Bridging the Digital Divide: Examining the Challenges of E-Service Delivery and Their Impact on Inter-Agency Coordination in Emergency Management

A Research Paper on the Effects of Digital Public Service Delivery Challenges on Coordination in Emergency and Disaster Risk Management

Emenike Umesi, PhD, CEM

Faculty, African University of Science and Technology, Abuja, Nigeria

DOI: https://doi.org/10.68050/JAMS.2026.885

Received: 16 October 2026; Accepted: 22 October 2026; Published: 30 October 2026

ABSTRACT

Electronic service (e-service) delivery has become a central pillar of modern emergency management, promising faster early warning dissemination, more efficient resource mobilisation, and stronger collaboration among the many agencies that share responsibility for disaster response. Yet the very technologies designed to improve responsiveness frequently introduce new points of failure. This paper examines the challenges confronting effective e-service delivery in the emergency management sector and traces how these challenges undermine inter-agency and inter-organisational coordination during preparedness, response, and recovery operations. Using a qualitative secondary data analysis methodology, the study draws on peer-reviewed literature, government and inter-governmental reports, and case documentation from jurisdictions in North America, Europe, Asia, and sub-Saharan Africa, with particular attention to Nigeria's disaster risk management architecture. The analysis identifies seven interlocking categories of challenge: infrastructural deficits and the digital divide; interoperability failures between legacy and modern systems; cybersecurity vulnerabilities; inadequate digital literacy and workforce capacity; fragmented governance and policy frameworks; funding constraints; and trust or adoption barriers among both responders and citizens. The paper argues that these challenges do not operate in isolation but compound one another, producing cascading coordination failures of the kind documented in Hurricane Katrina, the 2013 Washington Navy Yard shooting, and pandemic-era emergency responses across low- and middle-income countries. The paper concludes with policy-oriented recommendations, including standardised data-exchange protocols, sustained investment in interoperable infrastructure, and deliberate capacity-building for emergency management personnel.

Keywords*:* e-service delivery, emergency management, coordination, Public service,

1. INTRODUCTION

Emergency management is, at its core, a coordination problem. A flood, an epidemic, an industrial accident, or an act of terrorism rarely respects institutional boundaries, yet the responsibility for managing such events is almost always distributed across multiple agencies, tiers of government, and sometimes national borders. Fire services, police, health authorities, meteorological agencies, the military, non-governmental organisations, and community volunteers must act in concert, often within minutes, to save lives and limit damage. Over the past two decades, governments and humanitarian organisations have turned to electronic service delivery, commonly referred to as e-service, as a means of tightening this coordination: early warning platforms, computer-aided dispatch, geographic information systems, mobile alerting, social media monitoring, and cloud-based information-sharing portals have all been positioned as tools for making emergency response faster, more transparent, and more efficient (West, 2004; Wu, 2014).

The promise of e-service in emergency management is well documented. Digitised platforms can shorten the time between hazard detection and public warning, allow decision-makers to visualise unfolding events in real

time, and give citizens direct channels through which to report needs or receive instructions. However, a growing body of evidence suggests that the transition to digital service delivery in this sector has been uneven and, in many jurisdictions, deeply troubled. Legacy communication systems that cannot interoperate with newer platforms, inconsistent internet and electricity infrastructure, cybersecurity exposure in systems that were never designed with security in mind, and wide gaps in digital literacy among both responders and the public have all been identified as recurring obstacles (U.S. Government Accountability Office [GAO], 2004; CISA, n.d.). When these obstacles surface during an actual emergency, the consequence is not merely inconvenience but a breakdown in the very coordination that e-service was meant to strengthen, as seen most starkly in the communications failures documented after Hurricane Katrina (U.S. House of Representatives, 2006).

This paper investigates that relationship directly: what are the principal challenges undermining effective e-service delivery in the emergency management sector, and how do these challenges translate into coordination failures among the agencies responsible for disaster preparedness, response, and recovery? The question is especially pressing for developing economies such as Nigeria, where disaster risk management institutions are simultaneously trying to modernise service delivery and contend with foundational infrastructural and digital-divide constraints (NEMA, 2018; Digital divide narratives in Sub-Saharan Africa more broadly).

The question is equally pressing globally, because the international policy architecture that governs disaster risk management, most notably the Sendai Framework for Disaster Risk Reduction 2015-2030, explicitly calls on states to invest in accessible, multi-hazard early warning and information systems as a core component of resilience-building, effectively making e-service capability a matter of global policy commitment rather than a purely domestic administrative choice. Understanding why this capability so often falls short in practice is therefore relevant to national emergency managers, regional bodies coordinating disaster response across borders, and the donors and development partners who fund digital modernisation programmes.

