© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

An AI-Resilient Cybersecurity Framework for 5G Telecommunications Networks: Detecting Adversarial Machine Learning, Autonomous Intrusions, and Intelligent Edge Threats in Critical Infrastructure

KEN MUDZINGWA[1], STEWART MUNYARADZI NYAMUTSWA[2], ADMORE TAFADZWA MUGWADZI[3], PANASHE YOLANDA DHEGWA[4], MUNASHE NAPHTALI MUPA[5]

[1]*Yeshiva University, ORCiD: 0009-0005-1090-6492*

[2]*Yeshiva University, ORCiD: 0009-0009-2710-2617*

[3]*St Thomas University, ORCiD: 0009-0000-1501-0840*

[4]*University of Nevada Las Vegas, ORCiD: 0009-0002-3681-2804*

[5]*Hult International Business School, ORCiD: 0000-0003-3509-861X*

Abstract- ***Fifth-generation telecommunications networks are becoming a strategic layer of critical infrastructure because they connect public safety, financial systems, healthcare, logistics, energy, industrial control systems and intelligent edge services. The same characteristics that make 5G valuable - ultra-low latency, dense device connectivity, software-defined network functions, network slicing, cloud-native service-based architecture and edge computing - also create an expanded attack surface for adversaries using artificial intelligence. This paper develops an AI-resilient cybersecurity framework for 5G telecommunications networks by integrating 5G security literature, adversarial machine learning research, zero-trust architecture, AI risk management and empirical cyber-incident analytics. The empirical component uses the Kaggle Global Cybersecurity Threats (2015-2024) dataset, comprising 3,000 incident records across 10 countries, 7 industries and 6 attack categories, to model sectoral exposure, telecommunications-specific risk, loss severity and incident-resolution burden. The sample records USD 151.48 billion in aggregate estimated financial loss, 1.51 billion affected-user records and a mean resolution time of 36.48 hours. Telecommunications incidents account for 403 records and USD 20,459.09 million in estimated loss, with man-in-the-middle, DDoS, phishing and malware attacks showing elevated relevance for AI-enabled 5G threat scenarios. Heat-map analysis identifies telecommunications man-in-the-middle attacks as one of the highest AI-5G exposure cells, while random-forest triage demonstrates that affected-user scale, resolution time, year and the constructed AI-5G Exposure Index are the strongest predictors of high-impact incidents in the analytical design. The paper contributes a practical AI-Resilient 5G Cybersecurity Framework built around adversarially robust intrusion detection, zero-trust identity, slice isolation, secure edge orchestration, model-risk governance, threat-informed vulnerability prioritisation, incident-response automation, post-quantum crypto-agility and continuous assurance. The central finding is that 5G security cannot be reduced to conventional perimeter defence; it requires a converged operating model that secures networks, data, machine-learning pipelines, identities, cloud-native functions and critical service continuity together.***

Keywords: ***5G security; telecommunications; adversarial machine learning; AI-enabled cyber threats; critical infrastructure; intelligent edge; network slicing; zero trust; intrusion detection; post-quantum cryptography.***

I. INTRODUCTION

The security of next-generation telecommunications networks is now inseparable from the security of critical infrastructure. 5G networks are not merely faster mobile networks; they are programmable, virtualised, cloud-native and increasingly integrated with industrial automation, emergency communications, connected health, financial services, intelligent transport, energy management and defence-adjacent systems. The International

Telecommunication Union describes 5G as a networked environment connecting people, things, data, applications, transport systems and cities while processing large volumes of data with minimal delay (ITU, 2024). This combination of density, latency sensitivity and societal dependence makes 5G a high-consequence cyber target.

The threat environment is also changing. Artificial intelligence is improving the defender's ability to detect anomalies, triage alerts and automate incident response, but it is simultaneously strengthening the attacker's ability to conduct reconnaissance, generate phishing content, automate vulnerability discovery, evade machine-learning detectors, poison training data, spoof radio-frequency patterns and coordinate botnet activity at machine speed. Sagduyu, Erpek and Shi (2021) argue that 5G systems using machine learning for spectrum awareness and physical-layer authentication introduce an adversarial attack surface where inputs can be manipulated to mislead classifiers. Usama et al. (2020) similarly warn that 5G automation must be examined through an adversarial lens because machine-learning-enabled control and optimisation create new modes of attack and failure.

The research problem addressed in this paper is therefore not whether 5G telecommunications networks need cybersecurity; that is already settled. The central problem is how to make 5G cybersecurity resilient against AI-enabled and AI-targeting threats while keeping critical services operational. Conventional controls such as firewalls, endpoint protection and signature-based intrusion detection remain useful, but they are not sufficient where adversaries can use AI to generate novel variants, overwhelm alert queues, manipulate model inputs or exploit weak identity, edge and cloud configurations.
This paper proposes an AI-resilient cybersecurity framework for 5G telecommunications networks. It combines literature-based analysis with empirical incident analytics to identify risk patterns relevant to 5G critical infrastructure. It uses a Kaggle cybersecurity dataset for quantitative modelling and positions the results alongside 5G-specific datasets and scholarship such as 5G-NIDD, which was generated on a functional 5G test network for AI/ML-based intrusion-detection research (Samarakoon et al., 2022; Siriwardhana et al., 2025). The outcome is an applied framework suitable for telecom operators, cloud-edge providers, critical-infrastructure organisations and cybersecurity practitioners.

II. RESEARCH AIM, QUESTIONS AND CONTRIBUTION

The aim of the study is to design and empirically support an AI-resilient cybersecurity framework for 5G telecommunications networks that can detect, prioritise and mitigate adversarial machine-learning attacks, autonomous intrusions and intelligent edge threats in critical-infrastructure environments.

The study is guided by five research questions:

1. What are the principal AI-enabled and AI-targeting threat vectors affecting 5G telecommunications networks?
2. Which cyber-incident patterns in public data are most relevant to telecommunications and 5G critical infrastructure?
3. How can telecommunications-sector incident data be translated into a practical AI-5G exposure and resilience-priority model?
4. What architecture should govern adversarially robust detection, zero-trust access, edge hardening, slice isolation and recovery engineering?
5. How can post-quantum crypto-agility and AI model-risk governance be integrated into 5G security operations?

The contribution is threefold. First, the paper consolidates 5G, adversarial machine learning and critical-infrastructure cybersecurity scholarship into a single threat model. Second, it provides a replicable data-analysis workflow using public Kaggle incident data, including tables, heat maps, statistical tests and machine-learning triage. Third, it proposes a structured framework that translates the analysis into implementable controls for critical 5G and edge environments.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

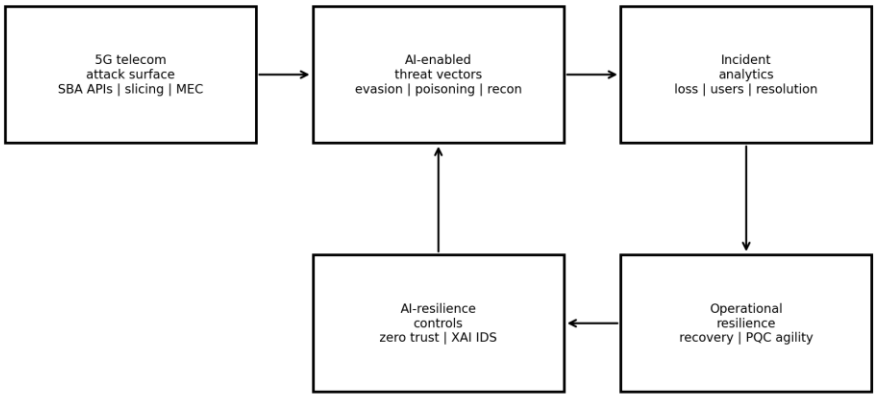

Figure 1. Research architecture linking 5G attack surface, AI-enabled threats, incident analytics and resilience controls.

