社会治理现代化视域下基层网络安全事件协同响应机制研究
——以巴中市为例

彭玉兰　赵柯玲杰

电子科技大学成都学院网络空间安全系 四川 成都 611731

【摘　要】：由于近年来数字化治理推进速度加快，基层网络安全事件处置中仍然存在风险发现滞后、技术支撑薄弱及协同不畅等问题，已成为当前最突出的问题。本文以巴中市为例，分析了巴中市基层网络安全事件及协同响应面临的挑战，提出了“基层发现，区县处置，市级统筹”的协同响应机制，再辅以事件规范上报、分级分权查看、协同响应、信息共享、协同处置诸种具体措施，切实提高基层网络安全事件处置效率。据此设计了符合巴中市情况的网络安全事件协同响应平台，旨在增强基层网络韧性，为社会治理现代化提供有利的理论借鉴和实践参考。

【关键词】：基层；网络安全；协同响应；数字化治理；协同处置

DOI:10.12417/2705-1358.26.12.005

1 引言

国家治理体系和治理能力的现代化要求基层治理具有敏捷性、精准性。网络空间是基层治理的新领域，网络空间的安全对基层社会的稳定、广大人民的生活质量有较大影响。欧阳飞认为，网络信息安全治理已从单纯技术防护逐步转向组织、制度与技术协同推进的综合治理体系，多元主体参与成为提升治理效能的重要路径[1]。赵维认为网络安全问题涉及部门性、行业性和区域性，依赖单一主体独立完成不足以防控网络安全风险、应对网络安全突发事件，需要多元协同来整合各类资源、联合协同处置[2]。基层网络安全事件具有突发性、爆发性和复杂性等特点，传统的单一主体来进行基层网络安全治理显然不适应要求，需要多方主体共同参与基层网络安全协同治理。

巴中市近年基层网络安全事件频发，2024 年“母猪肉”谣言引发公众心理恐慌，电话诈骗洗劫百姓钱财，暴露出处置基层网络安全事件当中涉及的“信息滞后”“条块分割”“反应滞后”等问题。田先红提出条块体制的分割性、低效性和惰性会直接阻碍基层及各部门合作，不利于基层治理效果提高[3]。更重要的是，此种条块体制在处置基层网络安全事件时的表现十分明显，即与经常发生的沟通脱节、职责不明等难题互为因果、彼此强化。另一方面，基层的治理重心偏向社会和服务工作，故基层人员处理的是相对单一的网络安全事件，对复合型网络安全事件的关注较少。因此，探索社会治理现代化条件下基层网络安全事件的协同响应机制，有较强的理论价值和现实意义。

本文以巴中市为例，探索社会治理现代化背景下基层网络安全事件协同响应机制和平台，旨在解决基层网络安全事件协同响应过程中的瓶颈，为提升基层网络韧性、实现社会治理现代化提供有益可复制、可推广的经验。

2 协同响应需求分析

2.1 基层网络安全事件分析

2024 年，巴中市巴州区发生了一起非法倒卖个人信息的事件。在相关行政处罚通告中可知，当事人作为信息利用和流转过程中的利益主体，未遵守网络安全相关的行为要求，对个人信息权利和隐私权构成威胁，被行政机关依法进行了行政处罚[4]。此网络事件说明，除外部网路侵害外，基层的网络安全管理也要提高内部数据管理、监督内部消耗的技巧等。

2024 年在有人在网络平台发布“巴中某市场发现母猪肉”等谣言，引发大量的社会关注。而后公安机关及时辟谣，纠正虚假信息，并依法处理相关人员[5]。这表明，突发事件中主动、透明的信息协同及信息公开对遏制网络谣言扩散、降低负面社会影响都有直接而重大的积极作用[6]。但如果基层单位在信息查证、舆论掌握和引导群众等方面做不到位，也容易造成谣言加速蔓延。

上述案例表明，基层网络安全事件具有类型多样、影响面大以及处置主体多等特点。因此也给现有治理体系带来新的、更大的难题。

2.2 治理机制面临的挑战

（1）协同响应压力增大：由于网络技术迅猛发展。

巴中市哲学社会科学规划项目：BZ26ZC020。

网络安全事件有扩散速度快、波及面广的特点，而基层单位又要同时处置隐患排查、风险研判、舆情引导诸种任务，故而现有的网络安全问题绝不是单纯的技术问题，实质上也是个人信息安全、公共服务、网络舆情诸种问题的交织。因此，对协同响应能力提出了更高要求[7]。（2）协同处置需求增强：由于基层网络安全事件一般都牵涉公安、网信、宣传诸种主体，故单一处理模式难以很好地解决复杂事件的处置问题，而事件处理效率又直接取决于信息共享、职责衔接、资源协同诸种因素，因此，建立多主体参与的协同治理机制是提高事件处理效率的关键。（3）专业能力要求增高：网络安全事件复杂性日趋复杂，故对基层专业处置能力提出更高的要求。不同类型的网络安全事件传播渠道不同、影响程度有别、处理方法不同，需要兼顾技术处置与治理协调两方面工作。目前不少地区仍存在网络安全专业人才匮乏、技术支撑能力薄弱以及实践经验不足等问题。因此，提升处置网络安全事件专业能力仍面临一定挑战[8]。