The significance of this inquiry is reinforced by the sheer diversity of actors that a modern emergency operation must bring together. A single flood event, for instance, may simultaneously require the coordinated involvement of a national meteorological agency issuing forecasts, a disaster management agency mobilising relief materials, a health ministry tracking waterborne disease risk, local government emergency committees managing evacuation, telecommunications operators keeping networks online, and international humanitarian organisations providing supplementary capacity. Each of these actors typically maintains its own information systems, its own reporting cadence, and its own institutional culture. E-service, in principle, is the connective tissue meant to bind these disparate systems into a single operating picture. This paper's central concern is what happens, operationally and organisationally, when that connective tissue is weak, inconsistent, or absent altogether.

The paper is structured as follows. Section 2 clarifies the key concepts of e-service and coordination as used in the emergency management literature. Section 3 outlines the theoretical framework guiding the analysis. Section 4 describes the secondary data analysis methodology. Section 5 presents the principal challenges to effective e-service delivery identified in the literature. Section 6 analyses the effects of these challenges on coordination. Section 7 discusses illustrative cases. Section 8 offers recommendations, and Section 9 concludes.

2. CONCEPTUAL CLARIFICATION

2.1 E-Service in Emergency Management

E-service, in the emergency management context, refers to the use of information and communication technology (ICT) to plan, deliver, and manage the functions of hazard mitigation, preparedness, response, and recovery. This spans a wide spectrum of applications: early warning and mass-notification systems built on standards such as the Common Alerting Protocol (CAP) (UNDRR, 2025); computer-aided dispatch (CAD) systems that route emergency calls to the nearest available resource (DHS Science and Technology Directorate, 2024); geographic information systems (GIS) used for hazard mapping and resource allocation

(ROK Technologies, 2024); social media platforms used for public communication and crowdsourced situational awareness (Lorini et al., 2021); and cloud-based portals that allow multiple agencies to share incident data. E-service quality in this domain is typically assessed along dimensions such as system reliability, information accuracy, responsiveness, ease of use, and security (Alalwan, 2018).

It is useful to distinguish between three functional layers of e-service in this sector, because the challenges documented later in this paper tend to cluster differently across each layer. The first is the sensing and detection layer, comprising the sensors, satellites, and monitoring networks that generate raw hazard data. The second is the processing and decision-support layer, comprising the analytic and mapping platforms, including GIS and, increasingly, artificial-intelligence-assisted forecasting tools, that convert raw data into actionable warnings and resource-allocation recommendations. The third is the dissemination and coordination layer, comprising the alerting systems, dispatch platforms, and inter-agency information-sharing portals through which decisions are communicated and enacted. A weakness at any one layer can undermine the value of investment in the other two; a highly accurate detection system, for example, delivers little coordination benefit if the dissemination layer cannot reach responders or the public in time (Besleaga, 2025; Intersec, 2025).

2.2 Coordination in Emergency Management

Coordination refers to the deliberate alignment of the actions, information, and resources of multiple actors toward a shared objective. In the emergency management literature, coordination is frequently discussed at three levels: intra-agency coordination among units of a single organisation; inter-agency coordination among distinct government bodies (for example, a fire service and a health ministry); and multi-sectoral coordination involving government, private-sector, and civil-society actors, including international humanitarian organisations. Effective coordination depends on shared situational awareness, compatible communication systems, clear command structures, and trust among the parties involved (Office of Justice Programs, n.d.). E-service delivery is, in principle, a coordination-enabling technology; when it functions poorly, however, it becomes a coordination liability rather than an asset.

3. THEORETICAL FRAMEWORK

This paper draws on two complementary theoretical strands. The first is the Technology Acceptance Model (TAM), originally developed by Davis (1989) and subsequently extended into the Unified Theory of Acceptance and Use of Technology (UTAUT). TAM holds that a technology's perceived usefulness and perceived ease of use jointly determine whether it will be adopted and used effectively by its intended operators. Applied to emergency management, TAM helps explain why e-service platforms that are technically sound but poorly matched to the working conditions of first responders, or that impose a steep learning curve, often see low or inconsistent uptake (Springer Nature, 2021; ResearchGate conceptual model of e-government acceptance).

The second theoretical strand is interoperability and network-coordination theory, which frames emergency response as a distributed system in which the overall performance of the network is constrained by its weakest or least compatible node. Under this view, coordination failure is not simply a matter of individual agency competence but an emergent property of how well systems, protocols, and data formats align across organisational boundaries (GAO, 2004; Office of Justice Programs, n.d.). Taken together, these two frameworks suggest that e-service challenges in emergency management operate on two levels simultaneously: a human-adoption level, where usefulness, usability, and trust determine whether responders and citizens actually use the tools provided; and a systems level, where technical incompatibility, infrastructure gaps, and security weaknesses determine whether the tools can function together at all. Both levels must be addressed for e-service to translate into effective coordination.

