

(English version)

**Question for written answer E-002849/24
to the Commission
Auke Zijlstra (P/E)
(10 December 2024)**

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

**Answer given by Ms Albuquerque on behalf of the European Commission
(3 March 2025)**

Undersea communication cables operated by public telecommunication service providers, as the ones in question transporting financial sector data would be subject to cybersecurity measures under the directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) ⁽¹⁾, which includes also their protection from physical threats.

The Commission is closely following the recent incidents affecting submarine cables. It is reflecting on possible measures to improve security and resilience of this critical infrastructure, in cooperation with Member States, in addition to the recent Recommendation (EU) 2024/779 ⁽²⁾ on the topic.

The Commission is not aware of disruptions of a systemic nature in the provision of financial services as a result of the recent incidents affecting the submarine cables.

In addition to the NIS2 Directive, the Digital Operational Resilience Act (DORA) ⁽³⁾, referred to by the Honourable Member, is also relevant for enhancing the financial sector’s resilience against such kind of incidents.

Under DORA, EU regulated financial entities are required to put in place contingency measures and plans (e.g. business continuity, etc.) to counter such incidents affecting their systems and networks, as well as to perform third-party risk assessments on the providers of information and communication technology (ICT)-services, including of communication and data transmission solutions.

⁽¹⁾ OJ L 333, 27.12.2022, p. 80-152, <http://data.europa.eu/eli/dir/2022/2555/oj>

⁽²⁾ C/2024/1181, OJ L, 2024/779, 8.3.2024.

⁽³⁾ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333, 27.12.2022, p. 1-79.