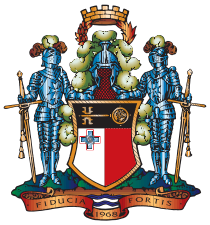


BANK ĊENTRALI TA' MALTA
EUROSISTEMA
CENTRAL BANK OF MALTA

SPECIAL FEATURE: USING T2 TO ASSESS PAYMENT-SYSTEM FLOWS RELEVANT FOR CYBER STRESS TESTING IN MALTA

Article published in the Financial Stability Report 2025, pp. 85-93

SPECIAL FEATURE: USING T2 TO ASSESS PAYMENT-SYSTEM FLOWS RELEVANT FOR CYBER STRESS TESTING IN MALTA[1]

In recent decades, the financial services sector has undergone a profound transformation driven by digitalisation and increasing interconnectedness. As a result, dependence on information and communications technology (ICT) infrastructure has become critical for the provision of essential economic functions, including customer services, risk management, and payment settlement. Against this backdrop, cyber incidents have become a growing source of operational disruption. In severe cases, such incidents could impair critical financial functions at increasing speed and scale, trigger second-round effects, and ultimately give rise to financial stability concerns.[2] Rising geopolitical tensions – increasingly manifesting as cyber threats – alongside greater reliance on ICT and a growing concentration among payment infrastructure providers have brought this issue to the forefront of the policy agenda. In response, several international institutions, including the Financial Stability Board (FSB), the European Systemic Risk Board (ESRB), the European Union Agency for Cybersecurity (ENISA), the World Economic Forum (WEF), and the International Monetary Fund (IMF), have developed policy recommendations and analytical frameworks to strengthen cyber resilience and assess cyber-related systemic risk.[3]

Payment infrastructures deserve particular attention in this context. Cyber incidents could result in their partial or complete freeze, preventing a targeted institution from sending and/or receiving payments. Such an event could spread rapidly to other institutions, accelerating the speed at which risks become systemic. In the euro area, these dynamics are especially relevant in the context of T2 (TARGET2), the Eurosystem's real-time gross settlement system, introduced in its current form in March 2023 as part of the TARGET Services consolidation project. By providing transaction-level information of payment flows, T2 offers a useful basis for analysing the financial stability implications of ICT disruptions affecting payment infrastructures and for assessing systemic risk arising from cyber events.

This document provides a first step towards a cyber stress-testing framework for Maltese payment systems. T2 transaction-level data is used to map payment network topologies, identify critical nodes and connections, and detect potential vulnerabilities that could be tested in future scenario-based exercises. The first section introduces T2 and its role in the domestic payment system. The second section uses transaction-level indicators to identify potential cyber vulnerabilities. The third section complements this evidence with a network-based analysis of domestic payment flows, highlighting the centrality and connectivity of key participants. The final section summarises the main findings and outlines the next steps towards a structural framework for assessing payments-related cyber risk and its implications for financial stability.

T2 and the Maltese payment system

T2 is the Eurosystem's real-time gross settlement (RTGS) system for euro payment transactions supporting monetary policy operations, bank-to-bank transfers, and commercial payments. In 2023, the EU's harmonised market infrastructure, TARGET Services, consolidated T2 with TARGET2-Securities (T2S) and a TARGET Instant Payment Settlement (TIPS). This led to a consolidated Eurosystem market infrastructure for transaction settlement in central bank money. T2 comprises two modules, a central liquidity management (CLM) platform and an RTGS service. The former supports the settlement of central bank operations and the management of participants' liquidity, while the RTGS platform handles payment transactions and

[1] Authored by Matteo Panfilo and Francesco Ricciutelli, Research Economists, and Pedro Polvora, Deputy Head within the Macroprudential Policy, Stress Testing and Research Department of the Central Bank of Malta. The authors would like to thank Alan Cassar, Christine Balzan, Wendy Zammit, Tiziana Grech, Francesca Bozza, Mariah Dimech, Edward Magro, Claudine Psaila, and Shaun Vella for their helpful inputs and suggestions.