3 角色分工

本文按照“基层发现—区县处置—市级统筹”的总体思路，构建分层协同响应体系。不同主体依据职责分工参与网络安全事件发现、研判和处置，实现信息共享与协同联动。

3.1 白帽用户

白帽用户都是事件的发端，负责发现异常信息，并对初始异常进行上报，是基层风险识别的首要来源。白帽用户的角色大多由基层员工和网格员等基层人员来承担，平时在巡查中首先发现异常信息等。发现了异常信息之后，相关责任人员按照要求进行事件填报，并提交至协同响应平台用于后续研判。该角色在风险的早期发现和传递中起到比较重要的作用。

3.2 应急组

应急组一般由区县的网信部门、公安局网安部门及相关单位人员组成，负责对上报事件的真实性和危害性进行判断，根据事件类型、等级采取相应的措施。对于技术类事件（如系统漏洞、攻击）需要进行事件的排查、补救；而对谣传、诈骗类事件又需要同时进行查验、舆论引导等。应急组既涉及对事件的具体处置，也会对后续协同整体处置的效率产生影响。

3.3 管理员

由于管理员在协同响应机制中承担组织协调、统筹调度的重要职能。按职责的不同将其划分为区县管理员和市级管理员。具体而言，区县管理员负责辖区内事件流转、分类研判、协调处置，组织应急组推进事件处理，对跨区域或影响重大的事件及时上报市级管理员。市级管理员则负责跨区域事件统筹、资源调配、整体监督，并对典型案例加以总结，不断优化完善协同响应机制。

4 协同响应机制

结合巴中市基层网络安全治理的实际需求，本文针对“基层发现、区县处置、市域统筹”的响应思路，建立市级、县区级、乡镇（街道）三级响应机制，将不同层级中各自角色的信息组织和协作协调起来，高效地实现网络安全事件的快速发现、分类处置和统一协调工作，如图 1 所示。

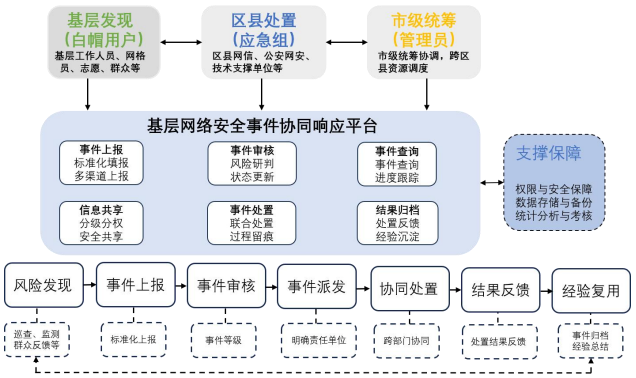

图 1 基层网络安全事件协同响应机制图

4.1 机制设计

（1）标准化事件上报机制：基层网络安全事件处置中最突出的问题就是信息来源分散、各要素描述标准不统一，增加了后续研判和处置的时间成本。为解决这个问题，本文考提出了针对上报事件信息做结构化约定的思路：统一事件上报所含字段（事件类型、影响区域、异常表现、证据材料等）。与单纯依靠事件文字描述或截屏报送的方式相比，此种方式能避免场景中反复交流、反复补充的情况，但也对基层人员的信息填报规范性提出更高要求。（2）分级审核与风险研判机制：网络安全事件的危害性和影响力有所不同，因此需要对网络安全事件适当分级。网络安全事件上报后，县区技术人员首先对事件真实性进行核验，并结合历史案例、影响范围和潜在危害程度开展风险研判。在此基础上，对事件划分不同风险等级，并给事件不同的处置路径。普通情况下，低风险的网络安全事件仅需基层自己解决。较高风险的事件，需要协调调用部门一起解决；重大事件上报至市级牵头。（3）协同事件流转机制：事件进入处置阶段以后即予以细分、下分，统筹部门根据事件的类型、等级把任务合理、有层次地分派给不同部门或责任人，同时厘清任务的处理范围、责任主体、完成时限，各有关单位在任务处理中主动、及时地反馈任务进展，故整个处置过程都处在可控、可监的状态之下。与传统单一部门处置模式相比，该机制更有利于促进跨部门协作及资源共享。（4）知识共享与经验沉淀机制：基层在处理网络安全事件过程中，由于网络安全事件的类型不同、事件变化快而很难有固化的经验。因此，应加强处置案例的积累和经验的共享，为后续类似事件处置提

