网络安全形势与我国标准化竞争策略研究

王 淼[1]　朱思婧[2]

（1.中国标准化研究院；2.商务部国际贸易经济合作研究院）

摘　要：当前全球网络安全事件频发、多种风险叠加，各界高度关注并积极应对，网络安全问题日益凸显，成为国家战略的重要组成部分，而相关标准化解决方案也“备受青睐”。我国该领域有基础、存挑战、需发力。本文旨在分析当前网络安全形势，评估我国网络安全监管体系的建设情况，并探讨我国在国际标准化竞争中的策略。

关键词：网络安全，标准化，国际竞争，监管体系

DOI编码：10.3969/j.issn.1674–5698.2024.08.006

Research on Network Security Situation and China's Standardization Competitive Strategy

WANG Miao[1]　ZHU Si-qi[2]

（1. China National Institute of Standardization; 2. Chinese Academy of International Trade and Economic Cooperation）

Abstract: At present, with the frequent occurrence of global network security incidents and multiple risks superposition, all walks of life are highly concerned about the network security issue and actively respond to it. The issue becomes increasingly prominent, and is an important part of the national strategy, which needs the standardization solutions. China also faces challenges in the aspect and needs to find solution. This paper aims to analyze the current situation of network security, evaluate the construction of China's network security supervision system, and discuss China's strategy in the international standardization competition.

Keywords: network security, standardization, international competition, supervision system

0 引言

在信息时代，网络安全已成为国家安全的重要组成部分，其重要性随着数字经济的蓬勃发展而日益凸显。网络安全的标准化是确保技术安全、促进国际合作和提升国家竞争力的关键。它为网络安全实践提供了统一的规则和指南，有助于构建一个更加安全、稳定和可预测的网络环境。全球网络安全形势的复杂性和不确定性要求各国加强监管体系的建设，提升网络防御能力。标准化工作在此过程中发挥着至关重要的作用，它不仅涉及技术规范的制定，还包括了对网络安全风险的评估、管理和缓解策略的制定。

我国作为数字经济大国，面临着维护网络安

基金项目：本文受中央基本科研业务费项目“技术性贸易措施影响评估方法与实证研究”（项目编号：292023Y–10407）资助。

作者简介：王淼，研究实习员，主要研究方向为技术性贸易措施。

朱思婧，硕士研究生。

全和推动国际标准化进程的双重任务。在这一背景下，我国网络安全监管体系的构建与完善，必须与国际标准接轨，以确保在全球范围内的兼容性和互认性。同时，积极参与国际标准的制定和修订，能够为我国在全球网络安全治理中争取更多的发言权和影响力。然而，当前我国在网络安全监管体系构建和国际标准化竞争中仍存在诸多挑战。

1 全球网络安全形势与标准化动态现状

1.1 网络安全国际形势严峻

近年来，网络安全问题频发，成为国际社会共同面临的挑战。例如：2017年爆发的“WannaCry”勒索软件攻击，迅速蔓延至全球范围内，导致众多国家的医院、学校、企业以及政府机构遭受重创，凸显了网络安全威胁的跨国性质。2020年末，SolarWinds供应链攻击事件再次震惊世界，攻击者通过SolarWinds软件更新系统对全球多个国家的政府和企业网络进行了长期的秘密渗透，这一事件不仅暴露了供应链的安全漏洞，也突显了国家级网络战的复杂性。去年，世界经济论坛（WEF）举办2023年年会，发布《全球网络安全展望》年度报告。该机构调查显示，全球网络犯罪集团数量持续增长，网络攻击手段花样不断翻新，特别是勒索软件等攻击形式影响广泛，导致诸多企业、机构数据泄露并遭受损失；91%受访者认为，未来两年内可能发生灾难性网络事件，悲观预期与当前地缘政治乱局密切相关，尤其是俄乌冲突引发世界范围的国家级网络战，商业运营所处网络环境也不断恶化，供应链及数据安全恐遭受连带冲击。

1.2 标准化提升“网络韧性”