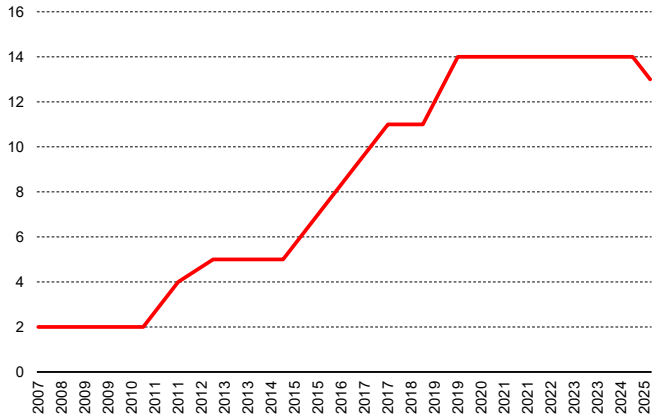
[2] According to the FSB Lexicon 2023, a cyber incident is defined as "cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not".

[3] The main bibliographic references involve: ENISA Threat Landscape 2025 (ENISA, 2025), Systemic Cyber Risk (ESRB, 2020), Mitigating Systemic Cyber Risk (ESRB, 2022), Advancing Macroprudential Tools for Cyber Resilience (ESRB, 2023), Advancing Macroprudential Tools for Cyber Resilience – Operational Policy Tools (ESRB, 2024), Global Cybersecurity Outlook (WEF, 2025) and Global Financial Stability Report, April 2024 (IMF, 2024).

ancillary system (AS) settlement.[4] By recording the full sequence of payment events, T2 modules enable the detection of potential stress patterns consistent with disruption, such as rising levels of unsettled payments, abnormal delays, and network fragmentation. These patterns are particularly relevant in a small and highly interconnected banking system, where a limited number of participants account for a large share of overall transactions.

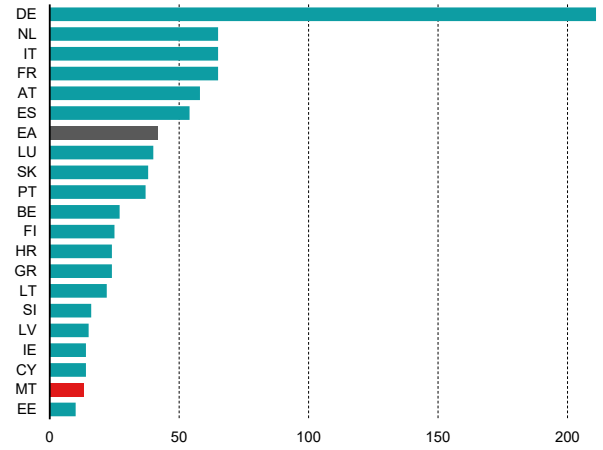
Operated by the Central Bank of Malta, the Maltese component of T2 (T2-Malta) provides Maltese participants with access to central bank money settlement. Since its adoption in 2007, the total number of direct participants in T2-Malta has increased, reaching 13 participants by the first quarter of 2025 (see Chart 1).[5] Despite being a small open economy, Malta's participation in T2 reflects the relative complexity and depth of its financial sector (see Chart 2).

Chart 1
NUMBER OF T2-MALTA DIRECT PARTICIPANTS OVER TIME



Source: ECB Statistical DataWarehouse (SDW).
Notes: Number of direct participants in the payments system (PSN), yearly and semiannual collection; the annual time-series has been augmented by integrating the semiannual observation from H1 2025.

Chart 2
NUMBER OF T2 DIRECT PARTICIPANTS IN THE EURO AREA IN 2025



Source: ECB Statistical Data Warehouse (SDW).

T2-Malta also identifies critical participants according to entities' activity. A T2 participant is usually considered critical if it meets at least one of two criteria related to the generated turnover in T2,[6] and the amount of unsettled T2 payments generated by simulating a technical failure of the credit institution, conditional on time dependence.[7]

From an aggregate perspective, both the average daily volume and value of transactions settled by critical participants in T2-Malta declined in the corresponding quarter over the last three years. This decline in transacted value was mainly driven by the four largest domestic banks, while the value transacted by

[4] Ancillary systems (AS) are systems in which payments and financial instruments are exchanged and cleared. In turn, resulting obligations are settled in TARGET. Examples of AS include retail payment systems, large-value payment systems, foreign exchange systems, money market systems, automated clearing houses, central counterparties (CCPs) and securities settlement systems.

[5] "A party owning an RTGS DCA or RTGS CB Account and having direct access to RTGS" as per T2 Glossary definition.