III. LITERATURE REVIEW

3.1 5G telecommunications as critical infrastructure

5G security must be understood as a critical-infrastructure problem because 5G networks support services that extend beyond consumer connectivity. Their service-based architecture, virtual network functions, software-defined networking, multi-access edge computing and network slicing make them suitable for industrial automation, smart cities, connected vehicles, telemedicine and public safety. Barakabitze et al. (2020) emphasise that network slicing depends on SDN, NFV, MEC and cloud/fog computing, creating flexible service delivery but also introducing new management and orchestration challenges. Khan et al. (2020) show that 5G security and privacy require attention to network softwarisation, physical-layer security, privacy, monitoring and standards-based controls.

Network slicing is particularly important. A slice can be engineered to support different service-level requirements such as ultra-reliable low-latency communications, enhanced mobile broadband or massive machine-type communications. De Alwis et al. (2024) show that network slicing creates security scenarios specific to slice-enabled networks, including isolation failures, cross-slice resource abuse, orchestration compromise and multi-tenant privacy risks. In a critical-infrastructure context, a compromised slice supporting emergency services or industrial control may have consequences far beyond ordinary consumer service disruption.

3.2 AI-enabled and AI-targeting threats

The term AI-enabled threat refers to the use of artificial intelligence by adversaries to increase the speed, scale, stealth, personalisation or autonomy of attacks. Examples include generative phishing, automated malware mutation, synthetic-identity attacks, vulnerability discovery, adaptive botnets, reinforcement-learning-based evasion and deepfake-enabled social engineering against network operations personnel. The term AI-targeting threat refers to attacks against the models and data pipelines used by defenders, such as evasion, poisoning, backdoors, model extraction, membership inference and data manipulation.

NIST's adversarial machine-learning taxonomy places these concerns within a formal vocabulary of attacks and mitigations and links them to AI system security, resilience and robustness (NIST, 2025). The CSET workshop report by Musser et al. (2023)

similarly argues that AI vulnerabilities differ from ordinary software vulnerabilities and require security processes that cover the full AI lifecycle. For 5G, this matters because machine-learning systems may be embedded in spectrum sensing, authentication, network optimisation, anomaly detection, resource allocation, fraud detection and incident triage.

Sagduyu, Erpek and Shi (2021) demonstrate how adversarial attacks can manipulate 5G systems that rely on learning-based spectrum sensing or physical-layer authentication. Usama et al. (2020) provide a cautionary perspective on the broad adversarial dimension of machine learning in 5G and beyond. These studies show that 5G cybersecurity must secure not only packets, devices and interfaces but also the learning systems that increasingly interpret and manage them.

3.3 Intrusion detection and 5G datasets

AI-based intrusion detection is a central line of research for 5G networks because conventional signature-based detection cannot reliably identify novel or rapidly mutating attacks. Li, Zhao and Li (2017) proposed an intelligent intrusion-detection system for software-defined 5G networks, using centralised visibility and machine learning to detect unknown intrusions. Samarakoon et al. (2022) introduced 5G-NIDD, a fully labelled dataset built on a functional 5G test network, enabling the testing of AI/ML intrusion-detection models. Later work using 5G-NIDD has reported strong results for classification and visualisation, including PCA, t-SNE and UMAP analysis and detection metrics such as KNN accuracy of 97.2% in Ghani, Salekzamankhani and Virdee (2023).

The present paper does not claim to reproduce packet-flow experiments on 5G-NIDD because the analytical objective is different. 5G-NIDD is a flow-level benchmark for 5G intrusion-detection models, whereas the Kaggle Global Cybersecurity Threats dataset used here is an incident-impact dataset. The value of the latter is that it allows sectoral analysis of financial loss, affected users, incident-resolution time, vulnerability type, attack source and defence mechanism. Together, these datasets represent two complementary levels: packet-level detection and enterprise-impact prioritisation.

3.4 Zero trust, AI risk management and post-quantum readiness

Zero trust is necessary for 5G critical infrastructure because location-based trust assumptions collapse in cloud-native and edge-distributed networks. NIST SP 800-207 defines zero trust as a shift away from static network perimeters toward users, assets and resources, with no implicit trust granted solely because an asset is inside a network boundary (Rose et al., 2020). For 5G, this implies continuous authentication, least privilege, workload identity, device posture checks, microsegmentation and policy enforcement close to resources.

The NIST AI Risk Management Framework adds another layer by requiring governance, mapping, measurement and management of AI risks across the AI lifecycle (NIST, 2023). In the 5G security context, this means maintaining inventories of security models, testing robustness against adversarial examples, governing training data, documenting model limitations, monitoring drift, and ensuring that AI-generated recommendations remain explainable to analysts.

Post-quantum readiness is also relevant because 5G and edge devices may have long operational lifespans. NIST finalised its initial post-quantum cryptography standards in 2024, including ML-KEM, ML-DSA and SLH-DSA (NIST, 2024a; NIST, 2024b; NIST, 2024c). Critical 5G environments should therefore build crypto-agility now, particularly for identity, key exchange, device provisioning, SIM/eSIM security, certificates, secure boot and long-term data confidentiality.

3.5 Related work from the author's research profile

This manuscript also draws from the broader research profile of Munashe Naphtali Mupa, particularly work on 5G security, critical-infrastructure cybersecurity, AI operationalisation, governance-driven security automation and explainable vulnerability prioritisation. The ResearchGate and Google Scholar profiles list relevant publications such as Network Security in 5G - Threats, Vulnerabilities and

Mitigation Strategies; Cybersecurity of Critical Infrastructures: Challenges and Future Perspectives; Governance-Driven Security Automation for Municipal and SMB Cloud Modernization; and Explainable Risk-Based Vulnerability Prioritization in Hybrid Cloud (Chisora et al., 2026; Nemure et al., 2026; Agyei et al., 2026a; Agyei et al., 2026b). These works support the practical orientation of the present framework, especially its emphasis on governance, risk scoring, AI-assisted detection, critical-infrastructure resilience and vulnerability prioritisation.

IV. METHODOLOGY

4.1 Research design

The study uses a mixed conceptual-empirical design. The conceptual layer synthesises 5G security, adversarial machine learning, zero trust, AI governance and post-quantum security literature. The empirical layer uses a public incident dataset to quantify cyber-risk patterns and generate heat maps, descriptive statistics, non-parametric tests and a machine-learning triage model. The purpose is not to estimate national breach totals, but to demonstrate a defensible analytical method for ranking 5G-related cyber risk and translating it into controls.

4.2 Dataset selection and scope

A search of Kaggle identified two relevant data sources: the 5G-NIDD listing, which is a 5G-specific network intrusion dataset, and the Global Cybersecurity Threats (2015-2024) dataset. The empirical analysis uses the latter because it contains incident-level impact variables suitable for sectoral and economic analysis, including country, year, attack type, target industry, estimated financial loss, affected users, attack source, vulnerability type, defence mechanism and incident-resolution time. The 5G-NIDD dataset is used in the literature discussion as the flow-level benchmark most directly connected to 5G intrusion detection (Kaggle, 2025a; Kaggle, 2025b; Samarakoon et al., 2022).

Table 1. Dataset variables and analytical relevance to AI-resilient 5G cybersecurity

Variable	Analytical use	5G relevance
Country	Geographic comparison and heat-map grouping	Contextual exposure indicator
Year	Time trend analysis from 2015 to 2024	Temporal signal for evolving threats
Attack Type	DDoS, phishing, ransomware, malware, SQL injection and man-in-the-middle	Threat scenario classification
Target Industry	Telecommunications and other critical sectors	Sectoral criticality indicator
Financial Loss	Estimated loss in USD million	Economic impact
Affected Users	Number of affected-user records	Population-scale impact
Attack Source	Nation-state, insider, hacker group or unknown	Adversary capability proxy
Security Vulnerability Type	Zero-day, weak password, social engineering or unpatched software	Control weakness proxy
Defense Mechanism Used	Firewall, VPN, encryption, antivirus or AI-based detection	Defensive posture proxy
Incident Resolution Time	Hours to resolve incident	Operational resilience indicator

4.3 Constructed indices and analytical procedures

Three indices were constructed. First, a Composite Impact Score was calculated as a weighted standardised score: 45% financial loss, 35% affected users and 20% incident-resolution time. Second, an AI-5G Exposure Index was built as a transparent rule-based score that assigns higher exposure to telecommunications incidents, attack types likely to be amplified by AI, higher-capability sources, exploit-prone vulnerability classes and AI-contested defensive environments. Third, an AI-Resilience Priority Score combines the normalised Composite

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

Impact Score and AI-5G Exposure Index at 60% and 40%, respectively. These indices are not causal estimates; they are prioritisation tools designed for governance and triage.

