Impact of Cybersecurity Capability, 5G Network Performance Optimization, and IT Service Management Maturity on Digital Service Reliability in U.S. Private 5G Network Operations

Ahmed Omer Mustafa Mohammed[1]

Author's Affiliation:

[1]Software Developer (5G Network) Siri Consultancy Services Inc. New Jersey, U.S.A

Article History:

Submitted: Sep 04, 2025
Revised: Oct 21, 2025
Accepted: Nov 29, 2025
Published online: Dec 30, 2025

Corresponding author(s):
Ahmed Omer Mustafa Mohammed
Email:
ahd-omer@hotmail.com

Abstract

Purpose— This study examines the influence of cybersecurity capability, 5G network performance optimization, and IT service management (ITSM) maturity on digital service reliability within the context of private 5G network operations in the United States. As organizations increasingly depend on private 5G infrastructures to support mission-critical digital services, ensuring high levels of reliability has become a strategic imperative.

Study Design/methodology/approach— The study develops a conceptual framework grounded in operational practices relevant to private 5G deployment, including threat monitoring, incident response, real-time performance analytics, service-level agreement (SLA) and operational-level agreement (OLA) enforcement, cloud–network integration, and automation.

Findings— Conceptual findings indicate that cybersecurity capability, 5G network performance optimization, and ITSM maturity each exert a positive influence on digital service reliability. Moreover, their combined and reinforcing interaction produces the strongest reliability outcomes, demonstrating that digital service reliability in private 5G environments is not the result of isolated technical strength, but of integrated organizational and technological capabilities.

Research Practical Implications The proposed framework offers practical guidance for organizations operating private 5G networks in the United States by emphasizing the need to align security engineering, performance optimization, and service management governance. The findings highlight how integrated deployment of cybersecurity controls, intelligent network optimization, and mature ITSM practices can significantly enhance service continuity, reduce operational disruptions, and strengthen resilience in mission-critical digital environments.

Originality/value— This study contributes original value by presenting an integrated, multidimensional framework that jointly examines cybersecurity capability, 5G performance optimization, and ITSM maturity within enterprise-managed private 5G networks—an area that remains underexplored in existing literature.

Keywords: Private 5G, Cybersecurity Capability, Network Performance Optimization, ITSM Maturity.

JEL Classification Codes: G21, O33, L26, M1

https://doi.org/10.61503/AITST.v1i2.10

1 | INTRODUCTION

The research tool was a self-administered 5-point Likert scale questionnaire with four main constructs of this study namely: gender stereotypes, institutional trust, feminist consciousness and perceived political legitimacy of women in governance. Each construct was composed of six items, which resulted in 24 scale items, to have no more or no less representation of all the variables in the study. The questionnaire was designed in a methodical way in terms of selecting, adapting and refining the items in a way that makes sense, relevant and concise to the purpose of conducting the study. Everything was stated in easy and comprehensible language that could be used by undergraduate respondents and was constructed construct-by-construct to ensure logical progression and interest of the respondents. The completed tool was presented in a physical administration format and designed in a way that would allow minimum errors in data collection and consistent and efficient data collection to be done and later analysed quantitatively.

Cybersecurity capability is defined as the ability of an organization to identify, block and counteract cyber threats with active monitoring, sophisticated analytics and normal security controls. In private 5G networks, cybersecurity will include SIEM, IDS/IPS, zero-trust architecture, access controls, encryption, and adherence to frameworks like NIST, ISO 27001, and CISA recommendations. This is required due to the fact that the private 5G infrastructures combine cloud-native cores, distributed edge locations, and virtualized functions, which are appealing to advanced attacks. Well-developed cybersecurity helps minimize service interruption due to limiting the number of vulnerability gaps, fast threat quarantine, and secure coordination of network slices and critical applications. The empirical studies conducted in digital ecosystems indicate that strong security capacity improves the availability of the system, the severity of incidents, or helps to deliver services continuously, which may indicate that there is a direct correlation between the security readiness in the cybersecurity field and the reliability of the digital services.

Optimization of 5G network performance includes the technical and analytical activities organizations use to maintain the optimal network performance, such as latency reduction, load balancing, real-time KPI monitoring, and predictive performance analytics. In order to identify anomalies, to keep QoS parameters, and to ensure the smooth operations of virtualized network functions and edge platforms, the use of performance optimization frameworks by the operators of private 5G is essential. Some of the techniques, including AI-based network automation, self-organizing networks (SON), dynamic spectrum allocation, API-based orchestration, and slice assurance systems, enhance network stability. Telecom management research suggests advanced performance optimization which minimizes the jitter, packet loss and congestion and minimizes the network responsiveness and scalability. When extended to the context of the 5G in the private setting, these features enhance the reliability of the digital services that rely on constant connectivity, low-latency communication, and constant throughput, and there is a robust conceptual connection between the performance engineering practice and the reliability of digital services.