[6] The T2 turnover is computed as the sum of the traffic generated by each credit institution at the technical platform level, where generated means that transactions where the credit institution is debited but that are not initiated by the credit institution have to be filtered out. Notice that the average daily traffic includes customer, interbank and Continuous Linked Settlement (CLS) transactions, as well as liquidity transfers to T2S.

[7] The criteria for determining the criticality of participants are based on the information guides regularly published by the European Central Bank. As a general guideline, the Eurosystem considers a credit institution to be a critical TARGET (CLM and RTGS) participant if it consistently settles at least 1% of the value of the CLM and RTGS turnover as a daily average in the first quarter of the year (so-called Criterion 1). This includes interbank payments, customer payments, liquidity transfers and AS-related transactions where (i) the initiator is the debited participant and (ii) the debited and credited parties are not the same or do not belong to the same technical platform. In addition, criticality depends on the previous year's classification for both critical and non-critical participants. Further details are available at the following link, in the subsection T2 Participation/Registration, Information Guide for TARGET participants, Part 2 CLM and RTGS: T2 documents and links.

the remaining institutions increased significantly. Nevertheless, in 2025 Q4, around three-quarters of the daily average transacted value was accounted for by the four largest domestic banks, down from 85% and 80% in 2023 and 2024. By contrast, the daily average transacted value of the remaining credit institutions increased from 14% in 2023 to 20% in 2024 and further to 24% in 2025.

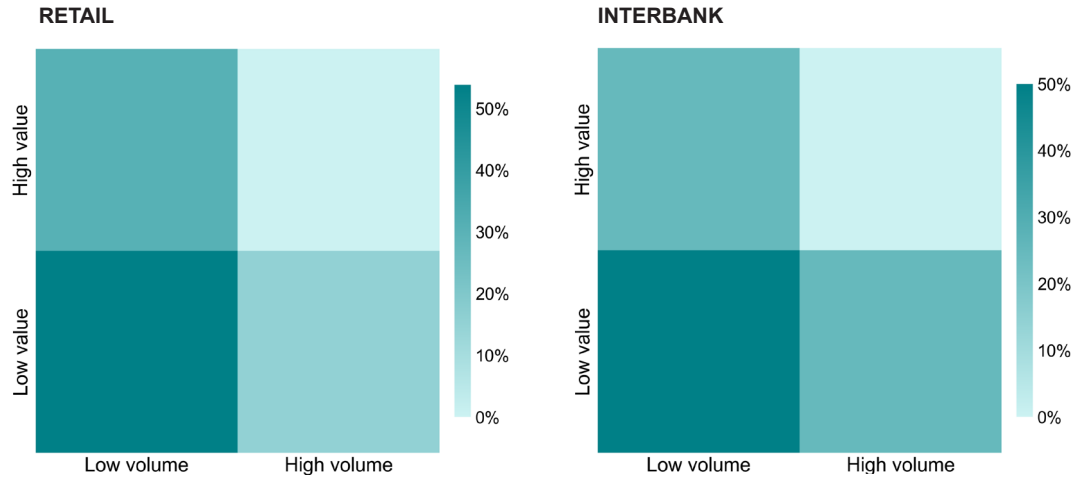
Determining cyber-risk systemic vulnerabilities from payment system activity

The identification of potential transaction-related systemic vulnerabilities involves assessing transactional configurations and financial structures that may trigger or amplify systemic losses due to a cyber threat targeting one or more financial institutions.[8] In the context of payment systems, this includes scenarios in which critical T2-based services are compromised and can no longer guarantee a minimum operational level or be restored within an appropriate recovery window. Such disruptions could generate material second-round effects on counterparties' liquidity and, more broadly, on the functioning of financial intermediation. The potential impact is likely to be greater in high value transactions, even if these are relatively less relevant in terms of volumes.

Chart 3 illustrates the share of participants across transaction-value and transaction-volume categories in 2025. It shows whether institutions are above or below the banking system average in terms of average transaction size and transaction volume, separately for the retail and interbank segments. The darker the colour gradient, the higher the share of participants – expressed as a percentage of the total population – in each quadrant of the matrixes. Most T2-Malta institutions are characterised by low transaction volumes and low average transaction values in both the retail and interbank segments, as illustrated in Chart 3.[9,10] However, a non-negligible share of observations falls within the low-volume, high-value cluster, particularly in the retail segment.

