The Declining Reliability of Telecommunications Networks: Causes, Consequences, and a Framework for Resilience

Author: Technology Audit Partners

Abstract

Telecommunications networks underpin modern society, yet the industry is experiencing a significant and sustained increase in outage frequency and severity. This paper examines the growing crisis of declining service reliability across global telecommunications providers, identifies two principal drivers — economic stress and network complexity — and proposes a structured approach for operators to reverse this trend. Drawing on outage data from the Uptime Institute, subscriber experience research from Opensignal, workforce analysis from industry sources, and a peer-reviewed categorization of large-scale outage triggers, we demonstrate that telecommunications networks stand apart from other critical infrastructure sectors in its failure to reduce outage rates over the past decade. We further show that a class of centralized network dependencies termed "sovereign functions" — including BGP routing, DNS, time synchronization, and authentication services — are implicated in approximately one-third of all major outages. Human error, frequently linked to these sovereign functions, accounts for a substantial additional share of reported outages. To address these systemic vulnerabilities, we present the Network Resilience Capability Framework, a structured methodology for evaluating and improving the people, processes, and technology that collectively determine service availability. The framework proceeds through six pillars spanning organizational establishment, network design, implementation, operations, incident response, and foundational capabilities, producing objective, repeatable assessments that enable targeted improvement and longitudinal benchmarking.

Index Terms — network resilience, service availability, telecommunications outages, sovereign functions, IP networks, network reliability framework, human error, telecom operations

I. Introduction

Online services are inherently subject to failures. When such a failure results in the inability to provide a committed service to users, this constitutes an outage event. Outages arise from a wide range of causes including hardware failures, operator errors, natural events, software defects, and cyberattacks [1], [2]. As society's dependence on telecommunications has deepened, the consequences of outages have escalated from customer inconvenience to

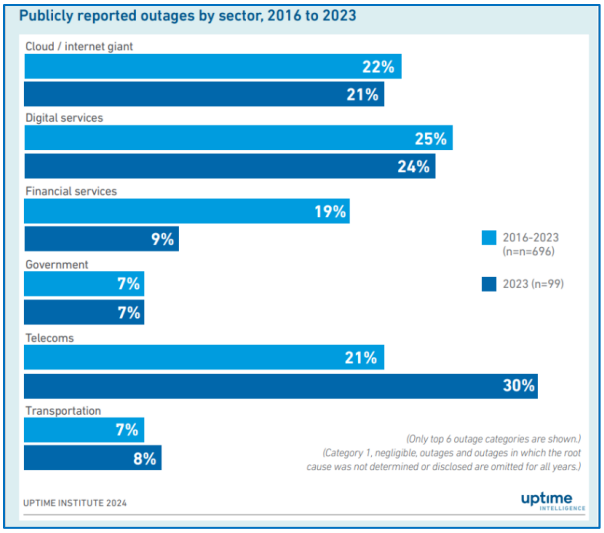
business disruption, financial losses, and direct hazards to life and safety — particularly where emergency calling services (e.g., 911, 000, 112) are affected.
Telecommunications operators have historically promoted the reliability of their networks as a core value proposition. Yet recent industry data reveals a troubling divergence: while most critical infrastructure sectors have achieved continuous improvements in reducing outage frequency, the telecommunications sector is experiencing a significant relative increase [1]. Large-scale, publicly visible outages have affected millions of users across multiple carriers, countries, and regions over the past several years, suggesting that the problem is not endemic to any single operator or geography [2].

This paper provides a structured analysis of this reliability crisis. Section II characterizes the current state of telecommunications service reliability and its consequences. Section III examines two key drivers — economic stress and network complexity — that are accelerating outage frequency and severity. Section IV presents the Network Resilience Capability Framework as a systematic approach for operators seeking to evaluate, improve, and sustain their network resilience posture. Section V draws conclusions and identifies priorities for the industry.

II. The State of Telecommunications Service Reliability

A. Outage Trends Across Critical Infrastructure

The Uptime Institute's Annual Outage Analysis reports provide one of the most comprehensive cross-sector views of service disruption trends. Their 2024 analysis reveals that while industries such as financial services, healthcare, and cloud computing have broadly reduced outage frequency over the past decade, the telecommunications sector has moved in the opposite direction, experiencing substantial increases in both the frequency and scale of outage events [1]. This finding is corroborated by the Uptime Institute's 2025 analysis, which documents continued acceleration of this trend [3].



[Source: Uptime Institute Webinar: Annual Outage Analysis 2024

Independent analysis conducted by Owen et al. at the University of Technology Sydney (UTS) National Telecom Resilience Centre (NTRC) further confirms this pattern. Their peer-reviewed study catalogued large-scale publicly reported telecommunications outages and found that major disruptions have affected the largest and most reputable operators globally, with no single carrier, country, or region immune to the problem [2].

