

# Synthetic Threats, Real Costs: Assessing the Macroeconomic Exposure of Emerging EU Economies to AI-Enabled Cyber Threats Targeting Financial Systems

Narciz BĂLĂȘOIU\*

*Bucharest University of Economic Studies, Bucharest, Romania*

*\*Corresponding author, narciz.balasoiu@rei.ase.ro*

**Abstract.** *Artificial intelligence has introduced a qualitatively new layer of risk to cybersecurity in the financial sector, and the consequences reach well past the operational boundaries of any single institution. This paper looks at how exposed the emerging economies of the EU (Romania, Bulgaria, Poland, and Croatia in particular) are to AI-driven cyber threats aimed at financial systems. Working with secondary data from ENISA, the European Central Bank, Europol, and the IMF, the study traces the shifting threat landscape (deepfake fraud, AI-powered phishing, automated exploitation of software vulnerabilities) and maps it against indicators of digital maturity, financial depth, and institutional cyber readiness in the selected countries. The methodology blends documentary analysis with descriptive statistics, bivariate correlations, and a purpose-built composite index of cyber-financial vulnerability. What emerges is that the EU's converging economies face a disproportionate risk profile: lower cybersecurity spending relative to GDP, heavier reliance on imported ICT services, and weaker institutional capacity for rapid incident response all contribute. These findings are discussed against the backdrop of DORA and NIS2, and the paper argues that fiscal exposure to AI-enabled cyber risk ought to be woven more deliberately into the macroeconomic surveillance frameworks that govern economic convergence in the EU.*

**Keywords:** artificial intelligence, cybersecurity, financial systems, macroeconomic exposure, emerging EU economies, DORA, cyber-financial vulnerability.

## Introduction

Banks have always been attractive targets, but what makes the current moment different is not a change in the appeal of the target but a transformation in the tools available to those who attack it. Since late 2022, when generative AI capabilities became broadly accessible, the threat landscape confronting European financial institutions has been reshaped in ways that economists (not just technologists) need to take seriously. The old metaphor of an arms race between attackers and defenders still applies, but the asymmetry has shifted: the cost of mounting a sophisticated attack has fallen dramatically, while the cost of defending against one has not.

The numbers give some sense of the scale. ENISA's Threat Landscape 2025 (European Union Agency for Cybersecurity, 2025) documented close to 4,900 cybersecurity incidents across the EU between July 2024 and June 2025, with finance sitting alongside public administration and transport among the hardest-hit sectors. More troubling than the volume, though, is a qualitative shift that the same report flags: the appearance of stand-alone malicious AI systems, purpose-built for offensive use. This is a departure from the pattern of recent years, when threat actors were merely borrowing consumer-grade AI to polish their existing toolkits. Something more autonomous is taking shape, and the implications for financial stability are anything but theoretical.

Curiously, the economic dimension of all this remains somewhat underexplored. There is plenty of work on the technical side (how attacks function, how defences might be improved) and a growing body of literature on regulatory responses. But surprisingly little effort has gone into asking how AI-enabled cyber threats translate into macroeconomic risk, particularly for the cluster

of converging EU economies that are simultaneously digitising their financial sectors and building their institutional capacity from a lower base. Romania, Bulgaria, Poland, and Croatia share this predicament: expanding digital footprints, ambitious but still-maturing financial systems, and cyber defence capabilities that lag behind those of Western Europe.

Three questions organise this paper. First, in what specific ways has artificial intelligence altered the taxonomy of threats facing EU financial systems? Second, what do these threats cost, and why might the emerging economies of the EU be disproportionately exposed? Third, how well does the current regulatory architecture - DORA and NIS2, principally - account for the fiscal and macroeconomic dimensions of AI-driven cyber risk in converging economies?

## Literature review

### *AI as a threat multiplier in financial cybersecurity*

There is, by now, a reasonably broad consensus in the literature that artificial intelligence functions as a threat multiplier in cybersecurity, though the term itself risks becoming a cliché if not anchored in specifics. What does the multiplication actually look like? At its core, AI compresses three variables simultaneously: cost, scale, and plausibility. The banking and financial sector has always constituted a prime target for cyber threats owing to the critical nature of the information it handles (Darem et al., 2023), but attacks that once demanded significant human effort and a certain craftsman's touch can now be mass-produced with minimal overhead. Large language models generate phishing content that, according to several recent analyses, achieves click-through rates above 50 percent (Entrust, 2024). Compare this with the roughly 12 percent typical of manually written campaigns, and the efficiency gap becomes difficult to ignore. More troubling still is the economics: automating the phishing pipeline through LLMs reportedly cuts costs by as much as 95 percent, which effectively democratises a capability that was once the preserve of relatively well-resourced criminal organisations.

