ISSN：3078-8994
EISSN：3104-4492

等级保护制度下关键信息基础设施攻防对抗研究

佘帅彦　佘瑾南　文瑞阳　王宇博　范　军

联通数字科技有限公司系统集成事业部，北京 100032

摘　要：随着数字化和信息化进程的加速，关键信息基础设施在国家经济、社会及安全稳定中扮演着越来越重要的角色。等级保护制度作为我国信息安全的核心保障框架，已在多个行业得到广泛应用。本文围绕等级保护制度下关键信息基础设施的攻防对抗展开研究，分析了当前体系在实施中的难点和存在的问题。通过探讨等级保护制度实施的难度、信息安全防护措施的不足以及攻防对抗能力的低效性，揭示了现有制度面临的挑战。基于此文章提出了强化制度实施与监督、提升信息安全技术防护水平以及推动攻防对抗能力提升的优化对策，以期为进一步完善等级保护制度提供理论支持与实践指导。研究表明通过制度完善与技术创新的双重驱动，可以有效提升关键信息基础设施的整体安全防护能力。

关键词：等级保护制度；关键信息基础设施；攻防对抗；信息安全

0. 引言

信息技术飞速发展，关键信息基础设施逐步变成国家安全跟社会稳定的重要支柱，它不只助推经济发展，还为维护国家安全跟公共服务给予重点助力，伴随网络攻击技术的持续发展，怎样保障关键信息基础设施避开各类安全威胁，变成政府、企业以及学术界急切需要解决的重要问题。我国的等级保护制度推行以来，为关键信息基础设施的安全防护给出了规范框架，但是在实际执行时，制度遇到实行难度大、技术手段落后、攻防对抗能力不足等问题，减少了保障关键信息基础设施安全的效果，本文意在分析等级保护制度下相关问题，提出优化对策，助力增进信息安全防护能力。

1. 等级保护制度下关键信息基础设施的重要性

1.1 保障国家安全

关键信息基础设施占据国家安全体系中的重要位置，承载经济、政治、军事等多个重点功能，一旦信息基础设施遭到攻击或瘫痪，引发社会运行的严重混乱，甚至危及国家的稳定与安全，能源、电力、交通等系统的正常运转对国家的安全防线十分重要，任何网络攻击引发系统瘫痪，致使社会不安或国家安全危机。等级保护制度的推行，凭借分级管理与防护明确了基础设施的安全要求，明显减少了关键信息基础设施遭受攻击的可能性，借助技术防护手段、风险分析和响应机制的精进，保证关键信息基础设施在复杂多变的安全环境中稳定运行[1]。

保障国家安全时，等级保护制度不光注重技术层面的安全防护，也加强了管理层面的监督跟约束，凭借分类管理不同等级的基础设施，把有限资源和技术力量集中到最核心、最薄弱的地方，增强了安全防护的准确性与高效性，这一类结构化的安全体系，有利于妥善应对网络空间的各类安全威胁，保证国家在繁复国际环境中依然可以实现独立自主与稳步发展。

1.2 推动数字化转型与创新

伴随信息技术快速发展，数字化转型变成各行业增强重点竞争实力跟实现可持续发展的重点方向，关键信息基础设施是数字化转型的基础，可以助推社会各领域创新，无论是制造业的智能化升级，还是金融行业的大数据使用，都需要靠着稳定安全的信息系统来保障。等级保护制度发挥了保证系统安全跟信息完整性的关键作用，凭借为不同层级的信息系统给出严格的安全防护，该制度助力数字化转型，保障企业在转型中有效避免信息泄露跟数据篡改等风险。

数字化转型一般伴随着新技术的引入，特别是在云计算、物联网跟人工智能领域，这些技术快速发展，让信息基础设施面对更高标准，等级保护制度为新兴技术的安全使用给予了框架与方向，凭借保障创新技术的安全性，可以防止快速更新带来的隐患，保证企业跟社会的信息安全。伴随信息安全防护水平的增加，数字化转型更加顺畅，创新能力得到全面释放。

1.3 提升社会治理与公共服务能力

信息化社会来临让传统社会治理方式遇到重大改变，关键信息基础设施不只是经济活动的基础，也是社会治理和公共服务的重心，公安、交通、教育、医疗等领域的设施包含众多公共数据跟管理信息，保障此类系统的可靠跟稳定，变成社会治理中的重要问题。等级保护制度在此起到关键作用，保证上述核心领域的信息系统高效运转，同样防止恶意攻击或数据泄露，

ISSN：3078-8994
EISSN：3104-4492

助力社会平稳运行[2]。

借助为关键信息基础设施给出不同等级的安全防护，不光增强了信息系统的抗攻击水平，还助力各类公共服务的创新优化，打下了稳固基础，智慧城市的建设离不开信息基础设施的助力，等级保护制度为交通、环境、能源等众多信息系统给予了核心保障，防止了信息安全问题的发生，助推了公共服务水平与能力的加强。