Date	Provider	Country	Impact (Users)	Cause	Duration
May 20, 2025	Telefonica	Spain	Millions	Technical fault [19]	Several hrs
Jan 2, 2025	NTT Docomo	Japan	Unknown	DDoS attacks [20]	~12 hrs
Sep 30, 2024	Verizon	US	Millions	Network issue [21]	~10 hrs
Feb 22, 2024	AT&T	US	Millions	Misconfigured network element [22]	~12 hrs
Dec 26, 2024	Airtel	India	Millions	Technical glitch [23]	Several hrs
Nov 8, 2023	Optus	Australia	10 million	Network issue [16]	~12 hrs
Dec 12, 2023	Kyivstar	Ukraine	Millions	Cyberattack [24]	~6 hrs
Jun 25, 2023	BT	UK	~14000 emergency calls	Technical faults [15]	~10.5 hrs
Jul 2, 2022	KDDI	Japan	30 Millions	Misconfigured router route [17]	~61h 25m
Jul 8, 2022	Rogers	Canada	Millions	ACL misconfiguration [14]	~15 hrs
Feb 9, 2022	Telefónica	Spain	Thousands	4G network issue [25]	~2 hrs
Jun 2,2021	Orange	France	11,800 failed emergency calls + 5 deaths	Bug in the Call Server software [26]	~7 hrs
Jun 15, 2020	T-Mobile	US	Millions	Hardware failure, software bug, and Misconfiguration [27]	+12 hrs
Feb 12,2020	Deutsche Telekom	Germany	Millions	Software update [28]	~7 hrs

[Source: Failures and Resilience in the IP Era: Navigating the Fragility of Modern Telecommunications Networks: The Sovereign Functions, submitted for publication in IEEE Access - DOI 10.1109/ACCESS.2025.3602054]

B. Financial and Operational Consequences

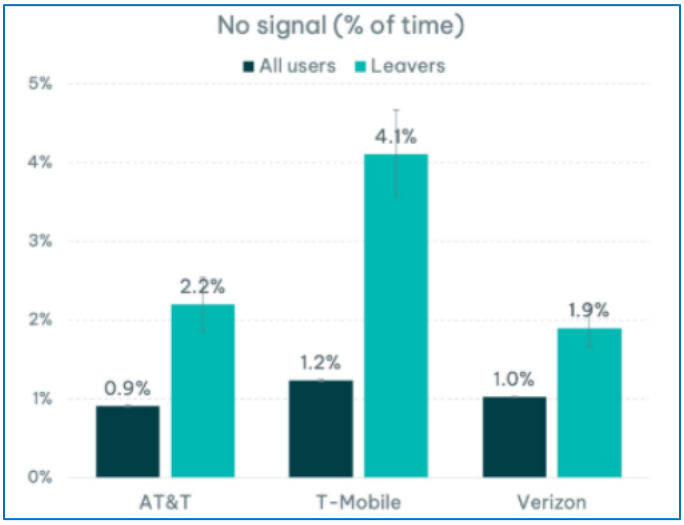
The cost of outages to operators is multidimensional and substantial. Direct costs include the labor and equipment required for mitigation and repair, as well as lost revenue from calls and services that could not be carried. For a large carrier such as Verizon, a system-wide outage is estimated to cost approximately $15 million USD per hour in direct revenue loss alone. Beyond direct carrier costs, the economic impact of disrupted commerce — including failed

transactions, unproductive employee time, and lost sales — can reach hundreds of millions of dollars for major outage events [2].

Of particular gravity is the potential for loss of life. Emergency service calls represent an immediate hazard to life and property; failure to carry such calls creates both a direct safety risk and a significant legal liability for the operator. Finally, long-term reputational damage from repeated outages drives subscriber churn, a metric closely watched by the investment community as an indicator of carrier health.

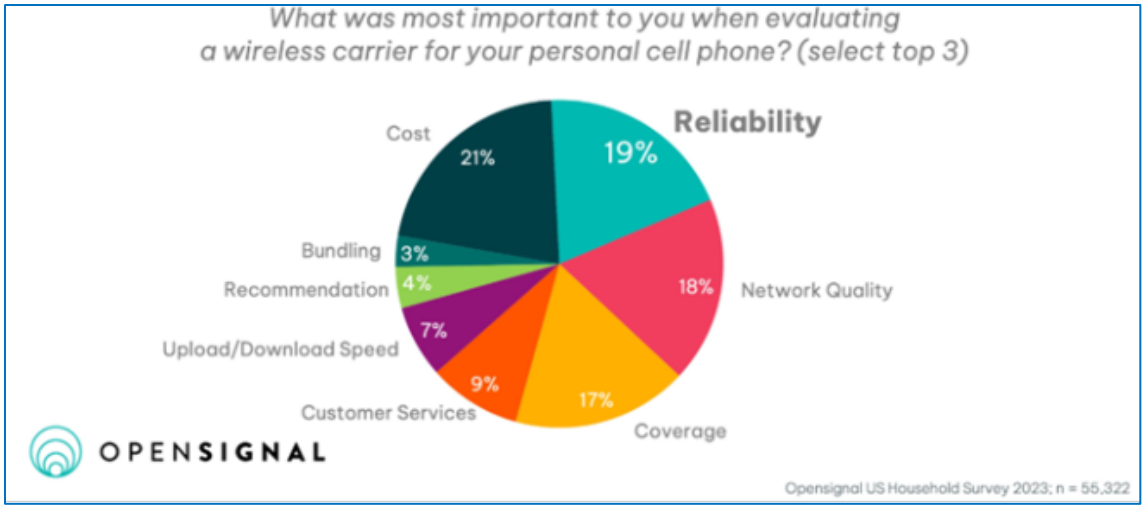
C. The Subscriber Experience and Churn

Opensignal's research on mobile network experience and subscriber churn in the United States provides empirical evidence linking outage exposure to customer loss. Their 2022 analysis demonstrated that subscribers who left a carrier ("leavers") were significantly more likely to have experienced periods of no signal compared to subscribers who remained [4]. As network coverage has generally expanded through infrastructure investment and industry consolidation, the increasing incidence of outages has become a more prominent contributor to signal unavailability and, consequently, to subscriber dissatisfaction and churn.



