

Analysis of the Development of Emergency Management for Natural Disasters-Driven by Information Technology

Yi Wang

Wuhan University of Technology, Wuhan, China
2787228748@qq.com

Abstract. When disaster strikes—an earthquake that cracks highways, a flash flood that turns a neighborhood into an island, or a typhoon that knocks out power for days—emergency management is the machinery that has to move fast and still make sense. It brings together government agencies, businesses, community organizations, and other actors who may not work side by side in daily life but suddenly need to coordinate as if they have rehearsed for years. In this paper, I look at what happens when that machinery is rewired with modern information technologies—big data, cloud computing, the Internet of Things (IoT), and artificial intelligence—specifically through the lens of natural-disaster response in China. China’s emergency management has been shifting from experience-driven, department-by-department handling toward a more standardized system built around unified command and quick, disciplined response. On paper, that transition sounds straightforward. In practice, it’s messy in the way real operations tend to be: legacy equipment still sits in the field, information travels through parallel chains, and many digital tools never make it past “pilot project” status into everyday use. So the question is not whether technology helps—of course it can—but how deeply it is embedded into decision-making when time is tight and uncertainty is the norm. I argue that the next step is not simply adding more platforms or collecting more data. What makes the difference, in most cases, is tighter integration: sensors and IoT devices that capture conditions as they change; big-data pipelines that turn scattered reports into a coherent operational picture; and AI methods that support early warning, resource allocation, and dynamic dispatch. If emergency systems can learn to treat data as a living stream rather than a static report, preparedness becomes less of a slogan and more of a capability. Strengthening these technological foundations, while keeping them usable for frontline responders, matters because the stakes are concrete—people’s lives, families’ homes, critical infrastructure, and the broader stability that depends on crises being contained rather than amplified.

Keywords: Emergency management, natural disasters, information technology, IoT, big data

1. Introduction

When a major earthquake hits at night, or a river suddenly overtops its banks after days of relentless rain, the first question is rarely theoretical. Who sees it in time? Who calls whom? And how quickly do warnings, people, supplies, and decisions move to the places that need them most? Emergency

management sits in that practical space. It covers what governments, enterprises, social organizations, and other actors do when sudden incidents occur—natural disasters, industrial accidents, public health emergencies, and social security events [1]. In most cases, it is less a single action than a chain of work that has to hold together under pressure: prevention and preparedness, monitoring and early warning, response and rescue, and then the long, often overlooked phase of recovery and reconstruction [2]. Done well, emergency management lowers the likelihood that hazards spiral into full-blown crises, reduces losses when emergencies do occur, protects lives and property, and helps preserve public security and social stability.

The modern idea of emergency management matured in the mid-to-late twentieth century, largely as countries learned—sometimes the hard way—that ad hoc mobilization is not a strategy. China’s more systematic development accelerated in the twenty-first century through the rollout of relevant laws and regulations and the establishment of dedicated emergency management agencies. Many countries now operate relatively complete mechanisms, and China has shaped an approach often described as “unified command, a combination of routine and specialized forces, swift response, and vertical coordination” [3]. Even with the progress already made, complex, compound disasters—and the newer risks that seem to appear each year—still strain coordination, information flow, and on-the-ground execution. Things get especially fragile when hazards stack on top of one another and the clock starts running faster than the system can comfortably keep up.

In this setting, natural disasters are not abstract “events” that sit neatly on a timeline. They are disruptions sparked by unusual shifts in the natural environment, and they tend to land where people live and work—bringing casualties, property loss, and, at times, a broader sense of instability. Emergency management functions as the response mechanism to that risk source: it tries to blunt harm through prevention, preparedness, and rapid action when conditions turn. The scale in China makes that logic hard to ignore. According to the Ministry of Emergency Management, natural disasters affected 94.13 million people to varying degrees in 2024, led to 856 deaths or missing persons, damaged 10.089 million hectares of crops, and caused direct economic losses of 401.11 billion yuan [4]. Those numbers are more than a year-end tally. They hint at what is at stake—households pushed into crisis, infrastructure stressed beyond its design assumptions, and development plans disrupted by a single season of extreme weather.