This configuration suggests that potential losses stemming from cyber incidents may be asymmetric. A subset of institutions appears particularly exposed to disruptions affecting low-frequency, high-value

Chart 3
TOPOLOGY OF TRANSACTIONS BY SWIFT MESSAGE CATEGORIES



Sources: T2 Data Warehouse and authors' calculations.

[8] T2 data can help identify operational and systemic vulnerabilities, but not all cyber-control vulnerabilities. It is suitable information for criticality, timing, concentration, substitutability, and contagion assessments. However, it is less appropriate for segmentation quality, threat detection maturity, backup immutability, forensics capability, or governance quality. Those require complementary evidence such as questionnaires, incident reports, DORA third-party information, or TLPT/TIBER-style testing.

[9] TRN stands for Transaction Report; this represents the core T2 data entity for cash transfer orders/cash transfers. See Data Warehouse User Handbook v. R2026.JUN for further details about T2 reporting.

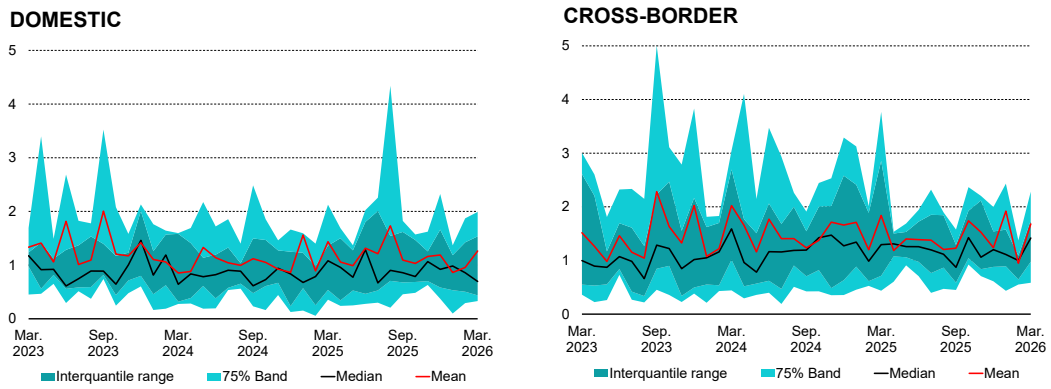
[10] The sample comprises settled 2025 transactions of T2-Malta participants active in 2025, involving Maltese banks and other T2 participants holding a Maltese T2 account; excluding transactions with monetary authorities, direct debit and internal transfers between accounts held by the same entity.

transactions in the retail segment, where even limited operational impairment in sending or receiving payments could generate disproportionately large operational and financial consequences. For instance, a temporary inability to send a small number of large corporate or customer payments could create sizeable liquidity shortfalls for counterparties, while a failure to receive high-value inflows could impair the affected institution's ability to fund subsequent payments. Similarly, in the interbank segment, disruptions to a participant that is mostly engaged in either fewer but larger-value transactions or, additionally, very frequent but low-value transactions could also interfere with liquidity redistribution. This highlights why transaction value, and not only frequency, is relevant for identifying cyber-related systemic vulnerabilities.

The outflow-to-inflow ratio shown in Chart 4 provides a complementary perspective by indicating whether, on average, a bank sends more funds to the financial system than it receives from it, or vice versa. The ratio may therefore signal short-term liquidity imbalances, contingent on the institution's broader funding position. Values above one indicate net outflows, while values below one reflect net inflows. Pronounced imbalances can be relevant in cyber stress scenarios because they help identify institutions or payment corridors where disruptions to outgoing or incoming payments could generate liquidity pressures.

At the domestic level, the outflow-to-inflow ratio remains broadly stable over time and close to one. This means that, on average, the value of payments sent by Maltese participants to other domestic participants is broadly matched by the value of payments received from them. In other words, domestic payment flows appear relatively balanced, with no persistent evidence of large net outflows or inflows at the system level. In contrast, the cross-border outflow-to-inflow ratio shows more volatile episodes and a mild upward trend, reflecting a gradual increase in net outflows abroad relative to the inflows received over the period. Overall, the median of the ratio remains close to unity, suggesting that payment flows are generally balanced on average. The mean, consistently above the median, indicates that the distribution is pulled upward by a relatively small number of high-value transactions from a subset of institutions with comparatively elevated ratios. The dispersion captured by the quantile bands highlights substantial heterogeneity across