[Source: Opensignal.com]

Opensignal's 2024 Global Reliability Experience Report, based on a survey of over 55,000 US respondents, found that reliability ranked as the second most important factor in carrier selection — behind only cost — with 58% of respondents identifying it as a key consideration [5]. Network quality, which ranked third at 54%, also encompasses reliability-related concerns. Notably, speed ranked substantially lower at 19%, indicating that the industry's traditional emphasis on bandwidth as a competitive differentiator has diminished in relevance [5]. These findings underscore that, from the consumer perspective, the ability to use a network when and where needed has become more important than raw performance metrics.



[Source: Opensignal.com]

III. Drivers of Declining Reliability

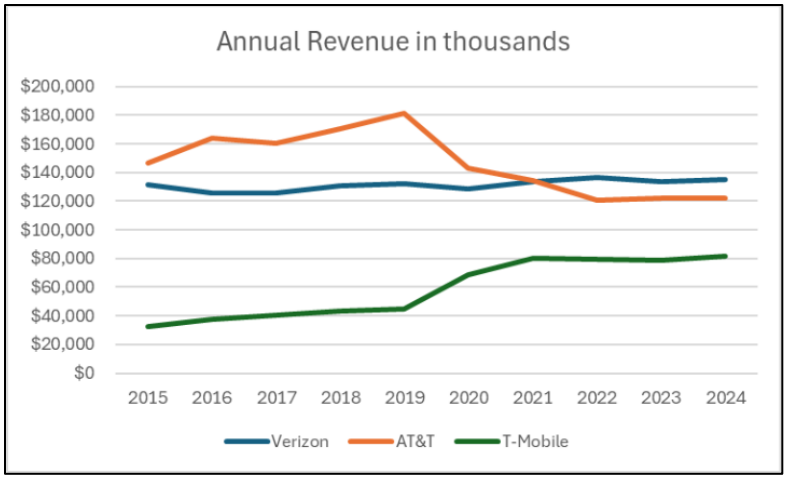
The decline in telecommunications service reliability is driven by two principal and interacting forces: economic stress on service providers and increasing network complexity. These forces, if not addressed systematically, will continue to accelerate the frequency and severity of outages.

A. Economic Stress

1) Market Saturation and Revenue Stagnation

Telecommunications service providers historically relied on subscriber growth and premium pricing for advanced features or higher bandwidth to drive revenue. Both of these growth vectors have substantially diminished. Network features are now largely standardized, and over-the-top services have captured most of the innovation and value creation occurring above the transport layer. Bandwidth, once a meaningful differentiator, no longer commands a premium: at current data rates, consumer applications including video streaming and conferencing are well supported, and consumers are increasingly unwilling to pay for incremental speed improvements that offer no perceptible benefit [5].

Subscriber growth has also flattened. With approximately 8.6 billion mobile phone subscriptions against a global population of 8.1 billion, the opportunity for net subscriber additions is inherently limited [6]. Financial data for the three largest US carriers — Verizon, AT&T, and T-Mobile US — confirm minimal revenue growth over the past five years [7]–[9], a pattern reflected in their stock price trajectories.



[Source: Macrotrends.net]

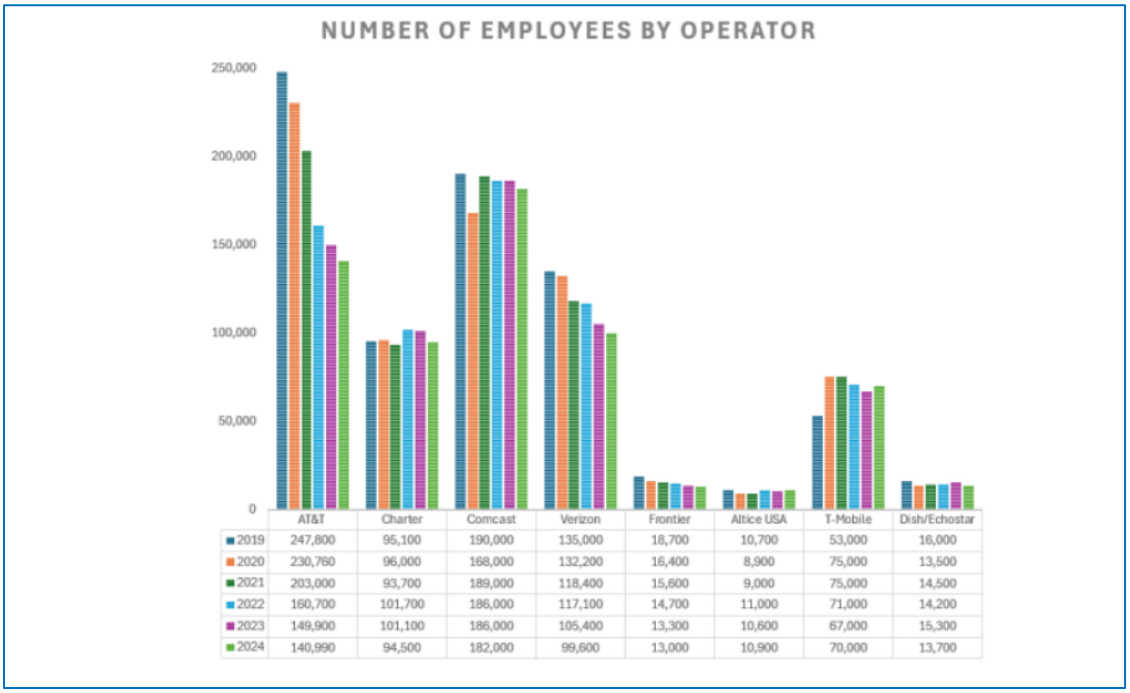
Webb characterizes this transition as "telecoms sufficiency" — a point at which the industry moves from the underpinnings of growth, technology innovation, and market expansion to one of delivering a relatively static service reliably and cost-effectively [6]. In this framing, telecommunications services are transitioning from a growth industry to a utility, albeit one operating in a competitive market. This transition demands a fundamental reorientation toward operational excellence.