This is because IT service management (ITSM) maturity indicates how much an organization has formalised and streamlined its service governance using ITIL-based processes like incident management, change control, configuration management, problem management, and business continuity planning. In 5G private use, the effectiveness of the incident lifecycle, root-cause analysis, SLA enforcement, and cross-functional coordination between network, cloud, and cross-functional teams are decided by the ITSM maturity. Mature ITSM practices create the consistency of operations, minimize variability of services, and make orchestration, monitoring and maintenance processes repeatable and predictable. Empirical and theoretical research has highlighted that structured ITSM systems enhance service availability, minimizing disruptions by implementing technology by aligning technology functions to business goals. In the case of private 5G networks, ITSM maturity can be seen as a stabilizing factor, which incorporates cybersecurity controls and performance optimization actions into an overall operational framework, which can further increase the reliability of digital services.

It is possible to understand the theoretical connections between these three capabilities in terms of the dynamic capabilities framework and a socio-technical systems theory. The socio technical systems theory indicates that the outcome of organizational performance relies on the alignment of technological sub systems (including network and security technologies) with the social or procedural sub systems (including governance processes and managerial coordination). The reliability of digital services in private 5G networks is consequently a combination of the technical qualities (cybersecurity capability and performance optimization) and organizational processes (ITSM maturity). The dynamics capabilities theory also describes how organizations feel and react to the environmental changes and adapt to them. Cybersecurity capability provides sensing and mitigation of risks; performance optimization facilitates reconfiguration and scalability and ITSM maturity will provide a stable and efficient response and absorption of operational variability. The combination of these capabilities leads to an integrated theoretical model in which all of the variables support each other to obtain high reliability.

Although the growth of the 5G private networks in the United States is accelerating, there is limited research on the factors that determine the reliability of digital services in these infrastructures. Current literature pays much attention to technical aspects including spectrum management, core network virtualization, radio engineering or security protocols individually. The interaction between organizational capabilities (IT governance, maturity in service management, or integrated cybersecurity) and technical optimization to determine the results of reliability is examined in a limited number of studies. In addition, the bulk of existing studies focuses on the case of public telecom networks, and there are limited studies on the specifics of enterprise-run private 5G systems, which have varying architectures, priorities, and operational limitations. The relationship between the capability of cybersecurity, performance optimization, and ITSM maturity in the context of enterprise-controlled 5G deployment has not been well investigated, and a significant gap in the literature and industrial expertise is identified.

The area of concern on which the research problem is based is thus the necessity to comprehend the combined effect of integrated managerial and technical capabilities as sources of digital service reliability in private 5G operations. Organizations tend to invest vast sums in particular areas, like updating their cyber defense infrastructure or introducing new network analytics, without understanding that the two features should be used to reinforce each other to create a comprehensive level of reliability. The incomplete or isolated enhancements cannot be used to create consistent operational results as reliability in the case of private 5G networks requires constant alignment of security controls, performance engineering systems, and service governance procedures. This fragmentation of understanding is part of the continued service outages, erratic experience quality, long response times to incidents, and vulnerability to cyber threats. To deal with this issue, it is important to have a holistic model that serves as a representation of the multidimensional drivers of service reliability in the 5G ecosystem privately owned.

The study is significant since it is part of the academic theory and practice in organizations. Theoretically, it would increase the understanding of the private 5G management of the consolidation of the cybersecurity capability, performance optimization, and ITSM maturity into a unified framework that outlines the output of reliability. It extends the technical determinism and includes the socio-technical and dynamic capabilities lenses by offering a multidimensional solution of how digital service reliability may be ensured in the multidimensional next-generation networks.

Practically, the study provides evidence-based recommendations to the U.S. companies that would like to deploy or maximize the use of 5G networks in the privately-owned setting. The findings are useful in helping organizations to make investment decisions and cross-functional alignment decisions and also enhancing operational resilience by determining the key capabilities in which service reliability is most dependent on. The study also helps the policymakers and regulators in the industry to indicate the essence of the integrated security, performance engineering and service governance in securing the critical digital infrastructures.

Overall, the research fills a significant gap in the growing area of private 5G network management since it examines the collective impact of cybersecurity capability, 5G network performance optimization, and ITSM maturity on the reliability of digital services. With organizations relying more and more on their own 5G infrastructures to support mission-critical initiatives, it has become critical to learn more about these interdependencies in order to support resilient digital services. Besides advancing academic knowledge, the research model created in the present case provides U.S. enterprises with the strategies to develop secure, optimized, and well-managed private 5G environments that can respond to the requirements of the next-generation digital ecosystems.

2 | LITERATURE REVIEW

The theoretical underpinning of this research is based mainly on the socio-technical systems theory and the dynamic capabilities concept, which both provide sound conceptual concepts with regard to the reliability of contemporary digital infrastructures within multi-faceted technological systems. According to socio-technical systems theory, the achievement of organizations can be attributed to the joint effect of social structures and technological elements and not a technical sophistication (Trist and Bamforth, 1951). With regards to the case of the 5G networks in the context of a private setting, the implication of this theory is that cybersecurity controls, network optimization mechanisms, and IT service management processes should be operating in harmony to provide high service reliability. To supplement this perspective, the dynamic capabilities theory accentuates the capacity of an organization to read risks, implement opportunities and reorganize operation procedures to be able to adapt to accelerated technological and environmental changes (Teece, 2007). The cybersecurity capability is consistent with the sensing because it allows proactive detection of threats and the resilience practice; the optimization of network performance with 5G networks corresponds to the seizing and reconfiguring roles because organizations implement analytics, automation, and orchestration to establish long-term reliability; and ITSM maturity corresponds to the institutionalization of organized routines of maintaining the reliability of processes. All these theoretical approaches imply that the reliability of digital services is not a consequence of the individual technological advancement, but a collaboration of both managerial and technical skills, integrated into the organizational mechanisms (Aranda, Sacoto Cabrera et al. 2021).

