基于政务系统的应急管理体系建设研究优化与改进

岳 翔[1] 高健凯[2]
1. 南京城市云计算中心有限公司 江苏 南京 210000
2. 曙光云计算集团股份有限公司 天津 300000

摘 要：本文深入研究基于政务系统的应急管理体系建设，阐述应急管理体系建设的必要性，针对当前应急管理中的不足，提出优化与改进策略。通过加强制度建设，实现应急管理的体系化；借助信息化与智能技术的融合应用，显著提升应急响应的速度与精准度；积极探索不同组织间信息共享，提升政务系统应急管理水平。优化与改进措施有效提升政务系统应急管理体系的整体效能，为应对各类突发事件提供有力保障。

关键词：政务系统；应急管理；体系建设；优化与改进

1 政务系统应急管理体系的重要性

政务系统安全稳定运行，关乎社会稳定和国家安全。政务系统应急管理是指政务系统在面对各种突发事件和灾害时采取的一系列紧急应对措施和管理活动。这些事件可能包括自然灾害、电力系统故障、设备故障以及网络攻击（如DDos攻击、勒索病毒攻击、APT攻击等），以及其他突发事件。政务系统应急管理体系建设目的是保障政务系统的安全、稳定运行和连续的对外服务能力。《中华人民共和国网络安全法》第二十五条规定网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。第二十九条规定国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。依据网络安全法条款分析，政务系统应急管理体系应至少包括应急预案编制、应急工作机制建设、应急处置、应急演练四部分，其中通过应急演练可以验证应急预案、优化应急处置、锻炼应急队伍协作、提升整体风险方案意识。

2 政务系统的应急管理体系建设现状与问题

随着云计算技术的发展和应用，政务系统主要分为自运营和上云运营两类。自运营政务系统由系统所属单位独立运行，对政务系统安全整体负责。政务系统上云后由云服务商和系统所有方共同运营，两方均对政务系统安全负责。政务系统不同运营模式均需应急管理体系建设，其中上云运营模式应急管理体系更为复杂，本文以电子政务云运营模式阐述应急管理体系建设。首先，在电子政务云的应用下，用户对数据和系统的控制管理能力减弱，安全责任存在重叠交叉，多数省市级电子政务云为多云建设模式，对于应急管理体系建设更为复杂[1]。

3 应急管理体系改进方法

3.1 新技术在应急管理中的应用

优化与改进应急管理体系的方法与路径多种多样，新技术应用作为应急响应体系建设的重要手段之一。故障和攻击监控告警系统基于大数据技术的应用能够显著提升告警的准确率，通过收集、整合和分析各类监控告警数据，可以实现对事件的实时预警和预判，为应急处置决策提供科学依据[2]。人工智能在应急管理体系中也发挥着重要作用，借助人工智能技术，可以实现应急预案的自动匹配和优化，提高应急响应的速度和精准度。人工智能技术可实现协助政务系统进行风险评估和模拟攻击分析，通过分析历史数据和实时告警信息，快速识别潜在风险，为应急处置提供智能决策支持。

3.2 构建多组织协同联动的响应机制

在应对突发事件的过程中，政务系统需要与其他组织或部门紧密配合，共同构建高效、协同的应急响应机制。政务系统应加强与网安、电力、消防、行业安全服务商等相关组织的沟通与协作，事前共同制定应急措施，实现不同组织间建立信息共享，为决策提供及时、准确的数据支持。可依据GB/T20985.1-2017、GB/T20985.2-2020、GB/T20986-2007、GB/T38645-2020等国家标准[3]，建立多组织融合的事件响应小组，实现应急管理体系组织架构统一[4]，根据事件分类分级制定逐级上报协同流程，联合网信、公安等有关部门建立联防联控机制，强化统筹合作，一旦发生网络和数据安全事件（如发生数据安全、网络攻击等主观人为破坏活动时），各应急处置组织可迅速开展调查溯源工作，评估影响范围和危害性，采取措施阻断现实危害。

3.3 基于演练与评估的应急管理体系优化

改进应急管理体系的方法中，基于应急演练与考核评估结合方式显得尤为关键。演练是检验应急预案有效性和应急管理体系完整性的重要手段，定期的应急演练，能够发现现有体系中的不足，进而针对性地进行优化和改进。评估是优化应急管理体系的基础，通过对应急预案、演练方案、演练实施等各个方面的考核评估，可以深入了解现有体系的运行状况，识别存在的风险和问题。

