PLANNING FOR SATELLITE-SERVICE DISRUPTION: A MANAGEMENT AND POLICY ANALYSIS OF THE SENDAI FRAMEWORK FOR CRITICAL INFRASTRUCTURE RESILIENCE

Aulia Malik Affif
Alan March
Yulesta Putra

Satellite systems now underpin navigation, timing, communications, emergency response, and other critical services, yet governance frameworks for service disruption remain underdeveloped. This article examines the Sendai Framework for Disaster Risk Reduction 2015–2030 (SFDRR) as a management and planning instrument for large-scale satellite-service disruption. Using a structured qualitative documentary analysis, the paper reads the SFDRR through a transparent three-stage protocol and interprets it alongside contemporary scholarship on satellite security, disaster recovery, and critical infrastructure resilience. The analysis identifies a bounded but consequential asymmetry. The framework contains planning-relevant guidance on local preparedness, stakeholder coordination, technical and scientific capacity, public awareness, and international cooperation, all of which can support continuity planning and recovery. At the same time, its treatment of satellite risk remains indirect. The SFDRR contains no direct reference to satellites; explicit space-related terminology appears only four times, and the terms digital *and* cyber *do not appear. Cross-checking the framework against contemporary disruption pathways shows that this omission materially limits its usefulness for managing global, politically contested, and technologically complex outages affecting multiple sectors simultaneously. In response, the article develops a management-oriented interpretation of the framework, clarifies the boundary conditions of that interpretation, and sets out practical planning priorities for risk mapping, redundancy design, cross-sector role allocation, and cross-border coordination. The study positions satellite disruption as a contemporary management and planning problem as much as a technical or security challenge.*

https://doi.org/10.66033/jmpr2025-215

INTRODUCTION

Satellite systems are no longer peripheral technical assets. They support positioning, navigation, and timing services, enable communications in remote environments, contribute to emergency response, and sustain operational continuity across transportation, finance, energy, and public administration [20, 6]. As dependence has deepened, the consequences of disruption have become more severe and more managerial. A significant outage would not only be an engineering failure; it would be a planning crisis involving cascading interdependencies, degraded service delivery, role ambiguity across institutions, and time-critical decisions about continuity, prioritization, and recovery.

This problem is increasingly salient because satellite systems are exposed to a broad threat landscape. Physical risks include orbital collision, debris generation, and extreme space weather, while digital risks include cyberattacks against ground stations, signals, and connected services [9, 21, 7]. The possible effects are transboundary. A disruption in space can generate immediate consequences on the ground, affecting users who may have no visibility into the infrastructure on which they rely.

The Sendai Framework for Disaster Risk Reduction 2015–2030 (SFDRR) is one of the most influential international frameworks for organizing disaster risk reduction and recovery. Its broad, multi-hazard orientation makes it potentially relevant to technologically mediated disruption, even though it was not written specifically for satellite systems [24, 12]. The central question for management and planning research is therefore not whether satellite security is a technical issue alone, but whether an established disaster-governance framework can be used to structure planning, coordination, and recovery for a digitally driven infrastructure shock.

This article addresses that question through a focused documentary analysis of the SFDRR and the recent literature on satellite disruption. The paper makes three contributions. First, it identifies the specific portions of the SFDRR that are directly relevant to planning for satellite-service disruption. Second, it applies a transparent interpretive test to clarify the framework's principal omissions from a management perspective, particularly in relation to global coordination, digital risk, intentional disruption, and supply-chain dependence. Third, it translates these findings into a set of concrete planning implications suitable for governments, infrastructure operators, and cross-sector decision makers.

The article is framed explicitly for management and planning scholarship. Rather than treating satellite disruption only as a technical-security problem, it examines how responsibilities are allocated, how continuity can be organized, how risk can be communicated, and how institutions can plan for a high-impact systems failure. Its distinctive contribution is to connect a high-level disaster-governance framework to concrete questions of governance capacity, decision architecture, and operational preparedness—core concerns within management and planning research.

