EDITORIAL

Edition 1, Volume 2, August 2022
ARIS^2 - Advanced Research on Information Systems Security
an International Journal

Nuno Mateus-Coelho, PhD *

1. INTRODUCTION

As the year 2022 enters its middle range, the world is assisting an abnormal event with a heavy impact on cyber security, the Russian-Ukraine conflict. Since the beginning of this conflict that two immense groups have been created and explore security flaws within each side and to do so with success, they resort to vulnerabilities, coercion, or social engineering techniques. Protecting information, actors, and their frameworks has emerged as a critical struggle and science has an immense role in performing and maintaining security actors one step forward in this scenario.

In the first regular issue of 2022 of the ARIS2 - Advanced Research on Information Systems Security, an International Journal, two research articles were accepted from ten submissions, resulting in an acceptance rate of 20 percent. These two papers show that information security, awareness, and resilient systems are foundational elements of contemporary information systems, and they now have an additional duty, specifically and above all, to keep safe user-provided private information. Industry-led research indicates that 45 percent of major enterprises and 29 percent of SMEs have already experienced some sort of security attack [1].

* Editor-in-chief of ARIS^2, Portugal. E-mail: nuno.coelho@islagaia.pt

Before making products available to the general public, companies must take into account the new risks and problems brought about by the widespread use of resources that enable quick connectivity, such as the smartphone, thus anticipating vulnerabilities and allowing risk mitigation [2].

Academic research surfaces at this precise time with consistent answers that should be announced to the world as the direction to go in the form of scientific research [3].

Furthermore, according to recent studies, the area of information security research is expanding but is neither straightforward or linear [4]. According to research, a new zero day or loophole is generated for every security advance, and the media ignores these developments. After a significant amount of time spent operating covertly, Zero-Day can have an impact on both companies and people in general [5]. Societies can forecast the effects of a zero-day vulnerability, leading to a more secure usage of technology, through research and inquiry that frequently uses methods like forensics and threat analysis [6].

2. STRUCTURE

In the first Issue of the ARIS^2 - Journal, the reader will have *online* access to two research works about:

1. Artificial Intelligence as a Support Tool to Cybersecurity Activities.
2. Analysis of Infrastructural Challenges, Cybercrime, and the Cashless Policy in Nigeria.

The papers evaluated by double blind review system belong to authors who presented the results of their studies that fit in the scientific areas of the ARIS^2 Journal; so, they were accepted for publication in this international scientific journal.

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 ARIS² - Journal is a strong reason for other authors to submit works for future Regular and Special Issues.

REFERENCES

[1] M. M. Cruz-Cunha and N. R. Mateus-Coelho, *Handbook of Research on Cyber Crime and Information Privacy*. IGI Global, 2021. DOI: 10.4018/978-1-7998-5728-0

[2] N. Coelho, B. Fonseca, and A. Castro, "Paranoid operative system methodology for Anonymous & Secure Web Browsing, doctoral project," *Atas da 17ª Conferência da Associação Portuguesa de Sistemas de Informação*, 2017. DOI: 10.18803/capsi.v17.127-143

[3] 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.

[4] 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

[5] 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.

[6] F. Alves, N. Mateus-Coelho and M. Cruz-Cunha, "ChevroCrypto – Security & Cryptography Broker," *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, 2022, pp. 1-5, doi: 10.1109/ISDFS55398.2022.9800797.

How to cite this article:

Mateus-Coelho, N. (2022*). The Editorial of ARIS2 - Advanced Research on Information Systems Security, an International Journal*, Vol. 2, No. 1, 1-3.