国际标准化组织（ISO）2月发布新闻“科技巨头如何建立‘网络韧性’？”，指出微软、苹果、谷歌等头部企业通过使用ISO/IEC 27001（信息安全管理体系）国际标准来应对“数字威胁”；该标准于去年10月完成修订，通过更新信息保护范围、集中管理框架等内容，帮助企业、机构更好应对网络攻击、数据泄露，进一步增强组织“网络韧性”。欧洲标准化组织（ESOs）——欧洲标准化委员会（CEN）、欧洲电工标准化委员会（CENELEC）、欧洲电信标准化协会（ETSI）与欧盟网络安全局（ENISA）也于2月合办年会，重点就“支持欧盟网络安全立法的欧洲标准化”开展讨论，涉及“区域与国际”视阈下的欧盟标准化、《网络韧性法案》制定与标准化技术支撑、电子签名信任体系与数字身份等议题，相关研讨着眼于网络安全新形势、新政策、新实践，试图为欧盟网络安全立法提供标准化解决方案。

2 我国网络安全监管体系与标准动态分析

2.1 我国网络安全监管体系“已具雏形”

党的二十大报告指出，要“加快建设数字中国”。按照党中央决策部署，我国经济社会各领域发展数字化转型加速推进，监管体系建设也不断发力，除陆续出台《网络安全法》《数据安全法》《个人信息保护法》等安全法规外，还发布353项国家标准（截至2022年12月），涉及密码技术、鉴别与授权、安全评估、通信安全、安全管理、云计算和大数据安全等多个领域，为我国相关法规落地实施和网络安全治理优化提供技术支撑。在监管技术方面，我国积极探索和应用新的监管技术，如：人工智能、大数据、区块链等，以实现对网络安全的智能化、精准化监管。面对新技术和新应用的不断涌现，我国网络安全标准体系也在不断地扩展和更新。尽管我国在网络安全的动态适应方面取得了一定的成绩，但新技术和新应用的发展速度极快，而相关法律法规和标准体系往往难以同步更新。且部分新技术和新应用具有高度的复杂性和隐蔽性，给网络安全监管带来了极大的难度。

2.2 网络攻击频繁考验我国标准“供与用”

近年来，境外网络攻击“来势汹涌”，截至2022年，360公司已监测到5200多起针对我国的国家级网络攻击行为，攻击手段方式不断“推陈出新”，如：美国国家安全局（NSA）近期使用41种专属网络攻击武器，窃取我国西北工业大学核心技术数据超140GB。各类网络攻击已严重危害我国国家安全、科技安全和信息安全，也暴露出我标准化工

作尚存短板。相关研究发现，我国网络安全技术类和应用类标准建设较好，但管理体系和隐私保护相关标准发展滞后。更不利的是，我国网络安全国家标准多为推荐性标准，社会化应用推广机制还不健全，加之部分标准制定与政策法规、监管需求脱节，导致标准实施应用效能有待提升。

2.3 国际竞争加剧“挤压”我国标准国际化

网络安全国际标准是当前各国标准化竞争热点领域，发达国家长期占据主导地位，持续将本国标准打造为国际规则，如：美国、英国、德国分别掌握网络安全框架、信息安全管理、身份与隐私保护国际标准制定话语权。相比而言，我国在网络安全国际标准化方面差距明显，参与制定发布标准21项，占比约15%，优势领域少、话语权小。究其原因，美西方采用多种手段对我该领域发展遏制打压，阻碍我国标准提案有效推进，加之近年疫情限制跨境工作沟通，导致我国标准国际化协调“突围”难度增大。

2.4 网络安全监管体系普及“有待成熟”

在我国网络安全监管体系中，尽管已经建立了一套国家标准，但在实施和普及方面还存在一些挑战。虽然《网络安全法》等相关法律法规为网络安全标准化提供了法律基础，但在实际执行过程中，由于缺乏足够的专业人才和资源投入，一些标准并未得到充分的实施。此外，公众和企业对于网络安全标准的认知度不高，导致标准推广和应用不够广泛。国内网络安全标准化的普及也面临挑战，许多中小企业由于成本和专业知识的限制，在网络安全标准的采纳上进展缓慢。此外，网络安全标准的更新速度可能跟不上技术发展的步伐，导致一些标准在发布时已经过时或不完全适用于当前的网络环境。

3 措施与建议

随着我国数字经济的快速发展和国际地位的提升，我国网络安全标准在“一带一路”沿线国家的影响力逐渐增强。我国应积极利用这些机遇，通过加强与发展中国家的合作，推动我国网络安全标准的国际化，同时，也应积极参与国际标准的制定，争取在新兴技术领域如：5G、物联网、人工智能等方面，为国际网络安全标准贡献中国智慧和中国方案。

3.1 完善顶层设计，做好“按需供给”