2) Cost Reduction Pressures and Their Reliability Implications

With subscriber and revenue growth constrained, operators can only improve financial performance through expense reduction. Several common cost-reduction strategies carry direct implications for service availability:

- **Equipment and redundancy.** Service availability can be improved by deploying redundant equipment, selecting components with lower failure rates, and designing architectures with smaller failure radii (blast zones). These measures carry incremental cost. When operators economize on equipment quality or redundancy, the risk to service availability increases.
- **Equipment replacement cycles.** Extending hardware and software replacement cycles reduces capital expenditure but increases the proportion of unsupported, end-of-life, or obsolete components in the network, all of which are associated with elevated failure rates.
- **Staffing reductions.** Workforce reduction is a major cost-control lever, but the newer IP-based network technologies are more complex to design and operate than their predecessors, requiring a critical mass of skilled personnel. Industry data from Fierce Network documents that the eight largest US wireless and wireline operators reduced their combined workforce from 766,300 employees in 2019 to 624,690 by end of 2024 [10]. This reduction has occurred even as networks have grown larger and more complex. The resulting loss of institutional knowledge — a "brain drain" — has direct reliability consequences. Evidence from Owen et al. indicates that misconfigurations account for 21.8% of all large-scale publicly reported outages, and a further 29.1% of

outages had no publicly reported cause; in the authors' direct engagements, human errors and mis-execution of changes are commonly found to be root causes within this category [2].



	AT&T	Charter	Comcast	Verizon	Frontier	Altice USA	T-Mobile	Dish/Echostar
2019	247,800	95,100	190,000	135,000	18,700	10,700	53,000	16,000
2020	230,760	96,000	168,000	132,200	16,400	8,900	75,000	13,500
2021	203,000	93,700	189,000	118,400	15,600	9,000	75,000	14,500
2022	160,700	101,700	186,000	117,100	14,700	11,000	71,000	14,200
2023	149,900	101,100	186,000	105,400	13,300	10,600	67,000	15,300
2024	140,990	94,500	182,000	99,600	13,000	10,900	70,000	13,700

[Source: fierce-network.com]

- **Outsourcing.** Operators also reduce expenses by outsourcing functions including network operation, management, outage detection and recovery, and change management. While this may reduce operational costs, it introduces risks including loss of institutional knowledge for critical design and diagnostic functions, and communication delays or misunderstandings at the operator-vendor interface. These factors have demonstrated potential to cause or aggravate outage situations.

B. Network Complexity and Sovereign Functions

1) The IP Transformation and Centralized Dependencies

Nearly all modern telecommunications service providers carry their traffic over Internet Protocol (IP) networks. IP technology is mature, economical, and capable of supporting a remarkable range of traffic types. However, the IP architecture introduces a class of centralized service dependencies that Owen et al. term "sovereign functions" [2]. When these sovereign functions experience failure, major portions of the network can cease to operate.

The sovereign functions identified in the literature include:

- IP routing protocols (BGP, IP-MPLS, OSPF) used to determine next-hop forwarding decisions between routers.
- IP addressing and naming services, including DNS for name-to-address resolution and DHCP for dynamic address assignment.

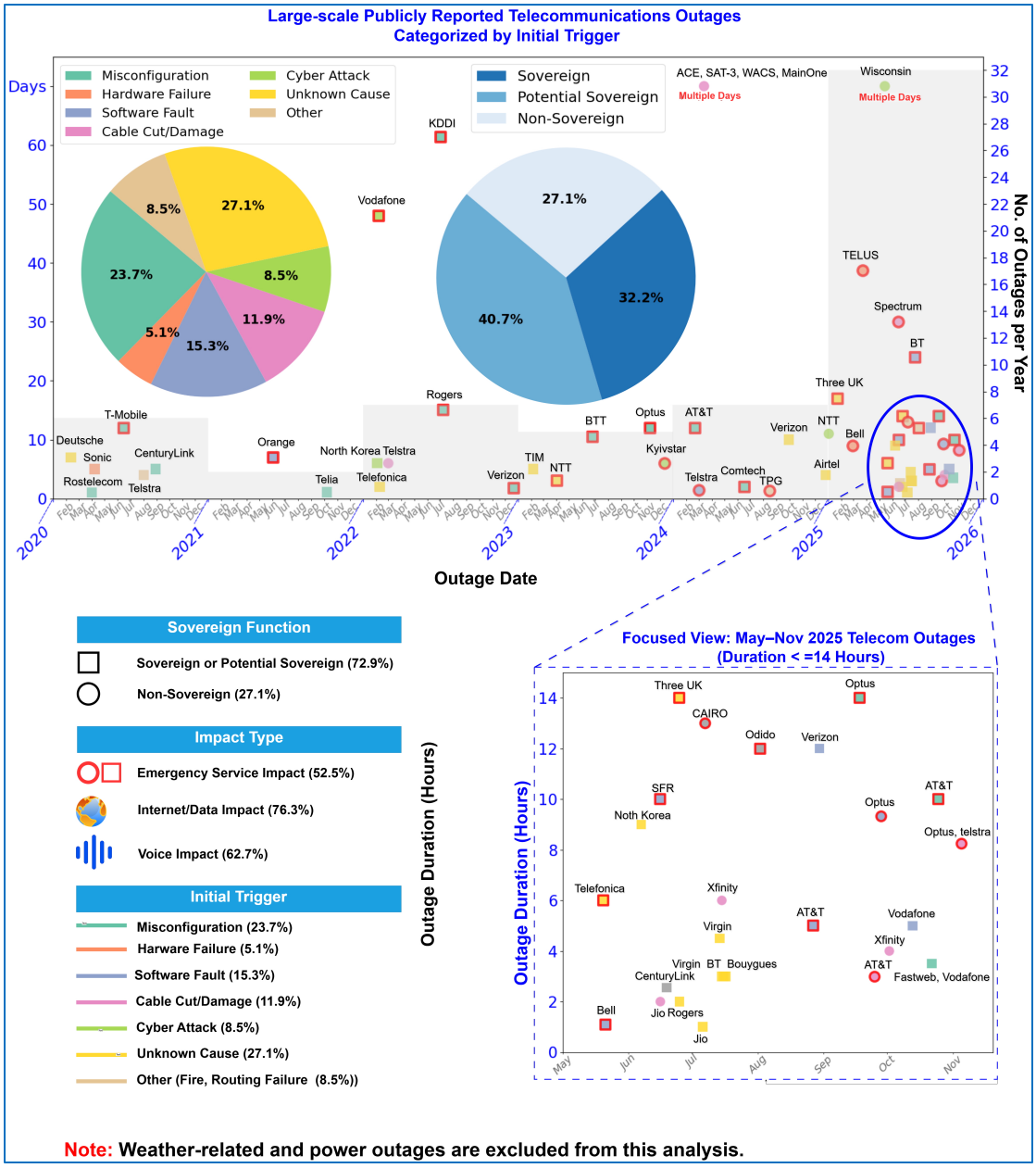
- Time synchronization functions (NTP, PTP).
- License and certificate management systems.
- Authentication services including Active Directory, LDAP, and X.500.

