A picture containing text

Description automatically generatedText, letter

Description automatically generatedText, letter

Description automatically generated

A ‘fully digital enterprise’ is an organisation that has no barriers between its business units and any others involved in the value chain (Banergi, 2019; Kargin et al., 2021). Such a company leverages a digital business model, thus harnessing the power of data and relevant digital technologies to streamline the relationships amongst the various actors in the value chain and deliver further value to the customers (Banergi, 2019; Mordecai et al., 2022).

Whilst fully digital enterprises have IT departments in charge of cyber security, employees may not be all involved in safeguarding it collectively (Spreić & Šimunic, 2018). Thus, Spreić & Šimunic (2018) suggested adopting a holistic approach to establish company-wide cultural initiatives to ensure cyber security is not treated as an add-on technology, but it is an integral governance-related component of the organisation’s business strategy.

Bricks and mortar SMEs seeking to become a digital enterprise, besides implementing and driving intelligent and efficient checks to prevent cyber attacks or detect them promptly, should innovate in advancing their knowledge and technologies to stay abreast of emerging cyber attacks (Spreić & Šimunic, 2018).

In light of the energy crisis and conflicts faced in 2022 (Johannesson & Clowes, 2022; Liadze et al., 2022), the idea of peer-to-peer energy trading (Banergi, 2019) does not seem realistic, nor focusing on energy-related data services (Banergi, 2019) given the decline experienced in this sector; nevertheless, alternative sources of energy should be explored, including more sustainable (Gatto, 2022) and renewable energies (Żuk & Żuk, 2022), to prepare for and mitigate further exacerbations of the current crisis.

**References**

Banerji, R. (2019) Will the T&D utility of the future have a digital DNA?

Gatto, A. (2022). The energy futures we want: A research and policy agenda for energy transitions. *Energy Research & Social Science*, *89*, 102639.

Johannesson, J., & Clowes, D. (2022). Energy resources and markets–Perspectives on the Russia–Ukraine War. *European Review*, *30*(1), 4-23.

Kargin, Y. O., Barnes, A. A., Uysal, O. D., Pinon-Fischer, O. J., Balchanos, M. G., Mavris, D. N., ... & Matlik, J. F. (2021). Digital Enterprise Across The Lifecycle. In AIAA Scitech 2021 Forum (p. 0240).

Liadze, I., Macchiarelli, C., Mortimer-Lee, P., & Juanino, P. S. (2022). The economic costs of the Russia-Ukraine conflict. *NIESR Policy Paper*, *32*.

Mordecai, Y., de Weck, O. L., & Crawley, E. F. (2022). Toward an Enterprise Architecture for a Digital Systems Engineering Ecosystem. In *Recent Trends and Advances in Model Based Systems Engineering* (pp. 653-663). Springer, Cham.

Spremić, M. & Šimunic, A. (2018). Cyber Security Challenges in Digital Economy. Proceedings of the World Congress on Engineering 2018 (1).

Żuk, P., & Żuk, P. (2022). National energy security or acceleration of transition? Energy policy after the war in Ukraine. *Joule*, *6*(4), 709-712.