The analysis includes descriptive statistics, sector and attack summaries, telecommunications-specific analysis, heat maps, Kruskal-Wallis tests for loss differences across categories, a chi-square test for attack-sector dependence, Spearman correlations and a random-forest classifier for high-impact incident triage. Random forests were used because they can handle non-linear interactions among categorical and numerical predictors after one-hot encoding and provide interpretable feature importance for governance discussion.

V. RESULTS AND DATA ANALYSIS

5.1 Dataset overview

Table 2. Overall descriptive profile of the Kaggle incident dataset

Metric	Value
Incident records	3,000
Countries	10
Industries	7
Attack types	6
Total estimated loss (USD million)	151,478.91
Mean loss per incident (USD million)	50.49
Affected-user records	1,514,052,409
Mean resolution time (hours)	36.48
Telecommunications incidents	403

The dataset contains 3,000 records and permits a structured view of incident burden across sectors. Telecommunications accounts for 403 records, with an aggregate estimated financial loss of USD 20,459.09 million and 199,567,110 affected-user records. The mean telecommunications resolution time is 37.06 hours, slightly above the full-sample mean of 36.48 hours.

5.2 Sectoral and attack-type distribution

Table 3. Sector-level incident impact and AI-5G exposure

Target Industry	Incidents	Total loss USD m	Mean loss USD m	Mean affected users	Mean resolution hours	Mean AI 5G Exposure Index
IT	478	24,809.83	51.90	523,210.94	36.17	41.30
Government	403	21,205.33	52.62	499,352.43	37.59	40.48
Banking	445	22,772.39	51.17	505,839.11	35.74	41.54
Telecommunications	403	20,459.09	50.77	495,203.75	37.06	71.15
Retail	423	21,119.55	49.93	488,833.06	37.22	42.02
Healthcare	429	21,041.29	49.05	504,130.34	35.81	40.44
Education	419	20,071.43	47.90	513,137.79	35.91	41.40

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

Table 4. Attack-type impact profile in the full analytical sample

Attack Type	Incidents	Total loss USD m	Mean loss USD m	Mean affected users	Mean resolution hours	Mean AI 5G Exposure Index
DDoS	531	27,630.92	52.04	499,437.41	35.69	53.48
Phishing	529	26,693.29	50.46	487,179.54	35.91	51.77
SQL Injection	503	25,156.56	50.01	512,469.83	36.91	30.56
Ransomware	493	24,479.32	49.65	502,825.37	36.53	29.91
Malware	485	23,967.95	49.42	508,780.23	37.07	53.79
Man-in-the-Middle	459	23,550.87	51.31	520,064.32	36.87	51.63

DDoS and phishing are the most frequent attack types in the sample, while man-in-the-middle attacks show the highest mean loss among attack categories. These patterns are particularly relevant to 5G because DDoS can disrupt availability, phishing and deepfakes can compromise privileged telecom operators, malware can affect edge nodes and orchestration systems, and man-in-the-middle attacks threaten confidentiality and integrity across distributed networks.

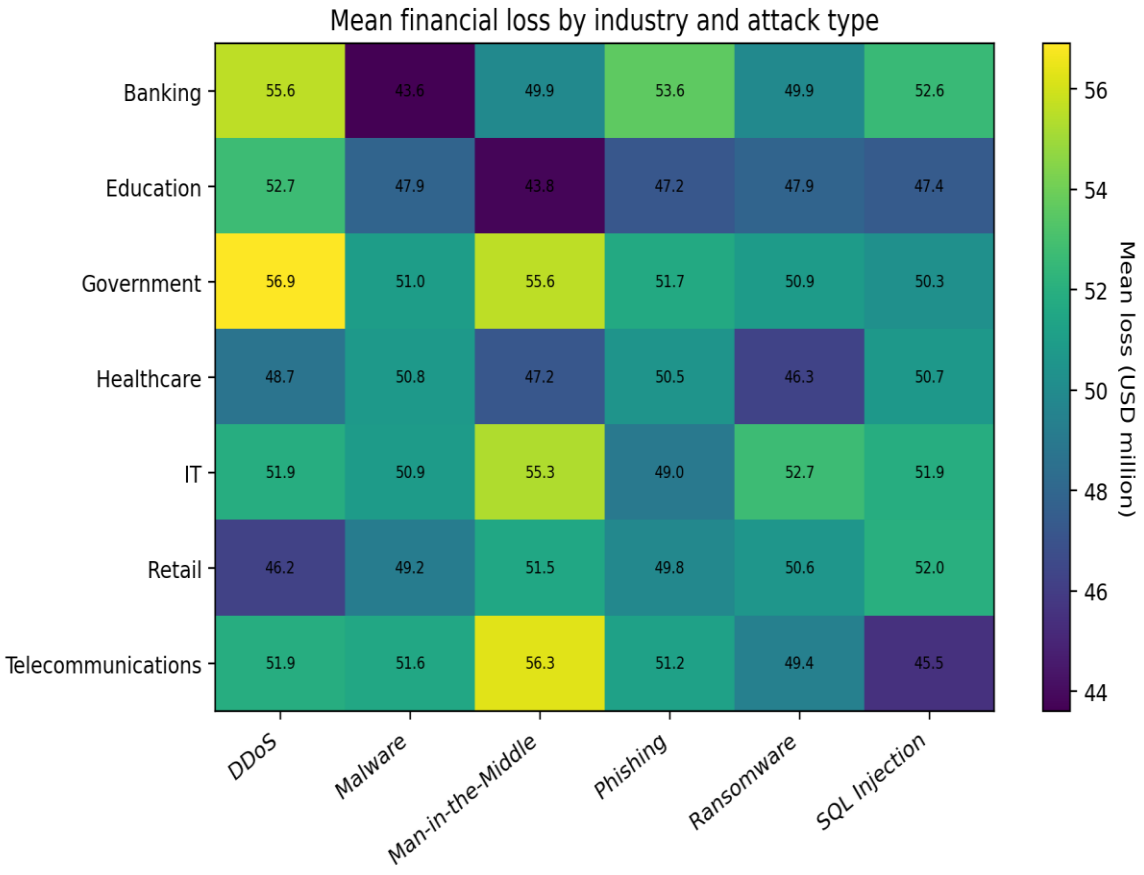

Figure 2. Heat map of mean financial loss by industry and attack type.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

5.3 Telecommunications-sector analysis

Table 5. Telecommunications-sector attack profile and AI-resilience priority

Attack Type	Incidents	Total loss USD m	Mean loss USD m	Mean affected users	Mean resolution hours	Mean AI 5G Exposure Index	Mean AI resilience priority
Man-in-the-Middle	56	3,150.10	56.25	517,250.43	34.59	77.93	63.33
Phishing	51	2,613.40	51.24	507,897.86	35.08	81.18	62.98
DDoS	85	4,410.58	51.89	492,486.65	36.73	80.28	62.77
Malware	74	3,819.35	51.61	467,132.93	36.88	78.81	61.53
Ransomware	59	2,915.85	49.42	450,203.71	38.37	56.71	51.91
SQL Injection	78	3,549.81	45.51	534,706.08	39.68	53.44	51.64

The telecommunications subset shows that man-in-the-middle incidents have the highest mean loss at USD 56.25 million and the highest mean composite impact among telecommunications attack categories. DDoS has the largest number of telecommunications incident records, which is consistent with the centrality of availability in telecom service continuity. The AI-5G Exposure Index assigns elevated scores to telecommunications DDoS, phishing, malware and man-in-the-middle scenarios because these attack families are susceptible to automation, evasion, credential compromise and adversarial manipulation.