These functions are, by their nature, most efficient and simpler to implement when centralized. However, centralization creates inherent risk: a single failure or misconfiguration can propagate rapidly and widely across the network, affecting services at a scale disproportionate to the triggering event.

2) Outage Attribution Analysis

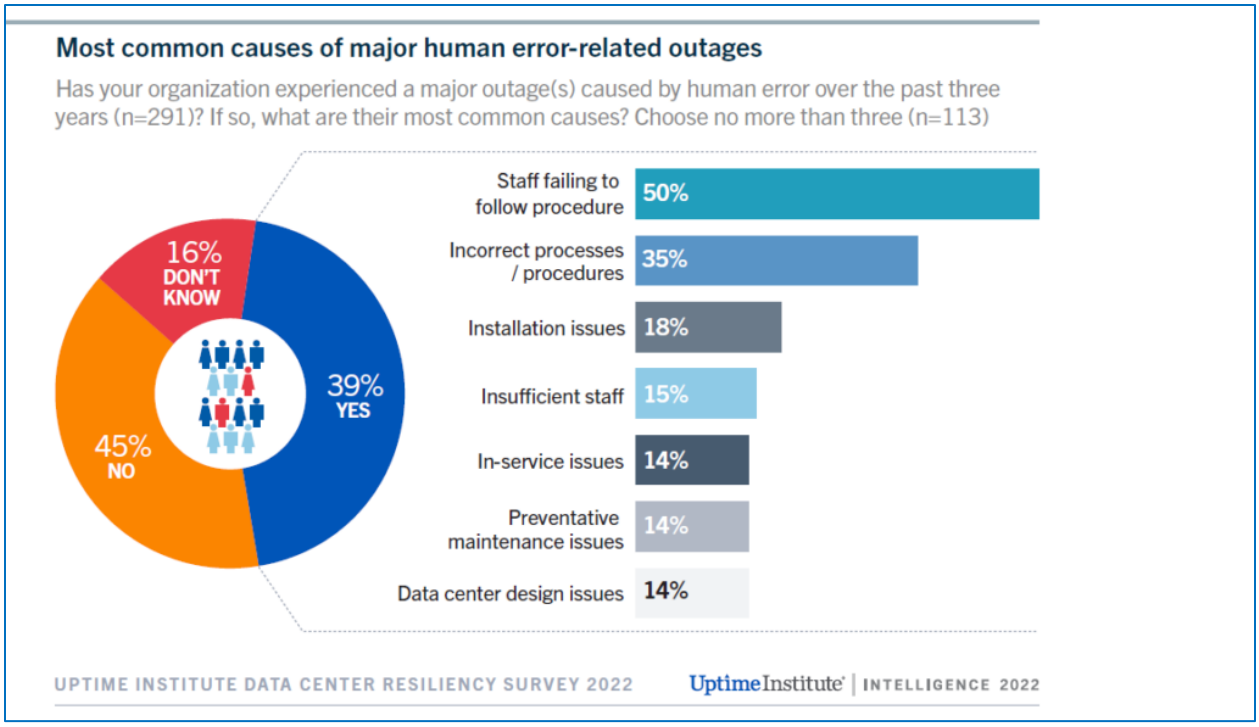
Analysis conducted by the UTS National Telecom Resilience Centre, as reported in Owen et al. [2], found that sovereign functions are associated with approximately 72.9% of total large-scale outages, with roughly one-third explicitly attributable to sovereign function failures. These functions are characterized as increasingly brittle: they are stretched beyond their original design intent, complex to configure and maintain, and exhibit a high degree of fault propagation that cannot be contained through traditional blast-zone segregation methods.

