

Cybersecurity and Innovation in the Evolving Digital Economy

Michael de Percy
University of Canberra

Abstract: This editorial introduces the September 2025 issue of the *Journal of Telecommunications and the Digital Economy*, spotlighting the intersection of cybersecurity, emerging technologies, and historical lessons in the digital economy. As digital transformation accelerates, threats to IoT, cloud, and 5G ecosystems proliferate, demanding innovative, resource-efficient solutions for SMEs and emerging markets. Contributions in this issue – from machine learning-driven threat detection to zero-trust architectures and reflections on telecom automation – highlight human and organisational factors in resilience. They bridge legacy telecommunications with future-oriented strategies, underscoring the journal's commitment to fostering adaptive digital ecosystems amid persistent vulnerabilities.

Keywords: Editorial, Editor-in-Chief, Digital Economy, Cybersecurity, IoT Security.

Introduction

This editorial welcomes readers to the September 2025 issue of the *Journal of Telecommunications and the Digital Economy*, with a focus on cybersecurity's pivotal role in sustaining the digital economy. The post-COVID 'new normal' has entrenched online interactions as essential infrastructure, yet it has also amplified vulnerabilities in interconnected systems. From IoT-enabled healthcare to cloud-dependent SMEs, the digital economy thrives on innovation but grapples with escalating threats like ransomware, bandwidth exploitation, and supply-chain attacks. Decades-old technologies now underpin global commerce, but social and organisational norms lag, exposing gaps in preparedness.

The articles in this issue illuminate these tensions, offering practical insights into securing emerging technologies while drawing on historical precedents. They emphasise the human element – talent, awareness, and adaptive business models – as key to bridging challenges in resource-constrained environments. By integrating machine learning, zero-trust principles, and 5G reconfiguration, contributors reveal pathways for resilient digital growth, particularly in developing contexts.

Cybersecurity Imperatives in IoT and Cloud Ecosystems

A dominant theme is the fortification of IoT and cloud infrastructures against sophisticated threats. Anjikumar & Chakravarthy (2025) propose a lightweight encryption framework for remote healthcare, blending elliptic curve cryptography with grasshopper optimisation to slash latency and energy use. Simulation results affirm its efficacy in 5G-smart health setups, addressing privacy pitfalls in real-time data sharing.

This work underscores the digital economy's fragility: IoT's proliferation generates vast data streams, but without tailored, efficient defences, it risks amplifying breaches. As SMEs – 90% of global businesses – adopt these technologies, the emphasis on low-overhead tools like zero-trust architectures becomes imperative.

Reconfiguring Business Models and Organisational Resilience

Shifting to strategic adaptation, Banda & Feukeu (2025) employ qualitative case studies across Sub-Saharan Africa to unpack 5G's disruptive potential. Interviews reveal internal (e.g., infrastructure costs), external (e.g., regulatory hurdles), and hybrid factors reshaping value chains, urging operators to pivot toward fixed-wireless access and spectrum-sharing for GDP gains projected at US\$10 billion by 2030. This analysis extends beyond developed markets, spotlighting emerging economies' leapfrogging opportunities amid debt and poverty constraints.

Echoing organisational dynamics, Moya *et al.* (2025) deploy PLS-SEM on 112 Colombian SME surveys, identifying human talent and resources as top predictors of resilience. With 33% of respondents hit by attacks like phishing, the study stresses cyber awareness and supplier vetting, filling gaps in emerging-market research and advocating integrated frameworks like NIST for proactive defence.

Dinh *et al.* (2025) validate a bespoke LZTA, outperforming baselines in throughput and response times under high loads. By fusing multi-factor authentication with role-based controls, it democratises zero-trust for budget-strapped SMEs, countering the 70% disruption rate from breaches and aligning with global calls for 'never trust, always verify' paradigms.

Navaratna & Saxena (2025) expose self-regulation gaps in AI chatbots, advocating for a standard compliance score on app stores and enhanced citizen digital awareness to bridge divides. The above issues are becoming increasingly commonplace and deserve our continued attention.

Historical Reflections and Enduring Lessons

This issue also honours telecommunications' legacy, reminding us that today's digital challenges echo yesterday's innovations. Moorhead (2025) considers seminal 1981–1982 papers on Telecom Australia's DAS/C rollout, juxtaposed with Ian Campbell's (2025) commentary revealing deployment delays and union frictions that yielded suboptimal efficiency versus U.S. benchmarks. These pieces, amid AI's rise, caution against repeating historical pitfalls in workforce transitions.

Complementing this, Leith Campbell's (2025) obituary for Dr. Clemens W. Pratt celebrates a 38-year PMG/Telstra career in teletraffic engineering, from theses on congestion to ITC advisory roles. Pratt's mentorship and statistical advocacy underscored the human intellect driving telecom evolution – timely as ML automates threat detection.

Conclusion

The digital economy's 'new normal' demands vigilance: cybersecurity is not merely technical but profoundly human and historical. This issue's contributions – from IoT safeguards to 5G pivots and archival wisdom – enrich our grasp of these dynamics, fostering collaboration across disciplines. As threats evolve, the *Journal of Telecommunications and the Digital Economy* remains a vital forum, bridging telecom's storied past with innovative futures to empower resilient, inclusive growth. We invite readers to engage with these insights and submit their own.

References

- Anjikumar, T. & Chakravarthy, A. S. N. (2025). An Energy-Efficient Based Secure IOT Data Transfer with Hashed Data Access Policy Using ACROT-DHSKECC and LSCRC32. *Journal of Telecommunications and the Digital Economy*, 13(3), 145–175. <http://doi.org/10.18080/jtde.v13n3.1301>
- Banda, L. & Feukeu, E. A. (2025). The Impact of 5G on Business Models for Mobile Operators in Emerging Markets. *Journal of Telecommunications and the Digital Economy*, 13(3), 71–105. <http://doi.org/10.18080/jtde.v13n3.1230>
- Campbell, I. (2025). Comments on the Two Historical Reprints in Automation of Directory Assistance. *Journal of Telecommunications and the Digital Economy*, 13(3), 191–195. <http://doi.org/10.18080/jtde.v13n3.1340>
- Campbell, L. (2025). Clemens William (“Clem”) Pratt, 2 July 1936–16 January 2025. *Journal of Telecommunications and the Digital Economy*, 13(3), 196–204. <http://doi.org/10.18080/jtde.v13n3.1322>
- Dinh, T. D., Le, T. D., Nguyen, T. T. H., & Do, H. G. (2025). A Lightweight Zero-Trust Architecture Implementation for Enhancing Cybersecurity in Small and Medium-

- Sized Enterprises. *Journal of Telecommunications and the Digital Economy*, 13(3), 106–144. <http://doi.org/10.18080/jtde.v13n3.1284>
- Moorhead, S. (2025). Automation of Directory Assistance. *Journal of Telecommunications and the Digital Economy*, 13(3), 176–190. <http://doi.org/10.18080/jtde.v13n3.1330>
- Moya, L. P., Giraldo, M. C. B., Lozano, J. A. A., Arias, A. V., & Rodríguez-Correa, P. A. (2025). Human and organisational factors influencing the preparedness of small and medium-sized enterprises against cyber attacks in developing countries. *Journal of Telecommunications and the Digital Economy*, 13(3), 30–70. <http://doi.org/10.18080/jtde.v13n3.1197>
- Navaratna, A. R. & Saxena, D. (2025). Digital Governance Through Self-Regulation: A user-developer perspective of AI chatbots. *Journal of Telecommunications and the Digital Economy*, 13(3), 1–29. <http://doi.org/10.18080/jtde.v13n3.1077>