Quantifying the Cyber Resilience of Maltese Banking Sector, Insights from T2

MATTEO PANFILO
Financial Stability Stress Testing & Research Office



BANK ĊENTRALI TA' MALTA
EUROSISTEMA
CENTRAL BANK OF MALTA

Agenda

1

Introduction

Some recent development, the EU framework and some statistics about the Maltese context

2

BoF PSS-3

Deep dive into the Bank of Finland PSS-3 Simulator

3

Impact Results

An overview of the main results. 640 simulations were run to collect data on the simulator's main statistics

4

System-Wide Perspective

Insights at banking system level and statistical aggregation of granular results

5

Way Forward

Some concluding remarks, technical recommendations, and some additional research ideas

target services | T2

PSS BOF-PSS3 THE BANK OF FINLAND PAYMENT AND SETTLEMENT SYSTEM SIMULATOR

1. Introduction

The institutional Framework

Integrity

ESRB 2022, Mitigating Cyber Risk
Introducing the concept of SITO

EU Regulation 2022/2554, DORA
Regulating digital operations for the financial sector

EU Regulation 2024/2847, Cyber Resilience Act
Mandatory operational requirements

ESRB 2026, Warning on systemic cyber risks from frontier AI
Introducing AI-enabled cyberattack

The Eurosystem Cyber Resilience Strategy (ECB, 2024) aims to strengthen the cyber resilience of financial market infrastructures through three complementary pillars:

Entity Readiness

Pillar1

Strengthen cyber maturity through harmonised oversight, cyber resilience assessments and penetration testing (TIBER-EU) to enhance prevention and response capabilities.

Sector Resilience

Pillar 2

Enhance sector-wide resilience by identifying critical dependencies, sharing information and conducting joint cyber crisis simulations and market-wide business continuity exercises.

Industry Coop.

Pillar 3

Foster regulator–industry collaboration through pan-European forums, the Euro Cyber Resilience Board (ECRB) and cyber intelligence sharing (CIISI-EU) to build trust and collective preparedness.

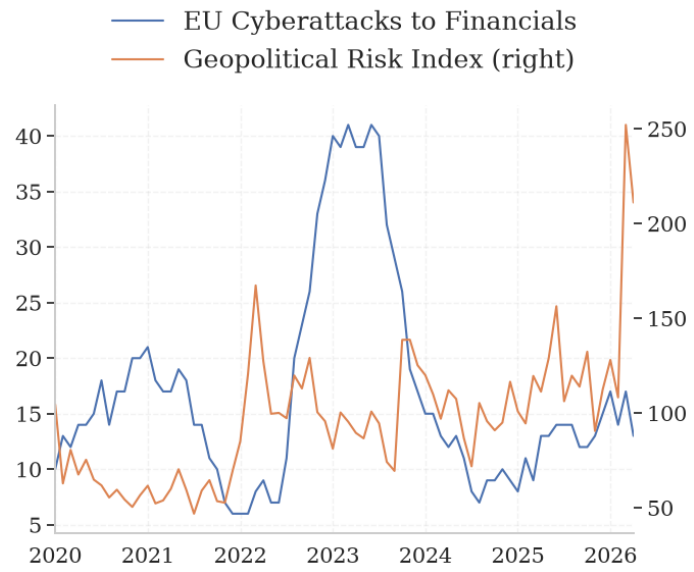
Introducing Cyber Risk

Cyberattacks targeting financial institutions appear to increase alongside **heightened geopolitical risk**. They are unevenly distributed across EU countries, with pronounced **geographical clustering**.

A severe or prolonged liquidity shock, induced by a denial of ICT services, can translate into bank and system impairment through several channels: **fire sales**, **higher funding costs**, **operational losses** and **contagion**.

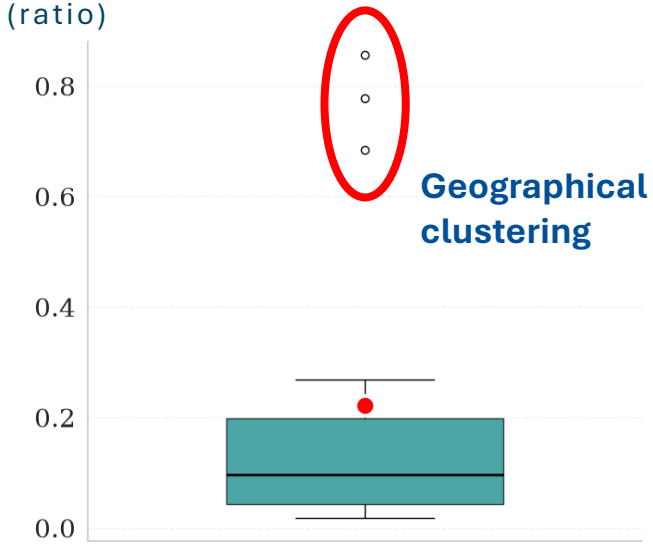
Geopolitical & Cyber Risk

(count; percentage (rhs))

