



建立铁路网络空间安全治理新格局的实践探索

孙远运

Practice and exploration of establishing new pattern of railway cyberspace security governance

SUN Yuanyun

引用本文:

孙远运. 建立铁路网络空间安全治理新格局的实践探索[J]. 铁路计算机应用, 2021, 30(11): 1-4.

SUN Yuanyun. Practice and exploration of establishing new pattern of railway cyberspace security governance[J]. *Railway Computer Application*, 2021, 30(11): 1-4.

在线阅读 View online: <http://tljsjy.xml-journal.net/2021/I11/1>

您可能感兴趣的其他文章

Articles you may be interested in

新形势下铁路网络安全工作探索与发展展望

Exploration and development prospect of railway network security under new situation

铁路计算机应用. 2020, 29(8): 1-5

铁路网络安全威胁及漏洞管理平台研究

Railway network security threats and vulnerability management platform

铁路计算机应用. 2020, 29(8): 61-65

铁路网络安全攻防仿真实验平台方案设计

Scheme of railway network security attack and defense simulation experiment platform

铁路计算机应用. 2020, 29(3): 51-54,59

基于等级保护2.0的铁路网络安全技术防护体系研究

Research on technical systems of railway network security based on Classified Protection 2.0 of Cybersecurity

铁路计算机应用. 2020, 29(8): 19-23,27

铁路信息化资产知识图谱测绘工作的构想

Ideas of mapping knowledge graph of railway information assets

铁路计算机应用. 2020, 29(8): 15-18

基于自适应安全的铁路网络安全框架设计研究

Railway network security framework based on adaptive security

铁路计算机应用. 2020, 29(8): 6-10



关注微信公众号，获得更多资讯信息

文章编号: 1005-8451 (2021) 11-0001-04

建立铁路网络空间安全治理新格局的实践探索

孙远运

(中国国家铁路集团有限公司 科技和信息化部, 北京 100844)

摘要: 随着新兴技术的应用和发展, 网络的边界越来越模糊, 铁路面临的安全风险挑战愈发激烈, 加强铁路网络安全空间治理, 建立治理新格局势在必行。文章从政治、经济、社会和技术4个维度分析我国网络空间安全治理现状, 结合铁路实际, 总结铁路网络空间安全治理实践及取得的成效。为了构建铁路网络安全立体化综合防御、协同共治的新发展格局, 从多维度统筹考虑, 研究提出铁路网络空间安全治理在政治引领制度落地、产业促进服务支撑、以人为本重点防护和创新技术融合发展等4个层面的改进路径。

关键词: 网络空间; 安全治理; 铁路网络安全; 实践成效; 改进路径

中图分类号: U29 : TP393 **文献标识码:** A

DOI: 10.3969/j.issn.1005-8451.2021.11.01

Practice and exploration of establishing new pattern of railway cyberspace security governance

SUN Yuanyun

(Department of Science, Technology and Information Technology, CHINA RAILWAY, Beijing 100844, China)

Abstract: With the application and development of emerging technologies, the boundaries of the network have become more and more blurred, the security risks faced by railway have become more and more fierce, and the space governance of railway network security has been strengthened, it is imperative to strengthen the governance of railway network security space and establish a new pattern of governance. This paper analyzed the current situation of China's cyberspace security governance from four dimensions of politics, economy, society and technology, and comprehensively combined with the reality of railway, summarized the practice and achievements of the railway industry in cyberspace security governance. In order to build a new development pattern of three-dimensional comprehensive defense and collaborative governance of railway network security, considering from multiple dimensions, the paper studied and put forward the improvement paths of railway cyberspace security governance in four aspects: system implementation of political guidance, industrial promotion service support, people-oriented key protection and the integrated development of innovative technologies.