Chart 4
DYNAMIC DISTRIBUTION OF OUTFLOW-TO-INFLOW RATIO



Sources: T2 Data Warehouse and authors' calculations.
Notes: Quantiles over time of the outflow-to-inflow ratio for T2-Malta participants spanning from March 2023 to March 2026. The ratio is calculated by dividing the total nominal outflow value (debited transactions) by the total nominal inflow value (credited transactions) of transactions excluding monetary authorities and internal transfers. A value equal to one indicates perfect matching between outgoing and incoming payment values; values above one indicate net outflows, while values below one indicate net inflows. Eligible transactions include domestic transactions and cross-border transactions, both excluding T2-relevant authorities, the Central Bank of Malta, and technical or operational transactions.[1]

[1] For the sake of filtering eligible transactions, this study prioritizes material financial transactions across entities, to represent the network of actual payments on a best effort basis, so as to focus on transactions not involving central bank core operations, technical transfers and operational tests, billing procedures and routing of funds across accounts owned by the same T2 participant. This approach excludes all the transactions involving the Central Bank of Malta and the ECB as main counterparty, EBA Clearing and other related operators, ASs and CCPs.

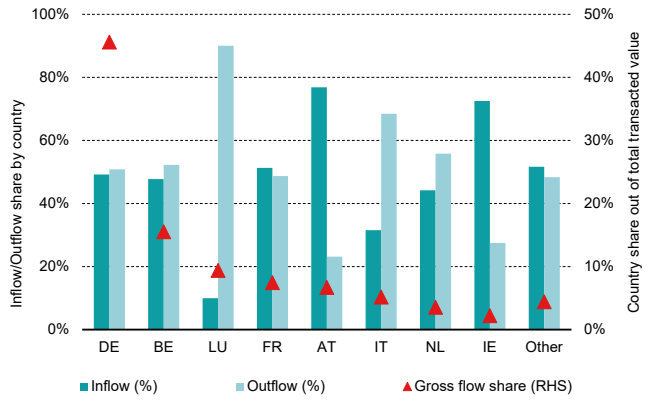
banks and over time, with occasional spikes in the upper tail. These episodes are notably more frequent in cross-border transactions.

From a Maltese financial stability perspective, however, one vulnerability of particular interest is banks' reliance on sizeable incoming cross-border payments from specific foreign jurisdictions. If a cyber incident were to impair the ability of a foreign counterparty or jurisdiction to execute outgoing payments towards Malta, Maltese recipient institutions could face liquidity pressures, especially where expected inflows are used to fund subsequent payments. In this sense, net inflow patterns are particularly informative for identifying foreign countries and payment corridors that should remain on the Bank's assessment radar. Jurisdictions that act as important sources of inflows for Maltese banks may therefore be especially relevant when designing cross-border variants of cyber stress-test scenarios.

Chart 5 depicts the extent to which the main T2 euro area partners contribute to total cross-border transacted value for the year 2025, by decomposing the total nominal flows exchanged with each country into inflow and outflow percentage shares. For instance, Germany is the most significant jurisdiction in this system, representing 46% of the overall transacted value, of which roughly 51% are outflows and 49% inflows. This deep dive into the geographical distribution of Maltese cross-border financial flows reveals a marked concentration of transacted value with a limited number of euro area jurisdictions, with fewer than five countries accounting for more than 80% of total cross-border activity. This points to a high degree of geographic concentration in payment flows. Moreover, the asymmetry between debited and credited transactions across countries highlights the presence of net-sender and net-receiver jurisdictions, reflecting directional dependencies in liquidity movements. Such a structure implies that ICT disruptions affecting key jurisdictions could have disproportionate systemic effects, particularly when payment activity is concentrated in a small number of systemically relevant institutions.

Malta appears to be strongly interconnected, particularly with a subset of large euro area economies that exhibit relatively high inflows and outflows. Exposure is also pronounced towards a smaller group of mainly unidirectional actors, whose monetary flows are either primarily absorbed by, or channelled outward from, the Maltese economy. However, given the small size of the Maltese payment system, these flows are unlikely to be material from the perspective of the recipient jurisdictions. For Malta, the more relevant vulnerability stems from countries that are important sources of inflows, such as Austria and Ireland. In this context, a payment disruption could propagate and impact the Maltese system as well, since cyber disruptions targeting institutions or payment infrastructure in these countries might critically reduce incoming payments to Maltese banks and cause liquidity pressures for domestic recipients. Overall, Malta's cross-border vulnerabilities appear concentrated along a limited number of critical payment corridors, which can help inform the design of cross-border cyber stress-test scenarios.