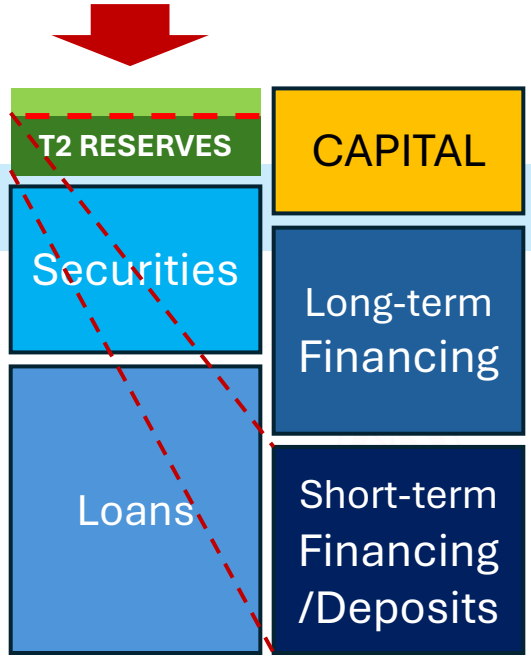


EA Country ratio of cyberattacks to financial corps. per T2 actor

(ratio)



Impact of a **Cyber-Incident**



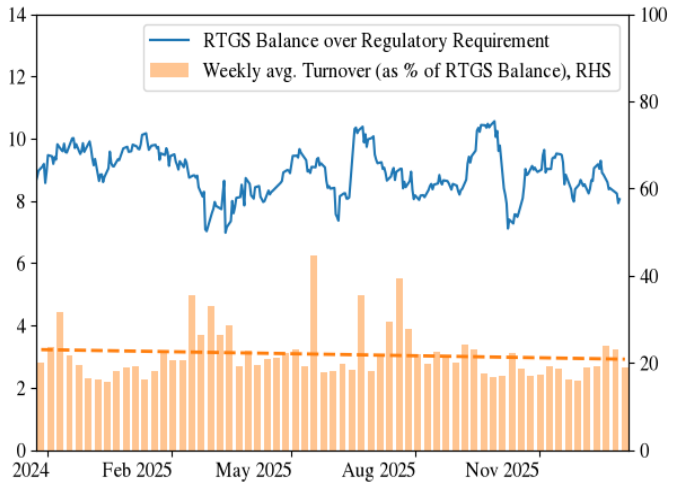
Insights from payments structure

The Maltese payment network is characterized by two main features:

1. The T2-Malta RTGS system exhibits **ample liquidity**, with balances consistently exceeding regulatory requirements (Chart 1).
2. Most interconnectedness and potential exposures arise from relationships with **non-domestic institutions** (Chart 2).

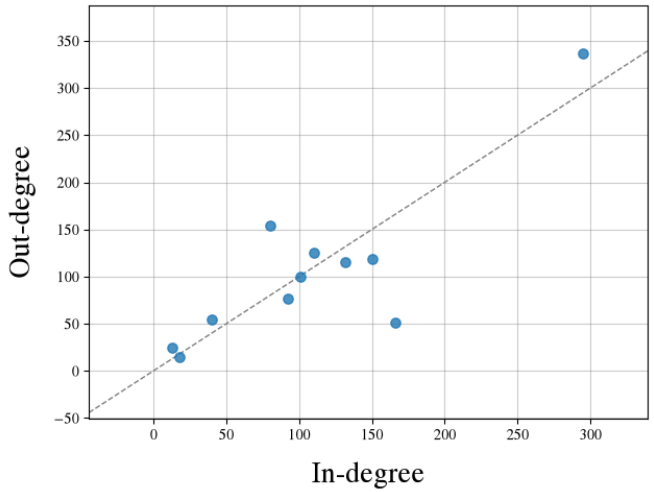
T2-Malta RTGS Balances

(ratio; percentage)