4. METHODOLOGY

This study adopts a qualitative secondary data analysis methodology. Rather than collecting new primary data

through surveys or interviews, the paper systematically reviews and synthesises existing secondary sources, including peer-reviewed journal articles, government and inter-governmental reports, official policy documents, and credible news and technical reporting published on the subject of e-government, e-service, and emergency or disaster management coordination. Secondary data analysis is well suited to a topic of this kind because the challenges of e-service delivery in emergency management have already been documented across a substantial and geographically diverse body of literature, spanning national audits (for example, U.S. congressional and Government Accountability Office reports), academic reviews of e-government adoption, and sector-specific studies of social media and cybersecurity in crisis response.

Sources were identified through targeted searches of academic databases, institutional repositories, and official government and inter-governmental websites, using search terms combining e-government, e-service, ICT, emergency management, disaster response, interoperability, and coordination. Sources were selected for relevance, credibility of the publishing body, and, where dated, continued relevance to current practice. A total of forty sources were retained for analysis and are listed in the References section. The material was then organised thematically using an inductive coding approach: recurring challenge categories were identified across sources and grouped into the seven themes presented in Section 5, after which their documented effects on coordination were extracted and synthesised in Section 6. This approach follows established practice in review-based emergency management scholarship, where thematic synthesis of secondary sources is used to build cumulative, cross-context understanding of persistent operational problems (Lorini et al., 2021; Social media applications and emergency management literature review, 2018).

As with any secondary data analysis, the study is subject to limitations. It cannot generate new primary evidence specific to any single jurisdiction, and it is dependent on the quality, currency, and framing of the sources reviewed. Where possible, the paper cross-references multiple sources addressing the same claim to reduce reliance on any single account, and it draws distinctions between findings that are broadly generalisable and those that are context-specific to a particular country or event.

5. CHALLENGES OF E-SERVICE DELIVERY IN THE EMERGENCY MANAGEMENT SECTOR

The literature reviewed for this study converges on seven recurring, mutually reinforcing categories of challenge. Each is discussed below.

5.1 Infrastructural Deficits and the Digital Divide

The most foundational challenge is unequal access to the infrastructure that e-service depends on: reliable electricity, broadband connectivity, and end-user devices. In low- and middle-income countries in particular, large sections of the population, and even some government field offices, lack consistent internet access, which limits both the reach of digital early warning systems and the ability of local responders to feed real-time data upward to national coordination centres. In Nigeria, factors such as inadequate electrical infrastructure, uneven education levels, and urban-rural disparities have been identified as key drivers of a persistent digital divide that constrains e-government and, by extension, e-service uptake in disaster-prone regions (digital divide literature on Nigeria). More broadly, the Asia-Pacific region, despite considerable investment, remains one of the most digitally divided in the world, illustrating that this is not solely a low-income-country problem but a structural challenge tied to geography, affordability, and infrastructure investment cycles (UN ESCAP, n.d.).

The digital divide is not only a matter of whether connectivity exists, but of how reliable and affordable it is where it does exist. Intermittent power supply degrades server uptime for the data centres and command posts that host emergency information systems, while the cost of mobile data can place continuous access out of reach for the very communities most vulnerable to disaster. These constraints mean that e-service architectures designed with high-bandwidth, high-reliability assumptions, often modelled on systems built for well-resourced urban centres, can perform poorly or fail outright when extended to the peri-urban and rural areas where a large share of disaster risk in Sub-Saharan Africa is concentrated. This mismatch between system design assumptions and operating environment is a recurring theme across the developing-country e-

government literature and helps explain why technology transfer alone, without parallel infrastructure investment, rarely closes the coordination gap (developing-country e-government literature review, 2017).

5.2 Interoperability Failures Between Systems and Agencies

Even where infrastructure exists, emergency management agencies frequently operate incompatible systems that cannot exchange data or voice communication with one another. The U.S. Government Accountability Office identified incompatible communication systems as directly impeding intergovernmental coordination efforts among first responders, a problem serious enough to warrant a dedicated federal leadership role (GAO, 2004). More recent assessments note that computer-aided dispatch systems used by neighbouring public safety agencies often cannot efficiently share information because each agency has adopted a different vendor platform, producing what one Department of Homeland Security review described as a situation in which responders 'cannot talk to some parts of their own agencies, let alone communicate with agencies in neighbouring cities, counties, or states' (DHS Science and Technology Directorate, 2024). This is compounded by fragmented information systems that operate on disparate servers, restricting effective data sharing even where a technical will to cooperate exists (communication inefficiencies in disaster response literature, 2025).

Interoperability failures are frequently procurement-driven rather than purely technical. Agencies tend to acquire dispatch, records-management, and alerting systems independently, on their own budget cycles, from vendors offering proprietary data formats and closed application programming interfaces. Absent a mandated common standard at the point of procurement, each new system purchase adds another silo rather than closing an existing one, so that the total number of incompatible platforms in a jurisdiction can actually grow even as individual agencies modernise. Pilot programmes such as the CAD-to-CAD interoperability initiative tested across New Hampshire and Vermont demonstrate that a single shared standard can allow previously siloed dispatch systems to exchange information, but such pilots remain the exception rather than the default mode of public safety procurement (DHS Science and Technology Directorate, 2024).