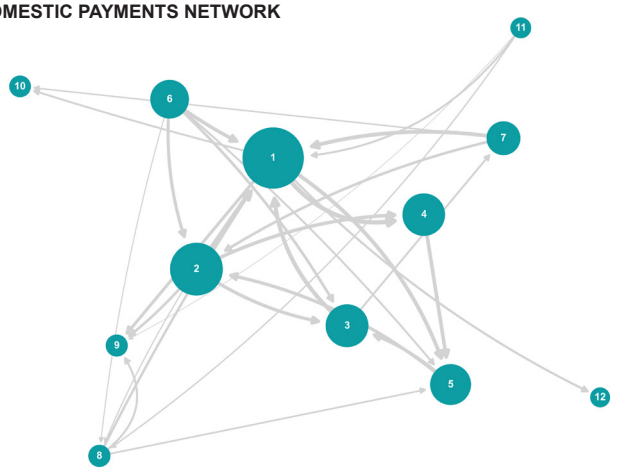
Chart 5
GEOGRAPHICAL DISTRIBUTION OF T2 MALTESE CROSS-BORDER TRANSACTIONS
(percentages)



Sources: T2 Data Warehouse and authors' calculations.

A bird's-eye view of the domestic payment network

Chart 6
DOMESTIC PAYMENTS NETWORK



Sources: T2 Data Warehouse and authors' calculations.

Network theory is used to complement the characterisation of T2-Malta and to provide a clearer understanding of its most relevant actors and interdependencies. Chart 6 provides a network perspective of this payment system.[11] Each node represents a bank, and node size is proportional to the total value transacted over the year, considering both sent and received payments.[12] The numbers displayed within the nodes rank institutions by node size, with 1 denoting the bank with the largest total transacted value. Directed edges represent bilateral payment relationships: edge thickness is proportional to the total transaction volume between each pair of institutions, while arrow direction indicates the direction of the bilateral net inflow, that is, towards the institution receiving the positive net balance of funds from its counterparty. Node positions are arranged to reflect the degree of weighted interconnectedness, with more strongly connected institutions placed closer to the centre and less connected institutions located towards the periphery.

The network displays an uneven, core-periphery structure. A relatively small group of institutions – comprising four banks – occupies a particularly prominent position within the network.[13] A further three institutions, identified by nodes 5 to 7, appear in an intermediate position, while the remaining five institutions, corresponding to nodes 8 to 12, are located in the periphery through fewer and thinner edges. Although the network appears broadly interconnected, payment activity is concentrated among a limited number of larger and more connected institutions. The direction of the arrows indicates that bilateral liquidity flows are asymmetric, with some institutions acting as net recipients (providers) in specific relationships.

Disruptions affecting the more central nodes could therefore have adverse implications for payment continuity, liquidity circulation, and the transmission of operational stress across the domestic network. From a systemic risk perspective, monitoring the evolution of this mapping and these connections over time can help assess the relative importance of individual banks and their activity within the system, and, therefore, the potential for heightened systemic risk.

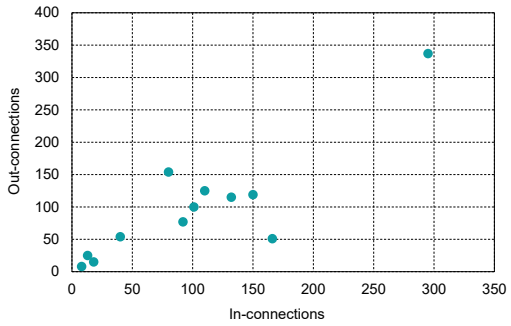
To assess the relative importance of individual banks in the domestic payment network, the analysis also relies on connectivity and centrality indicators, following Glowka et al. (2024). Chart 7 plots, for each institution, inflow against outflow unique nodes to quantify connectivity, where connectivity is measured as the number of unique counterparties from which an institution receives payments and to which it sends payments. It also reports the normalized in-degree and out-degree centrality measures, calculated for the domestic network only (i.e. excluding cross-border counterparties).