SATELLITE DEPENDENCE AND THE PLANNING PROBLEM

Satellite infrastructure has become integral to contemporary social and economic systems. Earth-observation satellites support hazard detection and situational awareness, while global navigation satellite systems (GNSS) provide positioning, navigation, and timing for aviation, emergency services, logistics, finance, and energy systems [26, 20]. Satellite broadband has also become increasingly important for remote and hard-to-serve locations.

The planning challenge lies in the fact that this infrastructure is deeply embedded yet unevenly

visible. Service users typically interact with downstream applications rather than with the satellite systems themselves. As a result, institutional dependence can grow faster than public awareness or contingency preparation. This creates a management gap: organizations may treat satellite-enabled services as routine until an outage exposes the absence of robust fallback plans.

The risks are not hypothetical. Orbital collisions can create escalating debris, as described in the classic Kessler syndrome scenario [13, 14]. The 2009 collision between Iridium 33 and Cosmos 2251 generated more than 1,500 debris fragments, illustrating how a single event can threaten wider space infrastructure [8]. Extreme space weather is another major concern. Carrington-type events, though infrequent, can damage space-based systems and produce severe downstream effects [9]. Operational avoidance maneuvers are already a routine part of managing orbital risk; between 2020 and 2022, the International Space Station carried out seven collision-avoidance maneuvers [16].

Digital threats are similarly important. Satellite systems can be compromised through attacks on the ground segment, link segment, and user-facing systems, not only through direct physical interference in orbit [21, 7]. The 2007 cyberattacks against Estonia demonstrated how prolonged digital disruption can affect government, banking, policing, and communications over an extended period [18]. More recently, disruption affecting Viasat's KA-SAT network in 2022 showed how satellite-linked attacks can affect both military communications and civilian Internet access across Europe [5]. These cases reinforce a basic planning insight: the consequences of satellite disruption are managerial and societal as much as technical.

ANALYTICAL APPROACH

This study uses a structured qualitative documentary analysis designed to make the interpretive steps explicit. The primary document is the *Sendai Framework for Disaster Risk Reduction 2015–2030* [24]. The analysis is complemented by published scholarship on disaster resilience, satellite security, critical infrastructure interdependence, and operational continuity, with the supporting corpus limited to sources that speak directly to governance, coordination, or continuity planning rather than narrow engineering performance alone [19, 22, 8]. The purpose is not to test a statistical hypothesis, but to evaluate with methodological discipline how well the SFDRR functions as a planning framework for a modern satellite-service disruption scenario.

The analytical procedure proceeds in three stages. First, the framework is reviewed for explicit space-related terminology and directly relevant provisions through close reading and targeted term tracing. Second, broader planning-relevant themes are coded into five operational categories—local preparedness, vulnerability mapping, stakeholder coordination, knowledge development, and international cooperation—so that the analysis rests on repeated textual patterns rather than isolated passages. Third, the paper evaluates the management implications of the framework's omissions by comparing those coded themes against disruption mechanisms emphasized in the supporting literature, especially where continuity planning would require clearer treatment of digital disruption, political intent, and supply-chain dependencies.

This approach is appropriate for the present topic because the core issue is one of governance design. The analysis does not claim causal inference or incident forecasting; instead, it evaluates policy fit by asking whether the language, priorities, and implementation logic of the SFDRR can plausibly guide planning decisions before, during, and after a severe interruption of satellite-enabled services. To reduce interpretive overreach, conclusions are retained only where the framework text and the secondary literature point in the same direction.

FINDINGS

Direct Space-Related References in the SFDRR

The first finding is a bounded textual result with important planning consequences: the SFDRR does not refer directly to satellites. Across the document, explicit space-related references appear only four times, and all four instances are indirect rather than infrastructure-specific [8, 24]. Those references are summarized in Table 1.