Keywords: cyberspace; security governance; railway network security; practice results; improvement path

信息技术的广泛应用和网络空间兴起发展, 极大地促进了经济社会繁荣进步, 同时也带来了新的安全风险和挑战^[1]。近年来, 国家级有组织的网络攻击持续发生, 数据泄露事件频发, 国家政治、经济、文化、社会及公民在网络空间的合法权益面临严峻威胁。铁路安全事关国家安全和公共安全, 规模庞大、影响广泛的铁路信息系统全天候不间断运行, 面临的网络安全风险与日俱增。进一步提升铁路网络安全治理能力, 已成为铁路助力国家网络安全治

收稿日期: 2021-08-31

基金项目: 中国国家铁路集团有限公司科技研究开发计划重大课题 (K2021W001)

作者简介: 孙远运, 正高级工程师。

理体系和治理能力现代化的必然要求, 为此, 本文采用多维度分析法, 分析我国网络空间治理现状, 系统总结铁路网络安全治理实践和取得的成效, 并从不同维度提出相应改进路径。

1 我国网络空间安全治理现状分析

政治 (P, Political)、经济 (E, Economic)、社会 (S, Social) 和技术 (T, Technological) 分析, 即 PEST 分析, 是指宏观环境的分析, 不同行业根据自身特点, 分析的具体内容会有差异, 但一般都包括政治、经济、社会和技术。基于此种分析方法, 本文从4个维度分析我国网络空间安全治理现状。

1.1 政治和法律维度

我国网络安全已上升到国家战略，相关政策布局和法律体系不断完善，为指导我国网络安全工作，以及维护国家在网络空间的主权、安全、发展和利益提供了良好的政策保障。以《中华人民共和国网络安全法》为基础的网络安全法律法规体系已成为国家网络安全保障体系的重要组成部分；将于2021年9月1日正式实施的《关键信息基础设施安全保护条例》^[2]更是为我国深入开展关键信息基础设施安全保护工作提供了有力的法治保障。

1.2 经济和产业维度

伴随各类新兴技术的研究发展、融合应用的推广落地，以及政策红利的持续释放，在数字经济的背景下，我国网络安全产业发展势头和规模持续向好，网络安全应用市场广泛，其中，政府、电信与金融领域应用网络安全产品和服务最多^[3]，众多细分领域的安全需求成为推动网络安全产业持续增长的动力。但在发展持续向好的背后，我国网络安全产业发展不平衡、不充分的问题依然突出，特别是在内部业务数字化和外部监管合规压力倍增的现状下，普适性安全教育投入方面仍然较少，网络安全人才基数仍需进一步扩充。

1.3 社会和保障维度

随着信息化和全球经济化相互促进，互联网已经融入社会生活的方方面面，也深刻改变了人们的生产和生活方式，但同时，网络安全威胁和风险也与日俱增。在新一轮产业数字化转型的大背景下，互联网已成为驱动产业创新变革的先导力量，能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标，为此，其相关保护体系得到持续优化。在大数据时代，个人信息已成为一种重要的社会资源，我国高度重视大数据时代带来的隐私威胁，不断强化个人信息保护力度，在执法监管与社会监督多管齐下的有力举措下^[4]，多措并举协同联动的个人信息保护体系建设已初见成效。

1.4 技术和创新维度

中华人民共和国工业和信息化部公布的《2020

年网络安全技术应用试点示范项目名单》^[5]，涵盖新型信息基础设施安全、网络安全公共服务、网络安全“高精尖”技术创新平台等3个大类共计177个项目，充分体现了国家对网络安全技术创新应用的迫切需求和政策支持。技术创新应用在对整个经济社会发展的融合、渗透和驱动作用日益明显的同时，也带来巨大的风险挑战，导致网络空间威胁和风险日益增多。更为严峻的是，我国科技，尤其是上游核心技术受制于人的现状仍未得到彻底解决。目前，国内重要信息系统、关键信息基础设施中使用的核核心技术产品和关键服务大多依赖国外^[6]，信息技术应用创新（简称：信创）生态体系的搭建和核心竞争力的提升问题亟待解决。

2 铁路网络空间安全治理的实践成效

铁路部门深入贯彻、积极落实网络强国战略部署^[7]，网络空间安全治理工作取得了显著成效，为铁路发展保安全、强管理、增效益提供了强有力的安全保障。

2.1 网络安全体制机制基本构建，制度保障体系初步形成

坚决贯彻落实网络安全工作责任制^[8]明确要求，2018年，中国国家铁路集团有限公司（原中国铁路总公司，简称：国铁集团）成立了网络安全和信息化（简称：网信）领导小组。国铁集团和所属各单位网信领导小组实行双组长制和双副组长制；铁路站段等二级单位网信领导小组组长由主要负责人担任。同时，坚持做好网络安全制度保障工作，以国家政策法规为指引，健全完善铁路网络安全有关管理制度和标准，先后印发了《中国铁路总公司网络安全管理办法》《网络安全事件调查处理和定责考核管理办法》等制度文件，基本构建了覆盖国铁集团、铁路局集团公司、铁路站段的网络安全管理规章制度体系。

