

## EMERGING RISKS IN THE INSURANCE SECTOR



### PETRA HIELKEMA

Chairperson – European  
Insurance and Occupational  
Pensions Authority (EIOPA)

### From fragmentation to emerging risks: a new framework for supervision

In recent years, geopolitical fragmentation has shifted from a tail risk to a defining feature of the global economy. Military conflicts, trade tensions and supply-chain disruptions are no longer just hypothetical scenarios, but persistent forces reshaping risks.

Geopolitical risks may take different forms, yet their common feature lies in the sustained uncertainty they generate. This uncertainty plays a fundamental role for economic agents, affecting their expectations, confidence and risk aversion. Simultaneously, it poses significant challenges for supervisors, who must adapt their frameworks to effectively account for these risks.

The materialisation of geopolitical risks can have far-reaching consequences, transmitting through the real economy and financial markets and, as an implication, affecting the insurance

sector<sup>1</sup>. A simple example is energy prices. When energy prices rise, inflation increases. To contain inflation, central banks may adopt tighter monetary policies, which can result in stricter financial conditions, slower economic growth, and a decline in real household incomes. Such conditions affect insurers not solely through elevated risk premia, asset devaluations, or adjustments to the discount rate applied to liabilities. They may also give rise to higher-than-anticipated claims inflation and more surrenders, as policyholders experience financial strain or reallocate capital toward competing products. Broad market stresses can also affect market liquidity, with more opaque assets like private debt to be affected the most. Rising uncertainty in recent years has coincided with resilient economies, but it also exposes their vulnerabilities if uncertainty persists. Moreover, geopolitical events can intensify pressures where sectors depend on cross-border infrastructure and may also involve state-sponsored cyberattacks, which test the sector's resilience – from an operational as well as underwriting perspective.

Supervisors, therefore, need to integrate such risks into their operational framework. This, however, requires moving beyond traditional backward-looking risk measures and treating geopolitical risk as a systemic factor that can simultaneously affect markets, counterparties, operations, and liquidity. The revised Solvency II provides supervisors with some effective tools to navigate this situation. Prime examples are the integration of macroprudential considerations and analysis in the risk management, the investment activities of undertakings, and the strengthened role of liquidity plans. Embedding these elements results in a deeper forward-looking understanding of common exposures, interlinkages and potential amplification effects across the sector. At the same time, the new framework allows for more risk taking while reducing capital buffers, which can have an impact in times of uncertainty.

In addition to geopolitical risks, supervisors must also consider cyber risks and risks related to artificial intelligence (AI). These risks should not be seen as standalone risks, but as amplifiers of weaknesses in governance, outsourcing, data quality and operational resilience. Insurers rely on technology to run

their core operations, underwrite risks, deliver services to policyholders and connect with partners. Higher levels of interconnectedness mean that cyber events can spread rapidly across entities. Concurrently, AI may also reinforce insurers' reliance on third-party providers and shared infrastructures, increasing concentration and dependency risks.

For supervisors, this implies a move towards holistic and forward-looking assessments. Expectations focus less on specific technologies and more on how digital tools interact with core functions, decision-making, and control frameworks. Boards are expected to integrate these interactions into their governance framework, rather than treating them as purely technical matters. Ultimately, viewing cyber risk and AI as amplifiers reinforces a key message: technology is not the risk. It does not alter fundamental prudential principles, but it can make existing weaknesses more visible, faster and more costly if left unaddressed.

**A forward-looking  
supervisory approach  
is essential as  
emerging risks amplify  
vulnerabilities.**

Finally, sound supervision, risk analysis and mitigation require access to relevant, high-quality data. The Solvency II reporting framework provides a robust basis for the insurance sector, but such frameworks need to evolve in light of emerging risks, while avoiding undue burden on industry. Recent initiatives at European level that aim to improve data sharing across EU financial services – such as the Better Data Sharing Regulation – should enable authorities to access, where justified, information already reported to other authorities. In this way, data exchanges would allow better use of already reported data, reduce duplication costs and streamline data flows.

1. *EIOPA 2024 insurance stress test exercise focused on the economic consequences of a re-intensification or prolongation of geopolitical tensions. The 2025 IORPs stress test had a similar focus.*