One of the most practical levers for improvement is technology—though it only earns its keep when it lives inside operations rather than in presentation slides. In this paper, “information technology” is not a vague buzzword. I use it in a concrete, operational sense: the hardware, software, networks, and digital tools that collect information, clean it up, move it where it needs to go, and turn it into something people can actually act on. In most contemporary emergency systems, that toolbox comes down to four workhorses—big data, cloud computing, the Internet of Things (IoT), and artificial intelligence—and each one earns its place in a different way. Big data helps teams pull usable signals out of huge, disorderly datasets—the kind that arrive in fragments and contradictions when a disaster is unfolding. Cloud computing provides scalable processing power and makes it easier to share resources across agencies and regions, instead of forcing everyone to compete for limited local capacity. IoT links devices so they can sense conditions and communicate in real time, giving the system a steadier stream of field-level facts. AI adds automated analysis and decision support, stepping in when the volume of inputs exceeds what any human team can reasonably absorb without missing something important. When these capabilities move from “installed” to truly “integrated,” they can tighten early warning, sharpen resource deployment, speed up the drafting—and constant revising—of response plans, and bring more discipline to post-disaster assessment. The practical difference is easy to imagine. One rescue team tries to coordinate

through scattered phone calls and partial updates; another works from a shared, live picture of road closures, rainfall intensity, shelter capacity, and medical demand. Which one is more likely to arrive in time, and with the right supplies?

And yet the system still has obvious friction points. Outdated monitoring equipment remains common in many areas. Departments still operate in silos, even when they face the same hazard. Information technologies also do not cover enough scenarios in a truly end-to-end way, which means some emergencies still unfold beyond the reach of real-time sensing, integrated analysis, and decision support. If the goal is to shift that trajectory, deeper integration matters more than scattered upgrades. IoT devices need to plug into workflows instead of behaving like standalone gadgets; big data and AI need to shape forecasting, rescue-plan design, and real-time dispatch rather than being limited to after-action reports. With that as a starting point, this paper offers a focused analysis of natural-disaster emergency management, identifies the constraints that continue to limit performance, and outlines the challenges future systems will have to confront directly. The objective is simple, if demanding: faster, more coherent responses as disasters unfold, and more dependable protection of lives and property when the margin for error disappears.

2. Categories and applications of information technology

In practice, when people talk about “information technology” in emergency management, they usually mean a handful of toolkits that have already proven themselves in other high-stakes settings: big data, cloud computing, the Internet of Things (IoT), and artificial intelligence (AI). They are not interchangeable, and they do not solve the same problems. Still, they often work best as a package—one gathers signals, another moves and stores them, another turns them into something intelligible, and another helps a team act on them before the window closes. This section looks at how each of these four technologies shows up in emergency management, especially when natural disasters force decisions to happen in minutes rather than days.

Big data refers to large-scale information assets with high volume, rapid generation, diverse formats, and potential value that only becomes visible after analysis [5]. It is already embedded in daily life, even if people rarely call it that. E-commerce platforms infer what a user might want next by reading browsing trails and purchase histories. Banks and financial institutions use profiles—income patterns, spending habits, risk tolerance—to tailor services and flag anomalies. Emergency management, by contrast, has historically run on stale reports, siloed databases, and risk assessments that arrive late or not at all. That is exactly the gap big data can narrow. In natural-disaster response, big data allows agencies to pull multi-source information into a shared operational picture in near real time—meteorological feeds, traffic conditions, satellite imagery, social media signals, hotline logs—and then translate that clutter into risk forecasts and decision support. The value is not the “massive dataset” itself; it is the ability to see patterns early enough to reposition resources, issue targeted warnings, and reduce blind spots when conditions change quickly.

Cloud computing matters for a simple, almost unglamorous reason: when the situation escalates, it keeps emergency systems from choking on their own workload. At the technical level, cloud computing spreads heavy processing across many servers, slices big tasks into smaller ones, and delivers results through cloud services. Outside emergency management, this has become ordinary infrastructure. Companies build collaborative workflows on platforms such as Alibaba Cloud and Tencent Cloud, and universities use cloud platforms to run online courses at scale, even when students sit in different provinces. The emergency world, though, rarely enjoys that kind of breathing room. Hardware capacity varies from one jurisdiction to another, local data-processing can bottleneck at exactly the wrong time, and coordination slows when platforms cannot exchange data

cleanly. Cloud computing helps by scaling computing resources quickly for emergency analytics, supporting cross-regional collaboration platforms, and keeping operations flexible as conditions change. In a large flood, for example, the gap between a local server buckling under demand and a scalable cloud environment can decide whether teams see updated maps, requests, and road closures in real time—or only after the situation has already moved on.