5.3 Cybersecurity Vulnerabilities

As emergency services digitise, they inherit the cybersecurity exposure of the systems they rely on. Much of the underlying infrastructure, including industrial control and supervisory control and data acquisition (SCADA) systems that govern utilities and, increasingly, autonomous emergency vehicles, was originally designed decades ago with little consideration for cybersecurity, and the interconnection of these systems with modern IT networks has expanded the attack surface considerably (IEEE Public Safety Technology Initiative, n.d.). The emergency services sector has been explicitly flagged as an increasingly likely target for cyberattacks precisely because it is becoming more interconnected and IT-dependent; disruption of core services such as 911 call-taking systems could delay response to genuine emergencies and directly threaten life and property (CISA, n.d.; Hacking 9-1-1 study, n.d.). Analyses of broader critical-infrastructure cyber risk point to insider threats, unpatched legacy systems, and unsecured access points as persistent vulnerabilities that emergency management systems, often built on or adjacent to this infrastructure, inherit by association (Pelco, 2026).

The consequences of these vulnerabilities are not hypothetical. Ransomware and denial-of-service incidents have already disrupted emergency communications and utility operations in multiple jurisdictions, and audits of defence and public-safety infrastructure continue to find only minimal progress in remediating known vulnerabilities even after they have been publicly flagged (Federal News Network, 2026). Because emergency management systems are, by design, meant to be highly available during precisely the moments when malicious actors, whether financially motivated criminal groups or state-linked actors, have the greatest incentive to cause disruption, the sector faces a structurally difficult security problem: the assets most valuable to protect are also the assets under the most acute pressure to remain accessible and interoperable, which can work against the more restrictive access controls that good cybersecurity practice would otherwise recommend.

5.4 Inadequate Digital Literacy and Workforce Capacity

Technology adoption research consistently shows that perceived ease of use and self-efficacy are decisive factors in whether public-sector personnel actually use the digital tools made available to them (Davis, 1989; Springer Nature, 2021). In emergency management, this translates into a persistent capacity gap: agencies may be small, under-staffed, and without dedicated technical personnel, meaning that producing high-quality digital content or operating sophisticated platforms competes directly with limited staff time during both routine operations and active crises (CNA, 2023). Surveys of e-government adoption in developing-country contexts similarly find that digital literacy gaps, interface usability issues, and general unfamiliarity with digital platforms remain significant barriers to sustained use, even where the underlying technology is sound (Indonesian e-government adoption study, 2025).

This capacity gap is compounded by high staff turnover in many emergency management agencies, which resets institutional knowledge of digital systems just as personnel begin to reach proficiency with them. Where training budgets are treated as discretionary rather than core operating expenditure, refresher training lapses first, leaving agencies with a workforce whose digital skills are unevenly distributed and whose confidence in using unfamiliar platforms during a live incident, as opposed to a training exercise, cannot be assumed. The TAM literature suggests this has a compounding effect on adoption: low self-efficacy not only slows initial uptake but also increases the likelihood that responders will revert to familiar analogue workarounds, such as manual radio relays or paper logs, at the exact moments when digital coordination tools are needed most (Springer Nature, 2021).

5.5 Fragmented Governance and Policy Frameworks

E-service challenges are not purely technical; they are frequently rooted in governance. Scholars analysing e-governance implementation in developing countries have argued that the barriers to effective digital public service are split between technical and non-technical, or sociotechnical, factors, with the non-technical share, encompassing leadership, organisational culture, and inter-agency politics, often estimated to be the larger of the two (developing-country e-governance literature). In the emergency management sector specifically, the absence of a single agency with clear authority over interoperability standards has repeatedly been identified as an obstacle; in the United States, this gap led directly to the creation of a dedicated Office of Emergency Communications after the failures of Hurricane Katrina (U.S. House of Representatives, 2006). In Nigeria, statutory reviews of the National Emergency Management Agency Act have similarly called for strengthened legal and institutional frameworks to ensure more effective coordination of disaster risk management functions across federal, state, and local levels (NEMA Act appraisal, 2018).

5.6 Funding Constraints

Digital transformation requires sustained capital and recurrent investment, and emergency management agencies, particularly at sub-national levels, are frequently among the more poorly resourced arms of government. Nigeria's own disaster risk management authorities have publicly acknowledged the need to shift from reactive, ad-hoc disaster funding toward a multi-stakeholder financing architecture that supports prevention, preparedness, and the systems, digital and otherwise, that underpin them (NEMA, 2025, cited in Voice of Nigeria, 2026). Where funding is unpredictable, agencies are less able to maintain, upgrade, or secure the digital platforms they already have, let alone invest in interoperable replacements for legacy systems.