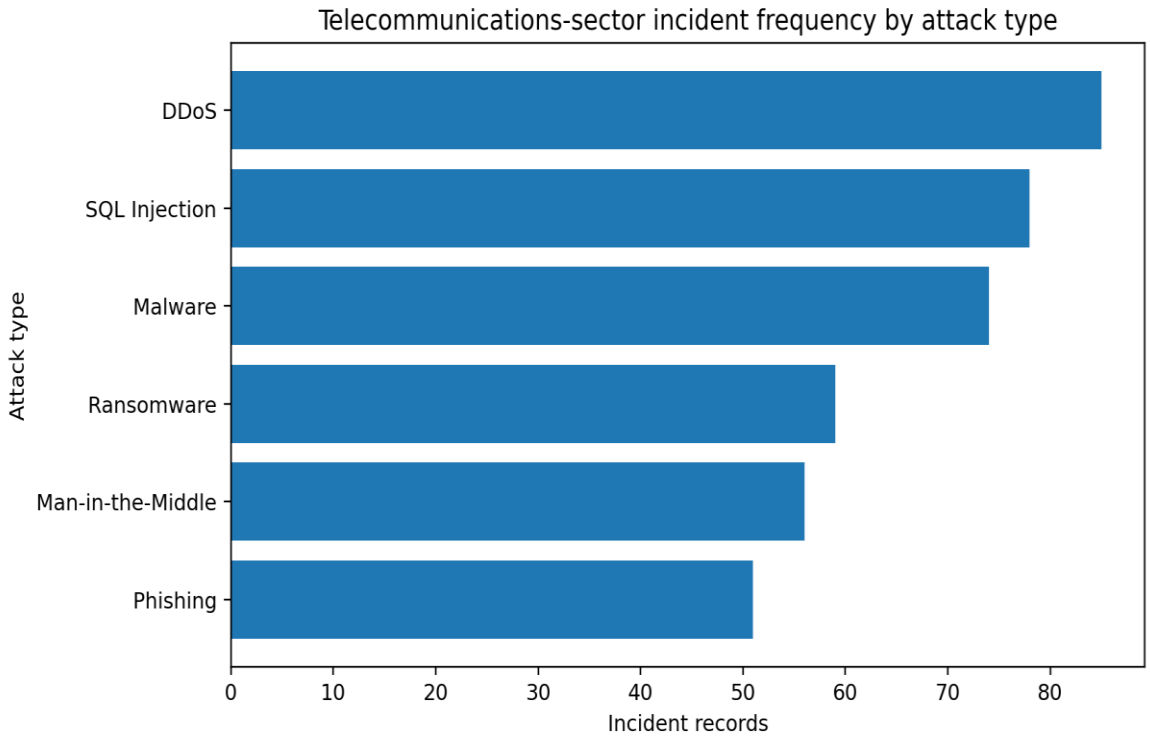

Figure 3. Telecommunications-sector incident frequency by attack type.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

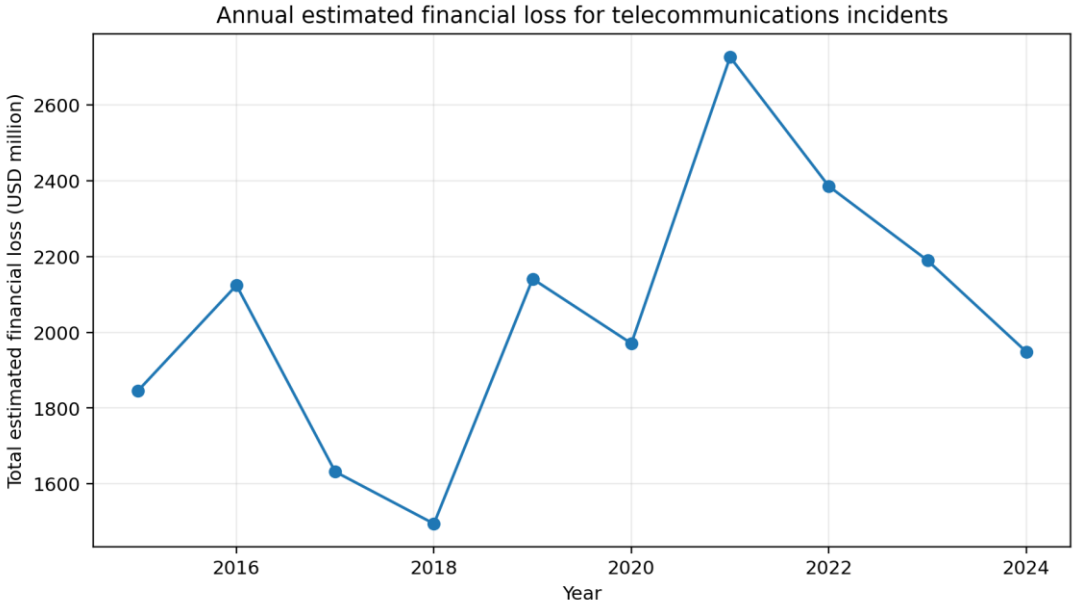

Figure 4. Annual estimated telecommunications financial loss in the analytical sample.

5.4 AI-5G exposure and resilience-priority heat maps

Heat-map analysis is useful because 5G cyber risk is not evenly distributed across all sectors and attack types. The AI-5G Exposure Index is expectedly highest in telecommunications cells and particularly elevated where the attack type is DDoS, phishing, malware or man-in-the-middle. The AI-Resilience Priority Score then combines this exposure with measured impact. This distinction matters operationally: a high-exposure cell may require model hardening and monitoring, whereas a high-priority cell requires board-level control validation, incident simulation and resilience investment.

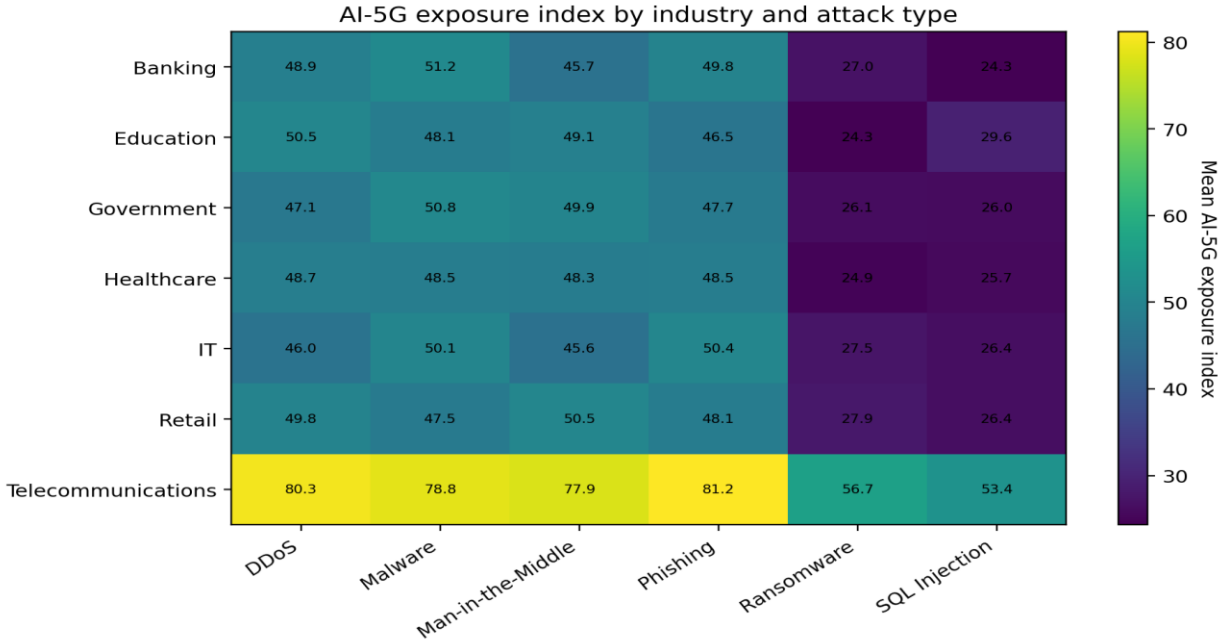

Figure 5. Heat map of AI-5G exposure index by industry and attack type.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

