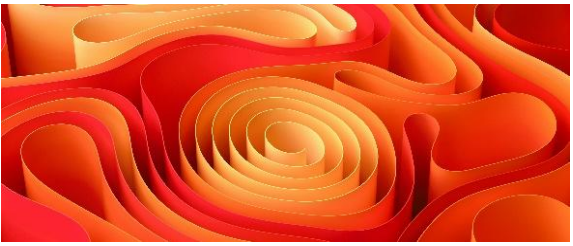
Pills

Regulatory/Supervisory Pills | N.140 September 2026

Author: Dario Esposito



TOPICS:

Crypto risk

SOURCE:

Bank for International Settlements

BIS: When Machines Attack - Frontier AI Cyber Threats and Policy Responses in the Financial Sector

- This paper assesses how increasingly capable **frontier AI models** are reshaping cyber risk and the supervisory response. It concludes that frontier AI represents a **step change in cyber threats primarily through greater speed, scale and autonomy**, rather than through fundamentally new attack techniques.
- **Frontier models** can autonomously identify vulnerabilities, develop working exploits and execute increasingly complex multi-stage attacks, substantially reducing the expertise, time and resources required by threat actors. Most importantly, the interval between vulnerability discovery and exploitation can shrink from weeks to minutes. However, these models also provide significant defensive benefits, including accelerated vulnerability discovery, threat detection, security monitoring and incident response.
- For financial institutions, the principal prudential implications are **compressed remediation timelines, increased breach probability and greater third-party/concentration risk**. Dependence on common cloud, software and frontier AI providers may transmit disruptions across multiple institutions and jurisdictions. Autonomous AI systems additionally require controls around permissions, activity logging, human approval and mechanisms for terminating agent activity.
- Financial authorities are broadly converging on a pragmatic approach: **reinforcing existing cyber risk management and operational resilience frameworks rather than creating separate AI-specific cyber regimes**. There are four core supervisory areas—governance, protection, detection, and response and recovery—supported by proportionality, third-party risk management, information-sharing and public-private collaboration.
- The supervisory priority is therefore **faster execution of established practices**: stronger board oversight, accelerated patching, continuous vulnerability management, realistic resilience testing, robust recovery arrangements and improved mapping of critical third-party dependencies. **Existing FSB, BCBS and IAIS frameworks provide the regulatory foundation**, but firms and supervisors must apply them with substantially greater urgency as cyber operations increasingly move at "machine speed."