Gent Sejko: Address - Israel Albania Cyber Summit

Address by Mr Gent Sejko, Governor of the Bank of Albania, at the Israel Albania Cyber Summit, Tirana, 12 May 2026.

* * *

Dear guests,

It is a privilege to participate in this Summit and address one of the defining challenges of our time: cybersecurity. In an increasingly interconnected global economy, the comprehensive management of cyber risk has become a strategic priority for financial institutions, regulators, and supervisory authorities worldwide.

We are all aware that we are living in a more uncertain and volatile world, where geopolitical tensions and conflicts increasingly evolve into sophisticated forms of hybrid warfare. In this reality, cyberattacks are no longer making headlines, but a frequent part of daily routine.

Rapid technological advancements, digital transformation, and the integration of artificial intelligence into everyday activities-particularly within the financial industry-are reshaping this landscape. As cyberspace continues to expand through the widespread adoption of advanced technologies, exposure to cyber risk inevitably continues to increase.

Cybersecurity is now widely recognized as a critical component of financial stability and national security, as well as a fundamental pillar of public confidence in the financial system. Disruptions affecting critical infrastructure, particularly within the financial sector, as well as data breaches resulting from cyberattacks, can significantly damage the reputation and values of institutions and their clients.

In light of these evolving dynamics, the Bank of Albania considers the gradual shift in prudential supervisory focus-from traditional risks, such as credit risk, without diminishing their importance, toward emerging risks, including cyber risk-as inevitable. The same approach applies to entities licensed by the Bank of Albania. In this context, it is no coincidence that the European Banking Authority (EBA) has identified cyber risk monitoring as one of its supervisory priorities for 2026.

For several years, the Bank of Albania has incorporated the regulation and supervision of cyber risk into its strategic agenda, with a particular focus on certain key priorities. Among them, we may highlight: (i) strengthening supervisory human capacities; (ii) enhancing close cooperation with relevant authorities, particularly the Albanian Association of Banks and the National Cyber Security Authority; (iii) implementing international best standards and practices for the monitoring and assessment of cyber risk; and (iv) developing a regulatory framework aligned with the legal framework of the European Union.

Allow me to go further in depth in two last priorities.

First, the implementation of best-in-class standards for supervision and monitoring. With the assistance of the U.S. Treasury, the Bank of Albania has developed and implemented a cybersecurity assessment methodology based on 93 controls, covering organisational aspects, human resources, as well as physical and technological security. To date, the first full assessment cycle for the entire banking system has been completed, while the horizontal reassessment is currently underway. This phase is expected to be finalised within the third quarter of this year. This process will continue to be repeated until the Bank of Albania ensures an appropriate and consistent level of cybersecurity maturity across all banks.

Second, the approximation of the regulatory framework with the EU acquis, in line with the strategic objective of the Government of Albania for full membership in the European Union by 2030. The Bank of Albania is working diligently to harmonise its regulatory framework with the EU Regulation on Digital Operational Resilience Act (DORA) for the financial sector, which entered into force in January 2025.

Finally, I would like to highlight that the Bank of Albania, as one of the key public institutions in Albania, is part of the national critical infrastructure. As such, it has continuously invested in building and strengthening a resilient and secure technological infrastructure capable of effectively preventing and responding to attacks on its platforms. Business continuity processes and procedures ensure high availability and a rapid recovery capability in the event of incidents, while the consolidation of regular training programmes for personnel at all levels helps maintain a solid level of cyber security awareness and preparedness among staff.

In conclusion, I would like to extend my appreciation to all public institutions that continue to demonstrate sustained attention and commitment in this area.

Wishing you fruitful proceedings of this Summit, I am confident that strengthened institutional cooperation, the further consolidation of processes developed to date, and the effective implementation of new initiatives will further enhance our cybersecurity capabilities and reinforce the resilience of the financial system and critical infrastructure.

Thank You!