5.7 Trust, Adoption, and Information Quality Barriers

Finally, even technically functional e-service platforms can fail to improve coordination if responders or the public do not trust the information they carry. Studies of social media use in emergency management describe a persistent challenge in verifying and integrating citizen-generated content with official data, given ongoing concerns about credibility, misinformation, and the risk of rumour propagation during fast-moving events (Lovari & Bowen, 2020; Social Networks in Crisis Management review, 2023). Research on e-government adoption more broadly finds that trust and perceived security are among the strongest predictors of citizens' willingness to use digital public services at all, meaning that a single high-profile data breach or service failure

can suppress adoption well beyond the specific system affected (conceptual model of e-government acceptance).

6. EFFECTS OF E-SERVICE CHALLENGES ON COORDINATION

The seven challenges identified above do not remain confined to the technical domain; they translate directly into measurable coordination failures across the phases of emergency management.

6.1 Delayed and Degraded Situational Awareness

When systems cannot interoperate, or when infrastructure gaps prevent data from reaching decision-makers, the shared, real-time picture of an unfolding event that effective coordination depends on is delayed or incomplete. Analysts of recent disaster responses point to complex, fragmented information systems and interoperability gaps as leading causes of poor situational awareness, which in turn produces suboptimal, delayed decision-making at exactly the moments when speed matters most (communication inefficiencies in disaster response literature, 2025).

6.2 Command and Control Breakdown

The clearest documented illustration of this effect is the response to Hurricane Katrina in 2005, where a bipartisan congressional investigation found a complete breakdown in communications that paralysed command and control and left situational awareness murky at best; agencies simply could not communicate with one another because of equipment failure and a lack of system interoperability (U.S. House of Representatives, 2006, as summarised in ASIS International, 2016). A similar pattern recurred in the response to the 2013 Washington Navy Yard shooting, where investigators found that responders lacked interoperable communication with other agencies due to a poor understanding of equipment capabilities and improperly configured radios, prompting renewed congressional concern that interoperable communications continue to be a challenge during disaster response (ASIS International, 2016).

6.3 Duplication, Gaps, and Misallocation of Resources

Where agencies cannot see one another's data or activity, resources are prone to duplication in some areas and neglect in others. Fragmented reporting structures and privacy-driven restrictions on data access have been shown to prevent agencies from accessing the information they need for effective disaster response, unilateral or top-down approaches then compound the problem by overlooking the ground-level expertise of local responders (communication inefficiencies in disaster response literature, 2025). The result is a coordination structure that looks unified on paper but functions, in practice, as a set of parallel and only loosely connected operations.

6.4 Public Trust and Compliance Effects

Coordination extends beyond government agencies to the public whose cooperation, whether through evacuation, self-reporting, or compliance with instructions, is essential to effective response. When digital communication channels are inconsistent, slow to update, or seen as untrustworthy, public compliance with official guidance weakens, and citizens increasingly turn to informal or unofficial channels for information, further fragmenting the overall information ecosystem during a crisis (Stolero, 2024; Lovari & Bowen, 2020). This dynamic was visible during the COVID-19 pandemic, when the rapid, sometimes improvised digitisation of public health communication produced both notable successes and documented gaps in reach, particularly among under-resourced or low-connectivity communities (Ndejjo et al., 2023).

6.5 Compounding Effects in Cross-Border and Multi-Agency Operations

The compounding nature of these challenges is most visible in complex, multi-agency operations that draw in international humanitarian actors alongside domestic agencies. Studies of the 2010 Haiti earthquake response found limited evidence of direct digital coordination between international medical response teams, even

though many organisations were active on the same platforms; instead, responders often broadcast information into a shared channel with little confirmation that it reached, or was acted on by, the parties who needed it, a pattern researchers have termed 'beaconing behaviour' rather than true coordination (social media and emergency management chapter, n.d.). This illustrates that the mere presence of a shared digital platform does not guarantee coordination; without common protocols, trust, and verification mechanisms, digital tools can create an illusion of connectivity while genuine coordination remains elusive.

6.6 Slower and Less Equitable Recovery

The coordination costs of weak e-service delivery persist well beyond the acute response phase and into recovery, when agencies must track needs assessments, disburse relief and compensation, and monitor reconstruction across potentially thousands of affected households. Where digital case-management and beneficiary-tracking systems are absent, fragmented, or trusted unevenly by the population, recovery coordination tends to revert to manual, paper-based processes that are slower, harder to audit, and more susceptible to duplication or exclusion errors, particularly for displaced or hard-to-reach populations who lack documentation or connectivity. This has direct equity implications: communities with the least digital infrastructure before a disaster are frequently the same communities that face the greatest coordination friction in accessing recovery support afterward, reproducing pre-existing inequality through the recovery process itself (Ndejjo et al., 2023; private sector engagement in COVID-19 response literature, 2022).