Among sovereign function failures, configuration mistakes and human errors are frequently implicated in the largest outages. Even minor changes to these functions can propagate rapidly throughout the network, causing widespread and often difficult-to-isolate disruptions. Personnel with deep domain knowledge, disciplined change processes, and attention to detail are therefore critical to managing these functions while minimizing outage risk.



[Source: University of Technology Sydney: National Telecom Resilience Centre]

The Uptime Institute's analysis of the human factor in outages supports these findings. Their data, based on 25 years of operational observation, estimates that human error plays a role in approximately two-thirds of all outage incidents. Specific contributing factors include staff failing to follow established procedures (48%), incorrect or insufficient staffing processes (45%), insufficient staffing levels (15%), and inadequate preventive maintenance frequency (14%) [1], [11].



[Source: Uptime Institute]

3) Emerging Complexity Vectors

Additional forms of complexity are emerging that, while often motivated by cost reduction, carry reliability implications if not managed with discipline:

- **Automation and artificial intelligence.** Increased adoption of automation and AI in network operations may reduce individual human errors but introduces an emerging trend of automated propagation of errors at speed and scale, a growing concern even with very large and sophisticated operations. [13]
- **Virtualization and softwarization.** The shift from appliance-based to function-based network services through software-defined networking (SDN) and network function virtualization (NFV) introduces new dependencies on cloud-scale computing infrastructure to underpin network services.
- **New service delivery models.** Capabilities such as network slicing add further architectural complexity to networks already under stress from the factors described above.

In summary, telecommunications service providers face a convergence of business transformation pressures and technological change. Economic stress drives cost reduction that can directly erode the people, processes, and equipment that sustain reliability, while increasing network complexity — particularly the proliferation and over-extension of sovereign functions — creates new vectors for large-scale failure. These two forces, if not addressed systematically, will result in continued acceleration of outage frequency and severity.

IV. A Framework for Network Resilience Capability

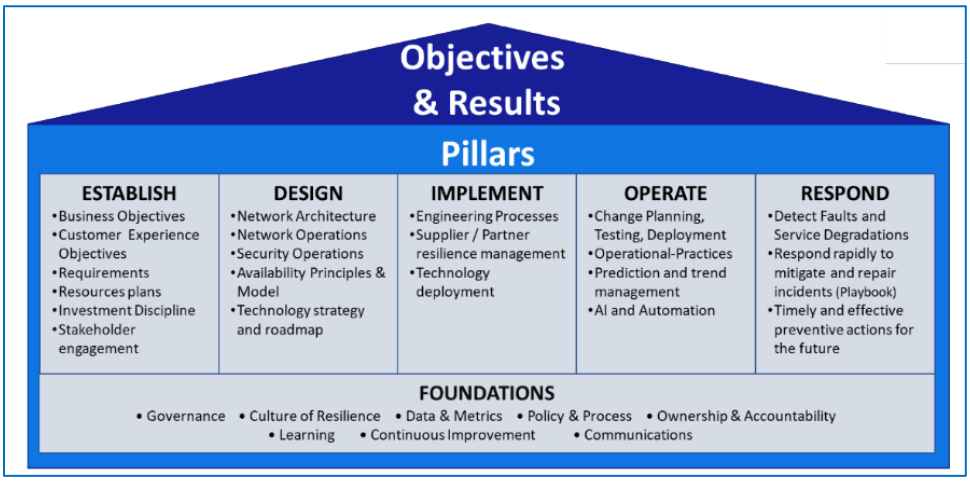
A. The Need for a Structured Approach

The analysis presented in Sections II and III demonstrates that network resilience and service availability are determined not only by the technology and topology of a network, but also by the people, processes, practices, and culture of the organization responsible for designing, implementing, and operating it. There is no substitute for skilled personnel in network design and operations. However, it is equally important for staff and leadership to maintain a holistic view of resilience as plans are developed and actions are undertaken. A decision to invest in higher-quality hardware and software, for example, can be entirely negated by the absence of a well-considered plan for deploying that equipment or by a lack of the skills needed to operate it. Similarly, new technology deployments without skilled design, configuration, and operational support may themselves become causes of outages — particularly in the sovereign functions discussed in Section III.

What is needed, therefore, is a repeatable structure for evaluating the current state of network resilience capability, developing improvement plans, guiding decision-making, and measuring progress. Such decisions span services, hardware and software selection, vendor relationships, staffing and skills, and operational practices. All levels of an organization must be engaged, as the achievement of network resilience is not a discrete action but an ongoing discipline requiring sustained commitment [12].

B. Framework Structure

The Network Resilience Capability Framework, developed by Technology Audit Partners [12], provides a holistic methodology for examining a telecommunications network and its supporting organization with a specific focus on outage prevention and management.



