Editorial

Aligning Ukrainian Concepts and Standards in Defence, Safety, and Cybersecurity to NATO and EU Developments

Volodymyr Zaslavskyi [iD]

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

http://www.univ.kiev.ua

A B S T R A C T :

Problems of global international security increasingly depend on high-tech solutions, computer systems and information technologies, which are aimed at adapting the security and defence of countries to new realities and challenges in the context of hybrid wars and the Covid-19 pandemic. In this context, this volume of "Information & Security" presents six original articles addressing development in NATO the European Union, and Ukraine, focusing on the challenges in attempts to align Ukrainian concepts and standards to established good practice in the experience of the West.

The rapid development and incorporation advanced communication and information technologies changes all spheres of life. Particularly challenging, and of high interest to the public, is the provision of safe and secure use of technology without slowing down the process of digital transformation while enhancing the resilience of services, the economy, communities, and the society at large.[1]

Often, NATO and the European Union play a lead role in establishing good practices. As Ambassador Peter Popchev points out in his contribution to this

volume, the cooperation among the two organisations turns into a driving factor for promoting values, approaches, and standards in enhancing the resilience to cyberattacks, in this case seen as a component of hybrid operations.[2]

Mariia Pleskach and co-authors add to the conceptual developments in the field of cybersecurity the standards of ISO, ITU, and ETSI and provide convincing rationale that the harmonization of Ukrainian with the international standards is essential for saving financial resources and time, and ensuring cross-border cooperation.[3]

Olha Izmailova et al. continue the topic of cyber/information security laying the foundation of an elaborate, rigorous decision-making approach in assessing risks to banking information systems with account of variety of losses.[4]

Major-General (ret.) Oleksandr Polischuk traces the origins of the idea of a "defence ecosystem" to the experience of the United Kingdom.[5] Upon its critical evaluation, the author reasons that it can be used as a model of Ukraine's security and defence organisation based on functional integration of the capabilities of all main security and defence actors and outlines necessary legislative challenges.

The two remaining contributions study the role of the human factor for preserving information security during the COVID-19 pandemic and the use of advanced UAVs for civilian purposes.

References

1   Todor Tagarev, Krassimir Atanassov, Vyacheslav Kharchenko, and Janusz Kasprzyk, eds., *Digital Transformation, Cyber Security and Resilience of Modern Societies*, in *Studies in Big Data*, vol. 84 (Cham, Switzerland: Springer, 2021), https://doi.org/10.1007/978-3-030-65722-2.

2   Peter Poptchev "NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivaled Advantages," *Information & Security: An International Journal* 45, no. 1 (2020): 35-55, https://doi.org/10.11610/isij.4503.

3   Mariia Pleskach, Valentyna Pleskach, Andrii Semenchenko, Danylo Myalkovsky, and Taras Stanislavsky, "Standardization in the Field of Cybersecurity and Cyber Protection in Ukraine," *Information & Security: An International Journal* 45 (2020): 57-76, https://doi.org/10.11610/isij.4504.

4   Olha Izmailova, Hanna Krasovska, Kateryna Krasovska, and Volodymyr Zaslavskyi, "Assessing the Variety of Expected Losses upon the Materialisation of Threats to Banking Information Systems," *Information & Security: An International Journal* 45 (2020): 89-118, https://doi.org/10.11610/isij.4504.

5   Oleksandr Polischuk, "Ecosystem Platform for the Defence and Security Sector of Ukraine," *Information & Security: An International Journal* 45 (2020): 7-19, https://doi.org/10.11610/isij.4501.

About the Author

See the short CV on p. 118 of this volume, https://doi.org/10.11610/isij.4506.