2.2 安全产品和服务市场化推进，产业示范建设广泛布局

立足网络安全防护实际，积极推进网络安全产品研发和市场推广，按照“消化吸收再创新”的原

则，打造了一批技术过硬、易用性强的优势产品。产品体系涵盖了网络安全等级保护管理系统、移动终端接入平台、漏洞管理平台、一次性密码（OTP, One Time Password）动态验证、网络安全基线配置核查系统等，已经在铁路部分单位试点应用和落地实施。同时，紧跟铁路业务系统网络安全需要，探索打造“全领域”服务模式，以等级保护为基础，逐步拓宽服务面，全力做好攻防演习、安全检查、宣传教育等各项安全保障工作。在此基础上，着眼于为安全技术研究、信创体系完善、系统安全测试、安全人才培训等工作提供有力支撑，积极推进网络安全靶场实验室、铁路商用密码安全评估实验室和铁路信创适配实验室的规划建设。

2.3 安全保护体系逐步构建完善，个人数据安全有力维护

在切实落实网络安全等级保护工作的基础上，重点从机制制度、检测评估和防护措施等层面着手推进铁路关键信息基础设施安全保护工作。研究制定《关键信息基础设施认定规则》等规则制度，积极组织开展铁路关键信息基础设施认定工作，推动建立关键信息基础设施风险评估机制，以资产评估为核心，针对每一项需要保护的资产，识别可能被威胁利用的弱点，分析并及时整改其存在的脆弱性；推进制订了各关键信息基础设施专项应急预案，定期组织开展应急预案演练，并在重要保障期间，组织对关键信息基础设施进行全面安全检查和集中重点盯控。同时，特别针对部分涉及资金交易、个人敏感信息交互的关键信息基础设施，采用密码技术进行加密以实现信息隐藏；进一步优化完善铁路12306互联网售票系统隐私权政策，严格落实国家网络安全有关隐私保护和数据安全要求。

2.4 示范工程促进技防能力提升，信创体系构建有序推进

铁路网络安全技术能力主要包括入侵防范、边界防护、计算环境、应用安全、数据安全、可信验证等内容。采用试点先行、全面推广的实施策略，有序推进铁路领域重要信息系统一体化安全保障示范工程（简称：铁网护栏工程）建设，初步构建了

符合实际、突出重点、防护得当的铁路网络安全技术保障体系，铁路系统性风险防范能力和网络安全保障水平进一步增强，网络安全技术防护能力进一步提升。同时，积极推进信创国产化工作，开展国产化产品的应用研究和适配工作，搭建了铁路信息化应用国产化适配平台，完成了相关产品开发、国产操作系统适配测试、铁路电子公文系统和电子支付系统的国产化适配等工作，推进铁路信创体系有序构建。

3 铁路网络空间安全治理的改进路径探索

进入新发展阶段，面对深刻变化的铁路内外部环境，铁路部门要贯彻新发展理念，坚持正确方向，释放产业支撑效能，强化核心重点防护，推进创新技术融合，构建铁路网络安全治理新发展格局。

3.1 加强政治引领，突破制度落地实施瓶颈

铁路网络安全治理工作要严格落实网络安全工作责任制要求，确保网络安全责任清晰、主要目标明确、工作任务和保护措施具体，不断强化网络安全工作的政治引领和指导力度，坚决杜绝不重视网络安全工作的情况发生。同时，本着“于法周延、于事简便”的原则，要在制度规章和标准细则上深入细化，明确等级保护测评、风险评估、密码测评、产品检测等方面的具体要求和实施指南，并加大检查考评力度，建立网络安全定期巡视巡查制度，对发现的问题实行闭环管理，逐项督促，落实整改，确保做到有制可依、有制必依、依必见效。

3.2 依托产业示范，促进服务支撑能力提升

随着我国对网络安全产业的重视程度不断增强，各项政策规划为网络安全产业的发展提供了有力保障和明确指引。要对标先进典型，充分结合自身实际，加快推进网络安全技术研究中心和靶场实验室等的建设^[9]，构建集训、试、测、仿、技术服务、资源共享等为一体的网络安全产业支撑机构，积极创新网络安全服务模式，依托技术研究中心和实验室的平台优势，全面开展网络安全技术研发，扩展等级保护测评工作深度，加快信创网络安全防护产品研制，推进网络安全大数据和商用密码应用，组织

