

**Question for written answer E-002849/2024  
to the Commission**  
Rule 144  
**Auke Zijlstra (Pfe)**

**Subject:** Impact on financial data traffic of hybrid attacks on Baltic Sea fibre-optic cables

In November 2024, two important fibre-optic cables in the Baltic Sea were severely damaged. This may have been an act of sabotage within the broader context of ‘hybrid warfare’ targeting European critical infrastructure.

Apparently, through these cables, the C-Lion 1 and the BCS East West Interlink, a lot of financial information was also exchanged between banks and stock exchange platforms, including SWIFT data. Cross-border financial transactions were thus involved.

1. Do European banks have sufficient alternatives for re-routing, and were such alternatives implemented in time immediately after the cables sustained damage?
2. Is current EU legislation in this area, such as the Digital Operational Resilience Act (DORA), adequate for this kind of incident?
3. Does the Commission have any recommendations for us in our capacity as co-legislators on how to better arm our financial institutions against this kind of hybrid attack?

Submitted: 10.12.2024