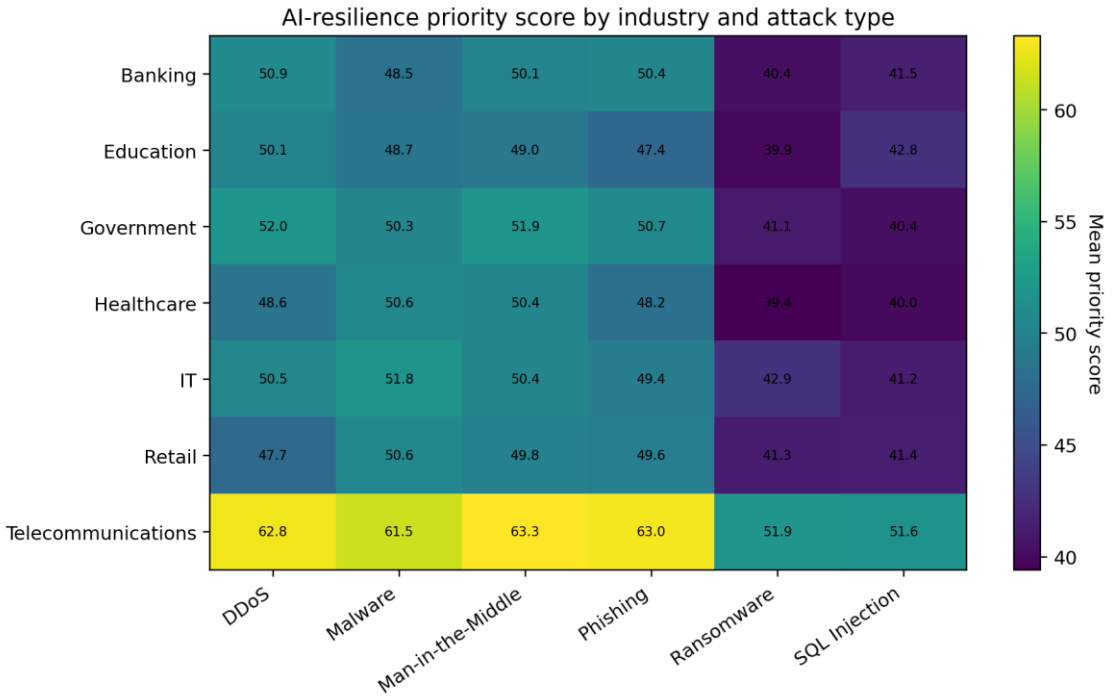

Figure 6. Heat map of AI-resilience priority score by industry and attack type.

Table 6. Top sector-attack cells by AI-resilience priority score

Target Industry	Attack Type	Incidents	Mean loss USD m	Mean affected users	Mean resolution hours	Mean AI 5G Exposure Index	Mean AI resilience priority
Telecommunications	Man-in-the-Middle	56	56.25	517,250.43	34.59	77.93	63.33
Telecommunications	Phishing	51	51.24	507,897.86	35.08	81.18	62.98
Telecommunications	DDoS	85	51.89	492,486.65	36.73	80.28	62.77
Telecommunications	Malware	74	51.61	467,132.93	36.88	78.81	61.53
Government	DDoS	71	56.92	511,390.24	39.37	47.07	51.96
Telecommunications	Ransomware	59	49.42	450,203.71	38.37	56.71	51.91
Government	Man-in-the-Middle	53	55.61	492,063.55	37.42	49.92	51.88
IT	Malware	67	50.92	540,373.01	38.34	50.06	51.82
Telecommunications	SQL Injection	78	45.51	534,706.08	39.68	53.44	51.64
Banking	DDoS	71	55.56	516,340.01	31.18	48.93	50.86
Government	Phishing	68	51.71	514,186.68	39.34	47.71	50.69
Healthcare	Malware	81	50.79	524,813.59	37.37	48.52	50.61

5.5 Vulnerability, defence mechanism and country-level heat maps

The vulnerability-defence heat map shows differences in mean incident-resolution time across vulnerability and defence-mechanism combinations. Although the dataset does not reveal control maturity or incident complexity, longer resolution-time cells should be treated as candidates for deeper root-cause

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

analysis. In 5G environments, long resolution times may indicate inadequate telemetry, poor ownership between network and cloud teams, limited automation, unclear vendor accountability or insufficient runbook maturity.

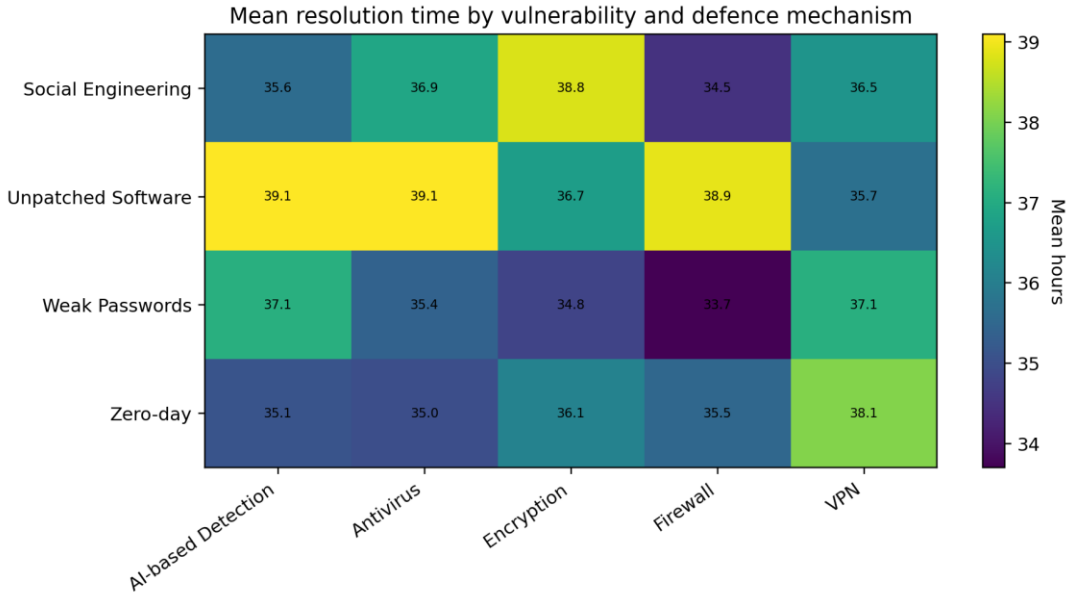

Figure 7. Heat map of mean resolution time by vulnerability type and defence mechanism.