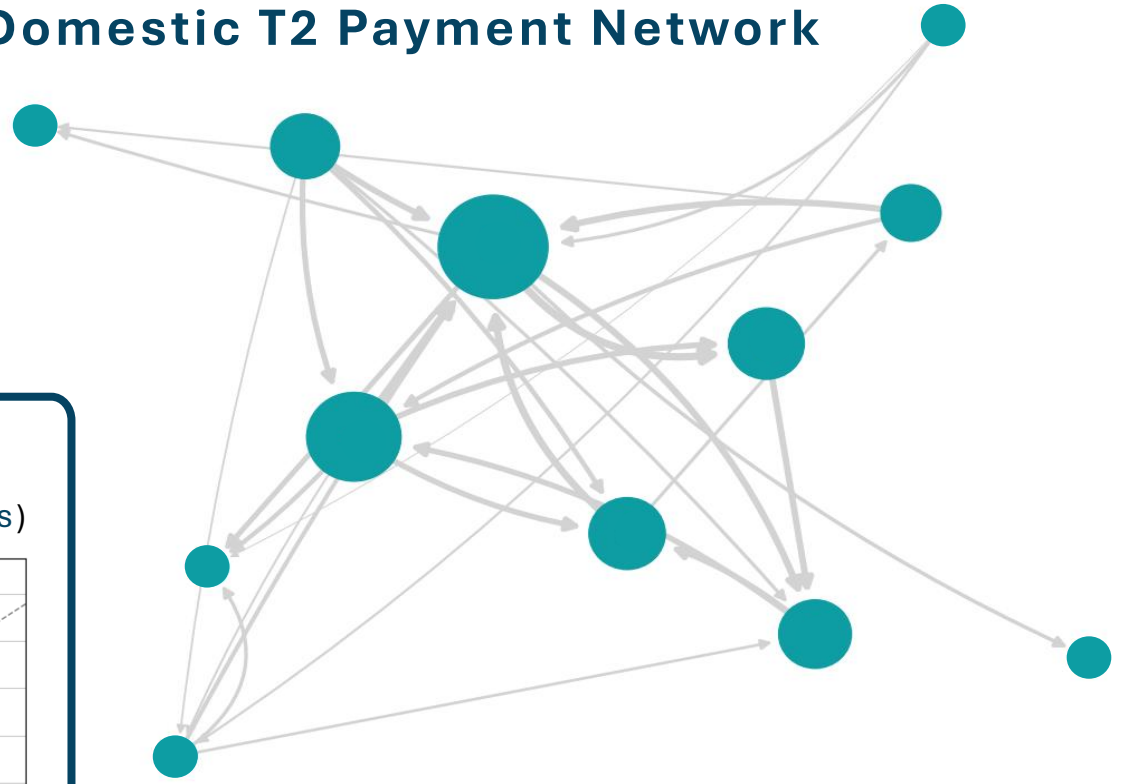


Payment Network Total Connectivity

(node counts)



Domestic T2 Payment Network

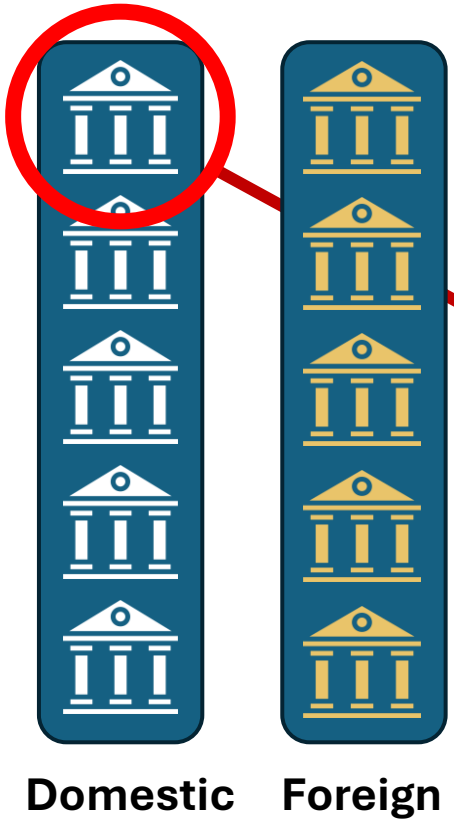


The domestic payment network exhibits a **core-periphery structure**.
Domestic links provide an insight about contagion, but underestimate Maltese banks exposure to cyber risk.

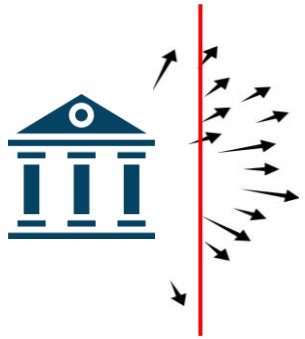
2. Bank of Finland PSS-3

Designing the scenarios

A cyber incident is modelled under the **liquidity sink assumption** (Eisenbach, 2022). The ICT disruption prevents the affected bank from executing outgoing payments, causing it to accumulate liquidity while other T2 participants experience shortfalls.



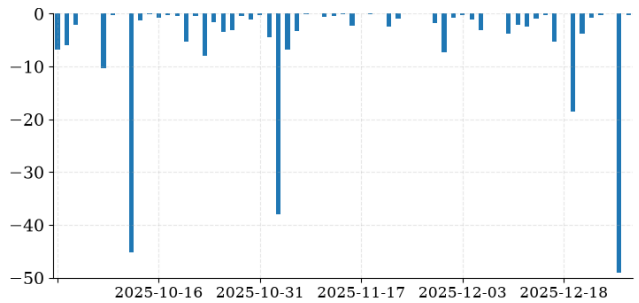
Liquidity Sink
The cyber incident prevents outflow orders to be processed …



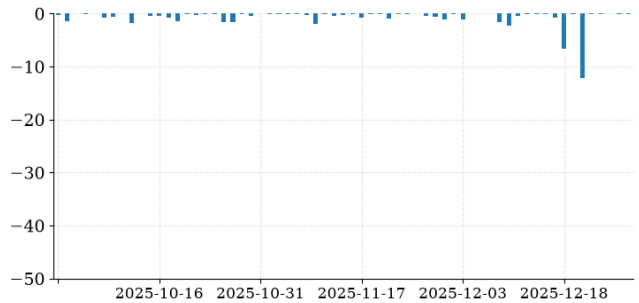
… As a result, other banks cannot receive central bank money while the target bank accumulates reserves

Repeat for any day in Q4 2025!