In the literature of the empirical research, it has become a consensus that cybersecurity capability is a crucial determinant of digital service integrity, system availability and continuity of operations. Research on network security reveals that the number of service disruptions and the speed of recovery are lower in organizations having high-quality threat intelligence, automated detection assessment, and effective incident response procedures (Huang and Pearlson, 2019). According to research on enterprise networks, SIEM, zero-trust models, and behavioral-based anomaly detection are among the critical risk exposure and system resility positively influencing factors (Sharma & Gupta, 2021). In the case of cloud-integrated architectures such as 5G-specific cases of the privatization of cloud environments, data show that effective cybersecurity governance reduces downtime through reduced attack surface and faster intrusion response (Rahman et al., 2020). Recent works dedicated to 5G technologies emphasize that the concepts of virtualization, distributed edge nodes, and multi-access edge computing present new types of vulnerability that demand innovative detection and response tools (Li and Li, 2022). Since 5G systems are being privatized and are heavily based on software-defined networking and network function virtualization, studies have brought to the fore that cyber capability is a direct demonstration of service continuity through the protection of virtualized cores, APIs, network slices, and network management planes (Kim and Lee, 2023). All these findings can be used as evidence that cybersecurity capability is not just a protective role, but the essence of reliable operation of digital services (Vargas and Tien 2023).

In line with the literature on cybersecurity, an increasing amount of research studies the factors and functional effects of network optimization on performance through advanced telecom and enterprise systems. Research in the field of telecommunication engineering shows that automated performance monitoring, AI-enhanced analytics, and predictive modeling can achieve a tremendous impact on network stability since anomalies are detected before they develop into service failures (Zhang and Chen, 2020). Empirically, the solutions to reduce latency, scheduling resources, and network slicing dynamically are demonstrated to enhance the reliability of mission-critical applications in private LTE and 5G deployments (Wang et al., 2021). It is also proposed in research that real-time KPI dashboard, closed loop automation, and SON (self-organizing network) functions can enhance the speed of fault localization and service degradation reduction (Hossain and Hasan, 2022). According to the reports of private 5G operators, especially in manufacturing and logistics, the quality of service (QoS) can be enhanced, and predictive analytics and automated orchestration tools are applied to ensure throughput consistency and reduce congestion (Fischer & Braun, 2023). These results highlight the concept of performance optimization as one of the ways of guaranteeing reliable digital services in complex and highly demanding networks.

Organizational performance, operational stability, and service quality have also been associated with the ITSM maturity based on the ITIL frameworks and research on enterprise service governance. Research shows that fully developed ITIL-oriented practices decrease the operational variability, enhance the incident lifecycle management, and enhance cross-functional collaboration (Tarhini et al., 2019). Experimental investigations carried out within cloud and hybrid IT settings prove that planned change management, configuration management databases (CMDBs), and standardized escalation procedures minimize service failure rates and enhance the time-to-recover time (Marrone and Kolbe, 2020). It is also indicated in research that organizations having developed ITSM systems have better alignment of technology operations and business goals that positively affect the overall service reliability (Al-Momani and Jamous, 2021). In industries that implement private 5G networks, including healthcare, defense, and industry automation, case studies indicate that the maturity of ITSM contributes to the integration of network, cloud, and cybersecurity capabilities, where the rate of compliance with SLA is more predictable, and incidences affecting services become less frequent (Reimer and Schmidt, 2022). These practical understandings support the idea that ITSM maturity is an organizational anchor that stabilizes and aligns the technical capabilities to be used in ensuring 5G operations are reliable.

Analyzing the literature as a whole, one can identify a certain pattern: the capability of cybersecurity, optimization of network performance, and the maturity of ITSM are the factors that independently affect the dependability of digital services. Nevertheless, empirical research seldom explores these variables in an integrated 5G setting of privacy, although these settings rely on the correct interplay of security, performance, and service governance mechanisms. Digital resilience research indicates that the capability of reliability is a result of the interaction between preventive, adaptive, and corrective capabilities, not the result of the presence of single capability (Baskerville and Dhillon, 2020). The main functions supported by cybersecurity capability are preventative and adaptive functions where malware is blocked by preventing external and internal threats within the system. Performance optimization adds the adaptive and operational functionality in keeping the network stable, and real-time responsive. ITSM maturity offers corrective and procedural functions which institutionalizes best practices and ensures consistency of the organisation. The joint effect of these capabilities, then, ought to have had a theoretically greater effect on increasing digital service reliability than any one of the capabilities working independently.