2. 等级保护制度下关键信息基础设施存在的问题

2.1 等级保护制度的实施难度

等级保护制度执行到关键信息基础设施时，面对不少难题，各类基础设施繁复多样，涉及的技术范围差别较大，执行起来大多不容易顾及所有细节，许多行业信息系统，特别是新兴技术领域的设施，缺少一致的标准与规范，致使详细操作中显得格外棘手。针对不同级别的保护要求，需对每个系统实行细化分析，但实际操作中，信息系统种类多样，安全需求繁杂，执行时容易出现监管漏洞，比较难保证每个环节都执行到位[2]。

制度实行时大多缺少足够的技术协助和人员培训，致使相关部门跟企业对等级保护制度的理解与执行出现偏差，特别是一些技术能力较弱的中小型企业，缺乏专业的安全人员以及技术保障，等级保护工作不光受限于资源，还缺少详细的帮助和参照。上述企业在技术帮扶、资金投入和人员安排上存在不足，使得制度在实际操作时不容易全面落实，部分企业对等级保护制度相关政策以及要求理解不深，无法准确选择和执行适合自身的安全措施，所以等级保护制度针对不同层次、不同规模的基础设施效果不够理想，部分系统甚至难以达到最低安全要求，无法有效应对越来越繁复的网络安全威胁。此类问题不只减少了等级保护制度的实行成效，还拖慢了整体信息安全防护体系的精进进度。

2.2 信息安全防护措施的不足

关键信息基础设施面对越来越繁复的网络威胁时，现有的信息安全防护手段没能很好应对新攻击方式跟安全漏洞，虽然等级保护制度为传统安全防护给出了框架保障，但黑客攻击手段不停变化，许多现有措施已不容易满足新的安全需要。许多信息系统依旧靠着传统的防火墙、入侵检测等技术，此类手段面对现代高级持续性威胁（APT）以及零日攻击这类新型风险时显得不容易应对，攻击技术一直升级，基础设施的防护方式已经落后，无法有效抵挡高等级的网络攻击。

信息安全防护技术的投入跟更新速度较慢，一些关键信息基础设施里，企业和政府单位的安全防护预算较少，这使得安全技术采购以及更新显得迟缓，这一些防护设施比较难跟上网络威胁的快速变化，让系统面对持续增加的风险。伴随攻击者利用新的攻击途径渗透系统，现有防护措施不容易给予足够防范能力，致使信息安全防护体系出现巨大漏洞，直接危及关键信息基础设施的安全与稳定。

2.3 攻防对抗能力的低效性

目前关键信息基础设施的攻防对抗能力较低，特别是在面对高强度攻击时显得不足，许多基础设施的攻防体系仍处于起步阶段，尚未形成完整的方针与机制，虽然部分地方已开始实行网络攻防演练以及模拟，但实际效果常受技术、人员及设备条件限制，比较难真正还原冗杂的网络攻击环境。企业以及政府面对网络攻击时，缺少实际应接经验跟紧急处理能力，问题出现后比较难迅速解决，导致损失扩大[3]。

攻防对抗技术的更新与迭代速度较为缓慢，许多防御手段仍停留在传统模式，没能及时融入新兴技术，攻击方式越来越繁复，防守方总是只能被动应对，缺少主动防护跟迅速反应的能力，攻防对抗体系实战环境中应用能力远低于预期，关键信息基础设施面对大规模、多元化攻击时反应速度低，抗压能力差，这对安全性与稳定性带来了明显问题。

3. 等级保护制度下关键信息基础设施优化对策

3.1 强化等级保护制度的实施与监督

为了有效助推等级保护制度的实行，需要增强各级政府部门与企业之间的配合，保证执行力度和覆盖范围，政府应履行监管职责，根据各行业特性制定详细细则，明确任务以及标准，保证每个环节都能执行到位，特别是在执行时，必须建立更严密的监督跟审查机制，定期检查各类基础设施的安全状况跟保护措施，发现问题立即提出精进要求。凭借设立全国范围的等级保护安全检查体系，增强对关键信息基础设施安全的整体监管能力，特别是规模较小、技术力量相对薄弱的企业，政府可借助政策帮助和技术培训等手段，助力加强信息安全管理水平。

助推等级保护制度的精进，需要加强信息安全人才的培养与引进，增进企业跟管理部门的安全意识跟技术水平，安全意识的增加是制度执行的基础，企业和政府可凭借定期培训、演练等活动，让各级人员深度领会等级保护制度的核心内容跟重要性。定期的安全审查，不光能协助企业快速找到问题，又能借助外部专业机构的监督，增强整体制度的执行效果，保证等级保护的各项要求高效准确执行。