IoT solves a different, more field-level problem: emergency management often operates with an incomplete, delayed view of what is actually happening on the ground. The Internet of Things links physical objects to the internet through sensing devices that follow standardized protocols, enabling identification, positioning, tracking, monitoring, and management. People already live with it at home—lights, air conditioners, and televisions controlled remotely—and industry uses it to monitor equipment health and catch failures before they cascade. Disaster response deals with the same visibility challenge, just with less tolerance for uncertainty. Teams lose precious time when on-site information arrives late, or when they cannot monitor critical infrastructure—bridges, tunnels, substations, reservoirs—in a continuous, reliable way. IoT can act as the system’s “eyes and ears.” Sensor networks can stream conditions from disaster sites in real time, track the location and safety of rescue personnel, and watch key infrastructure as hazards evolve. With that kind of concrete, time-stamped information, leaders can make faster calls and avoid the improvisation that creeps in when decisions rest on partial, outdated reports.

AI enters when the information load overwhelms human attention—something that happens quickly in complex disasters. Artificial intelligence develops methods and systems that simulate, extend, and enhance aspects of human intelligence, including perception, learning, reasoning, and decision-making. Most people recognize its everyday versions: voice assistants such as Siri and Xiao Ai interpret natural language; autonomous driving systems fuse sensor inputs to perceive surroundings and plan actions. Emergency management has long relied on manual analysis and experience-based judgment, which can be effective—right up until the moment it is not. When a disaster unfolds, information rarely arrives in a neat queue. It comes as a rush of radar feeds, sensor readings, field reports, hotline calls, and shaky videos—often all at once, and often pointing in slightly different directions. Human teams can only absorb so much at speed, and the instinct to lean on “what worked last time” can turn into a liability when the context has shifted. AI can help close that gap. Built into emergency workflows, it can scan heterogeneous data streams for early signs of escalation, surface emerging risks before they become obvious, and model plausible paths of disaster evolution so planners can draft and revise rescue strategies with fewer blind spots. It can also support the use of intelligent robots for tasks that are simply too hazardous for people—entering unstable structures, working in toxic environments, or operating where secondary collapses are likely. The point is not to chase an all-knowing algorithm that replaces human judgment. The point is to create a sharper decision environment—one where teams spot threats sooner, stress-test options faster, and keep more responders out of harm’s way.

3. Strengths and weaknesses of information technology in natural disaster emergency management

3.1. Advantages of information technology in natural-disaster emergency management

When a disaster begins to move, the real challenge is rarely a lack of “knowledge” in the textbook sense. People generally understand the basic playbook—warn, evacuate, rescue, stabilize. The challenge is timing and clarity: seeing what is changing early enough, getting that picture to the right desks and the right teams, and repositioning people and supplies before roads wash out, slopes fail,

or weather closes the next window. Viewed that way, information technology is no longer a side tool that sits behind the scene. It increasingly behaves like the connective tissue of modern natural-disaster emergency management. It cannot remove uncertainty—nothing can—but it can shorten the delay between field conditions and leadership decisions, cut down blind spots, and push response from improvised reaction toward more deliberate, coordinated action.

3.1.1. Faster, clearer information flow that speeds up response

Information technology lets responders pick up disaster signals while they are still subtle—before the damage announces itself in the most painful way. Sensor networks, satellite remote sensing, and drones can capture early warnings and follow conditions as they shift in real time. During an earthquake, for example, seismic sensors can register crustal movement and transmit readings almost instantly, giving decision-makers a precious head start when they decide where to send teams and which routes are still viable [6]. In a response world that runs on minutes, that small advantage can mean the difference between reaching a site before bottlenecks form and rolling in after traffic, debris, and confusion have already tightened the streets.

This sensing capacity also redraws the “visible map” of emergency management. Traditional monitoring naturally clusters around accessible, populated areas, while risk often gathers at the edges—mountain valleys where landslides can cut off villages, or open-water zones where typhoons organize and accelerate. With modern observation tools, agencies can watch unstable slopes deep in rugged terrain and track storm development far offshore without depending on occasional human reports. That continuity is not a luxury. A scene that looks manageable at 8 a.m. can deteriorate by noon, and technology helps teams stay aligned with what is actually happening rather than chasing yesterday’s situation.