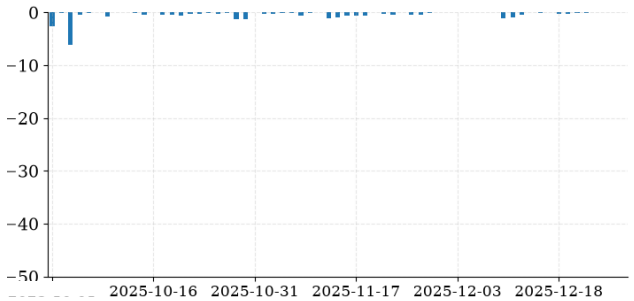
Affected Bank A



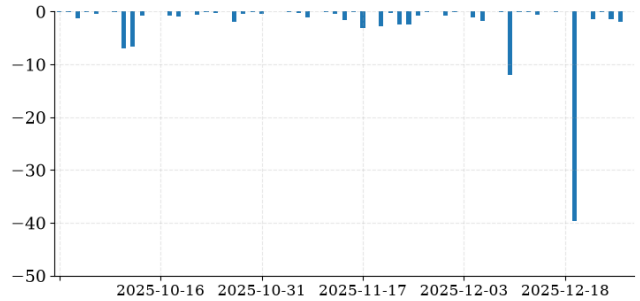
Affected Bank B



Affected Bank C



Affected Bank D



3. Impact Results

Cyber-Risk Topology

Scenarios

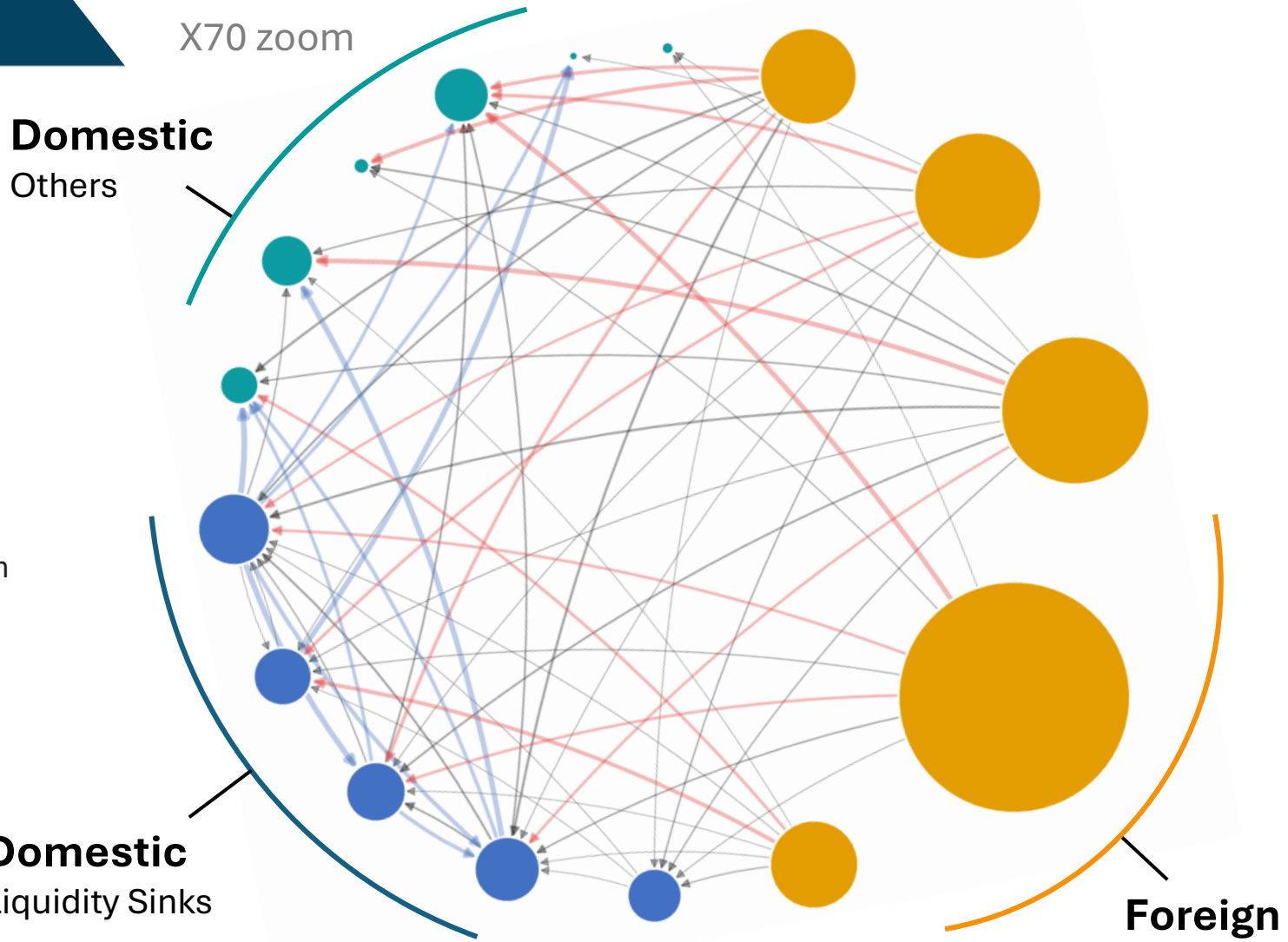
- Q4 2025 Daily Events = 64 operational days
- 5 Most Active T2 banks = 5 Liq. Sinks
- 5 Top Foreign Senders = 5 Liq. Sinks

Total: 640 Daily Simulations

The network reveals a heterogeneous distribution of **worst-case liquidity deterioration**, with the largest exposures concentrated among a few domestic institutions.

T2 participants' **interconnectedness** highlights potential channels through which cyber-related disruptions could propagate across the banking system.