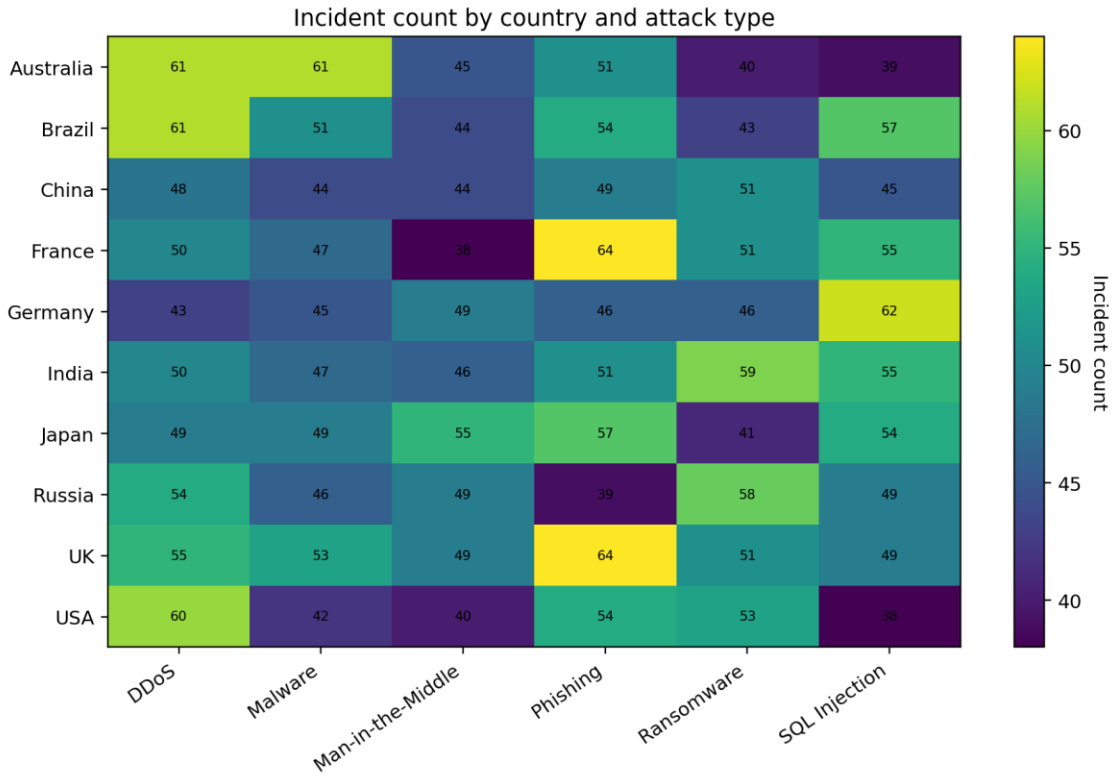

Figure 8. Heat map of incident counts by country and attack type.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

5.6 Statistical tests and model results

Table 7. Non-parametric tests for attack-sector dependence and loss distribution differences

Grouping variable	Kruskal-Wallis H	p-value	Interpretation
Attack Type x Target Industry	38.4550	0.1384	No statistically significant attack-sector dependence
Target Industry	8.1700	0.2259	No statistically significant difference in loss distributions
Attack Type	3.1910	0.6705	No statistically significant difference in loss distributions
Attack Source	4.2180	0.2388	No statistically significant difference in loss distributions
Security Vulnerability Type	0.2750	0.9646	No statistically significant difference in loss distributions
Defense Mechanism Used	1.6190	0.8054	No statistically significant difference in loss distributions

Table 8. Spearman correlations with estimated financial loss

Variable correlated with financial loss	Spearman rho	p-value
Number of Affected Users	0.0017	0.9244
Incident Resolution Time (in Hours)	-0.0127	0.4853
Year	0.0106	0.5631
AI-5G Exposure Index	0.0183	0.3151

The chi-square test does not show statistically significant attack-sector dependence at the 5% level in this sample. Kruskal-Wallis tests also do not show statistically significant differences in financial-loss distributions across industry, attack type, attack source, vulnerability type or defence mechanism. This finding should not be interpreted as proof that these factors do not matter in real incidents. Rather, it suggests that the dataset lacks important explanatory variables, such as asset criticality, control maturity, cloud architecture, privileged-access exposure, vendor dependency, insurance effects, public disclosure rules and regulatory penalties. For governance purposes, this is a critical insight: high-quality cyber-risk prioritisation requires asset and control context, not threat labels alone.

Table 9. High-impact incident triage model performance

Metric	Value
Train/test split	75% / 25% stratified
Algorithm	Random Forest Classifier
Target	High-impact quartile of composite impact score
ROC-AUC	0.8000
Accuracy	0.7707
F1-score	0.5249
Confusion matrix [[TN, FP], [FN, TP]]	[[483, 80], [92, 95]]

The random-forest triage model achieves ROC-AUC of 0.800, accuracy of 0.771 and F1-score of 0.525. Affected-user scale and resolution time dominate feature importance because the target is a composite

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

impact measure that includes these variables. The AI-5G Exposure Index appears among the top features, supporting its use as a governance signal rather than as a stand-alone loss predictor.

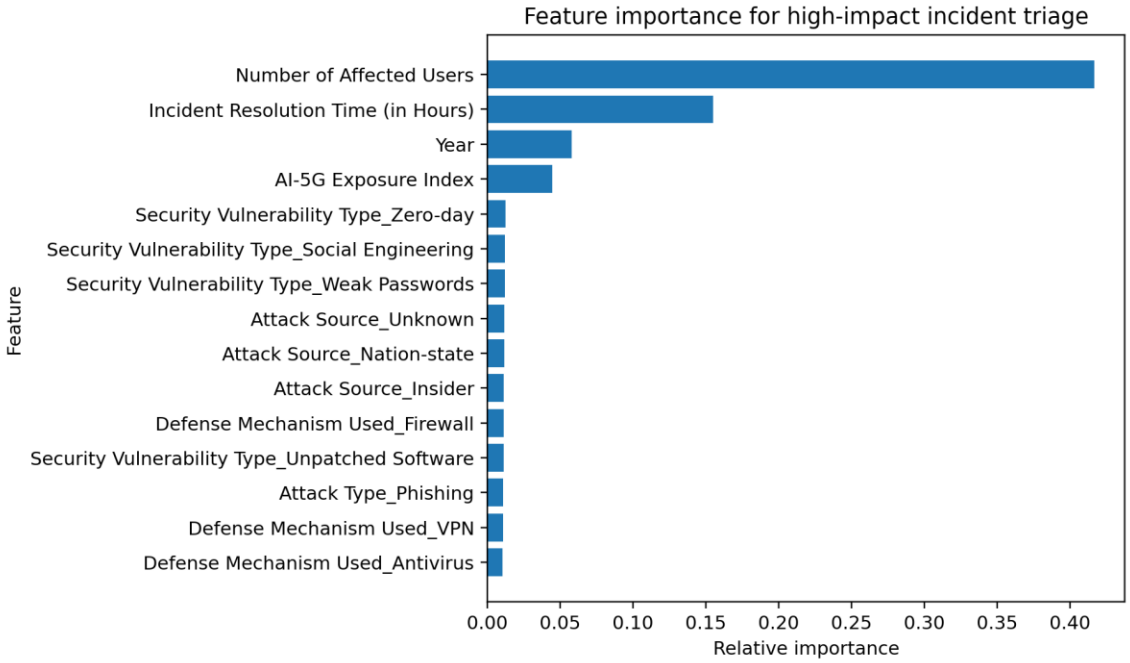

Figure 9. Feature importance for high-impact incident triage model.

VI. DISCUSSION

6.1 What the data imply for AI-resilient 5G security

The empirical analysis supports four practical conclusions. First, telecommunications risk is not limited to one attack category. DDoS, man-in-the-middle, phishing and malware each map to distinct 5G failure modes: availability loss, confidentiality breach, privileged-user compromise and edge/cloud workload compromise. Second, financial loss alone is an inadequate control target because critical-infrastructure risk also includes public trust, service continuity, safety, affected-user scale and incident-resolution time. Third, threat labels do not explain impact without asset context. A ransomware attack on a non-critical test environment is not equivalent to a ransomware attack affecting a network operations centre, subscriber identity system or public-safety slice. Fourth, AI-resilient security must govern both attacker AI and defender AI.

For 5G telecommunications networks, the most consequential insight is that AI-enabled threats target the seams between systems: identity and access, API orchestration, edge nodes, model pipelines, telemetry, network slices and human operators. A zero-day vulnerability matters more when it touches a high-criticality network function; phishing matters more when it compromises a privileged orchestration engineer; an adversarial example matters more when it blinds an intrusion-detection model protecting a critical slice.

6.2 Adversarial machine learning as a control-plane risk

Machine-learning models used in 5G security operations can become part of the control plane. If a model ranks alerts, tunes radio resources, detects anomalies, authenticates devices or recommends containment actions, compromising the model's inputs, training data or decision boundary can become a route to operational disruption. This is why adversarial robustness must be treated as a security requirement. Defensive controls should include adversarial testing, drift monitoring, data lineage, model access control, model cards, anomaly explanations, challenger models, human approval for

high-impact automated actions and red-team exercises against AI components.