Table 1: Explicit space-related references in the SFDRR relevant to disaster planning

Term or phrase	Planning relevance in the framework	SFDRR location
Space	Encourages real-time access to reliable data through the use of space and in situ information, including geographic information systems.	National and local levels (Point 24)
Geospatial information technology	Supports the development, updating, and dissemination of location-based disaster-risk information and risk maps for decision makers and exposed communities.	National and local levels (Point 24)
Geospatial and space-based technologies	Promotes international cooperation, technology transfer, and the sharing of non-sensitive communications, geospatial, and space-based technologies and related services.	Global and regional levels (Point 25)
Geospatial information technology	Encourages dissemination of risk information using geospatial information technology.	Global and regional levels (Point 25)

The framework contains no direct mention of satellites. The four entries above represent the principal explicit space-related terms identified in the documentary analysis [8, 24].

From a management standpoint, this is a thin but still usable foundation. These provisions show that the SFDRR already recognizes the value of geospatial data, information dissemination, and international technological cooperation. However, it consistently treats space primarily as a source of information for responding to terrestrial disasters, not as an infrastructure domain whose disruption may itself generate a multi-sector emergency.

Planning-Relevant Strengths of the Framework

Despite its indirect treatment of satellite systems, the SFDRR contains several elements that remain immediately useful for planning and management when read through a critical-infrastructure lens.

First, the framework's local-to-global logic is highly relevant. Satellite disruption would rarely be experienced uniformly. Communities differ in their level and form of dependence, whether through GNSS-enabled transport, satellite broadband, or infrastructure synchronization. This makes localized vulnerability assessment essential. The SFDRR's emphasis on understanding risk, exposure, capacity, and vulnerability therefore provides a strong basis for place-specific planning [24, 22].

Second, the framework supports multi-actor coordination. It emphasizes the role of government officials at different levels, alongside private-sector actors, volunteers, and other stakeholders [24].

This is crucial because satellite systems span multiple segments—ground, user, link, and space—and each segment involves different organizations, expertise, and responsibilities [21, 17]. From a management perspective, the practical value of the SFDRR lies in its capacity to encourage role mapping, responsibility clarification, and coordinated response planning across institutional boundaries.

Third, the framework's focus on technical and scientific capacity is especially useful. Satellite disruption is not only a response problem but also a knowledge problem. Organizations need to understand dependencies, redundancies, and fallback arrangements in advance. Strengthening technical and scientific capacity, as encouraged by the SFDRR, supports planning for continuity, including the identification of backup systems and degraded-mode operating procedures [24, 8].

Fourth, the SFDRR's emphasis on public education and awareness is directly applicable. Many critical satellite-enabled functions are effectively invisible to the public and even to some service managers. Yet public and organizational awareness is necessary for realistic planning. Preparedness improves when users and managers understand what may fail, what services are likely to degrade first, and what substitute procedures are available [4, 1].

Finally, the framework's provisions for regional and international cooperation are highly valuable. Satellite infrastructure is designed, manufactured, launched, and operated across borders. Risk data and recovery planning therefore cannot be contained within national silos. The SFDRR's support for international information sharing and best-practice exchange aligns well with the management needs of globally distributed infrastructure, even if it does not by itself specify the operational protocols required to make that cooperation effective [24, 10].

Strategic Gaps from a Management and Planning Perspective

The documentary analysis also identifies major gaps that materially limit the SFDRR's adequacy as a planning framework for satellite disruption. These gaps were retained only where the framework text, the supporting literature, and the documented disruption examples discussed above pointed to the same operational deficiency. They are therefore not minor wording issues; they affect how institutions would organize decision making under pressure.

The most important omission is digital specificity. The terms *digital* and *cyber* do not appear in the SFDRR, even though digital vulnerabilities can trigger or amplify major infrastructure failures [8]. The term *technical* appears repeatedly in the framework, but in broad terms and without directly addressing cyber-physical interdependence. For satellite-service disruption, this textual absence creates a planning shortfall. Managers may find broad resilience language useful, but they still need explicit recognition of the kinds of digital dependencies that shape response options.