Network distribution of worst-case liquidity deterioration, Q4 2025



A Map of Cyber-impact

Scenarios

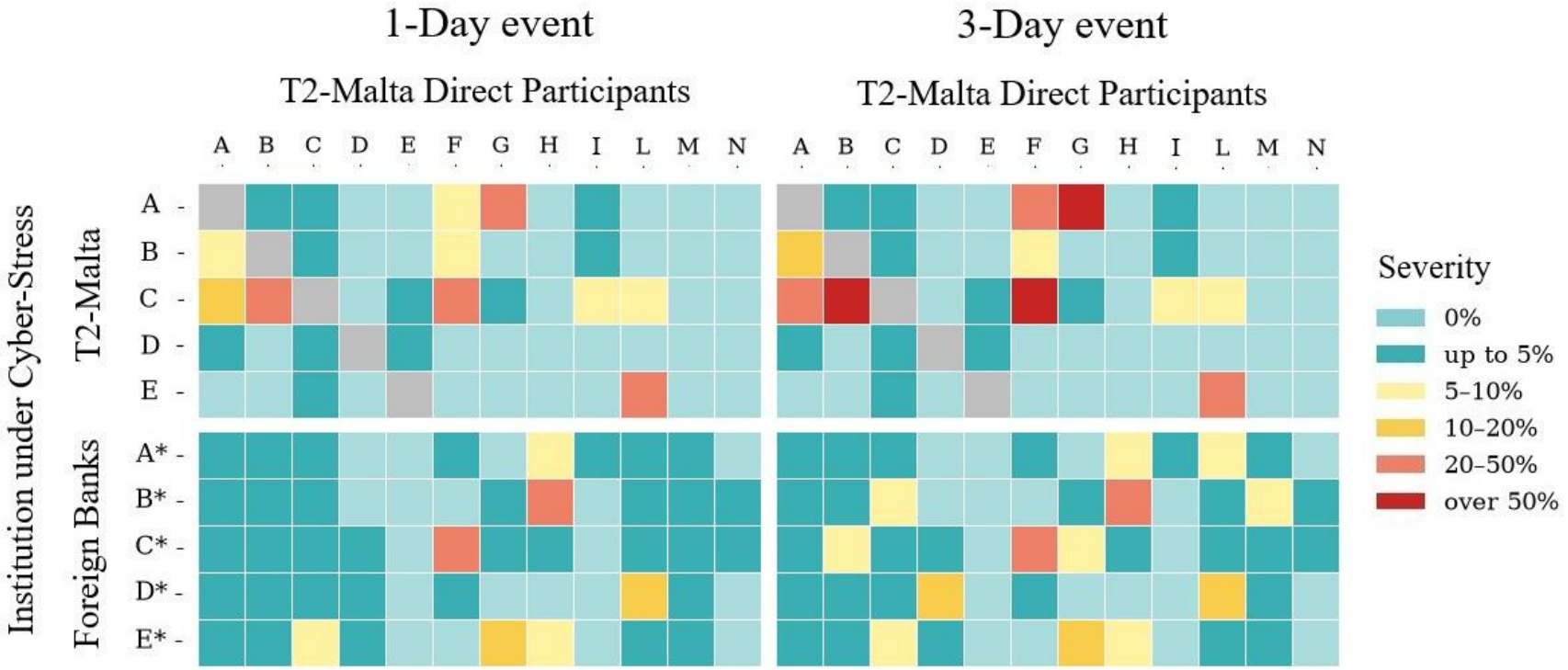
- Q4 2025 Daily Events = 64 days
- 5 Most Active T2 banks = 5 Liq. Sinks
- 5 Top Foreign Senders = 5 Liq. Sinks

Total: 640 Daily Simulations

Domestic institutions generate **liquidity deterioration**, particularly under prolonged cyber disruptions.

Conversely, **foreign institutions** tend to produce lower deterioration but **more widespread impacts**. The number of affected institutions increases with the duration of the disruption.

Worst *liquidity deterioration* across Q4 2025 daily exercises, who-to-whom matrix



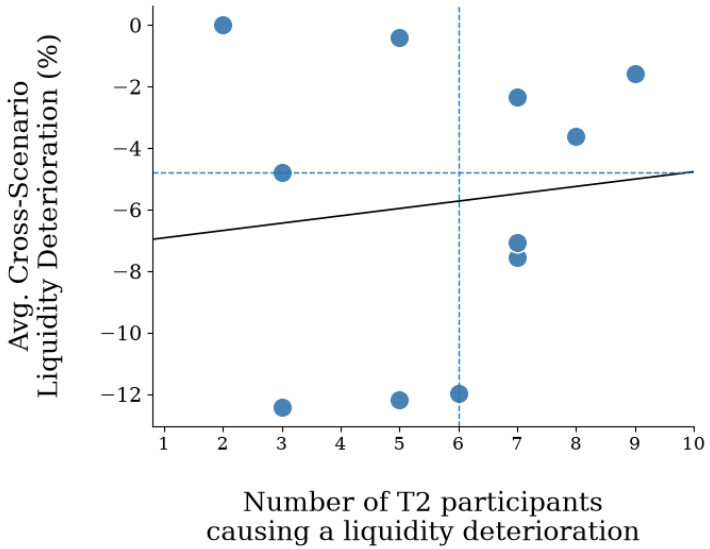
4. A System-Wide Perspective

Different risk profiles

The relationship between the **number of nodes causing liquidity deterioration** and the **average liquidity deterioration caused**, varies. Domestic banks exhibit a positive correlation between the two; foreign banks show a slightly negative relationship.