供参考[9]。积累的经验可以逐步形成内部知识库，为后续类似事件提供参考依据。此外，各地区在事件处理中形成的经验也可以相互交流，为后续事件处置积累经验。

4.2 平台设计

结合巴中市的基层网络安全事件处理需求，文章设计了“网络安全事件联动处置、协同响应的平台”，用于提升不同部门间、不同层级间的信息共享和协同事件处置能力。协同响应平台主要包括事件上报、事件查看、事件审核、事件处置等模块，如图 2 所示。

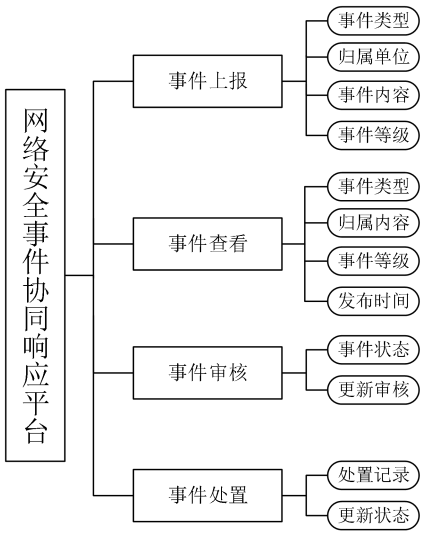

图 2 平台核心功能图

事件上报负责规范采集信息，为各种社会力量（志愿者、社会机构等）参与共治提供技术通道。白帽用户可以查看历史上报过的事件，但无法对已上报的事件做修改，这样即可以避免重复上报浪费资源，还可以避免数据遭受恶意修改。

事件查看实现事件跟踪与信息查询。查看过程中用户分级分权访问，角色不同查看的信息不同。不同权限，展示相关区域上报的网络安全事件信息不同。此外，还可以根据事件的审核状态进行筛选并对事件生命周期进行全面跟踪。

由于事件审核的基本职能是真实性核验、风险评估。应急组用户可以从“待审核事件”直接查看当前任务中需优先处理的安全事件，然后组织有关人员对事件的真实性、危害性、紧急程度三者作联合评估，据此形成初步协同处置建议。

事件处置要承担事件协同处置、过程记录、结果反馈诸种职能，为保证事件从提出、处置到结果反馈都全程留痕，形成完整的管理闭环，因此应急组用户可在“所有事件"中方便地跟踪所提交事件的全生命周期。

图 3 平台核心功能界面

5 结束语

本文围绕巴中市基层网络安全事件处理面临的挑战展开分析，并对网络安全事件和现实治理困境进行梳理，提出“基层发现—区县处置—市级统筹”的三级协同响应机制，并围绕事件上报、查看、审核、处置环节进行详细设计。并在此基础上构建协同响应平台，用于信息汇集与网络安全事件分派，有利于提高网络安全事件处理过程的可追踪性与协同效率。

参考文献：

[1] 欧阳飞.高校网络信息安全治理体系构建[J].网络安全和信息化,2025,(10):26-28.

[2] 赵维.网络安全的协同治理路径探析[J].湖南警察学院学报,2024,36(5):29-37.

[3] 田先红.中国基层治理:体制与机制——条块关系的分析视角[J].公共管理与政策评论,2022,11(01):43-54.

[4] 王利明.数据共享与个人信息保护[J].现代法学,2019,41(01):45-57.

[5] 巴中长安网.打击网络谣言!巴中发布 8 起整治典型案例[EB/OL].2024-04-25[2026-05-26].

[6] 邹雪琴.突发公共事件中网络谣言治理的现实困境与对策分析[J].网络安全技术与应用,2023,(06):161-163.

[7] 王林,魏嘉贺.数字经济时代下网络安全情报共享与协同防控策略研究[J].情报杂志,2025,44(11):107-113+89.

[8] 仇蓉蓉,孙雨生,王淼.信息安全联动治理的组织架构研究——以云环境下国家数字学术资源为例[J].情报资料工作,2024,45(6):102-108.

[9] 蒋勋,苏新宁,周鑫.适应情景演化的应急响应知识库协同框架体系构建[J].图书情报工作,2017,61(15):60-71.