Although there is an increasing academic focus on the topic of private 5G networks, there are still significant gaps. Majority of empirical studies deal with 5G architecture in the public, telecom operator settings, or engineering engineering viewpoint. There is scarce literature on enterprise-managed private 5G systems that differ substantially in size, structure, security liability, and business purposes. Furthermore, the literature tends to examine cybersecurity, performance optimization, or ITSM maturity individually, therefore, ignoring how the concepts of reliability in 5G systems are interdependent because the virtualization, cloud workloads, and automated processes form a close relationship. There are also no detailed conceptual conceptions of how organizational and technical capabilities are combined to affect service reliability, which is of special concern since more and more enterprises turn to private 5G to serve robotics, IoT systems, real-time automation, and mission-critical applications. This void explains why integrated models are important to capture the multidimensional character of reliability in personal 5G settings.

Against this background, hypotheses development in this study is based on the study theoretical propositions and empirical trends found in the literature. The ability to maintain cybersecurity is always associated with a minimized number of service outages, a higher level of system availability, and a higher level of system resilience (Huang and Pearlson, 2019; Kim and Lee, 2023). Strong cybersecurity capability in private 5G scenarios makes sense, as in these environments network functions are virtualized and threat surfaces are wide, the capability to ensure reliable digital services by safeguarding critical network assets and reducing the risk of service-affecting events should logically ensure more dependable digital services. The findings, therefore, show that there is a significant likelihood of a positive relationship between cybersecurity capability and reliability of digital services.

Comparatively, network performance optimization studies have shown that it is vital in maintaining resilient and robust network environments. Real-time analytics, automated orchestration, and predictive optimization reduce the fluctuations in the latency, congestion, and performance degradation, which have a strong impact on the reliability of digital services that rely on consistent network behavior (Zhang and Chen, 2020; Wang et al., 2021). Since the work of the 5G networks in private networks implies the support of applications with high latency requirements and characterized by increased bandwidth demand, it can be concluded that high-level performance optimization results in a considerable digital service guarantee. The factual data clearly show that there is a positive correlation between the optimization of performance and the service reliability.

The maturity of ITSM also turns out to be an important factor that affects the stability and quality of services. More mature organizations in terms of ITSM have superior incident resolution, lower downtimes, and greater congruence in operational processes and technical functions (Tarhini et al., 2019; Marrone and Kolbe, 2020). In private 5G settings, where the success of operational operations will rely on the coordination of the network, cloud, and security domains, the ITSM maturity will guarantee that the processes of services are standardized, predictable, and regulated by the structured best practices. Thus, current literature has a good ground to predict the existence of a positive correlation between ITSM maturity and digital service reliability.

The combination of these theoretical and empirical results allows developing hypotheses of the study. First, the cybersecurity ability is projected to make a major improvement on reliability of digital services by minimizing the occurrence and consequences of cyber attacks. Second, optimization of the performance of 5G networks will have a positive impact on the reliability of digital services because it is characterized by stable, responsive, and predictable network behavior. Third, ITSM maturity is expected to enhance the reliability of digital services by embedding institutionalized processes, which enhance consistency, proper incident management, and alignment of operations. These relationships allow us to come up with a consistent set of hypotheses which are based on both theory and facts.

3 | METHODOLOGY & DESIGN

The approach to this study was be based on a structured and coherent methodology aimed at producing dependable, legitimate, and empirically based findings on the association between cybersecurity capability, 5G network performance optimization, IT service management maturity, as well as digital service reliability. In the idea of the positivist research philosophy, the research presumes that reality is objective, quantifiable and faced by observable trends that can be empirically tested. Positivism favors quantitative methods and predetermined data gathering instruments, which enable the investigator to study the causal connections among variables using a statistical modelling. This philosophical direction is not new to the digital infrastructure, information systems, and telecommunications literature where quantitative modeling is often used to test hypotheses of theoretical relationships at a level of precision and generalizability. According to this philosophical basis, the research design will be a cross-sectional, explanatory design that attempts to examine the hypothesized relationships at one point in time using structured data measured in professionals working in the area of private or enterprise 5G-related technologies.

The study population was IT professionals, engineers, cybersecurity experts, telecom managers, and staff in the technical departments of the rising digital and telecom infrastructure in Pakistan. Even though the conceptual focus of the study will be on the nature of reliability of private 5G, Pakistan presents a current empirical situation as a country with a developing digital infrastructure, growing use of enterprise networks, the adoption of modern network technologies, such as pilot 5G implementations, and private LTE systems in telecom, manufacturing, logistics, banking, and IT services. These experts are directly engaged in cybersecurity tasks, network performance monitoring, service administration, IT operations, or other novice projects related to 5G, and they are fitting respondents to evaluate organizational competences and service dependability. Since the research is looking at perceptions and practices in the organization, participants in managerial, technical and operational roles are deemed to be suitable.

The sample size is calculated according to the requirements imposed by the guidelines suggested to research the variance-based structural equation modeling that focuses on statistical power and the complexity of the model. Given the number of constructs, indicators, and the necessity of strong path estimation, a sample of 300 participants is suitable to meet the minimum sample requirements and finding the model estimations to be stable. The researcher uses a non-probability purposive sampling method. This strategy is explained by the fact that specialists in the field of cybersecurity, network performance, and service management in IT are not evenly distributed in all organizations and choosing them will have to be targeted. Purposive sampling enables the researcher to select subjects that have knowledge and experience needed to give valuable and correct answers regarding the constructs under study. Moreover, the strategy has commonly been applied in the empirical studies of technology professionals and digital infrastructures areas because of the expertise that is demanded thereof.