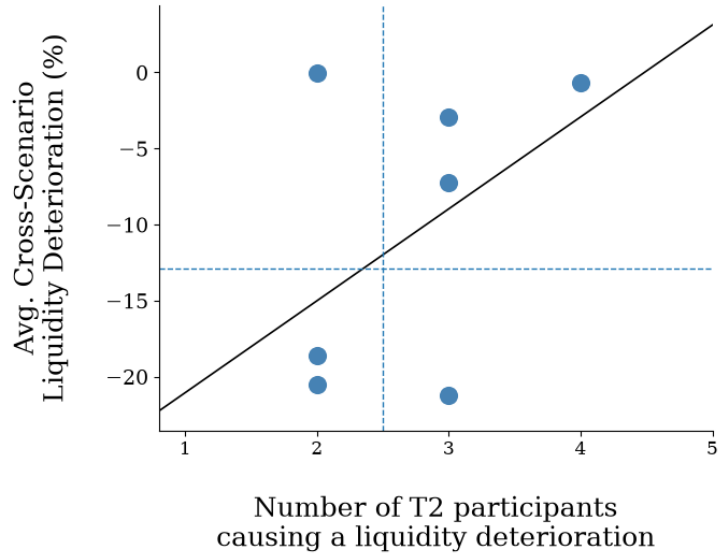
All *Liquidity Sinks*

(percentage; count)



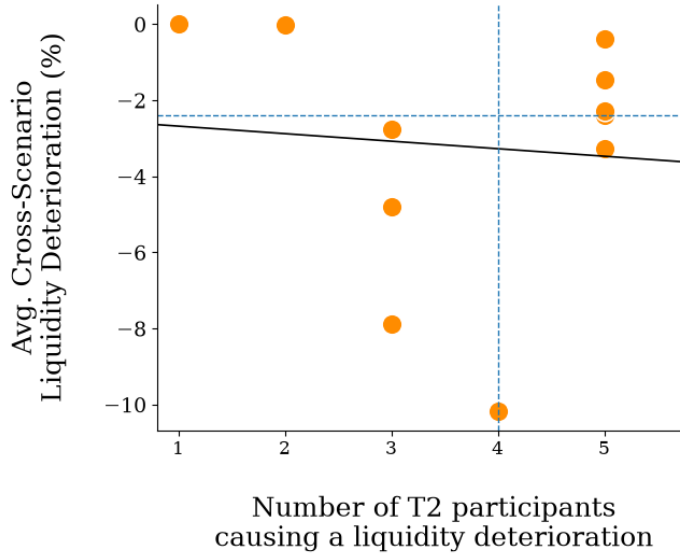
Domestic *Liquidity Sinks*

(percentage; count)



Foreign *Liquidity Sinks*

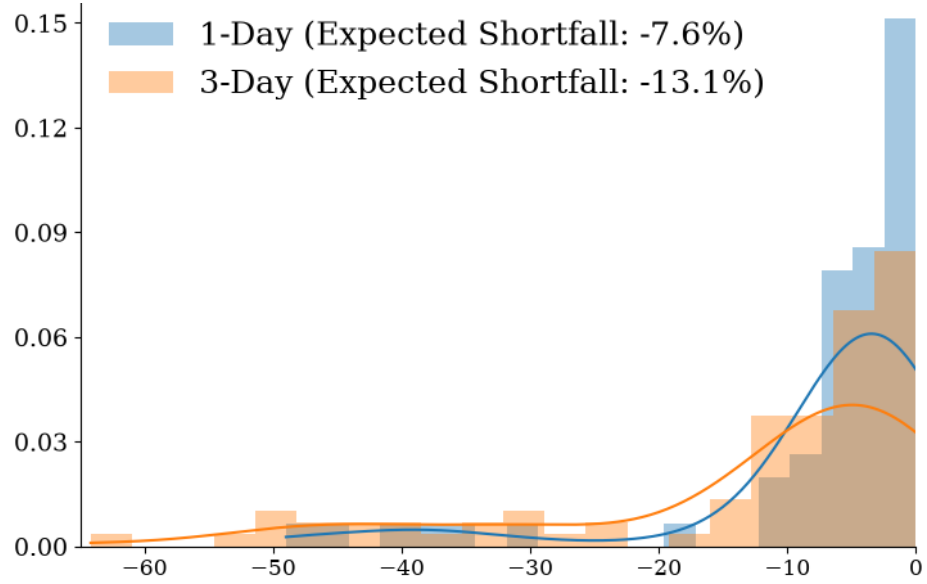
(percentage; count)