Table 10. AI-enabled and AI-targeting threat matrix for 5G telecommunications networks

Threat vector	Attack mechanism	5G impact	Recommended control
Evasion attacks against IDS	Adversarial traffic perturbations cause benign classification	Blind spots in detection; delayed containment	Adversarial training; ensemble detection; robust feature engineering; analyst review
Data poisoning	Compromised telemetry or labelled data contaminates training	Model learns attacker-preferred behaviour	Data provenance; quarantine of suspicious labels; training-set integrity checks
Model extraction and inference	Adversary probes API or SOC tooling to infer model behaviour	Circumvention of detection thresholds	Rate limiting; API monitoring; output restriction; watermarking and audit logs
Autonomous reconnaissance	AI agents map exposed telecom APIs, edge services and identities	Faster vulnerability discovery and attack chaining	Attack-surface management; deception; continuous external scanning; least privilege
Deepfake/social engineering	Synthetic voice/video targets network operations or executives	Privileged access compromise and fraudulent change approval	Out-of-band verification; phishing-resistant MFA; approval workflows
RF and physical-layer spoofing	Generated signals mimic legitimate devices or confuse spectrum models	Authentication failure; jamming; network-slice compromise	Signal authentication; multi-factor device identity; RF anomaly detection
SOC copilot manipulation	Prompt injection or malicious context alters AI assistant output	Faulty triage or unsafe response guidance	Prompt hardening; tool isolation; retrieval controls; human-in-the-loop response
Botnet-assisted DDoS	AI optimises traffic patterns and target selection	Service availability loss and congestion	Anycast DDoS mitigation; anomaly detection; traffic scrubbing; slice-level QoS protection

6.3 Post-quantum and crypto-agile 5G resilience

Although quantum attacks are not the immediate source of most telecommunications incidents, crypto-agility is a long-horizon resilience requirement. Telecommunications equipment, SIM/eSIM systems, IoT devices, operational technology and edge appliances often remain deployed for many years. A harvest-now-decrypt-later threat model is relevant where adversaries capture encrypted traffic today and decrypt it in the future when quantum capability matures. 5G organisations should therefore inventory cryptographic dependencies, prioritise long-lived secrets, test hybrid key exchange, plan certificate lifecycle changes and ensure vendor roadmaps align with NIST post-quantum standards (NIST, 2024a; NIST, 2024b; NIST, 2024c).

VII. PROPOSED AI-RESILIENT 5G CYBERSECURITY FRAMEWORK

The proposed framework is designed as an operating model rather than a narrow technical checklist. It contains ten mutually reinforcing domains that should be governed through measurable indicators, executive accountability and continuous validation.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722431

Table 11. AI-Resilient 5G Cybersecurity Framework

Framework domain	Core implementation logic	Suggested KPIs
1. 5G asset and dependency intelligence	Inventory 5G core functions, RAN assets, MEC nodes, APIs, identities, vendors, models and critical service dependencies.	Percentage of critical assets inventoried; crown-jewel services mapped; unknown assets eliminated.
2. Zero-trust identity and access	Apply least privilege, phishing-resistant MFA, workload identity, device posture and microsegmentation across network, cloud and edge.	Privileged MFA coverage; number of excessive privileges; policy violations per month.
3. Slice isolation and service assurance	Validate network-slice separation, tenant isolation, QoS enforcement and blast-radius limits for public-safety and industrial slices.	Slice isolation test pass rate; critical-slice failover performance; segmentation drift.
4. Adversarially robust intrusion detection	Use AI/ML IDS with adversarial testing, ensemble models, robust features, explainability and drift monitoring.	Detection rate; false-positive rate; robustness test score; model drift alerts.
5. Secure edge and MEC orchestration	Harden containers, APIs, service mesh, edge workloads, secrets, image registries and CI/CD pipelines.	Critical misconfigurations; signed image coverage; edge patch latency.
6. Threat-informed vulnerability prioritisation	Combine CVSS, EPSS, CISA KEV, exploit intelligence, asset criticality and exposure rather than relying on CVSS alone.	KEV remediation SLA; internet-exposed critical vulnerabilities; risk-weighted patch backlog.
7. AI model-risk governance	Maintain model inventory, data lineage, access control, evaluation records, red-team results, explainability and human oversight.	Models with governance records; red-team completion; high-impact automated actions reviewed.
8. Autonomous response with guardrails	Use SOAR and AI-assisted triage for enrichment, containment recommendations and playbook execution with approval controls.	Mean time to detect; mean time to contain; percentage of playbooks tested.
9. Recovery engineering and crisis communication	Test backup integrity, restore critical services, rehearse DDoS/ransomware/vendor compromise scenarios and communicate clearly.	Recovery-test success rate; RTO/RPO compliance; tabletop exercise maturity.
10. Post-quantum crypto-agility	Inventory cryptography, prioritise long-lived secrets, test hybrid deployments and align vendors with ML-KEM/ML-DSA migration.	Crypto inventory coverage; PQC migration roadmap; legacy algorithm exceptions.

The framework should be implemented in three phases. Phase 1 establishes visibility, governance and risk scoring. Phase 2 hardens identity, slices, edge workloads and detection pipelines. Phase 3 matures adversarial testing, autonomous response, recovery engineering and post-quantum migration. The phased approach matters because many organisations attempt to buy advanced AI security tools before establishing asset visibility, identity control and governance. This reverses the correct order of operations: AI improves mature security operations but cannot compensate for weak inventories, excessive privileges or absent recovery plans.

Table 12. Implementation roadmap for AI-resilient 5G security

Horizon	Priority actions	Expected resilience outcome
0-90 days	Establish 5G asset register; map critical services; baseline telecom exposure; require phishing-resistant MFA for privileged	Immediate reduction in unknown exposure and privileged-access

	users; review public-facing APIs.	risk.
3-6 months	Deploy risk-based vulnerability prioritisation; validate slice isolation; integrate SIEM/SOAR telemetry; define AI model inventory and governance procedures.	Improved detection, triage and remediation governance.
6-12 months	Conduct adversarial ML testing; run DDoS, ransomware and network-slice compromise exercises; introduce explainable AI-assisted triage.	Operational readiness against AI-enabled attacks and autonomous intrusions.
12-24 months	Build crypto-agility roadmap; test PQC/hybrid key exchange; integrate third-party assurance and continuous control monitoring.	Long-term resilience against quantum and supply-chain risks.

VIII. RECOMMENDATIONS

- Treat 5G cybersecurity as critical-infrastructure resilience, not only as network protection. The protected object is the continuity of essential services.
- Prioritise telecommunications man-in-the-middle, DDoS, phishing and malware scenarios for control validation because they map directly to confidentiality, availability, privileged-access and edge-compromise risks.
- Adopt zero trust across users, devices, workloads and APIs before scaling edge and network-slicing services. Identity should become the primary enforcement plane.
- Make adversarial machine-learning testing mandatory for AI-based intrusion-detection systems and SOC copilots. Every model used in security operations should have an owner, purpose, data source, evaluation method and misuse case.
- Combine threat intelligence with asset criticality. CISA KEV, EPSS, CVSS and exploit telemetry should be weighted by whether the vulnerability touches critical 5G functions, public-safety services or privileged orchestration systems.
- Use AI for detection and triage, but keep human approval for high-impact containment actions that may affect service availability.
- Build post-quantum crypto-agility into 5G security roadmaps now, especially for long-lived devices, certificates, key-exchange mechanisms and supply-chain contracts.
- Measure resilience through recovery outcomes: mean time to detect, mean time to contain, recovery time, recovery point, slice-isolation test results and tabletop exercise performance.