Deepfakes present a different, and in some ways more unsettling, problem. The case of Arup in January 2024 has been widely discussed, but it bears repeating because of what it reveals about the state of the art. An employee in the firm's Hong Kong office joined what appeared to be a routine video call with the UK-based CFO and several colleagues. All of them turned out to be AI-generated. The employee, convinced by what seemed like overwhelming visual and auditory proof, authorised fifteen separate wire transfers amounting to 25 million dollars (Institute for Financial Integrity, 2025). This was not a breach of firewalls - it was, as Arup's own CIO later put it, technology-enhanced social engineering. Deloitte's projections suggest that generative AI could push fraud losses to 40 billion dollars in the US alone by 2027 (Deloitte Center for Financial Services, 2025). In Europe, ENISA's first dedicated analysis of cyber threats to the finance sector catalogued 488 incidents between January 2023 and June 2024 (European Union Agency for Cybersecurity, 2025); banks bore the brunt, accounting for roughly 46 percent of all cases. One notices, though, that ENISA itself cautions against reading these numbers as a straightforward measure of threat increase; better reporting and improved detection may inflate the count.

A third vector, less visible but arguably no less consequential, targets the defensive architecture itself. Banks and payment processors now rely heavily on AI-based fraud detection, anomaly scoring, and behavioural biometrics to screen transactions. But these systems are not invulnerable. Adversarial machine learning techniques carefully crafted inputs designed to confuse classifiers) can degrade detection accuracy by 45 to 50 percent under real-world conditions, a far cry from the performance these tools show in controlled laboratory settings. As prior research has noted, existing cyber defence infrastructures risk becoming inadequate to address the increasing speed and complex decision logic of AI-driven attacks (Yeboah-Ofori & Islam, 2019). The result

is something of an arms race, with offensive and defensive AI capabilities evolving in tandem, neither side achieving a durable advantage. The World Economic Forum's 2025 Cybersecurity Outlook (World Economic Forum, 2025) frames this aptly as a test of whether trust can be sustained in a world where seeing and hearing are no longer grounds for believing.

### ***The economic costs of cyber incidents: from micro to macro***

Estimating the economic cost of cyberattacks is a frustrating exercise, not because data are lacking but because the data that exist are methodologically inconsistent. IBM's annual Cost of a Data Breach report (IBM Security, 2025) has become the most commonly cited micro-level benchmark: the 2025 edition put the global average at 4.44 million dollars per breach, with financial services running higher, around 5.56 million. These figures are useful but narrow. They capture direct costs (forensics, notification, legal fees, downtime) and miss the slower-moving damage that ripples outward. Recent work on AI-based cybersecurity in financial management has similarly emphasised that the real cost extends beyond immediate losses to encompass reputational erosion and systemic trust degradation (Mishra, 2023). At the macro end of the spectrum, a World Bank literature review (World Bank, 2024) found global cost estimates ranging from 172 billion dollars in 2017 to a staggering 10.5 trillion by 2025, roughly 9 percent of world GDP. The authors themselves acknowledged, somewhat disarmingly, that many of these headline figures rest on methodologies that cannot be independently verified.

The more analytically interesting work, to my mind, concerns indirect costs and systemic transmission. A serious cyber incident hitting a major bank does not just cost that bank money. It can push up sovereign risk premia, unsettle equity markets, trigger contagion through interbank exposures, and erode the kind of diffuse public confidence in digital finance that takes years to build. In smaller, more concentrated financial systems, the kind typical of emerging EU economies, these channels can amplify the initial shock out of all proportion to the incident's nominal cost. Howden Group's 2025 report (Howden Group, 2025) estimated that cyberattacks cost Europe's four largest economies roughly 307 billion euros between 2020 and 2025. Perhaps the most striking finding was that about two-thirds of this (around 204 billion) could have been prevented through basic cyber hygiene and insurance uptake.