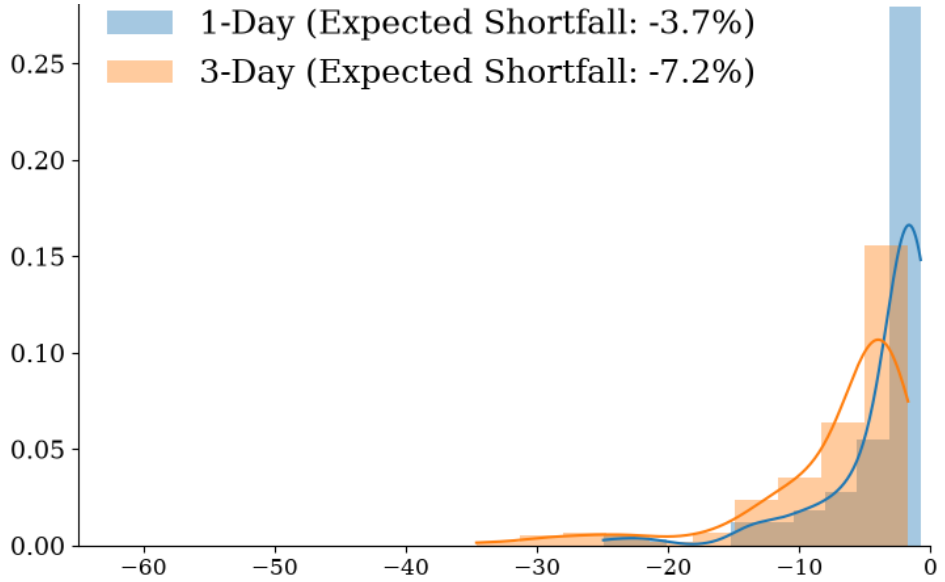
The Severity of Cyber Shocks

Liquidity deterioration is highly heterogeneous across banks. By focusing on individual **banks' highest liquidity shortfalls** (i.e. the worst 10% of cases generating negative liquidity gaps), we can assess how the **severity of extreme outcomes** differs between 1-day and 3-day stress horizons. Domestic liquidity sinks exhibit substantially heavier downside tails.

Distribution of bank-specific extreme liquidity deterioration across scenarios, Domestic *liquidity sink*



Distribution of bank-specific extreme liquidity deterioration across scenarios, Foreign *liquidity sink*

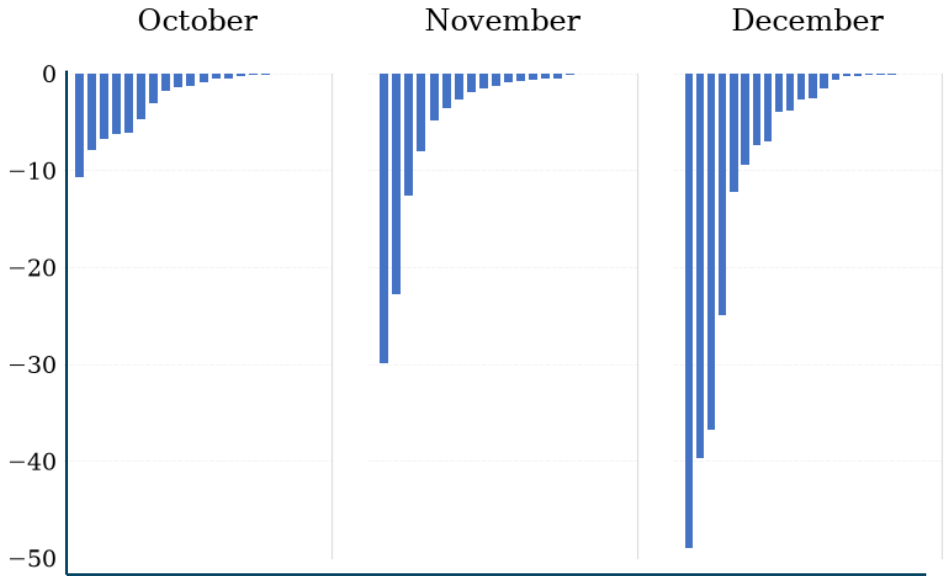


Exploring the time dimension

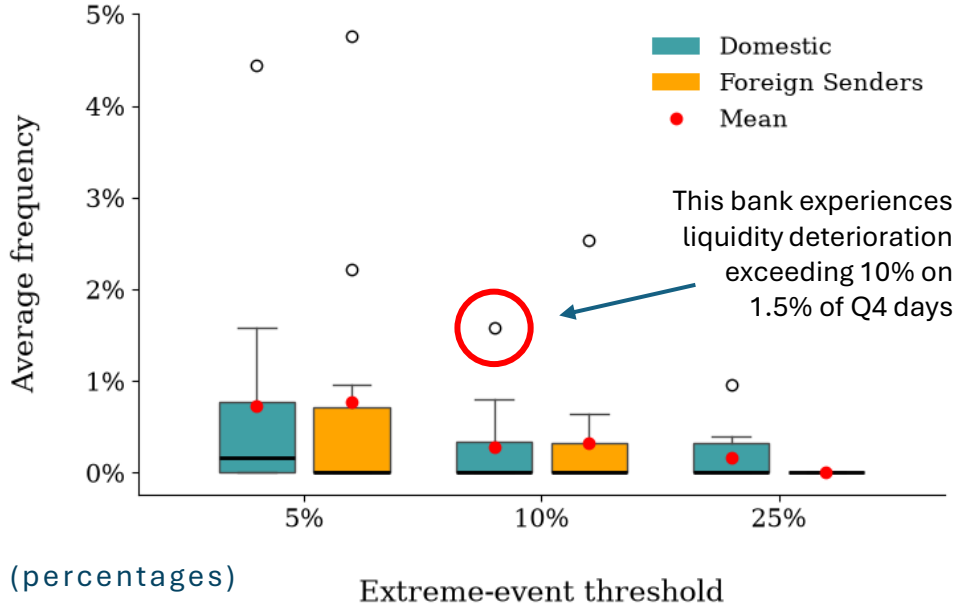
Worst-case liquidity deterioration exhibits a clear **time dimension**, with the magnitude of extreme shocks increasing markedly towards end-year. **Extreme liquidity deterioration is relatively infrequent** across banks, with the most severe episodes concentrated in a limited number of institutions and days.