ISSN：3078-8994
EISSN：3104-4492

3.2 提升信息安全技术防护水平

加强信息安全技术防护水平是关键信息基础设施安全保障的重要部分，攻击技术越来越繁复，传统防护手段不容易应对新型威胁，需要使用更先进的安全技术，核心基础设施需要使用高效的加密技术、防火墙、入侵检测以及防御系统等传统手段，同样融合人工智能、大数据分析、区块链等新技术。人工智能可以借助实时监控与数据解析发现攻击行为，快速找到网络中的安全隐患并采取应接措施，增强信息系统的修复能力跟防护效果，大数据技术可以实时收集跟分析海量的网络流量与安全日志，发现异常行为并提前发出警告，缩短应接重大安全事件的时间。区块链技术应用于数据完整性和透明性，能有效避免数据被篡改或泄露，增强信息系统的可靠性跟安全性 [4]。

防护体系建设里，技术持续更新升级是保障系统安全的重点，信息安全防护产品以及技术的开发需紧跟时代步伐，保证能有效应接目前及出现的安全威胁，企业跟政府可凭借加强多行业协作，助推信息安全技术共同研发跟资源共享，构筑更加牢靠的安全屏障。技术人员的培训和安全意识的增强是保证防护体系高效运行的关键环节，定期升级信息安全技术、修复漏洞也十分重要，经常开展系统跟应用的漏洞扫描，及时处理已知漏洞，同样防范出现的新型攻击，有益于增强信息系统的抗攻击能力，加强整体防护效果。在此基础上，系统的持续改良和技术的动态优化是保证长期安全防护的重点要素。

3.3 推动攻防对抗能力的提升

增进攻防对抗能力是保证关键信息基础设施应对冗杂网络威胁时可以妥善处理的重点，为了增强攻防对抗的实际效果，需建立全面且多层级的攻防对抗体系，开展攻防对抗演练跟模拟，是增加攻防能力的重要方式，借助真实的演练条件，还原各类网络攻击场景，让防守方能在实际条件下检验防御技术及应急反应水平。这一些演练不只能帮助找到现有防御措施里的漏洞，还能助推攻防两方技术以及方针的改良，增强应对大规模攻击的实力，需要安排定期的安全攻防演练，融入最新的网络攻击技术，保证演练的真实性与效果，除了上述所说，模拟演练还需依据网络安全态势的改变，逐步引入新的攻击手段和应急响应场景，保证防御方在多变的攻击环境中具备灵活应接跟快速反应的能力。

攻防对抗能力的提升还需要加大信息共享和协作的力度。在网络攻防对抗中，单一的企业或机构往往难以独立应对复杂的攻击手段，必须依靠跨部门、跨行业的合作与信息共享，形成攻防协同效应。建立更加开放的信息安全共享平台，将各类安全事件和防护经验共享给其他部门和企业，有助于提高整体的攻防对抗水平。通过共享数据和技术成果，提升对攻击行为的识别与防范能力，从而形成强大的安全防护网。政府与企业也应加强与国际信息安全组织的合作，及时了解全球范围内的网络安全威胁动态，提升跨国界的攻防对抗能力，以更好地应对日益复杂的网络安全挑战。同时促进国内外技术交流与合作，能够为攻防对抗体系注入更多创新思维与先进技术，进一步提升其应对能力。

4. 结论

关键信息基础设施的安全防护已成为国家安全体系中不可或缺的组成部分。等级保护制度作为我国信息安全治理的重要制度基础，对保障基础设施的安全运行发挥了关键作用。通过对制度实施难点、技术防护不足与攻防对抗低效等问题的系统分析，可以看出当前安全体系在执行层面、技术层面和协作层面仍存在较大改进空间。面对不断升级的网络攻击手段，仅依靠传统防护已难以满足复杂多变的安全需求。制度的强化与监督、技术的创新与融合、攻防对抗的体系化建设，是未来提升整体防护能力的主要方向。应持续完善等级保护标准，健全审查评估机制，推动安全责任落实到每一个环节。要加大信息安全技术的研究投入，推动人工智能与大数据在威胁检测与响应中的深度应用，形成智能化、动态化的防御体系。攻防演练和信息共享机制的建立，将为安全防护提供更强的实战支撑。

参考文献：

[1] 杨轶 , 宋延成 , 迟宏哲 . 等级保护 2.0 时代下的电力系统身份安全研究 [J]. 网络安全技术与应用 , 2019(12):2-7.

[2] 陈晓 , 代琪怡 . 等级保护 2.0 下的物联网安全防护措施 [J]. 科学技术创新 ,2020,(03):80-81.

[3] 王昊宇 . 网络安全等级保护制度下大数据安全存储与传输技术研究 [J]. 移动信息 , 2025, 47(1):145-147.

[4] 顾珊菁 . 网络安全管理与网络安全等级保护制度研析 [J]. 中国科技期刊数据库 工业 A, 2023(4):4-10.

作者简介：佘帅彦（1998.7—），男，汉，北京，本科，研究方向：网络安全。