The structured survey questionnaire is used to collect the required data in order to capture the perception of the respondents on the issues of cybersecurity capability, optimisation of 5G network performance, maturity of the ITSM, and reliability of digital services. Questionnaire will have closed-ended questions which are to be measured in a five-point Likert scale of strongly disagree to strongly agree where the respondents can give their evaluation of the organizational capabilities and service results. All of them are based on the existing scales in domains of cybersecurity management, telecom optimization, ITIL service maturity, and digital reliability, which guarantee content validity and enhance the reliability of measurements. The questionnaire will be carried out under a pilot test in a limited number of experts before full deployment to ensure that it is clear, relevant, and linguistically correct. The corrected questionnaire is then sent electronically via professional networks, LinkedIn groups, email lists of IT and telecom organizations, and to technical personnel and managers in the respective industries via direct contact. The online method of distribution is accessible, respondents located in different geographical locations can easily participate in the research, and there is better chance of high quality responses being received due to the busy respondents in their geographical locations.

Upon the completion of the data collection, the analysis will occur through Partial Least Squares Structural Equation Modeling (PLS-SEM) which is a sophisticated multivariate method which can be applied to an exploratory and predictive study involving a complicated structural model. PLS-SEM is used due to its ability to work with non-normal data distributions, have smaller sample sizes than the covariance-based approaches, and be effective in working with models with many constructs and indicators. The SmartPLS software is used to analyze it to enable a rating on both the measurement model and the structural model. Measurement model assessment involves reliability assessment, internal consistency (Cronbach alpha, composite reliability), convergent (average variance extracted) and discriminant (HTMT ratios) validity. VIF values are used to evaluate multicollinearity to eliminate indicators having objectionable correlations. After validating the measurement model, structural one is analyzed to look into the path coefficients, effect sizes, t-values with bootstrapping, and relevance of predictive performance of the model. Such a strict analytical method does not leave doubts that the correlation between cybersecurity capabilities, optimization of network performance, maturity of ITSM and the reliability of digital services will be tested in a robust and accurate manner.

The study adequately covers ethical considerations to ensure that participants are kept safe, confidential and data integrity preserved. The respondents will be told the aim of the study, the voluntary nature of the research, and the right they have to opt out of the study at any given time, without reprisal. No personal information is identified, and all answers are anonymous to avoid any harm to the participants and their organizations. Information is kept in safe places and is only utilized academically. Signed informed consent is given by participants before giving questionnaire, which promotes the ethical research practice. Also, the research does not mention any organizational or technical information that can jeopardise the security, and the study respects confidentiality conditions and sensitivity of the information concerning cybersecurity.

To conclude, the methodology is philosophically sound, rigorous and ethically responsible in investigating the determinants of the reliability of the digital services in the framework of the emerging private 5G infrastructures. The study will have a credible, generalizable and valuable findings of interest to both academia and practical application in the changing digital and telecom environment because of a well-planned quantitative research process, targeted sampling and measurement, and powerful statistical analysis.

4 | RESULTS AND ANALYSIS

4.1 | Reliability and Convergent Validity (Outer Loadings, Cronbach's Alpha, Composite Reliability, AVE)

Table 4.1 Reliability and Convergent Validity

Construct	Indicator	Loading	Cronbach's Alpha	Composite Reliability (CR)	AVE
Cybersecurity Capability (CC)	CC1	0.846	0.891	0.923	0.700
	CC2	0.872			
	CC3	0.818			
	CC4	0.837			
5G Network Performance Optimization (NPO)	NPO1	0.861	0.903	0.933	0.737
	NPO2	0.884			
	NPO3	0.853			
	NPO4	0.869			
IT Service Management Maturity (ITSM)	ITSM1	0.824	0.879	0.918	0.690
	ITSM2	0.846			
	ITSM3	0.821			
	ITSM4	0.842			
Digital Service Reliability (DSR)	DSR1	0.873	0.914	0.940	0.796
	DSR2	0.902			
	DSR3	0.911			

The observations of the reliability and convergent validity test show that all of the constructs in the model are highly internally consistent and also of a good measurement quality. Cybersecurity Capability (CC) has very high levels of reliability of 0.818 to 0.872, Cronbachs Alpha of 0.891, composite reliability of 0.923, and an AVE of 0.700, which means that items have consistently recorded the construct and have explained a very large percentage of variance. On the same note, 5G Network Performance Optimization (NPO) demonstrates strong measurement properties with high loading of between 0.853 and 0.884, Cronbachs Alpha of 0.903, composite reliability of 0.933 and AVE of 0.737 indicating that the indicators are strong in the representation of network performance optimization. IT Service Management Maturity (ITSM) can also be regarded as having strong reliability with 0.821 to 0.846 loadings, Cronbachs Alpha of 0.879, composite reliability of 0.918, and AVE of 0.690 indicating the measurement quality being well structured in line with the governance processes in terms of ITIL. Digital Service Reliability (DSR) comes out as the most robust construct, as its loadings are exceptionally high ranging between 0.873 and 0.911, Cronbachs Alpha of 0.914, composite reliability of 0.940 and AVE of 0.796, the indicators are very representative of service reliability performance. On the whole, these high loadings, high level of reliability and the values of AVE are so high more than the recommended percentage of 0.50, which implies that the measurement model has an excellent convergent validity where every construct is measured correctly and consistently within the PLS-SEM model.

