Cybersecurity in Ukraine's Recovery:

Essential for Stability and Modernisation

To ensure that Ukraine post-conflict reconstruction lays the foundation for long-lasting national stability and economic resilience, cybersecurity must be at the forefront of the European Union rebuilding efforts.

For this reason, the European Union's Ukraine Facility program must prioritise cybersecurity initiatives, especially for the protection of critical infrastructure from cyber attacks and for the long-term development of a resilient cybersecurity ecosystem.

The Ukraine Facility and the Threat Landscape

In response to the economic challenges facing Ukraine for the conflict reconstruction, the European Commission's Ukraine Facility, with a budget of €50 billion from 2024 to 2027, aims to support Ukraine's immediate recovery and long-term reconstruction. This initiative underscores the EU's commitment to supporting Ukraine during a critical period, reflecting a broader vision of stability and security. Aligned with the December 2023 decision to open accession negotiations, the Facility will further Ukraine's integration within the European framework by providing crucial funding opportunities. Three pillars have been envisaged: financial support, investment mobilisation, and technical assistance - each designed to adapt to Ukraine’s evolving circumstances.

Beyond this economic support, it is important to acknowledge the current threat landscape encompassing physical and cyberattack. The challenges are countless: damaged or degraded national infrastructure, development resources diverted to meet immediate needs, brain drain due to migration abroad, and interrupted education and training.

Prioritisating Cybersecurity

Given the cybersecurity challenges arising from the conflict as well as the economic opportunities offered with the Ukraine Facility, cybersecurity must be a cornerstone of the reconstruction for two key reasons.

First, in a highly digitalised world, ensuring the security of cyberspace represents the foundations upon which most other pillars of life depend. Without secure cyber infrastructure, other investments in areas like energy, transportation, or finance are at risk of disruption or compromise. Second, cybersecurity must be integrally incorporated from the inception, whether in constructing infrastructures or formulating public administration procedures. When treated as a secondary consideration, the repercussions include escalated costs for remedying vulnerabilities and a heightened risk profile.

Therefore, cybersecurity should be considered in every project financed under the Ukraine Facility and investments should be encouraged to build resilient infrastructure, technologies, and organisations.

Call to Action

We call on the European Commission, and all EU institutions and bodies involved, to pay particular attention to the inclusion of cybersecurity through a transversal way in every project financed by Ukraine Facility.

In addition, we call on the European Commission, and all EU institutions and bodies involved, to prioritise dedicated projects for cybersecurity.

Following the signature of a Memorandum of Understanding, the Ministry of Digital Transformation of Ukraine and ECSO have formalised their willingness to cooperate to increase cybersecurity. We stand ready to provide expertise and support in this endeavour, leveraging our network of cybersecurity organisations and professionals.

European Cyber Security Organisation (ECSO) • https://www.ecs-org.eu • EU Transparency registry: 684434822646-91 • Avenue des Arts 46 Kunstlaan, 1000, Brussels, Belgium