Chart 7 reinforces the uneven structure of the domestic payment network. One institution stands out as a dominant hub, displaying a markedly higher degree of centrality than all others, while most participants are clustered at substantially lower levels. The positive association between in and out-degree suggests that

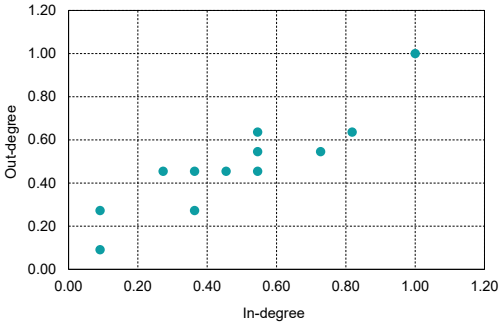
[11] The sample consists of T2-Malta participants active in 2025 and processing payments vs. other T2-Malta credit institutions.
[12] The sample comprises settled domestic transactions involving Maltese banks and other T2 participants holding a Maltese T2 account, excluding transactions with monetary authorities and internal transfers between accounts held by the same entity.
[13] Graph theory and network analysis provide tools to represent and analyse payment systems as networks, in which banks or other participants constitute the nodes, and payment flows the edges connecting them.

Chart 7
INTERCONNECTEDNESS OF T2-MALTA DIRECT PARTICIPANTS

TOTAL CONNECTIVITY



DEGREE CENTRALITY IN THE DOMESTIC PAYMENT NETWORK



Sources: T2 Data Warehouse and authors' calculations.

institutions that are more connected on the receiving side are also more connected on the sending side, although some asymmetries remain.

Taken together, the chart reinforces the evidence from the network map of a core-periphery configuration, in which a limited number of highly connected institutions coexist with a broader set of more peripheral participants. This concentration of connectivity points to a corresponding concentration of operational relevance, suggesting that disruptions affecting the most connected nodes could have disproportionate implications for payment continuity and the transmission of stress across the domestic payment network. This mapping also provides an empirical basis for designing plausible but severe cyber stress-test scenarios in the next phase of the analysis. In particular, the network indicators help identify which institutions could be selected as shock origins, focusing on participants that combine high connectivity, centrality, and transacted value.

At the same time, the analysis highlights which counterparties should be monitored for second-round vulnerabilities, especially those with strong bilateral exposures to the shocked node or with pronounced outflow-to-inflow imbalances. The cross-border evidence further supports the design of external variants of the shock by identifying the foreign jurisdictions and payment corridors through which disruptions could most strongly propagate to Maltese banks. In this sense, the descriptive indicators developed in this special feature are not only diagnostic but also provide the building blocks for calibrating institution-specific, network-based, and cross-border cyber stress scenarios.

Way forward and conclusions

The evidence presented in this document suggests that T2 data can serve as a useful operational and analytical tool for assessing potential cyber-related systemic risk in Malta. The Maltese component of T2 combines a manageable number of participants with sufficiently rich transaction-level information to identify critical actors, directional dependencies, concentration patterns, and potential channels of contagion.

Several findings emerge from this initial analysis. First, activity remains concentrated among a relatively small group of institutions. The share accounted for by the four largest domestic banks has decreased, but these institutions continue to represent a sizeable portion of overall transacted value. This justifies continued monitoring of the most active participants, while also recognising the growing relevance of the remaining institutions.

Second, the transaction topology for 2025 shows that most institutions are characterised by low transaction volumes and low average transaction values. However, a non-negligible share of activity is concentrated in low-volume, high-value transactions, especially in the retail segment. This suggests that the operational and financial consequences of a cyber incident may be highly asymmetric, since disruptions affecting a limited number of institutions may disproportionately impair large payment flows.

Third, the analysis of outflow-to-inflow ratios indicates that while domestic payment flows remain broadly balanced over time, cross-border positions display greater volatility and more frequent episodes of pronounced imbalances. This points to heterogeneity across institutions and payment corridors. From a Maltese financial stability perspective, particular attention should be given to sizeable incoming cross-border flows, as disruptions affecting key foreign counterparties or jurisdictions could reduce payments to Maltese institutions and generate liquidity pressures for domestic recipients.

Fourth, cross-border payment flows are geographically concentrated. A small number of euro area jurisdictions account for the bulk of transacted value, while cross-country asymmetries between credited and debited transactions reveal directional liquidity dependencies. This suggests that disruptions such as cyber incidents affecting key foreign jurisdictions could have a relatively large impact on Maltese participants through cross-border payment channels.

