

EN

E-003667/2025

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(18.11.2025)

The EU participates in crisis exercises to test its preparedness and capacity to manage complex, cross-sectoral crises, including of hybrid nature¹. Eurocontrol and the Commission jointly chair the European Aviation Crisis Coordination Cell (EACCC), which organises annual crisis exercises that include information and communication technologies (ICT) incidents (e.g. in 2013, 2018 and 2022). Additionally, the Cybersecurity Blueprint provides the framework for exercises to test the response to large scale incidents².

In addition, the Network and Information Systems Cooperation Group (NISCG), together with the Commission, may conduct cybersecurity risk assessments of critical infrastructure supply chains under the NIS2 Directive³ and the Council invited Member States to conduct stress tests for critical infrastructures based on EU-level common principles and joint scenarios⁴.

Finally, the NISCG and Commission are working on the ICT supply chain security toolbox which will recommend mitigation measures for risks stemming from ICT supply chains. The security and resilience of ICT supply chains and infrastructure will also be addressed in the upcoming revision of the Cybersecurity Act⁵.

¹ See also the European Preparedness Strategy for the wider approach to preparedness:

https://commission.europa.eu/document/download/526806b6-c4e1-43d1-81b7-947308efbab1_en?filename=Joint%20Communication.pdf.

² <https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation>.

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555>.

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023H0120%2801%29>.

⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148>.