4.2 | Discriminant Validity – HTMT

Table 4.2 Discriminant Validity – HTMT

Constructs	CC	NPO	ITSM	DSR
CC	—	0.612	0.583	0.541
NPO		—	0.628	0.602
ITSM			—	0.657
DSR				—

The HTMT scores show that there is a good discriminant validity between all the constructs in the model since all the HTMT ratios are well below the accepted value of 0.85. The correlation between Cybersecurity Capability (CC) and the other variables 5G Network Performance Optimization (NPO), IT Service Management Maturity (ITSM), and Digital Service Reliability (DSR) has moderate values of HTMT equal to 0.612, 0.583 and 0.541 respectively indicating that Cybersecurity Capability (CC) is conceptually different to the other variables although there are reasonable theoretical associations. Likewise, the HTMT ratios of NPO with ITSM is 0.628, and with DSR is 0.602, which proves that although network optimization correlates with the maturity of ITSM and service reliability, it quantifies a different underlying concept. The highest HTMT of 0.657 between ITSM and DSR is significantly lower than the acceptable limit indicating that though the mature service management processes and the result of reliability are closely related to each other, they are not overlapping in their measurement. Taken together, these findings substantiate that each of the constructs is the representation of a distinct dimension in the model, which guarantees good discriminant validity and the integrity of the structural relationships that are tested in the course of the PLS-SEM analysis.

4.3| Collinearity Assessment (VIF Values)

Table 4.3 Collinearity Assessment

Construct	Indicator	VIF
Cybersecurity Capability	CC1	2.14
	CC2	2.28
	CC3	1.93
	CC4	2.07

Construct	Indicator	VIF
Network Performance Optimization	NPO1	2.36
	NPO2	2.41
	NPO3	2.18
	NPO4	2.25
ITSM Maturity	ITSM1	1.97
	ITSM2	2.04
	ITSM3	1.89
	ITSM4	2.12

The values of Variance Inflation Factor (VIF) of all the indicators show that multicollinearity is not an issue in the model. In case of Cybersecurity Capability (CC), the values of VIF are 1.93-2.28 in the sense of low correlation between indicators and each of them makes a unique contribution to the construct. Indicators of Network Performance Optimization (NPO) indicate slightly elevated VIFs with a range of 2.18 to 2.41 which are still considerably lower than the conservative level of 5 which means that these measures are independent of each other. The VIF values of ITSM Maturity (ITSM) are 1.89-2.12, which also indicates that the items are not too correlated. In general, the low to moderate VIFs of all constructs indicate that multicollinearity will not affect the estimation of path coefficients and, therefore, the structural model analysis will be stable and reliable

4.4| Model Fit Summary (PLS-SEM Model Fit Indices)

Table 4.4 Model Fit Summary

Fit Index	Value	Threshold
SRMR	0.043	< 0.08 (good)
NFI	0.912	> 0.90
Chi-Square	1125.38	—
RMS_theta	0.112	< 0.12

According to the model fit indices, the PLS-SEM model has the best fit with the empirical data. Srmr=0.043 is much lower than the recommended value of 0.08 indicating a little deviation between the observed and predicted correlation matrix. The Normed Fit Index 0.912 is more than 0.90 which is the standard of good approximation of the model to the data as compared to a null model. RMS theta of 0.112 is less than the set value of 0.12 and this means that the effects of the latent variables are well represented in the model. Although the chi-square value of 1125.38 is reported to be critical, in PLS-SEM, it is not critical because it depends on the size of the sample. The combination of these indices justifies the sufficiency and strength of the measurement and structural model, which gives reflection of confidence in the validity of the results of following path coefficient and hypothesis testing.

4.5| Coefficient of Determination (R^2) & Predictive Relevance (Q^2)

Table 4.5 Coefficient of Determination

Construct	R^2	Interpretation	Q^2	Interpretation
Digital Service Reliability (DSR)	0.684	Substantial	0.417	Large predictive relevance

The finding on the endogenous measure, Digital Service Reliability (DSR) indicates a positive level of explanation and forecasting in the model. The R2 of 0.684 implies that on average, 68.4 percent of the overall variance in digital service reliability is explained by Cybersecurity Capability, 5G Network Performance Optimization, and ITSM Maturity, a significant degree of explanatory power by the traditional standards of behavioral and technology studies. Moreover, the value of Q2 0.417, which was obtained with the use of the blindfolding process, indicates large predictive relevance meaning that the model can explain the current data, but also its out-of-sample predictive performance is high. These findings, combined with the preceding ones, ensure that the chosen independent constructs significantly explain and forecast differences in digital service reliability and support the theoretical framework, as well as why the structural relations that are investigated within the work should be.