Equally important, information technology makes data move across institutional boundaries that used to slow response down. Meteorological updates, hydrological water-level readings, and geological indicators can flow into shared platforms instead of remaining trapped in separate departmental systems. When agencies can view consolidated information early—rather than stitching it together through phone calls and partial reports—they can act faster and with more confidence in the critical opening hours, when response speed often shapes the scale of loss.

3.1.2. Better forecasting and smarter resource placement

Forecasting is a practical exercise: it shapes who evacuates, where supplies go, and whether rescue teams arrive before roads wash out. Here, information technology helps because it can store and process far more data than a human team can handle under time pressure. Big data gives emergency managers a way to lean less on gut instinct and more on a fuller, better-grounded picture. By blending historical disaster records with live monitoring feeds and environmental datasets, teams can build predictive models that capture nuance instead of relying on a single indicator. Typhoons make this easy to see. When analysts read past track patterns, intensity swings, and weather “fingerprints” alongside current meteorological conditions, they can narrow the likely path and the most exposed impact zones [7]. Even a small improvement in accuracy matters. It can trigger an evacuation a few hours earlier, or shift medical support and rescue equipment to the right corridor instead of spreading resources thin.

The payoff shows up just as clearly in resource allocation. With geographic information systems (GIS) and IoT-based tracking, agencies can locate critical assets as they really are—supply depots, rescue teams, boats, pumps, generators—rather than trusting a spreadsheet that may have been

accurate last week. As forecasts update and field reports change the picture, coordinators can pre-position personnel and materials toward the areas most likely to take a hit, before roads close and access becomes a problem. In many responses, that is the dividing line between a calm, well-timed deployment and a late scramble that arrives after the best window has already passed.

3.1.3. A more prepared public, and a two-way channel during crises

Technology also reshapes the public-facing side of emergency management, and this piece is easy to undervalue until you watch how people actually behave in a crisis. Most people do not prepare because they have read a policy document. They prepare when advice feels clear, personal, and doable—something they can picture themselves doing at 2 a.m. when the ground shakes or the rain will not stop. Social media, public-education apps, and short-form multimedia can translate complex hazard information into formats people genuinely take in: short videos, simple animations, image-based checklists, and scenario-style walkthroughs that turn “recommended actions” into concrete steps. Regular content on earthquake safety, evacuation decisions, or fire response can draw attention in a way static pamphlets rarely manage. Some apps even let users rehearse through interactive simulations—essentially a low-stakes practice run—which, in many cases, makes the real thing feel a bit less unfamiliar and a bit more manageable.

During disasters, technology also strengthens the communication bridge between authorities and residents. Governments can push warnings and guidance quickly through SMS alerts, social platforms, and other channels, meeting people where they already look for updates. At the same time, residents can share on-the-ground conditions through dedicated reporting tools, turning communication into a two-way flow rather than a one-direction broadcast. That feedback loop is not always tidy—misreports and noise are inevitable—but it can still improve coordination and public participation. Perhaps more importantly, it changes the tone of response: instead of feeling like something done to communities from afar, emergency management starts to look, and feel, more like a shared effort.

3.2. Concerns regarding the application of information technology in natural disaster emergency management

Information technology has clearly improved how emergency systems detect hazards, coordinate response, and communicate with the public. Still, the more these systems rely on digital tools, the more they inherit digital risks. In real operations—where people act fast, systems stretch under load, and small mistakes can ripple outward—several concerns keep resurfacing. They do not negate the value of technology, but they can slow implementation, weaken trust, and in some cases create new vulnerabilities right when resilience matters most.

3.2.1. Information security and privacy risks

Effective emergency management increasingly depends on collecting and moving sensitive data. That includes personal information about affected populations, detailed geographic data about disaster-hit areas, and operational plans such as the locations and movements of rescue teams. Each step—collection, transmission, storage—creates an opening for security failures. A sensor network monitoring river levels, for instance, can become an attractive target: an attacker might tamper with readings, feed in false signals, or steal data outright. If command-and-control databases lack strong

protections, personal details such as identities and home addresses can leak, turning victims into targets at the worst possible moment.