4 某市政务系统应急管理体系优化与改进案例

4.1 某市应急管理体系框架

下面以某市应急管理体系为例，对应急管理体系框架进行说明。从图中我们可以看出应急管理体系框架须遵循安全法规以及评估标准，安全合规是体系框架建立的基础。

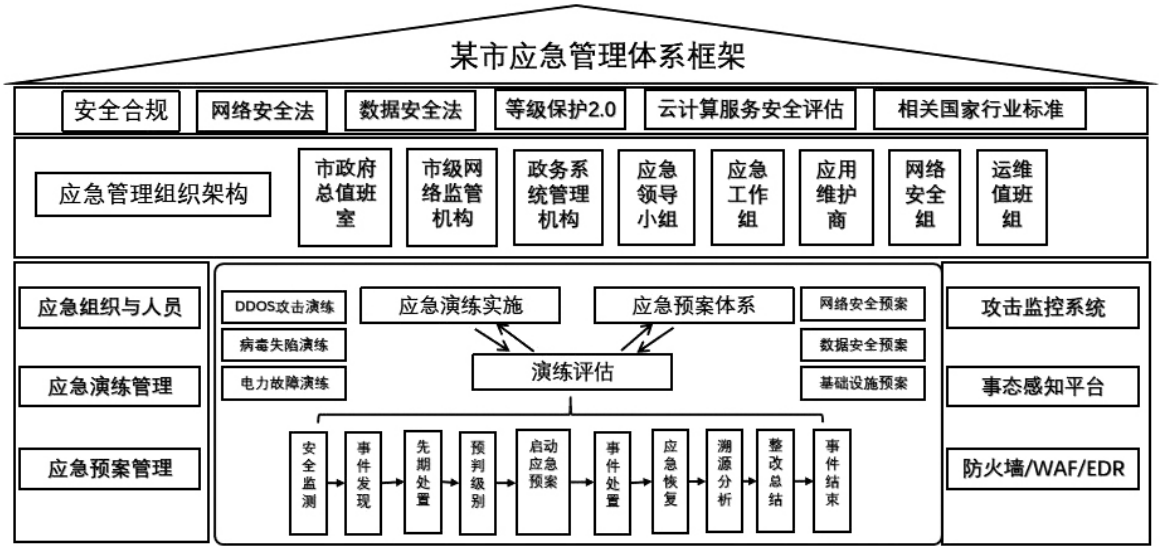

图1 应急管理体系框架

应急管理组织架构是应急管理实施的主体，他包含参与应急处置和应急演练的相关方。管理和技术是构建应急管理体系的两大支撑要素，应急管理方面包括人员组织管理，演练管理和预案管理；技术方面包括事件发现环节的监控技术，处置环节的边界防护技术，复盘环节的感知溯源技术。

4.2 应用新技术建设预警体系

某市应用最新的态势感知技术，构建了一套协同高效的演练模拟平台。首先，平台具有综合可视化功能，能够以图表、仪表板等形式直观展示政务系统安全健康值，实现攻击告警信息可视化，提升应急上报时效。其次，该平台能够实时监控应急演练的进展情况，包括攻击IP位置、资源分配、通信状态等，确保指挥中心能够快速获取决策所需信息，以便作出合理决策。另外，该平台也作为应急资源调度通信枢纽，实现应急响应团队之间的通信，确保应急指令的快速流通。最后，平台部署最新的边界防护设备，可以检测并防御演练中模拟的攻击，具备一键封堵攻击IP的功能，快速验证防护措施的有效性。

4.3 建立事件分级联动机制

应急演练包括桌面演练、模拟演练和现场演练等形式。应急演练科目可以模拟任意突发事件，如DDoS攻击、勒索病毒攻击、网页篡改以及电力故障等。某市2023年度应急演练选择现场模拟演练形式，模拟常见攻击形式有分布式拒绝服务攻击、移动介质病毒、钓鱼邮件以及弱口令爆破等方式。市级政务系统应急预案中对不同事件级别制定不同的联动流程，流程主要分为两部分。第一部分，事件发现和前期处理阶段，该阶段目标是快速阻断攻击降低影响，需对现场值守安全运维人员职责明确，并给予与职责一致的授权。第二部分，在研判后对突发事件定级，不同等级事件，上报部门级别不同，Ⅳ级别事件由本地的应急工作组完成，高级别事件如Ⅰ级事件，由政务系统主管单位研判上报给市级单位，由市级单位统筹联动市内的公安、消防、医疗等关键应急部门完成协作。下图是某市的政务系统应急预案中多梯度联动流程图。

4.4 建立演练评估标准

应急演练工作结束后，演练组织单位应对应急响应处置全过程进行复盘，全面分析和回顾，形成总结报告，将总结报告作为健全完善应急响应工作机制和工作预案的重要依据。某市政务系统应急演练后，依据处置阶段划分进行评估回顾有以下二点：一是事件发现环

节，原演练流程是值班工程师每小时对重要政务系统进行登录巡检或者用户发现问题之后主动上报，演练中事件被发现平均需要20分钟甚至更长，发现问题后采购补充新的统一告警系统，新设备的应用将事件发现时间控制在5分钟以内，应急预案中也同步做了调整。二是事件处置环节，原演练流程中不同等级事件统一都上报给市级政务系统主管单位研判定级和启动预案，复盘发现事件定级标准模糊，云服务商为规避责任低级别事件依旧通知政务系统主管单位，增加了不必要的沟通成本。另外，Ⅰ级事件政务系统主管单位无法实现与其他行业协同联动，在整合资源方面存在问题，针对该问题对应急预案调整，尝试进行不同级别事件多梯度联动。