IX. LIMITATIONS AND FUTURE RESEARCH

This study has three limitations. First, the Kaggle incident dataset is a public analytical dataset and does not represent official national breach statistics. It is useful for exploratory modelling and methodological demonstration but should not be interpreted as a complete measure of U.S. or global cyber loss. Second, the data do not include key variables needed for causal inference, such as organisation size, asset criticality, control maturity, cloud architecture, regulatory penalties, insurance recovery, incident disclosure rules and vendor dependencies. Third, the AI-5G Exposure Index is rule-based and transparent rather than statistically learned from verified AI-enabled attack labels. Future work should combine 5G-NIDD packet-flow data, CISA KEV vulnerabilities, EPSS probabilities, telecom asset inventories, SIEM logs and adversarial ML test results. A strong next step would be a two-level model linking 5G flow-level anomaly detection with enterprise-level impact prediction and recovery-time estimation.

X. CONCLUSION

5G telecommunications security is entering a phase in which the defender must secure both networks and the intelligence used to manage them. AI improves detection, triage and automation, but it also enables adversaries to operate faster, personalise attacks, evade models and manipulate the defender's learning systems. The data analysis in this paper shows that telecommunications incidents are materially exposed to attack categories relevant to AI-enabled 5G threats, especially man-in-the-middle attacks, DDoS, phishing and malware. The statistical analysis also

shows that threat labels alone are insufficient for financial-loss prediction, reinforcing the need for asset context, identity posture, vulnerability intelligence, recovery capability and governance maturity. The proposed AI-Resilient 5G Cybersecurity Framework addresses this gap by integrating zero trust, adversarially robust intrusion detection, secure edge orchestration, slice isolation, AI model-risk governance, threat-informed vulnerability prioritisation, recovery engineering and post-quantum crypto-agility. For critical infrastructure, the strategic objective is not only to detect attacks but to preserve service continuity, public trust and national resilience under intelligent adversarial pressure.

Declarations

Data availability: The empirical analysis uses the publicly listed Kaggle Global Cybersecurity Threats (2015-2024) dataset. The 5G-NIDD dataset is discussed as a relevant 5G-specific intrusion-detection benchmark but is not reproduced in the empirical analysis.

Ethics statement: The study uses public, aggregated incident data and does not process personally identifiable information beyond aggregate affected-user counts contained in the dataset.

Competing interests: None declared in this manuscript draft.

Reproducibility: Data processing, heat maps and model outputs were generated using Python, pandas, NumPy, SciPy, scikit-learn and matplotlib. The composite and AI-5G indices are fully defined in the methodology section for replication and critique.

REFERENCES

[1] Agyei, K.G., Nemure, T., Samushonga, C. and Mupa, M.N. (2026a) “Governance-driven security automation for municipal and SMB cloud modernization: A NIST CSF 2.0-aligned remediation operating model”, World Journal of Advanced Research and Reviews. Available at: https://www.researchgate.net/profile/Munashe-Naphtali-Mupa (Accessed: 21 June 2026).

[2] Agyei, K.G., Monjoma, M.B., Samushonga, C. and Mupa, M.N. (2026b) “Explainable risk-based vulnerability prioritization in hybrid cloud: Integrating CVSS, EPSS, and CISA KEV with asset criticality signals”, World Journal of Advanced Research and Reviews. Available at: https://www.researchgate.net/profile/Munashe-Naphtali-Mupa (Accessed: 21 June 2026).

[3] Barakabitze, A.A., Ahmad, A., Mijumbi, R. and Hines, A. (2020) “5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges”, Computer Networks, 167, 106984.

[4] Chisora, H.H., Mupa, M.N., Chitate, I.C. and Chiwanga, R. (2026) “Network security in 5G - threats, vulnerabilities and mitigation strategies”, World Journal of Advanced Research and Reviews. Available at: https://www.researchgate.net/profile/Munashe-Naphtali-Mupa (Accessed: 21 June 2026).

[5] De Alwis, C., Porambage, P., Dev, K., Gadekallu, T.R. and Liyanage, M. (2024) “A survey on network slicing security: Attacks, challenges, solutions and research directions”, IEEE Communications Surveys & Tutorials, 26(1), pp. 534-570. doi: 10.1109/COMST.2023.3312349.

[6] Ghani, H., Salekzamankhani, S. and Virdee, B. (2023) “Critical analysis of 5G networks traffic intrusion using PCA, t-SNE and UMAP visualization and classifying attacks”, arXiv preprint arXiv:2312.04864.

[7] ITU (2024) 5G - fifth generation of mobile technologies. International Telecommunication Union. Available at: https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx (Accessed: 21 June 2026).

[8] Kaggle (2025a) 5G-NIDD dataset. Available at: https://www.kaggle.com/datasets/humera11/5g-nidd-dataset (Accessed: 21 June 2026).

[9] Kaggle (2025b) Global Cybersecurity Threats (2015-2024). Available at: https://www.kaggle.com/datasets/atharvasoun

dankar/global-cybersecurity-threats-2015-2024 (Accessed: 21 June 2026).

[10] Khan, R., Kumar, P., Jayakody, D.N.K. and Liyanage, M. (2020) "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions", IEEE Communications Surveys & Tutorials, 22(1), pp. 196-248. doi: 10.1109/COMST.2019.2933899.

[11] Li, J., Zhao, Z. and Li, R. (2017) "A machine learning based intrusion detection system for software defined 5G network", arXiv preprint arXiv:1708.04571.

[12] Maglaras, L.A., Kim, K.H., Janicke, H., Ferrag, M.A., Rallis, S., Fragkou, P., et al. (2018) "Cyber security of critical infrastructures", ICT Express, 4(1), pp. 42-45.

[13] Musser, M., Lohn, A., Dempsey, J.X., Spring, J., Kumar, R.S.S., Leong, B., Liaghati, C., et al. (2023) Adversarial Machine Learning and Cybersecurity: Risks, Challenges, and Legal Implications. Washington, DC: Center for Security and Emerging Technology. doi: 10.51593/2022CA003.

[14] Nemure, T., Mupa, M.N., Agyei, K.G., Chisora, H.H., Mudzingwa, K. and Chiwanga, R. (2026) "Cybersecurity of critical infrastructures: Challenges and future perspectives", World Journal of Advanced Research and Reviews. Available at: https://www.researchgate.net/profile/Munashe-Naphtali-Mupa (Accessed: 21 June 2026).

[15] NIST (2020) Zero Trust Architecture, Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-207.

[16] NIST (2023) Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.AI.100-1.

[17] NIST (2024a) Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 203. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.FIPS.203.

[18] NIST (2024b) Module-Lattice-Based Digital Signature Standard, FIPS 204. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.FIPS.204.

[19] NIST (2024c) Stateless Hash-Based Digital Signature Standard, FIPS 205. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.FIPS.205.

[20] NIST (2025) Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, NIST AI 100-2e2025. Gaithersburg, MD: National Institute of Standards and Technology.

[21] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology.

[22] Sagduyu, Y.E., Erpek, T. and Shi, Y. (2021) "Adversarial machine learning for 5G communications security", arXiv preprint arXiv:2101.02656.

[23] Samarakoon, S., Siriwardhana, Y., Porambage, P., Liyanage, M., Chang, S.Y., Kim, J., Kim, J. and Ylianttila, M. (2022) "5G-NIDD: A comprehensive network intrusion detection dataset generated over 5G wireless network", arXiv preprint arXiv:2212.01298.

[24] Siriwardhana, Y., Samarakoon, S., Porambage, P., Liyanage, M., Chang, S.Y., Kim, J., Kim, J. and Ylianttila, M. (2025) "Descriptor: 5G Wireless Network Intrusion Detection Dataset (5G-NIDD)", IEEE Data Descriptions. doi: 10.1109/IEEEDATA.2025.3592888.

[25] Usama, M., Mitra, R.N., Ilahi, I., Qadir, J. and Marina, M.K. (2020) "Examining machine learning for 5G and beyond through an adversarial lens", arXiv preprint arXiv:2009.02473.

[26] Zhuwankinyu, E.K., Mupa, M.N. and Tafirenyika, S. (2025) "Graph-based security models for AI-driven data storage: A novel approach to protecting classified documents", World Journal of Advanced Research and Reviews, 26(2), pp. 1108-1124. doi: 10.30574/wjarr.2025.26.2.1631.