开展网络安全攻防技能竞赛,构建涵盖咨询规划、研究开发、检测试验、演练和培训等的全生命周期服务保障体系,为铁路网络安全工作提供全流程支撑和个性化服务。

3.3 强化重点防护,贯彻以人为本核心原则

关键信息基础设施和重要信息系统已逐渐成为网络战争的主战场,对其采取针对性的重点防护至关重要。要深刻把握“网络安全为人民,网络安全靠人民”这一网络安全观的核心要义,研究制定符合铁路实际的个人信息保护制度和个人信息分级分类标准,区分信息使用权限,明确相应级别的保护措施。同时,要严格按照最新法律法规和铁路关键信息基础设施认定规则程序,加快铁路关键信息基础设施认定进程,健全关键信息基础设施风险评估机制,推进系统国产化工作,推进网络安全设备和关键信息基础设施安全可控示范应用,切实做好源头管控。采取检测认证、供应商安全评估、安全审查等多种手段,加强铁路关键信息基础设施供应链安全管理。

3.4 完善信创体系,推进创新技术融合发展

新技术、新应用正在不断融入铁路业务、管理和服务之中,以人工智能、区块链等为代表的新技术,以及建设智能铁路带来的新风险^[10],将为铁路网络安全带来更大挑战。要采用“适度超前”的思维,分析安全需求,积极制定与智能铁路相匹配的网络安全技术框架和实施方案,明确整体架构、技术路线、技术策略,指导网络安全建设及技术措施实施工作,以推动新一代信息技术与铁路网络安全深度融合为牵引,打造现代智慧铁路系统,强化科技创新的支撑引领能力。同时,按照“适配、示范、推广”的技术路线,进一步完善网络安全信创体系,加强信创技术和产品攻坚,推进攻防技术装备标准化配备、国产化产品替代和国产密码应用,全面提升核心信息系统安全可控度。

4 结束语

基于PEST的多维度系统分析,总结了铁路网络安全治理实践及取得的成效,立足新发展阶段,充分认识铁路网络安全工作的重要性、复杂性和艰巨性。本文提出的改进路径还需分阶段、分重点地逐步推进实施,要始终坚持多维度、多角度、多方面、多层次、多措并举的分析方法,把握新发展阶段铁路网络安全治理的新路径,构建铁路网络安全立体化综合防御、协同共治的新发展格局,确保铁路网络和重要信息系统安全稳定运行。

参考文献

- [1] 中华人民共和国国家互联网信息办公室.国家网络空间安全战略[EB/OL].(2016-12-27)[2021-08-31].http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.
- [2] 司法部网信办工业和信息化部公安部负责人就《关键信息基础设施安全保护条例》答记者问[EB/OL].(2021-08-18)[2021-08-31].http://www.gov.cn/zhengce/2021-08/18/content_5631789.htm.
- [3] 中国信息通信研究院.中国网络安全产业白皮书(2020年)[R].北京:中国信息通信研究院,2020,9.
- [4] 中国电子信息产业发展研究院.2019—2020年中国网络安全发展蓝皮书[M].北京:电子工业出版社,2020:257-258.
- [5] 中华人民共和国工业和信息化部办公厅.中华人民共和国工业和信息化部办公厅关于公布2020年网络安全技术应用试点示范项目名单的通知:工信厅网安函[2020]273号[Z].北京:中华人民共和国工业和信息化部办公厅,2020,11.
- [6] 《网信自主创新调研报告》编委会.2020网信自主创新调研报告[R].北京:中国关键信息基础设施技术创新联盟,2021,4.
- [7] 中共中央党史和文献研究院.习近平关于网络强国论述摘编[M].北京:中央文献出版社,2021.
- [8] 中共中央办公厅法规局.中国共产党党内法规汇编[M].北京:法律出版社,2021.
- [9] 祝咏升,姚洪磊,崔伟健.铁路网络安全靶场设计与研究[J].铁路计算机应用,2021,30(8):52-56.
- [10] 王同军.智能铁路总体架构与发展展望[J].铁路计算机应用,2018,27(7):1-8.

责任编辑 王 浩