7. ILLUSTRATIVE CASES

7.1 Hurricane Katrina and Post-Katrina Reform (United States)

The 2005 Hurricane Katrina response remains the most-cited case of e-service and interoperability failure in the emergency management literature. The breakdown in inter-agency communications documented by the congressional investigation directly led to the establishment of the Office of Emergency Communications under the Post-Katrina Emergency Management Reform Act, and to the first National Emergency Communications Plan in 2008, which set out goals for improving interoperable communications capability at state and local levels (ASIS International, 2016). Nearly two decades later, however, similar interoperability complaints resurfaced following Hurricane Sandy and the Navy Yard shooting, underscoring that technical and policy fixes introduced after one crisis do not automatically resolve the underlying coordination challenge across all future events.

7.2 Nigeria's Disaster Risk Management Architecture

Nigeria offers an instructive case of a country actively working to modernise its emergency management coordination while still addressing foundational infrastructural and institutional gaps. The National Emergency Management Agency (NEMA) has expanded its offices for quicker state and community-level intervention and established national and sub-national disaster risk reduction platforms intended to improve coordination across government levels (NEMA official statement, 2024). The country's newly developed National Strategy for Disaster Risk Reduction (2025-2030), produced with the Office of the Vice President, NEMA, and international partners, explicitly aligns with the Sendai Framework and is designed to strengthen resilience through a more coordinated, cross-sectoral approach (UNDP, 2025). At the same time, Nigerian officials have publicly acknowledged that traditional, largely reactive emergency response systems are being tested by the increasing frequency of disasters, and that funding architecture must shift toward sustained, preventive investment, an implicit recognition that the digital and institutional backbone of coordination remains a work in progress (Voice of Nigeria, 2026).

7.3 COVID-19 as a Global Stress Test

The COVID-19 pandemic functioned as an unplanned, simultaneous stress test of e-service capacity across nearly every government in the world. Research on Uganda's pandemic response found that digital technology was used extensively for testing, contact tracing, surveillance, and risk communication, but that significant barriers, including connectivity gaps and limited digital literacy among health workers, constrained its

effectiveness in a low-resource setting (Ndejjo et al., 2023). More broadly, comparative research on public-sector digital transformation during the pandemic found that many organisations were forced to compress years of planned digital change into weeks, a pace that produced both valuable innovation and, in many cases, coordination strain between newly digitised functions and the legacy processes they were meant to replace (Moser-Plautz & Schmidthuber, 2023).

7.4 Cybersecurity Exposure in Emergency Call Systems

A fourth illustrative thread concerns the cybersecurity of the emergency call-taking systems that sit at the very front end of coordination. Technical analyses of 9-1-1 call infrastructure in the United States describe a chain of interconnected, IT-dependent components, from Automatic Number Identification at the telecommunications carrier level through to the dispatch centre, any one of which could be disrupted by a cyberattack targeting either data or physical infrastructure, with a resulting risk of delayed emergency response and compromised patient care (Hacking 9-1-1 study, n.d.). Because this system sits upstream of every other coordination function, a disruption at this single point can cascade through an entire jurisdiction's emergency response chain, underscoring why the Cybersecurity and Infrastructure Security Agency treats the emergency services sector as one of its designated critical infrastructure sectors requiring dedicated cyber-risk coordination (CISA, n.d.).

8. RECOMMENDATIONS

Drawing on the challenges and effects identified above, the paper offers the following recommendations for policymakers, emergency management agencies, and development partners.

8.1 Standardise Data and Alerting Protocols

Agencies should adopt and enforce common data and alerting standards, such as the Common Alerting Protocol, across all organisations involved in emergency response, so that systems from different vendors and jurisdictions can exchange information without manual translation. Adoption of CAP is deliberately low-cost and open-source, which removes the affordability objection often raised against standardisation in resource-constrained settings, and free tooling such as the CAP Editor already supports alerting authorities across more than two hundred countries (UNDRR, 2025). The priority for many jurisdictions, including Nigeria, is not building new standards from scratch but committing to consistent use of the standards that already exist.

8.2 Create a Dedicated Interoperability Authority

Governments should establish a dedicated, adequately resourced coordinating authority for emergency communications interoperability, along the lines of the United States Office of Emergency Communications, with the mandate to set standards, fund upgrades, and conduct joint training exercises across agencies. The Katrina experience demonstrates that interoperability rarely improves on its own through individual agency initiative; it requires a body with the explicit cross-government authority and recurring budget line to hold agencies accountable to shared standards over time (GAO, 2004).