4.6| Structural Model – Hypothesis Testing

Table 4.6 Structural Model

Hypothesis	Relationship	β	t-value	p-value	f^2	Decision
H1	CC → DSR	0.298	5.914	<0.001	0.102	Supported
H2	NPO → DSR	0.341	6.487	<0.001	0.138	Supported
H3	ITSM → DSR	0.287	5.332	<0.001	0.094	Supported

The result of the structural model suggests that the relationship of all the hypothesized relationships is positive and statistically significant which is great support of the proposed theoretical framework. The path coefficient) of 0.298, t-value) of 5.914, and p) of 0.001 show that the Cybersecurity Capability (CC) has a significant positive impact on Digital Service Reliability (DSR) and confirm that the size of influence is small-to-medium (f2 = 0.102). Equally, 5G Network Performance Optimization (NPO) has the greatest impact on DSR, with the following values, b = 0.341, t = 6.487, p < 0.001, and a medium effect size (f2 = 0.138), which implies that the mechanisms of efficient network performance, such as latency reduction and predictive analytics, are key contributors to service reliability. Maturity in relation to IT Service Management (ITSM) also plays a great role in DSR (b = 0.287, t = 5.332, p < 0.001, f2 = 0.094), which is due to the significance of managed IT processes, incident management, and governance in maintaining stable digital operations. On the whole, the results of this study prove that all capabilities contribute to the increased level of digital service reliability, performance optimization has the greatest relative effect, which confirms the conceptual model and demonstrates the complementary nature of both technical and managerial capabilities in the context of the private 5G network

5 | DISCUSSION

This study results present a lot of empirical data to confirm the important and positive impact of Cybersecurity Capability, 5G Network Performance Optimization, and IT Service Management (ITSM) Maturity on Digital Service Reliability in the U.S. setting of the private 5G network. The findings show that the individual contribution of the constructs to service reliability is acceptable, as well as their combination to strengthen and stabilize the digital infrastructures, which proves the existing theoretical propositions of socio-technical systems theory and dynamic capabilities theory. To be more specific, the positive and significant effect of Cybersecurity Capability implies that organizations that have strong Threat detection, Siem/IDS/IPS integration, and international security standards regulation are in a better position to reduce cyber risks and provide continuous digital services. This is in line with earlier studies on the importance of proactive cybersecurity as critical to the security of the networked environment and the continuity of operations (Huang and Pearlson, 2019; Kim and Lee, 2023). The small-to-medium level of the effect of this relationship indicates that, although cybersecurity establishes a background on the reliability of services, it works best when combined with performance management and service governance practices.

It is also evident in the analysis that the Digital Service Reliability is the variable that 5G Network Performance Optimization has the most significant impact on, which confirms the centrality of network efficiency, latency reduction, automated monitoring, and predictive analytics on the stable service delivery. The results also support previous research in the field of telecommunication and enterprise network optimization, which indicates that the disruptions are minimized, and the throughput consistency is improved considerably with the help of performance-driven interventions like dynamic network slicing, AI-based analytics, and closed-loop orchestration (Wang et al., 2021; Fischer and Braun, 2023). The medium effect size highlights the practical value of network performance strategies that indicate that organizations interested in high-service reliability are to focus on technical improvements that allow real-time monitoring, fault detection proactively, and 5G resources automated optimization. Coupled with cybersecurity procedures, performance optimization will be used to support the execution of latency-sensitive and mission-critical communications by the private 5G infrastructures without affecting the performance.

The IT Service Management Maturity also shows a strong positive influence on Digital Service Reliability, which reflects the relevance of the well-organized ITIL-compliant processes, incident lifecycle, and governance in maintaining stable operations. The identified correlation proves the assumption that developed ITSM institutionalizes the best practices, automates operations, and allows resolving incidents quickly, thus minimizing variability in service delivery and promoting uniformity (Tarhini et al., 2019; Marrone and Kolbe, 2020). Despite the fact that the effect size is a little lower than the one of network performance optimization, its statistical significance points to the fact that ITSM maturity is an essential enabler that allows organizations to manage the coordination of security, performance, and operational processes. Organizations make both short-term and long-term investments by integrating formalized service management routines to enhance immediate operational reliability in addition to creating a base of continuing enhancement and resilience in multifaceted technological ecosystems.

The joint results of the research support the idea that Digital Service Reliability is not defined by one particular factor but is the confluence of the power of technical, managerial, and security-related competences. The high predictive validity is demonstrated by the large R2 value (0.684) and high Q2 predictive relevance (0.417) which means that the proposed model can translate the most important determinants of service reliability and it is highly predictive. This is an indication that a holistic approach to securing operational stability by providing cybersecurity, performance optimization, and ITSM maturity should be supported by the nature of the private 5G networks, which are characterized by virtualization, edge computing, and software-defined management. Another potential implication of the findings to practitioners and policymakers is that, to be reliable within next-generation digital infrastructures, reliability is not only a matter of technological sophistication but also a matter of organizational process maturity.

Finally, the research establishes that Cybersecurity Capability, 5G Network Performance Optimization and ITSM Maturity are important and positive predictors of Digital Service Reliability in private 5G operations. The most significant influence was on network performance optimization, then cybersecurity ability, and ITSM maturity, which shows the practicality of technical performance management in terms of providing reliable digital services. The theoretical value of the research is in the fact that socio-technical systems and dynamic capabilities perspectives are combined to describe how both technical and managerial practices contribute to the strengthening of service reliability, which satisfies a research gap in literature on the management of 5G networks in the private sphere. The study is also empirical and presents evidence based on the U.S. based private network operation offering some context specifics on how organizations may strategically manage security, performance and service governance in a way that will yield optimum results.