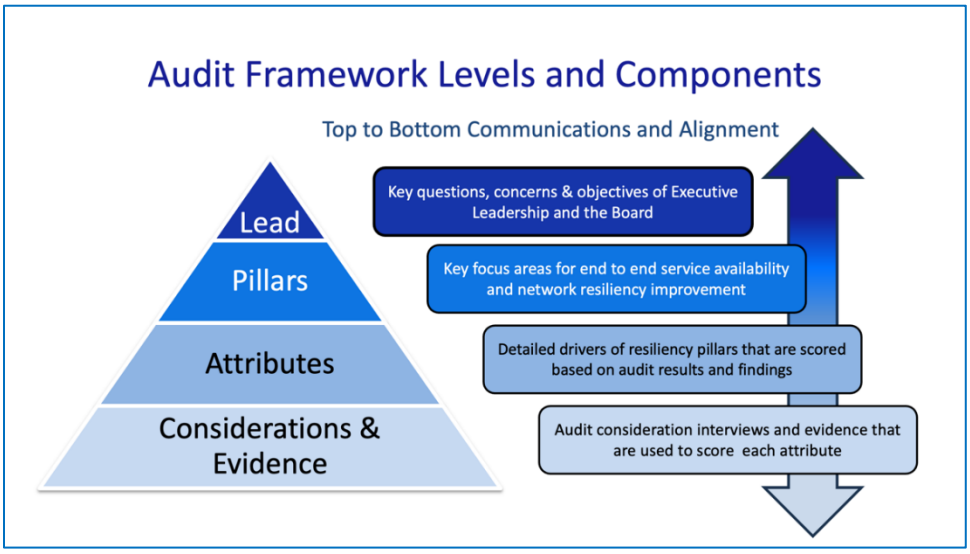
[Source: Technology Audit Partners]

The framework is structured around six pillars that follow the complete service provider lifecycle:

Pillar 1 — Establishment: How network resilience objectives, governance, and organizational commitment are defined and established.
Pillar 2 — Design: How the network architecture is designed with resilience as a primary consideration, including redundancy, failure radius management, and sovereign function hardening.
Pillar 3 — Implementation: How network designs are translated into deployed infrastructure, including equipment selection, configuration management, and testing.
Pillar 4 — Operations: How the network is operated on an ongoing basis, including monitoring, change management, maintenance, and capacity planning.
Pillar 5 — Outage Response: How the organization detects, responds to, and recovers from outage events, including root cause analysis and corrective action.
Pillar 6 — Foundational Capabilities: Core organizational capabilities that underpin excellence across all pillars, including leadership, workforce development, continuous improvement, and knowledge management.

C. Evaluation Methodology

Within each pillar, the framework defines specific evaluation areas, termed "attributes," that focus on particular practices. The evaluation process compares the network and organization against recommended practices using a predefined set of assessment criteria ("considerations") and a scoring rubric that measures the degree of deployment and effectiveness across the organization. Scores can be aggregated to produce assessments of network and organizational maturity, both in isolation and against industry best-practice benchmarks [12].



[Source: Technology Audit Partners]

This type of evaluation is typically performed by an independent third party via a formal audit or assessment, though it may also be conducted through internal self-evaluation or a combined approach.

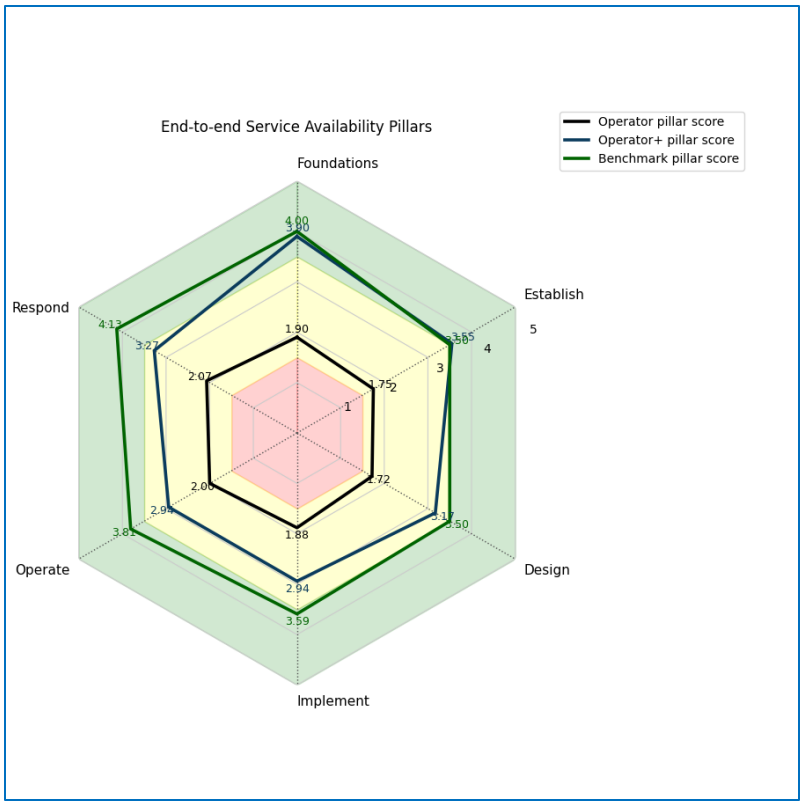
D. Benefits of Framework-Based Evaluation

The application of a structured, framework-based approach to network resilience evaluation offers several distinct advantages.

1. The framework ensures a comprehensive assessment across all relevant practices, rather than a deep investigation of a specific area. This breadth minimizes the risk of local optimization that overlooks other necessary components.
2. The framework enables an organization to benchmark itself against evolving industry best practices, as the attributes and considerations are constructed from — and updated in line with — current best practice.
3. Scoring is based on the depth and breadth of actual deployment, the achievement of measurable results, and evidence of ongoing continuous improvement.
4. The framework substantially reduces subjectivity in evaluation, producing an objective assessment that facilitates acceptance and focuses discussion on addressing identified issues rather than contesting the evaluation itself.
5. Specific improvement plans can be targeted to identified gaps and weaknesses, with execution measured and reported against the framework.
6. The evaluation can be repeated at subsequent intervals to measure progress; the use of a consistent framework and methodology enables results to be compared over time and across different evaluators [12].

E. Application and Benchmarking

Application of the framework to an organization-wide evaluation produces a high-level view of actual capabilities at a given point in time, benchmarked against best practice.



