# EDITORIAL

## Edition 2, Volume 3, December 2023

## ARIS² - Advanced Research on Information Systems Security

## an International Journal

Nuno Mateus-Coelho, PhD*

### 1. INTRODUCTION

Strong cybersecurity measures have never been more important than they are in the contemporary digital age [1] when our reliance on networked information systems is growing at an ever-increasing rate [3]. Individuals, corporations, and governments all face daunting difficulties as a result of the dynamic and ever-changing nature of cyber threats [3]. At this point in time, cybersecurity is not only a technical requirement; rather, it is an essential component in the process of protecting trust, privacy, and the integrity of the digital sphere [4].

While we are in the process of exploring this edition of "Advanced Research on Information Systems Security," our primary focus is on gaining a knowledge of the complex issues that are faced by those who work in the field of cybersecurity and finding solutions to those challenges. The landscape is characterized by a variety of risks, which range from sophisticated social engineering strategies to the ever-evolving techniques deployed by cybercriminals. These threats are threatening the landscape. The utilization of interdisciplinary research and creative techniques is absolutely necessary in order to successfully navigate this complex terrain.

---

* Editor-in-chief of ARIS², Portugal. E-mail: nuno.coelho@ulusofona.pt

## 2. STRUCTURE

In the second issue of the third Volume of the ARIS$^2$ - Journal, the reader will have *online* access to four research articles as follows:

1. ***Social Engineering as a Tool for Warfare - A Look at the 2022 Dollar Bill Rejection Hoax in Nigeria***

   Unraveling the intricacies of social engineering and its role in modern cyber warfare.

   Analyzing the 2022 Dollar Bill Rejection Hoax in Nigeria as a case study.

2. ***Phishing in Web 3.0 - Opportunities for the Attackers, Challenges for the Defenders***

   Exploring the escalating threat landscape of phishing attacks in the era of Web 3.0.

   Identifying opportunities for attackers and challenges faced by defenders in the evolving digital paradigm.

3. ***IoHTs - Cybersecurity Approach in Internet of Healthcare Things***

   Investigating the intersection of cybersecurity and healthcare in the era of Internet of Healthcare Things (IoHTs).

   Proposing a comprehensive cybersecurity approach to safeguard sensitive medical data.

4. ***Enterprise Transformation Projects, The Role of The Polymathic Security Learn Processes (ETP-PSLP)***

   Examining the vital role of Polymathic Security Learn Processes (PSLP) in large-scale Enterprise Transformation Projects (ETP).

   Emphasizing the need for a multidisciplinary approach to address intricate security challenges in enterprise settings.

We would like to express our appreciation for the rigorous contributions from researchers worldwide. While this edition received a significant number of submissions, only these four outstanding papers were accepted for publication. The selection was based on their academic rigor, relevance to the theme, and potential to contribute meaningfully to the advancement of cybersecurity knowledge. This edition brings together a diverse set of perspectives, each contributing uniquely to our understanding of cybersecurity in the contemporary landscape. From the human elements of social engineering to the challenges posed by emerging technologies, these accepted papers collectively provide a comprehensive view of the current state of cybersecurity and the innovative approaches required to secure our digital future.

Join us in this exploration as we delve into the complexities, vulnerabilities, and solutions that define the ever-evolving world of cybersecurity.

## 3. ACKNOLEDGEMENTS

We would like to thank the authors who have submitted their manuscripts and all the reviewers for their valuable contributions. The scientific importance of the publications in this Issue of the ARIS$^2$ - Journal is a strong reason for other authors to submit works for future Regular and Special Issues.

## REFERENCES

[1] N. Mateus-Coelho and M. Cruz-Cunha, "Serverless Service Architectures and Security Minimals," *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800779.

[2] N. Mateus-Coelho, "A new methodology for the development of secure and Paranoid Operating Systems," *Procedia Computer Science*, vol. 181, pp. 1207–1215, 2021. DOI: 10.1016/j.procs.2021.01.318

[3] M. Saraiva and N. Coelho, "CyberSoc Implementation Plan," *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800819.

[4] Mario Saraiva, Nuno Mateus-Coelho, CyberSoc Framework a Systematic Review of the State-of-Art, Procedia Computer Science, Volume 204, 2022, Pages 961-972, https://doi.org/10.1016/j.procs.2022.08.117.

## How to cite this article:

Mateus-Coelho, N. (2023*). The Editorial of ARIS2 - Advanced Research on Information Systems Security, an International Journal*, Vol. 3, No. 2, 1-3.

**DOI:** https://doi.org/10.56394/aris2.v3i2.33