Transmission poses its own challenges. Weak encryption, misconfigured systems, or procedural shortcuts can allow interception of sensitive information. And this is where reality bites: after a disaster, teams often prioritize speed over strict security checks. That instinct is understandable—people need help now—but it can lower the guardrails that normally prevent breaches. A leak in this context does not only violate privacy; it can also be weaponized to disrupt rescue operations, spread confusion, or undermine public confidence in official coordination.

3.2.2. Technological dependence and high maintenance costs

Digital tools can feel like a force multiplier—right up to the moment they turn into the system’s weak link. Many contemporary emergency workflows assume stable connectivity, functioning data platforms, and uninterrupted real-time communication. That assumption holds on normal days. It looks far less convincing when an extreme event tears into the very infrastructure those tools depend on. A major earthquake, for example, can topple base stations, damage data centers, and cut power across wide areas. When that happens, monitoring data may never make it to the command center, and the command center can lose the situational picture it needs to coordinate response. Orders then travel slowly, or not at all, and frontline teams are left to improvise. Delays can stack up fast—especially in the first few hours, when a slightly earlier deployment can translate into lives saved.

Maintenance brings a second, quieter vulnerability. Monitoring devices, data-processing systems, and communication networks do not remain “advanced” on their own. They need regular upgrades, repairs, replacements, cybersecurity patches, staff training, and routine testing—work that is unglamorous, continuous, and expensive. Regions with weaker fiscal capacity often struggle to carry these long-term costs. The result is a familiar pattern: some areas run modern platforms with trained support teams, while others depend on aging equipment and outdated functions that no longer match the risks they face. In the worst cases, the system exists more as a procurement record than an operational capability. Technology installed without the funding and personnel to keep it running can quickly become a sunk cost rather than something responders can rely on when conditions deteriorate.

3.2.3. Information asymmetry and regional imbalances in response capacity

Digital platforms can push lifesaving warnings to millions in seconds. They can also broadcast the wrong message just as quickly, and the consequences are rarely trivial. When people already feel uncertain—watching rain intensify, hearing rumors, wondering whether to move children or elders—information asymmetry and misinformation can amplify anxiety. If a platform issues an inaccurate warning because of processing errors, weak verification, or poor editorial control, the public may misread the seriousness of the situation. Weather alerts illustrate this problem well: if an app mistakenly labels an ordinary storm as the highest-level “red alert,” residents may rush to panic-buy supplies, flood roads trying to leave the city, or take other disorderly actions that strain logistics and public order. The deeper damage comes later. Each highly visible false alarm makes the next urgent warning harder to deliver. People start asking, implicitly or explicitly: is this real, or is it another system glitch?

Regional inequality makes all of this harder, because capability does not distribute itself evenly. Differences in economic development and resource allocation mean that western regions often lag behind eastern regions in both technology deployment and day-to-day operational capacity. In many

remote mountainous areas, monitoring networks and communications infrastructure remain patchy; alerts do not always travel the last few kilometers to every village, especially when weather, terrain, and weak connectivity combine. As a result, some communities only grasp what is happening once the hazard is already in motion—when the river has started to rise, when the slope has begun to slip, when the road is no longer passable. Hardware alone does not close that gap. Even where equipment exists, a shortage of trained technical staff can limit its usefulness. Without people who can operate systems confidently, troubleshoot failures under pressure, and maintain networks between disasters, “advanced” tools may sit idle or slowly deteriorate, and response efficiency suffers in exactly the places where time is hardest to buy. These disparities make it difficult to deliver equitable, reliable disaster management nationwide—and they lead to an uncomfortable but necessary question: if technology can improve safety, who benefits first, and who is still living just beyond the edge of the signal?

4. Discussion and conclusion

Natural-disaster emergency management sits closer to the foundations of social stability than most people realize—until something goes wrong. When warnings arrive late, agencies move side by side rather than as one team, or leaders operate without a believable sense of what might happen next, the system does not simply look inefficient. It leaves communities exposed. Traditional approaches still carry familiar weaknesses: information often reaches decision-makers after the situation has already changed; coordination can splinter under time pressure; and forecasting remains uneven, especially when hazards compound and a “bad day” turns into a chain reaction. This is where technology can genuinely help—not as a glossy upgrade, but as a practical way to narrow the gap between a fast-moving reality on the ground and the choices made in command rooms.