A second limitation concerns the global character of satellite disruption. The SFDRR's international cooperation provisions are valuable, but the framework was not written with a globally simultaneous outage in mind. Satellite disruption can affect multiple states at once, including highly digitized states whose service dependence is especially pronounced. A planning framework that assumes primarily localized or regional disaster patterns therefore does not fully capture the coordination demands of a large-scale cross-border service failure [8, 25].

A third gap concerns intentional disruption. The SFDRR briefly refers to "man-made" hazards, but it does not provide a developed vocabulary for attack, attacker intent, coercive disruption, or politically motivated interference [24]. This matters because some of the most consequential satellite

Table 2: Principal planning gaps in the SFDRR for satellite-service disruption

Domain	**Observed limitation**	**Management and planning implication**
Digital risk	No direct use of the terms *digital* or *cyber*; technical language remains broad and non-specific.	Continuity plans may lack a clear conceptual basis for cyber-physical dependency, degraded digital services, and coordinated fallback procedures.
Global coordination	The framework supports cooperation, but it is better suited to localized or regional disaster logics than to globally simultaneous infrastructure failure.	Managers need explicit cross-border escalation, information-sharing, and mutual-support procedures for globally distributed service disruptions.
Intentional disruption	Limited treatment of attacker intent, coercion, sanctions, and politically motivated infrastructure targeting.	Recovery planning must be integrated with crisis communication, attribution, and intergovernmental decision making, not treated as a purely technical task.
Supply-chain dependence	Interdependency is acknowledged only briefly, despite multi-sector reliance on satellite-enabled services.	Organizations need formal mapping of downstream service dependencies, critical suppliers, and sector-specific redundancy strategies.
Role allocation	Stakeholder roles are recognized, but the framework does not fully reflect fluid coordination among government, industry, academia, and technical standards bodies.	Planning should specify who leads, who shares information, who provides technical validation, and how responsibilities shift across outage stages.

risks are intentional, including cyberattacks and anti-satellite operations. From a management perspective, intentionality changes planning assumptions: organizations must consider deterrence, escalation, rapid attribution, communications strategy, and political coordination, not only technical recovery [15, 23].

A fourth weakness is the framework's limited treatment of supply chains. Satellite disruption can cascade through transport, logistics, search and rescue, energy, and communications. Even localized interference can generate wider operational effects. For example, suspected GPS interference was associated with Finnair's suspension of flights to an Estonian airport in April 2024, illustrating how a navigation problem can quickly become a transport-planning problem with broader network implications [3]. The SFDRR refers to supply chains, but not with the level of detail required for continuity planning across interconnected service systems [24, 6].

These findings are summarized in Table 2.

IMPLICATIONS FOR MANAGEMENT AND PLANNING

The findings indicate that satellite disruption should be treated as a management and planning problem in at least five practical respects. Each implication is intended as an implementable translation of the preceding analysis rather than as a generic resilience checklist.

Risk Mapping and Dependency Audits

Organizations should begin with structured dependency audits. The first planning task is to identify which services rely on satellite-enabled positioning, timing, communications, or Earth-observation inputs, and then distinguish between essential, important, deferrable, and time-critical uses. The SFDRR's emphasis on exposure and vulnerability provides an appropriate conceptual foundation for this task, but institutions must operationalize it through asset inventories, dependency mapping, and risk categorization [24, 22].

Redundancy and Continuity Planning

Managers should not assume that resilience will emerge automatically from general preparedness language. Redundancy requires specific planning: terrestrial timing backups, alternative navigation procedures, manual workarounds, and degraded-mode service protocols. The literature on GNSS disruption shows that continuity improves when operators already know what substitute systems to activate and how to use them under pressure [4]. In management terms, redundancy is not simply a technical matter; it is an organizational capability that must be documented, trained, exercised, and periodically updated.