8.3 Close the Underlying Infrastructure Gap

Sustained investment in foundational infrastructure, including reliable electricity and affordable broadband connectivity in disaster-prone and rural areas, must accompany any software or platform investment, since no e-service platform can outperform the infrastructure it runs on. This is properly understood as a disaster risk management investment in its own right, not merely a telecommunications-sector concern, given how directly it determines whether early warnings and coordination instructions actually reach the people and responders who need them (UN ESCAP, n.d.).

8.4 Institutionalise Cybersecurity as a Core Competency

Emergency management agencies should treat cybersecurity as a core operational competency rather than a

peripheral information-technology concern, with regular vulnerability assessments of dispatch, alerting, and data-sharing systems, and clear incident-response protocols that assume a cyber disruption could occur simultaneously with a physical emergency. This includes basic hygiene measures such as consistent patch management, which remains one of the most commonly cited and most preventable gaps in critical-infrastructure security (CISA, n.d.; Pelco, 2026).

8.5 Invest in Continuous Digital Capacity-Building

Agencies should build sustained digital literacy and capacity-building programmes for emergency management personnel, moving beyond one-off training sessions toward continuous, scenario-based practice with the tools responders are expected to use under pressure. Embedding digital-tool proficiency into routine simulation exercises, rather than treating it as a separate IT training track, helps ensure that skills are retained and that responders default to digital coordination channels rather than reverting to informal workarounds during real incidents (CNA, 2023).

8.6 Formalise the Integration of Citizen-Generated Data

Agencies should formalise protocols for integrating citizen-generated and social media data with official information systems, including clear verification workflows, to capture the benefits of crowdsourced situational awareness without amplifying misinformation. This requires dedicated staff time and tooling for triage rather than an assumption that social media monitoring can simply be absorbed into existing communications roles (Lorini et al., 2021).

8.7 Shift Toward Predictable, Preventive Financing

Finally, governments should shift disaster risk management financing toward predictable, multi-year investment in preventive and digital infrastructure rather than ad hoc, post-disaster funding cycles, a transition that Nigerian authorities have themselves publicly identified as necessary. Predictable financing allows agencies to plan multi-year system upgrades and staff training rather than making reactive purchases in the aftermath of the disaster those purchases were meant to help prevent (Voice of Nigeria, 2026).

9. CONCLUSION

E-service delivery holds genuine potential to transform emergency management, offering faster warnings, richer situational awareness, and more efficient use of scarce resources. But this paper's synthesis of the secondary literature shows that the potential is consistently constrained by a recognisable set of challenges: infrastructural and digital divides, interoperability failures, cybersecurity exposure, capacity gaps, fragmented governance, funding shortfalls, and trust deficits. These challenges rarely act alone; they compound one another, and their combined effect is a measurable erosion of the very coordination that e-service investments are meant to strengthen, a pattern visible from Hurricane Katrina to the COVID-19 pandemic to Nigeria's ongoing disaster risk management reforms. Addressing this requires treating e-service not as a discrete technology procurement exercise but as an integrated coordination system, one that demands common standards, sustained infrastructure investment, workforce capacity, and institutional authority in equal measure. Without this integrated approach, digital transformation in the emergency management sector risks reproducing, in electronic form, the very fragmentation it was introduced to solve.

REFERENCES

1. ASIS International. (2016). A failure to communicate. Security Management Magazine. https://www.asisonline.org/security-management-magazine/articles/2016/07/a-failure-to-communicate/
2. Besleaga (Nicolae), A. (2025). Emerging IT technologies for multi-hazard early warning systems. Medium – Predict.
3. CNA Corporation. (2023). Best practices in social media crisis communications for emergency management agencies.

4. Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). Emergency Services Sector. U.S. Department of Homeland Security. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/emergency-services-sector
5. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
6. Design characteristics and service experience with e-government services: A public value perspective. (2024). Government Information Quarterly.
7. Digital divide in Nigeria: Education, infrastructure, and policy responses. (2025). Overview compiled from FAO gender-responsive digitalisation reporting and Nigerian ICT policy sources.
8. Elevating e-government: Unleashing the power of AI and IoT for enhanced public services. (2024). PMC.
9. Exploring communication inefficiencies in disaster response: Perspectives of emergency managers and health professionals. (2025). International Journal of Disaster Risk Reduction. ScienceDirect.
10. Exploring intention to use e-government: The role of technology acceptance model with self-efficacy and system quality. (2021). Springer Nature.
11. Federal News Network. (2026). CISA tells critical organizations to prepare for cyber outages.
12. Homeland Security: Challenges and successes of e-government development in developing countries: A theoretical review of the literature. (2020). ResearchGate.
13. IBM. (2026). What is critical infrastructure? IBM Think.
14. IEEE Public Safety Technology Initiative. (n.d.). Cybersecurity of critical infrastructure with ICS/SCADA systems.
15. Intersec. (2025). Early warning system in disaster management.
16. Issues and challenges of implementing e-governance in developing countries. (2024). Cogent Social Sciences.
17. Lorini, V., Castillo, C., Peterson, S., Rufolo, P., Purohit, H., Pajarito, D., de Albuquerque, J. P., & Buntain, C. (2021). Social media for emergency management: Opportunities and challenges at the intersection of research and practice. Proceedings of the 18th International Conference on Information Systems for Crisis Response and Management (ISCRAM), 772–777.
18. Lovari, A., & Bowen, S. A. (2020). Social media in disaster communication: A case study of strategies, barriers, and ethical implications. Journal of Public Affairs, 20(1), e1967.
19. Ludwig, T., Reuter, C., Siebigteroth, T., & Pipek, V. (2015). CrowdMonitor: Mobile crowd sensing for assessing physical and digital activities of citizens during emergencies. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15).
20. Managing natural disasters: An analysis of technological advancements, opportunities, and challenges. (2023). ScienceDirect.
21. Moser-Plautz, B., & Schmidthuber, L. (2023). Digital government transformation as an organizational response to the COVID-19 pandemic. ScienceDirect.
22. National Emergency Management Agency (NEMA), Nigeria. (2018). National Disaster Risk Management Policy.
23. National Emergency Management Agency (NEMA), Nigeria. (2024). Nigeria official statement submitted at the Ninth Africa Regional Platform for Disaster Risk Reduction, Windhoek, Namibia.
24. National Emergency Management Agency (NEMA), Nigeria. (2025–2026). Official website news releases. https://nema.gov.ng/
25. Ndejjo, R., Kabwama, S. N., Namale, A., Tusubira, A. K., Wanyana, I., Kizito, S., Kiwanuka, S. N., & Wanyenze, R. K. (2023). Harnessing digital technology for COVID-19 response in Uganda: Lessons and implications for future public health emergencies. BMJ Global Health, 8, e013288.
26. Office of Justice Programs, U.S. Department of Justice. (n.d.). Disaster response: Interoperability and coordination.
27. Organizational disaster communication ecology: Examining interagency coordination on social media during the onset of the COVID-19 pandemic. (2021). PMC.
28. Pelco. (2026). Cyber attacks on critical infrastructure: Guide and risks.
29. Private sector engagement in the COVID-19 response: Experiences and lessons from the Democratic Republic of Congo, Nigeria, Senegal and Uganda. (2022). PMC.

30. Sarcevic, A., Palen, L., White, J., Starbird, K., Bagdouri, M., & Anderson, K. (2012). Beacons of hope in decentralized coordination: Learning from on-the-ground medical twitterers during the 2010 Haiti earthquake. Proceedings of the ACM Conference on Computer Supported Cooperative Work.
31. Social media applications and emergency management: A literature review and research agenda. (2018). International Journal of Disaster Risk Reduction. ScienceDirect.
32. Social media use in emergency management. (2015). Journal of Emergency Management.
33. Social Networks in Crisis Management: A literature review to address the criticality of the challenge. (2023). MDPI.
34. Solutions for sustainable and resilient communication infrastructure in disaster relief and management scenarios. (2024). arXiv.
35. Stolero, N. (2024). Using social media in disaster management: The perceptions of emergency responders versus the public. Risk, Hazards & Crisis in Public Policy.
36. The disaster risks and management policies and practices in Nigeria: A critical appraisal of the National Emergency Management Agency Act. (2018). International Journal of Disaster Risk Reduction. ScienceDirect.
37. The effects of website quality on adoption of e-government service: An empirical study applying UTAUT model using SEM. (2012). arXiv.
38. The role of artificial intelligence for early warning systems: Status, applicability, guardrails, and ways forward. (2025). ScienceDirect.
39. The role of e-government in disaster management: A review of the literature. (2023). Academia.edu.
40. U.S. Department of Homeland Security, Science and Technology Directorate. (2024). Interoperability is key to effective emergency communications.
41. U.S. Government Accountability Office. (2004). Homeland security: Challenges in achieving interoperable communications for first responders (GAO-04-231T).
42. U.S. House of Representatives, Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. (2006). A failure of initiative: Final report.
43. United Nations Development Programme (UNDP). (2025). National Strategy for Disaster Risk Reduction (2025–2030), Nigeria.
44. United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). (n.d.). ICT and disaster risk reduction.
45. United Nations Office for Disaster Risk Reduction (UNDRR). (2025). The Common Alerting Protocol.
46. Voice of Nigeria. (2026). Nigeria moves to mainstream disaster risk reduction.
47. West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. Public Administration Review, 64(1), 15–27.
48. Wu, Y. (2014). Protecting personal data in e-government: A cross-country study. Government Information Quarterly, 31(1), 150–159.
49. Xiao, J., Zhang, H., & Xu, X. (2014). Diffusion of e-government: A literature review and directions for future research.