There is a reason this moment feels different from earlier waves of “digital transformation.” The core technologies—big data, cloud computing, the Internet of Things (IoT), and artificial intelligence—are no longer experimental side projects. They already operate at scale in systems that also demand speed, reliability, and continuity: e-commerce platforms that react instantly to user behavior, financial systems that process risk signals in real time, smart-home networks that coordinate devices, and industrial environments where sensors track equipment health around the clock. That maturity gives emergency management something it has often lacked: a set of tools that can function under heavy load, not just in demonstrations. Building on that base, this study lays out the main application scenarios of information technology in natural-disaster emergency management and distills three broad benefits that show up repeatedly in practice: faster response through improved information flow, more disciplined resource allocation through data-informed scheduling, and stronger public preparedness through communication that people can actually use. At the same time, the analysis stays honest about the trade-offs. Security and privacy risks remain stubbornly real. Dependence on digital infrastructure can become fragility during extreme events. Regional disparities in technology access and technical capacity still shape who benefits first—and who, in effect, is left waiting for the signal to arrive.

So the next stage is less about applauding technology and more about fitting it to the realities of disaster work. Reducing security and privacy exposure requires more than good intentions: stronger encryption, clear tiered permissions, and routine security audits need to remain in place even when the response tempo rises and shortcuts feel tempting. Avoiding a single point of failure requires similar discipline. Agencies can build redundancy into communications, place edge-computing nodes closer to the field, and select lower-cost, easier-to-maintain technologies where budgets are tight—because resilience often depends on what keeps working when the “ideal” system loses

power or connectivity. Regional imbalance, in other words, needs fixes that work on ordinary days—not slogans that sound good after a crisis. Cross-regional information-sharing arrangements can help agencies see the same picture at the same time. Unified data standards can prevent the familiar “format mismatch” problem where systems technically exist but cannot exchange usable information. Sustained technical training at the grassroots level matters just as much as hardware purchases, because a platform only becomes a capability when local teams can run it, troubleshoot it, and trust it under pressure. Taken together, these steps can narrow gaps in both equipment and everyday operational competence.

If the goal is to push the upside further, a few directions look especially promising. One is a genuinely integrated “sky–air–ground” monitoring network—satellites, drones, and ground sensors feeding into a single, coherent picture rather than a stack of disconnected dashboards. Another is tighter coupling of big data and AI within prediction models. The point is not to claim perfect foresight; it is to trim the avoidable uncertainty, the kind that comes from missing signals or slow synthesis. Cloud computing and IoT can also support dynamic resource-scheduling platforms that track supplies and personnel in real time and adjust deployments as conditions shift—because in disasters, plans rarely survive first contact unchanged. New media and smart devices, meanwhile, offer a practical route to a two-way emergency-education system: government can push clear guidance quickly, while also listening—collecting credible field reports and responding with advice that feels timely and specific rather than generic.

Even with all of that, technology will not build a modern emergency management system on its own. Institutions, protocols, incentives, and training do most of the heavy lifting. They decide whether tools become routine practice or remain “features” that look impressive but sit unused. Still, when technological innovation lines up with institutional refinement, the system can move faster, coordinate with fewer fractures, and serve more people more fairly. That pairing—real capability matched with real governance—offers a realistic path toward a more resilient, equitable, and effective approach to natural-disaster emergency management.

References

- [1] Wu, Y. F. (2021). An analysis of the dilemmas of the emergency management system and possible solutions. *Public Administration Review*, 15(3), 78–85.
- [2] Li, L. Y., & Li, W. (2025). Theoretical analysis of the institutional innovation in the new Emergency Response Law. *Daqing Social Sciences*, (3), 112–118.
- [3] Editorial Department of the Journal. (2025). Coordinating development and security to forge a new chapter of safety. *Safety and Health*, (3), 1.
- [4] Editorial Department. (2025). Uniting efforts and taking responsibility—Disaster reduction and relief 2024. *China Disaster Reduction*, (02), 12–13.
- [5] Huang, L. (2024). Research on the application of data-driven business models in geological disaster emergency management. In *Proceedings of the 10th National Geological Disaster Prevention Academic Forum* (pp. 128–135). Xi'an: Shaanxi Science and Technology Press.
- [6] Sun, Z. Q. (2022). Design of an earthquake disaster emergency response platform based on big data and artificial intelligence analysis (Master's thesis). Institute of Geology, China Earthquake Administration, Beijing.
- [7] Ying, S. N. (2023). Application of big data intelligent analysis technology in emergency management. *China Emergency Management Science*, (2), 45–52.