Cross-Sector Role Allocation

The SFDRR is strongest where it encourages stakeholder involvement. For satellite disruption, this must be translated into a clearer division of labor across ministries, regulators, service providers, emergency managers, infrastructure operators, and external technical communities. Planning documents should specify who leads incident coordination at each outage stage, who validates technical status information, who communicates with affected users, and who authorizes fallback measures. Without explicit role allocation, outages are likely to produce delay, duplication, or contradictory decisions.

International Coordination and Information Sharing

Because satellite infrastructure is transnational, planning must include cross-border communication channels. The management challenge is not only to share technical information, but to share decision-relevant information in time for coordinated action. This includes threat reporting, operational status updates, continuity arrangements across sectors and jurisdictions, and pre-agreed escalation channels. The SFDRR's cooperative logic supports this direction, but practical implementation requires dedicated protocols and trusted institutional interfaces [24, 10, 11].

Strategic Integration of Technical and Policy Communities

A persistent weakness in the field is the separation between disaster-governance actors and specialist communities working on satellite cybersecurity, standards, and technical resilience. Planning improves when these communities are connected. Standards initiatives, including the IEEE P3349 working group and ISO/TS 20517:2024, show that technical governance is evolving, but these developments must be linked more deliberately to broader institutional planning and disaster-risk policy [11, 7]. Management research can make an important contribution here by examining how organizations absorb technical standards into planning practice, convert them into operating procedures, and sustain coordination across institutional boundaries.

CONCLUSION

Satellite-service disruption is often discussed as a technical or geopolitical problem, but it is equally a management and planning challenge. The analysis presented here shows that the Sendai Framework offers a credible, though incomplete, basis for organizing preparedness and recovery when it is read as a governance architecture rather than as a sector-specific operational manual. Its principal strengths lie in vulnerability assessment, stakeholder coordination, technical and scientific capacity-building, public awareness, and international cooperation. These are precisely the dimensions that matter when institutions must manage cascading service disruption across multiple sectors.

At the same time, the framework remains under-specified for the realities of satellite dependence. It does not directly address satellites as a disaster-generating infrastructure domain; it lacks explicit treatment of digital and cyber risk; it does not fully capture globally simultaneous outages; and it gives limited attention to intentional disruption and supply-chain interdependence. These omissions do not invalidate the framework, but they do impose substantive limits on its operational precision.

For management and planning research, the central implication is clear: resilience in satellite-dependent societies cannot be reduced to technical hardening alone. It also depends on governance design, contingency planning, role clarity, coordination across institutions, and the ability to translate abstract resilience principles into concrete operating arrangements. The contribution of this study is therefore to clarify both where the Sendai Framework is genuinely useful for satellite-service disruption and where supplementary planning instruments remain necessary. Framed in this way, satellite disruption belongs squarely within the field of management and planning research.

REFERENCES

[1] Baraniuk C (2016) GPS error caused “12 hours of problems” for companies. *BBC*, 4 February 2016.

[2] Berke P, Cooper J, Aminto M, Grabich S, Horney J (2014) Adaptive planning for disaster recovery and resiliency: An evaluation of 87 local recovery plans in eight states. *Journal of the American Planning Association* 80(4):310–323.

[3] Calder S (2024) Finnair suspends flights to Estonian airport after suspected Russian “GPS interference”. *Independent*, 30 April 2024.

[4] Castro D, Conceição V, Cavaleiro C (2022) PNT resilience and the impact of satellite radio positioning disruptions on piloting teams. In: *Proceedings of the International Naval Engineering Conference and Exhibition*. Delft University of Technology, Delft.

[5] Cyber Peace Institute (2022) *Case study: Viasat*. Cyber Peace Institute, Geneva.