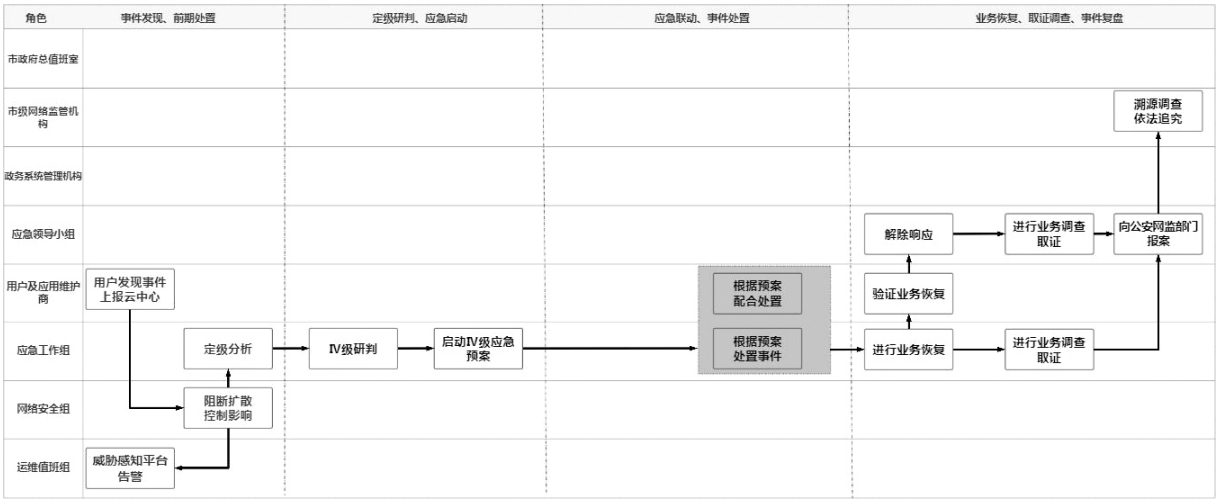

图2 某市Ⅳ级事件应急预案联动流程

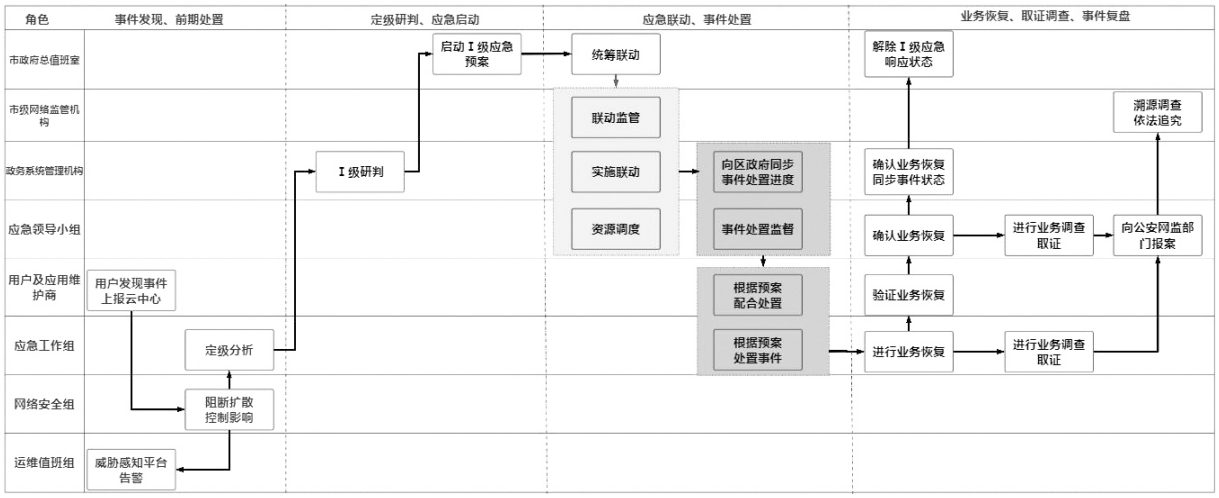

图3 某市Ⅰ级事件应急预案联动流程

结束语

随着社会的快速发展和变革，应急管理体系面临着前所未有的挑战与机遇。通过本文的研究与探讨，为优化与改进应急管理体系提供有益的参考与借鉴。应急管理体系的建设与优化是一个长期而持续的过程，需要不断适应新形势、加强创新与实践。未来将继续关注应急管理体系的发展趋势，深入探索更多优化与改进的策略与路径，为构建更加高效、智能、协同的应急管理体系贡献智慧与力量。

参考文献

[1]徐静.李华.电子政务视角下应急管理信息化建设研究[J].国家行政学院学报,2021.(5).139-145.

[2]陈玲.杨达.大数据与政务系统应急管理的结合研究[J].电子政务,2020.(12).54-60.

[3]龚亮华.尹丽波.王磊.等.GB/T 38645-2020 信息安全技术网络安全事件应急演练指南[S].北京:中国标准出版社,2017.

[4]闵京华.周亚超.王惠莅等.GB/T 20985.2-2020信息技术安全技信息安全事件管理 第2部分:事件响应规划和准备指南[S].北京:中国标准出版社,2017.