[Source: Technology Audit Partners]

The framework can also be used to establish improvement plans, predict future scoring based on planned interventions, and measure progress toward those improvements by comparing initial audit results with subsequent evaluations conducted after improvement actions have been implemented [12].

V. Conclusion

This paper has identified and characterized a significant and growing crisis in global telecommunications: the increasing frequency and severity of service outages, at a time when society's dependence on telecommunications infrastructure has never been greater.

The evidence is clear that telecommunication services stand apart from other critical infrastructure sectors in its failure to reduce outage rates. The Uptime Institute's cross-sector analyses [1], [3] show telecommunications diverging sharply from the improvement trajectories seen in financial services, healthcare, and cloud computing. The financial, operational, and safety consequences of this trend are substantial and escalating — from direct revenue losses measured in millions of dollars per hour for major carriers, to the disruption of emergency calling services that directly endangers lives.

Two principal forces are driving this decline. **First,** economic stress arising from market saturation and revenue stagnation [6]–[9] compels operators to reduce costs through measures — including equipment economization, extended replacement cycles, staffing reductions [10], and outsourcing — that directly erode the human and technical foundations of service availability. **Second**, increasing network complexity, particularly the centralization and over-

extension of sovereign functions within IP-based architectures, has created a class of vulnerabilities in which small failures or human errors can propagate rapidly into large-scale outages. These sovereign functions are implicated in approximately 72.9% of major outage events [2], and human error — frequently linked to configuration mistakes in these very functions — accounts for an estimated two-thirds of all outage incidents [1], [11]. Critically, these two forces are not independent: economic pressures reduce the skilled workforce and disciplined processes needed to manage increasingly complex sovereign functions, creating a compounding effect that, if unaddressed, will accelerate the reliability decline.

The Network Resilience Capability Framework [12] offers a systematic path forward. By evaluating the complete lifecycle of network resilience — from organizational establishment through design, implementation, operations, and incident response, underpinned by foundational capabilities — the framework provides operators with a comprehensive, objective, and repeatable methodology for identifying vulnerabilities, prioritizing improvements, and measuring progress. Its emphasis on breadth of assessment guards against the common pitfall of local optimization, while its benchmarking capability enables operators to track their resilience maturity over time and against industry best practices.

The telecommunications industry is at an inflection point. The transition from a growth-driven model to one of utility-like service delivery demands a corresponding shift in operational philosophy — from innovation-led expansion to disciplined, resilience-focused operational excellence. The tools, frameworks, and evidence base to support this transition exist. What is required is the organizational commitment to apply them systematically and sustain the effort over time.

References

[1] D. Donnellan and A. Lawrence, "Annual outage analysis 2024: The causes and impacts of IT and data center outages," Uptime Institute, UII Keynote Rep. 131, Mar. 2024. [Online]. Available: https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2024

[2] R. Owen, A. Bryant, L. Finch, D. Franklin, M. Abdollahi, and M. Abolhasan, "Failures and resilience in the IP era: Navigating the fragility of modern telecommunications networks—The sovereign functions," *IEEE Access*, vol. 13, pp. 155759–, 2025, doi: 10.1109/ACCESS.2025.3602054.

[3] Uptime Institute, "Annual outage analysis 2025," Uptime Intelligence, 2025. [Online]. Available: https://intelligence.uptimeinstitute.com/resource/annual-outage-analysis-2025

[4] R. Wyrzykowski and I. Fogg, "How mobile network experience affects churn in US wireless carriers," Opensignal, Oct. 20, 2022. [Online]. Available: https://insights.opensignal.com/2022/10/20/how-mobile-network-experience-affects-churn-in-us-wireless-carriers

[5] R. Wyrzykowski, "The Opensignal global reliability experience report," Opensignal, Feb. 8, 2024. [Online]. Available: https://www.opensignal.com/2024/02/08/the-opensignal-global-reliability-experience-report

[6] W. Webb, *The End of Telecoms History*. Independently published, 2024. ISBN: 979-8328402729.

[7] "Verizon revenue 2012–2025 | VZ," Macrotrends. [Online]. Available: https://www.macrotrends.net/stocks/charts/VZ/verizon/revenue. [Accessed: Mar. 5, 2026].

[8] "AT&T revenue 2012–2025 | T," Macrotrends. [Online]. Available: https://www.macrotrends.net/stocks/charts/T/at-t/revenue. [Accessed: Mar. 5, 2026].

[9] "T-Mobile US revenue 2012–2025 | TMUS," Macrotrends. [Online]. Available: https://www.macrotrends.net/stocks/charts/TMUS/t-mobile-us/revenue. [Accessed: Mar. 5, 2026].

[10] "All in the charts: Analyzing telecom's big workforce shrinkage," Fierce Network, 2025. [Online]. Available: https://www.fierce-network.com/broadband/there-any-rhyme-or-reason-behind-telecom-layoffs

[11] A. Lawrence, "Outages: Understanding the human factor," Uptime Institute Journal, Jun. 8, 2022. [Online]. Available: https://journal.uptimeinstitute.com/outages-understanding-the-human-factor/

[12] Technology Audit Partners, "Network resilience capability framework," techauditpartners.com. [Online]. Available: https://techauditpartners.com/. [Accessed: Mar. 5, 2026].

[13] Craig Hale, “Recent AWS issues blamed on AI tools - at least two incidents affected some Amazon service,” Techradar.com, [Online]. Available: https://www.techradar.com/pro/recent-aws-outages-blamed-on-ai-tools-at-least-two-incidents-took-down-amazon-services [Accessed: Mar. 16, 2026]