Finally, the domestic network analysis confirms that T2-Malta network exhibits a clear core-periphery structure. A limited number of institutions occupy central positions in the network, combining high transacted values with multiple bilateral links, while the remaining institutions are more peripheral. The connectivity and centrality indicators further reinforce this result, showing that one institution clearly acts as a dominant hub and that the most connected participants tend to be prominent on both the sending and receiving sides of payment flows. From a systemic risk perspective, this implies that operational relevance is concentrated in a narrow subset of participants, so that disruptions affecting the most central nodes could generate disproportionate effects, with implications for payment continuity, liquidity circulation, and the propagation of operational stress across the domestic network.

The indicators presented in this special feature provide a descriptive snapshot of payment-system structures that may be relevant under cyber-related disruption scenarios. They do not, on their own, measure all dimensions of cyber resilience, nor do they quantify the full systemic impact of a cyber incident. Rather, they provide a basis for further work by identifying potential shock sources, vulnerable counterparties, key bilateral links, and relevant cross-border corridors. The next phase of the analysis could develop a more structured framework to assess how payment-related operational disruption may translate into financial stability risk. This could include sensitivity analysis and scenario-based stress testing focused on selected critical participants, the transmission of stress through domestic payment links, and shocks originating from highly interconnected foreign jurisdictions. Such exercises could also support the development of dedicated Systemic Impact Tolerance Objectives (SITOs) for payments by linking severe-but-plausible disruption scenarios to measurable indicators such as affected payment values, liquidity shortfalls, unsettled transactions, recovery times and the number of institutions affected. In this way, T2 data could become an important empirical input into the broader assessment of cyber resilience in the Maltese financial system.

References

Eisenbach T., Kovner A., and Lee M., “Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis”, *Journal of Financial Economics*, Volume 145, Issue 3, 2022, pp. 802-826.

Glowka M., Müller A., and Weber A., “The Hierarchy of Critical Participants: A Clustering Approach Utilising Network-Based Indicators for Payment Systems”, *Latin American Journal of Central Banking*, Volume 7, Issue 2, 2026, pp. 100-169.

Heijmans R., and Wendt F., “Measuring the Impact of a Failing Participant in Payment Systems”, *Latin American Journal of Central Banking*, Volume 4, Issue 4, 2023, pp. 100-106.

Khiaonarong T., Korpinen K., and Islam E., “Using Simulations for Cyber Stress Testing Exercises”, *Working Paper Series*, No. 85, IMF, 2025.

Koo H., van der Molen R., Pollastri A., Verhoeks R., and Vermeulen R., “A Macroprudential Perspective on Cyber Risk”, *Occasional Studies*, Volume 20, Issue 1, De Nederlandsche Bank, 2022.

Kotidis A., and Schreft S.L., "The Propagation of Cyber-attacks through the Financial System: Evidence from an Actual Event", *Journal of Finance*, Volume 80, Issue 6, 2025.

"Advancing Macroprudential Tools for Cyber Resilience", *ESRB Report*, European Systemic Risk Board, February 2023.

"Advancing Macroprudential Tools for Cyber Resilience – Operational Policy Tools: A Review of National and Pan-European Frameworks", *ESRB Report*, European Systemic Risk Board, April 2024.

"Cyber Lexicon: Updated in 2023", Financial Stability Board, Basel, April 2023.

"Data Warehouse User Handbook. Version R2026.JUN, 22". TARGET Services 4CB, January 2026.

"ENISA Threat Landscape 2025", *ENISA Report*, European Union Agency for Cybersecurity, October 2025.

"Global Cybersecurity Outlook 2026", *Insight Report*, World Economic Forum, January 2026.

*"*Information Guide for TARGET Participants: Part 1 – Fundamentals. Version R2025.OCT*"*, European Central Bank, Frankfurt am Main, October 2025.

*"*Information Guide for TARGET Participants: Part 2 – CLM & RTGS. Version R2025.OCT*"*, European Central Bank, Frankfurt am Main, October 2025.

*"*Information Guide for TARGET Participants: Part 3 – TIPS. Version R2025.OCT*"*, European Central Bank, Frankfurt am Main, October 2025.

"Mitigating Systemic Cyber Risk", *ESRB Report*, European Systemic Risk Board, January 2022.

"Steadying the Course: Uncertainty, Artificial Intelligence, and Financial Stability", *Global Financial Stability Report*, International Monetary Fund, October 2024.

"Systemic Cyber Risk", *ESRB Report*, European Systemic Risk Board, February 2020.