网络安全、数据安全问题进行重新修订,在国际政治、外交、贸易等领域的网络安全监管更趋严格,为促进国内国际市场双循环安全、有序发展奠定基础,形成开放型产业链,提升供应链安全弹性。

2.3 网络边界日益模糊,防护思路从边界防护向角色控制转变

随着云边协同、云网融合、泛在接入等网络架构创新升级,基于边界安全的解决方案难以应对新一代信息技术的快速演进,防护思想的变革势在必行。作为一种以角色控制为核心的网络安全新思路,零信任架构秉承“从不信任并始终验证”的原则,融合身份认证、权限控制、环境评估等多种技术,在人、设备和业务之间构建虚拟的、基于身份角色的逻辑边界,构建细粒度、自适应的访问控制,实现网络架构的新变革。随着零信任国内应用实践逐步落地,未来发展前景广阔。

(1)灵活适配安全场景。可灵活适配云计算—大数据—物联网—移动互联网—人工智能的各种业务场景安全需求,满足网络虚拟化、软件定义网络、万物互联等多种复杂网络环境下的安全防护要求。

(2)升级防御能力。可增强基础设施动态防御能力,借助精细化身份管理和访问控制、动态的可信环境评价和人员行为评估,强化未知威胁防御能力。

(3)差异化管理策略。可支持第三方人员协同、外部资源访问等差异化管理策略,为多分支机构、跨区域协作提供安全保障。

当前,传统安全防御体系已无法动态适应新型业务场景安全需求,新旧网络安全架构将逐步历经并存、兼容与迭代的优化发展历程。

2.4 产业数字化、数字产业化快速发展,安全供给模式与能力加速演进

当前,数字产业化发展和产业数字化转型驱动网络安全技术保障、应用创新和产业供给能力不断提升。一方面,产业数字化加速催生场景化、融通化和应用型的按需安全供给模式。面向技术、场景、业态全向融通的数字安全保障能力将不断强化,传统 IT 安全技术向产业级安全应用平滑迁移,智能预测、主动防御、编排响应、大流量监测等技术在应用中验证扩展,产业数字化安全实践将加速安全应用从固化单一、松耦合形态走向全面云化即服务、紧耦合形态转变。另一方面,数字产业化需要夯实数字技术内生安全能力和应用安全保障。基础电信企业、设备制造商、自动化集成和应用服务提供商及安全企业将加强联合攻关,强化 5G+工

业互联网、车联网、工业大数据等融合领域的安全研发设计和产业化协同防护。

2.5 产业基础不断夯实,推动网络安全产业向高质量发展

在政策扶持、需求扩张、应用升级等多方驱动下,我国网络安全产业综合实力将显著增强。

(1)网络安全产业将长期保持高速增长。预计到2024年,通信、互联网等重点行业领域安全投入将大幅增加,网络安全投入占信息化投入的比重将升至10%,我国网络安全产业规模复合年均增长率预计将超过15%[12]。

(2)网络安全企业实力将持续增强。在企业发展方面,引领网络安全产业生态的龙头企业将初步形成,“专、精、特、新”独角兽企业数量也将逐步壮大。在投融资方面,我国产融合作将更加精准高效,多方资本力量将持续赋能网络安全投融资市场。

(3)安全技术产品智能化、主动化发展。入侵检测、DDoS防护、高级威胁检测等传统安全技术产品将持续升级,安全编排与自动化响应、用户实体行为分析等智能检测响应技术产品将不断落地,拟态防御、威胁狩猎等主动安全防御技术产品将逐步成熟,网络安全技术产品集约化、智能化、主动化水平不断提高。

(4)人才队伍日益壮大。覆盖高等院校、职业院校、企业与社会机构、人才培养基地、公共服务平台等的多层次网络安全人才培养体系将更加健全,一批创新型、技能型、实战型人才将更多涌现。

3 结束语

2021年是“十四五”开局之年,数字经济迅猛发展,网络安全也迎来发展新阶段。未来,我国将把握机遇,强化网络安全谋篇布局,不断完善网络安全法规政策体系,提升网络安全创新和供给能力,推动网络安全产业向高质量发展,全面增强网络安全综合实力,构建良好的网络空间安全生态。

参考文献

[1] 肖亚庆. 大力推动数字经济高质量发展[N]. 学习时报, 2021-07-16(001).

[2] 中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要[Z],2021.

[3] 全国信息安全标准化技术委员会. 2021上半年发布的重要网络安全标准速览[Z], 2021.

[4] 工业和信息化部, 教育部, 人力资源和社会保障部, 等. 加强工业互联网安全工作的指导意见[Z], 2019.

[5] 工业和信息化部. 车联网(智能网联汽车)网络安全管理工作的通知(征求意见稿)[Z], 2021.

[6] 人民网. 魏则西事件暴露医疗广告乱象 百度竞价排名引争议[EB/OL]. (2016-05-03)[2021-07-10]. http://media.people.com.cn/n1/2016/0503/c40606-28319177.html.

[7] 百度. 徐玉玉电信诈骗案[EB/OL]. (2016-08-19)[2021-07-10]. https://baike.baidu.com/item/%E5%BE%90%E7%8E%89%E7%8E%89%E6%A1%88.

[8] 中国信息通信研究院. 中国网络安全产业白皮书(2020年)[R], 2020.

[9] 万得. 网络安全上市企业2020年企业年报[Z], 2021.

[10] 中央网络安全和信息化领导小组办公室,国家发展和改革委员会,教育部,等. 关于加强网络安全学科建设和人才培养的意见[Z],2016.

[11] 桂畅旋. 对特朗普政府在信息通信领域供应链安全政策的初步分析[J]. 中国信息安全, 2019(6):78-83.

[12] 工业和信息化部. 网络安全产业高质量发展三年行动计划(2021—2023年)(征求意见稿)[Z], 2021.

作者简介:

魏亮 中国信息通信研究院副院长,正高级工程师,享受国务院政府特殊津贴,长期从事网络与信息安全领域工作,作为学科带头人在网络安全政策、法律、技术、产业、人才等方面深入研究,在支撑政府决策和服务信息通信行业发展中完成多项重大任务

田慧蓉 通信作者。中国信息通信研究院安全研究所总工程师,高级工程师,博士,长期从事网络与信息安全政策研究、标准制定和产业推进工作

Development status and trend of network security

WEI Liang, TIAN Huirong

(China Academy of Information and Communications Technology, Beijing 100191, China)

Abstract: Currently, network security has become an important basis of national security. Since the 13th Five-Year Plan period, China has made remarkable achievements in completing network security laws and regulations, improving network security technical capabilities, and promoting the industrial digital security and digital industrialization security. In this key period of transformation in the past hundred years, especially accompanying with novel coronavirus pneumonia, it is very significant to make the digital economy growing rapidly and stronger, and to strengthen the network security. Looking forward to the 14th Five-Year plan period, China will take the initiative to grasp the future trend of cyberspace development, improve the comprehensive network security capabilities on the aspects of forward-looking strategic planning, protection evolution and upgrading, security strengthening of industrial chain, development and growth of security industry, and vigorously promote the safe and high-quality development of digital economy. By analyzing the current development of digital economy and the security situation, this paper presents the achievements and future trends of network security in China.

Keywords: network security; cyberspace security; data security; security industry

(收稿日期:2021-07-17)