EDITORIAL

Securing the Cognitive Future in the Era of 6G and Beyond

Hamza Kheddar[1,*]

[1] LSEA Laboratory, Department of Electrical Engineering, University of Medea, Medea, Algeria

As we enter the era of 6G and beyond, the convergence of ultra low latency communication, edge intelligence, semantic aware networking, and holographic interfaces marks a fundamental transformation in how intelligent systems operate. Unlike earlier generations, 5G and 6G will not merely enhance performance, they will embed cognition, adaptability, and autonomy into the very fabric of digital infrastructure. However, this rapid evolution brings with it an expanded cybersecurity threat landscape that is *faster, stealthier, and more autonomous*, demanding innovative, interdisciplinary solutions.

Drawing on my research in areas such as deep learning based intrusion detection, adversarial attacks on AI systems, and digital twin security, it is increasingly clear that traditional defense paradigms are insufficient. Threat actors are targeting software defined infrastructures, autonomous transportation systems, smart grids, and IoT environments, leveraging AI and automation to outpace conventional safeguards. The cybersecurity community must respond with equal agility and foresight.

In this context, the *ICCK Transactions on Cybersecurity* emerges as a vital academic forum dedicated to advancing transformative research in cybersecurity. Our aim is to connect theoretical innovation with scalable, real world impact across academia, industry, and policy.

We encourage original contributions in a wide array of critical areas shaping secure and intelligent ecosystems for 6G and beyond. These include: 6G security frameworks and cognitive threat modeling for next generation networks; advanced deep learning techniques including reinforcement learning, federated learning, transfer learning, and transformer based architectures for adaptive defense and intelligent threat mitigation; smart grid security, anomaly detection, and resilient energy infrastructure; blockchain based identity management, access control, and data integrity; post quantum cryptography and quantum resilient architectures; privacy preserving computation in adversarial environments; explainable AI (XAI) and large language models (LLMs) for transparency and trust in cybersecurity and digital forensics; and hybrid deep learning systems for intrusion detection and cyber resilience.

Our editorial team is committed to fostering excellence in cybersecurity research. We uphold a rigorous peer review process focused on fairness, originality, and technical merit. Transparency and timeliness in editorial communication are central to our values, as is our dedication to promoting reproducibility through open data and code sharing practices. Furthermore, we actively encourage interdisciplinary work that bridges computer science, electrical engineering, artificial

Submitted: 20 July 2025
Accepted: 11 August 2025
Published: 30 August 2025

Vol. 1, **No.** 1, 2025.
10.62762/TC.2025.346449

***Corresponding author:**
✉ Hamza Kheddar
kheddar.hamza@univ-medea.dz

Citation
Kheddar, H. (2025). Securing the Cognitive Future in the Era of 6G and Beyond. *ICCK Transactions on Cybersecurity*, 1(1), 15–16.

© 2025 ICCK (Institute of Central Computation and Knowledge)

intelligence, and information security.

With the release of *Volume 1, Issue 1, ICCK Transactions on Cybersecurity* embarks on an ambitious journey to become a leading voice in cybersecurity research. We are excited to offer a journal that not only highlights emerging technologies but also addresses their real world risks and implications. Through this journal, we aim to inspire a new wave of secure, intelligent, and ethically responsible systems for the era of 6G and beyond. We invite the global research community, academics, practitioners, and innovators, to join us in this collective effort. In an age where 6G networks interface with AI native systems, blockchains establish digital trust, and deep learning governs cyber physical autonomy, your ideas and insights are essential. Together, let us shape the future of cybersecurity: *resilient, intelligent, and secure by design*.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

The author declares no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.



Hamza Kheddar is currently an Associate Professor at the University of Medea and a Researcher at the LSEA Lab in Medea, Algeria. He holds a Ph.D. in Telecommunications from USTHB University and a Master's degree in Telecommunications from the High School of Telecommunications and In- formation Technology (ENSTTIC). Previously, he served as a core network expert at Huawei for the Middle East and North Africa (MENA) region. In June 2021, he obtained his Habilitation to Direct Research. Dr. Kheddar has authored 30 research papers published in reputable international journals and conferences. He is an active reviewer for esteemed journals such as Computers & Security, IEEE Access, IEEE Transactions on Information Forensics and Security, Computer Speech & Language, Applied Intelligence, Speech Communication, and others. His research contributions span diverse areas, including speech processing and recognition, image classification, steganography and steganalysis, intrusion detection, covert channels, digital twins and deep learning, 5G/6G security, biometrics, generative AI, and large language models. Additionally, he serves as the Telecommunications track chair for several international conferences such as IC2M 2023 and ICTSS 2024. (Email: kheddar.hamza@univ-medea.dz)