[6] European Union Agency for the Space Programme (2024) *EUSPA EO and GNSS Market Report*. European Union Agency for the Space Programme, Prague.

[7] Falco G, Henry W, Aliberti M, Bailey B, Bailly M, Bonnart S, Boschetti N, Bottarelli M, et al. (2022) An international technical standard for commercial space system cybersecurity: A call to action. In: *ASCEND 2022*. American Institute of Aeronautics and Astronautics, Las Vegas.

[8] Hamill-Stewart J (2025) The Sendai Framework and satellite security. *International Journal of Disaster Risk Science* 16:117–127.

[9] Hudson HS (2021) Carrington events. *Annual Review of Astronomy and Astrophysics* 59:445–477.

[10] ICSMD (The International Charter Space and Major Disasters) (2024) *International Charter: Space and Major Disasters*. ICSMD.

[11] IEEE (2024) P3349 Space System Cybersecurity Working Group. IEEE Standards Association.

[12] Kelman I (2015) Climate change and the Sendai Framework for disaster risk reduction. *International Journal of Disaster Risk Science* 6(2):117–127.

[13] Kessler D, Cour-Palais B (1978) Collision frequency of artificial satellites: The creation of a debris belt. *Journal of Geophysical Research* 83(A6):2637–2646.

[14] Kessler D, Johnson N, Liou J, Matney M (2010) The Kessler Syndrome: Implications to future space operations. In: *33rd Annual AAS Guidance and Control Conference*. American Astronautical Society, Colorado.

[15] NASA (2021) NASA administrator statement on Russian ASAT test. National Aeronautics and Space Administration, Washington, DC.

[16] NASA (2022) International Space Station maneuvers to avoid another Russian ASAT fragment. National Aeronautics and Space Administration, Washington, DC.

[17] Ortiz F, Monzon Baeza V, Garces-Socarras LM, Vásquez-Peralvo JA, Gonzalez JL, Fontanesi G, Lagunas E, Querol J, Chatzinotas S (2023) Onboard processing in satellite communications using AI accelerators. *Aerospace* 10(2):101.

[18] Ottis R (2008) Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. Cooperative Cyber Defence Centre of Excellence, Tallinn.

[19] Panda A, Bower A (2020) Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment* 11(4):507–518.

[20] Parkinson BW, Morton YTJ, Diggelen F van, Spilker JJ (2020) Introduction, early history, and assuring PNT. In: Lo S, Gao G (eds) *Position, Navigation, and Timing Technologies in the 21st Century*. Wiley, Hoboken, pp 1–42.

[21] Pavur J, Martinovic I (2022) Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight. *Journal of Cybersecurity* 8(1):tyac008.

[22] Rathnayaka B, Siriwardana C, Robert D, Amaratunga D, Setunge S (2022) Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. *International Journal of Disaster Risk Reduction* 78:103123.

[23] UNGA (United Nations General Assembly) (2022a) *Prevention of an Arms Race in Outer Space*. United Nations, New York.

[24] UNISDR (United Nations International Strategy for Disaster Reduction) (2015) *Sendai Framework for Disaster Risk Reduction 2015–2030*. UNISDR, Geneva.

[25] Wisner B (2020) Five years beyond Sendai—can we get beyond frameworks? *International Journal of Disaster Risk Science* 11(2):239–249.

[26] Zhao Q, Yu L, Du Z, Peng D, Hao P, Zhang Y, Gong P (2022) An overview of the applications of Earth observation satellite data: Impacts and future trends. *Remote Sensing* 14(8):1863.

Aulia Malik Affif, Department of Architecture, Faculty of Engineering, Universitas Sumatera Utara, Indonesia

Alan March, Department of Architecture, Faculty of Engineering, Universitas Sumatera Utara, Indonesia

Yulesta Putra, Department of Architecture, Faculty of Engineering, Universitas Sumatera Utara, Indonesia

Manuscript Published; 11 November 2025.