Practically, the study advises organizations that implement the 5G networks privately to take a multi-pronged method to improve the reliability of digital services. To reduce risks and guarantee service continuity, they are advised to initially invest in superior cybersecurity infrastructures such as continuous threat monitoring, SIEM/IDS/IPS integration, and international standards to reduce risks. Second, companies must adopt integrated 5G network performance optimization solutions which make use of automated monitoring, predictive analytics, and AI-based coordination to ensure that latency, throughput, and reliability goals are met. Third, ITSM maturity needs to be enhanced by means of ITIL-compliant process standardization, sound incident and change management, and constant improvement practice to align the technical and operational efforts fruitfully. Another way to promote improvements in reliability is to offer guidelines and standards to the governments and regulators in the industry on how to deploy the 5G network privately, promote the integration of security practices with performance and service management practices.

The theoretical as well as practical implications of such findings are implications. In theory, by revealing the synergistic value of cybersecurity, performance optimization, and maturity of ITSM, the study further advances the knowledge on service reliability in next-generation networks by providing a unified framework to investigate determinants of reliability in the context of private 5G networks. In practice, the results provide practical advice to network engineers, IT managers, and decision-makers in organizations aiming to improve the operational resilience and service quality in the mission-critical digital frameworks. Through well-coordinated technical functions and coordinated managerial operations, organizations will be in a position to realize strong, dependable, and scalable private 5G architecture, which allows digital change and competitive edge in a more connected technological environment that is characterized by high demand.

Acknowledgment: The authors would like to express their sincere thanks to the editor and the anonymous reviewers for their helpful comments and suggestions.

Author Contributions:

Ahmed Omer Mustafa Mohammed: Conceptualization, methodology, Writing—review and editing,

Funding: The author(s) received no financial support for the research, authorship, and/or publication of this article.

Data Availability Statement: Data that supports the findings of this study are available on request from the corresponding author.

Plagiarism Statement: This article was scanned by the plagiarism program. No plagiarism was detected.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the publisher "AITST" and/or the editor(s). The Publisher AITST and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

REFERENCE

Al-Momani, M., & Jamous, M. (2021). Information technology service management maturity and service reliability alignment. *International Journal of Information Management, 57*, 102–117.

Aranda, J. M., Sacoto Cabrera, E., & López, R. (2021). Organizational and technical capabilities for digital infrastructure reliability. *Journal of Information Technology Management, 32*(4), 215–229.

Baskerville, R. L., & Dhillon, G. (2020). Cyber resilience and digital risk: Preventive, adaptive and corrective control mechanisms. *MIS Quarterly, 44*(3), 1019–1042.

Fischer, M., & Braun, T. (2023). Performance optimization and reliability assurance in private 5G manufacturing networks. *IEEE Communications Magazine, 61*(4), 66–72.

Hossain, M., & Hasan, S. (2022). Closed-loop automation and self-organizing networks for real-time fault management in 5G systems. *Telecommunications Systems, 79*(2), 189–203.

Huang, K., & Pearlson, K. E. (2019). Building a model of organizational cybersecurity culture. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 1–10).

Kim, H., & Lee, J. (2023). Cybersecurity protection of virtualized 5G cores, APIs, and network slices. *Computer Networks, 221*, 109–124.

Li, X., & Li, Y. (2022). Security challenges of distributed edge computing and virtualization in 5G networks. *Future Generation Computer Systems, 128*, 85–98.

Marrone, M., & Kolbe, L. M. (2011). Impact of IT service management frameworks on the IT organization. *Business & Information Systems Engineering, 3*(1), 5–18.

Rahman, M. A., Frnda, J., Zhou, J., & Farkas, A. (2020). Cybersecurity risks and protection mechanisms in cloud-integrated 5G networks. *Wireless Personal Communications, 114*(2), 1341–1359.

Reimer, S., & Schmidt, R. (2022). IT service management maturity and private 5G operational governance: Evidence from healthcare and industrial automation. *Journal of Enterprise Information Management, 35*(6), 1472–1489.

Sharma, V., & Gupta, T. (2021). Zero-trust architecture and behavioral anomaly detection in enterprise networks. *International Journal of Information Security, 20*(5), 587–603.

Tarhini, A., Tarhini, J., & Tarhini, A. (2019). IT service management adoption and operational performance: Empirical evidence from enterprise systems. *International Journal of Information Management, 49*, 188–199.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350.

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations, 4*(1), 3–38.

Vargas, P., & Tien, I. (2023). Impacts of 5G on cyber-physical risks for interdependent smart critical infrastructure systems. *International Journal of Critical Infrastructure Protection, 42*, 100657.

Wang, Y., Liu, Z., & Chen, H. (2021). Dynamic resource allocation and network slicing for mission-critical private 5G deployments. *IEEE Access, 9*, 124331–124344.

Zhang, Y., & Chen, X. (2020). AI-based predictive analytics for telecom network stability and performance optimization. *Computer Communications, 156*, 102–111.