密切结合当前数字中国建设布局、法律法规落实要求，提前研判大数据、区块链、元宇宙、人工智能、量子计算等新兴产业特定安全需求，系统梳理对我国网络攻击历史数据，明确自身网络安全薄弱环节，加强网络安全标准化工作基础研究和顶层设计。尽快研制并发布数据安全、管理体系、隐私保护等领域重要标准，为我国网络安全工作开展提供标准化解决方案。同时，为加强网络安全标准化工作的顶层设计，我国需建立一个跨部门协作机制，确保标准化工作与国家网络安全战略同步。实施细节包括但不限于：制定国家网络安全标准化战略规划、建立网络安全标准化技术委员会、推动关键技术领域的标准研制。预期效果是形成一套与国际接轨且符合国情的网络安全标准体系，提升国家网络安全管理的整体效能。

3.2 跟踪国际动态，做到“主动出击”

统筹分析国内外网络安全发展形势、信息技术前沿热点，及时跟踪相关领域国际标准最新进展，研究总结“网络韧性”等标准框架关键指标，在制定我国标准时借鉴转化吸收。依托利用我国数字经济领域优势，主动参与、积极引领网络安全国际标准和规则制定，为我国网络安全国际合作推进打造标准化底座。应深入分析国际网络安全标准的最新进展，并主动参与国际标准的制定和修订工作。具体措施包括加强与国际标准化组织的沟通与合作、派遣专家参与国际会议、在国际平台上积极推广我国的标准。预期效果是在国际网络安全标准化领域提升我国的话语权和影响力，促进我国标准成为国际认可的参考。

3.3 加强实施应用，做细“售后攻略”

精心选取典型行业与应用场景开展网络安全标准试点示范，持续通过互联网、新媒体和国家网络安全重大活动等渠道进行标准实施宣贯，协调推动各部门在政策文件制定、相关工作部署时积

极采用国家标准。定期组织标准复审、开展应用评估，修订或淘汰难以适应网络安全工作需要和技术产业发展需求相关标准，不断提升标准先进性、适用性和可操作性水平，为我国网络安全的“长治久安”保驾护航。通过在关键行业和领域开展网络安全标准的试点示范项目，加强标准的实施和应用。实施细节涉及选择具有代表性的行业、制定详细的试点方案、组织专业团队进行标准宣贯和技术支持。预期效果是提高网络安全标准的实施率和覆盖面，增强各行业网络安全防护能力。

3.4 构建综合评估框架，确保“质效并举”

为确保网络安全标准的质量与效果并重，必须构建一个全面、系统的综合评估框架。该框架将紧密围绕网络安全标准的制定、实施与应用，深入分析标准的适应性、有效性和前瞻性。通过梳理国内外网络安全发展形势，结合新技术、新应用的安全需求，系统评估标准的科学性和实用性。实施细节包括建立多维度评估指标，组织专家团队开展定期评估，并根据评估结果及时调整和完善标准。同时，该框架还将与国际标准进行对比分析，借鉴先进经验，提升我国标准的国际竞争力。预期效果是通过综合评估框架的构建，形成一套高效、科学的网络安全标准体系，不仅提升我国网络安全管理的整体水平，更为我国在国际网络安全领域赢得更多话语权与影响力。

4 结 语

本文深入探讨了网络安全在全球化背景下的重要性及其对国家安全的影响，同时评估了我国网络安全监管体系的现状，并针对国际标准化竞争提出了策略建议。尽管我国在网络安全法规建设与技术发展方面取得了显著成就，构建了一套较为完整的国家标准体系，但在国际标准的制定与推广上仍面临挑战。面对日益复杂的网络安全形势，我们必须加强顶层设计，紧跟国际动态，积极参与国际标准的制定，并强化国家标准的实施与应用。此外，建立科学的评估体系，定期审查并优化策略，是确保我国网络安全监管体系持续进步的关键。未来，我国需继续深化网络安全标准化工作，加强国际合作，提升国际话语权，以构建更加安全、稳定、开放的网络环境，助力数字经济的健康发展。

参考文献

[1] 杨建军. 努力开创网络安全标准化工作新局面[J]. 信息技术与标准化, 2022(05):1.

[2] 李盛葆,程姣,赵煜,等. 面向区域关键信息基础设施的网络安全形势分析和防护机制研究[J]. 网络安全技术与应用, 2021(07):27–29.

[3] 陈韵然,张卫博. 网络安全产品互联互通标准化研究[J]. 信息技术与标准化, 2024(04):57–61.