Seasonality of worst-case impacts

(percentages)



Distribution of bank-specific average threshold-breach frequencies



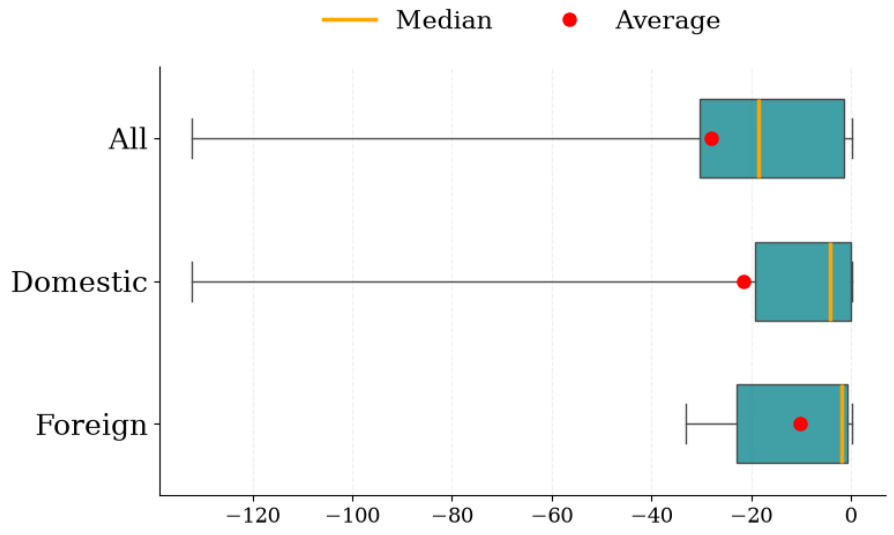
(percentages)

Surveillance Benchmarks

Cyber-related liquidity shocks can significantly **impact banks' LCR**, with pronounced downside risks and significant heterogeneity across banks. Differences in banks' **business models and liquidity profiles** shape their exposure to extreme shocks, and larger initial liquidity buffers do not necessarily ensure greater resilience.

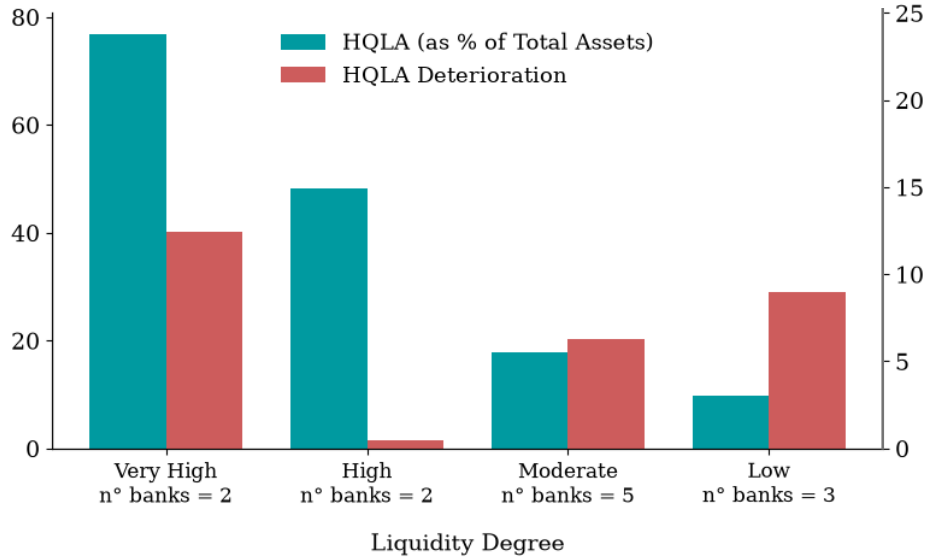
Distribution of counterfactual LCR worst-shifts

(percentage points)



Counterfactual HQLA deterioration & Banks' liquidity position

(percentages)



6. Way Forward

KEY FINDINGS

1

TIME IS KEY

The timing of cyber disruptions is crucial in determining their liquidity impact. Temporary interruptions generate material shortfalls when occurring during heightened interbank activity.

2

BUSINESS MODELS AS A DRIVER

Recorded liquidity deterioration varies according to reserve management practices and payment patterns. High interbank activity and reliance on big institutions play a crucial role.

3

THE LIQUIDITY TRADE-OFF

Larger institutions generally benefit from more substantial liquidity buffers, absorbing payment disruptions, but also retainining some the capacity of spreading any impact.

WAY FORWARD

1

MONITORING NEW DYNAMICS

Monitor counterparty and geographical concentration of payment flows, integrating multi-day disruptions into banks' liquidity contingency plans and operational resilience testing

2

DEFINE A SITO

Assess the severity, duration and systemic impact of disruptions to inform crisis escalation criteria and strengthen contingency frameworks.

3

EXTEND THE FRAMEWORK

To incorporate simultaneous disruptions, third-party failures, strategically timed cyberattacks and banks' liquidity management responses, including potential liquidity-to-solvency spillovers

Ending note



BANK ĊENTRALI TA' MALTA
EUROSISTEMA
CENTRAL BANK OF MALTA