For Central and Eastern Europe, the picture is thinner but not empty. An Oxford-led study (Bruce et al., 2024) ranked Romania as the sixth most significant source country for cybercrime globally, a position tied to the deep interconnections between its digital infrastructure and critical sectors: banking, energy, transport, defence. Romania's domestic cybersecurity market was estimated at around 350 million euros in 2024, growing at a brisk 15 percent annually. Yet the financial services sector absorbs only about 22 percent of that spending. The gap between what the threat environment demands and what is actually being invested is not just a technical shortfall, but a structural economic vulnerability with fiscal implications.

## **Methodology**

The approach here is mixed-method in the straightforward sense: documentary analysis of institutional reports combined with quantitative work on secondary data. On the documentary side, the study draws on publications from ENISA, the ECB, Europol, the IMF, the World Bank, and Deloitte, alongside the relevant EU regulatory texts. The quantitative side involves three components. First, a descriptive analysis of cyber incident trends over time. Second, bivariate correlation analysis between cybersecurity preparedness indicators and financial sector exposure metrics. Third, the construction of a composite Cyber-Financial Vulnerability Index, or CFVI, for the selected economies.

The CFVI brings together six normalised indicators, each scored on a 0 -100 scale where higher values mean greater vulnerability. The components are: cybersecurity spending as a share of GDP (inverted, so that low spending produces a high vulnerability score), a digital skills measure drawn from Eurostat’s DESI (also inverted), banking sector concentration as proxied by the Herfindahl-Hirschman Index for the top five banks, the share of ICT services sourced from non-domestic providers, and the inverse of the ENISA EU Cybersecurity Index score. The composite is an equally weighted arithmetic mean. One could object that equal weighting is a simplification, and the objection has merit. But for an exploratory index whose purpose is to map relative vulnerability rather than to generate precise risk scores, the approach is defensible.

Four emerging EU economies, Romania, Bulgaria, Poland, and Croatia, form the core of the analysis, with Germany and France serving as established-economy benchmarks. This selection is deliberate: it captures meaningful variation in financial depth, EU accession cohort, euro area membership, and cybersecurity maturity. The trend data cover 2020 to 2025, a period that brackets the most consequential AI-driven shifts in the threat landscape.

## Results and discussions

### *The evolving threat taxonomy*

Look at the period from 2020 to 2025 and a clear structural break emerges around 2023. Before that year, the threats facing EU financial systems were largely familiar: ransomware, DDoS campaigns pegged to geopolitical flashpoints (the Ukraine conflict being the obvious catalyst), and credential theft via conventional phishing. Generative AI changed the picture along three axes simultaneously (scale, believability, and economics) and it did so faster than most institutional defences could adapt.

Consider the trajectory of deepfake fraud alone. Between 2017 and 2022, a total of 22 incidents were recorded globally. In 2024, the number reached 150. Then, in just the first quarter of 2025, 179 new cases surfaced, thus surpassing the entire prior year by 19 percent (Entrust, 2024). These are not marginal increments; this is an exponential curve. On the credibility front, surveys from 2024 indicate that 53 percent of professionals in finance had already encountered a deepfake scam attempt, while separate research found that 99.9 percent of people are unable to reliably tell a deepfake from the real thing. On the cost-to-attacker side, AI-driven phishing cuts campaign expenses by roughly 95 percent and yields click-through rates about four times higher than human-written content. For criminal organisations, the return on investment has become extraordinarily attractive.

**Table 1. Taxonomy of AI-enabled cyber threats to financial systems (2023-2025)**

| Threat vector                        | AI enhancement mechanism                | Primary financial target           | Estimated impact trajectory          |
|--------------------------------------|-----------------------------------------|------------------------------------|--------------------------------------|
| Deepfake fraud (video/voice)         | Real-time face/voice synthesis          | Corporate treasury, wire transfers | +2,137% (2022–2025)                  |
| AI-augmented phishing                | LLM-generated personalised content      | Retail banking, credential theft   | 82.6% of phishing uses AI (2025)     |
| Synthetic identity fraud             | Composite identity generation           | Account opening, credit            | 244% rise in digital forgeries (YoY) |
| Automated vulnerability exploitation | AI-driven scanning and payload delivery | Banking infrastructure, APIs       | 21.3% of intrusions via exploits     |
| Adversarial ML attacks               | Evasion of AI-based fraud detection     | Transaction monitoring systems     | 45–50% detection accuracy drop       |

Source: Author’s compilation based on ENISA (2025), Entrust (2024), Deloitte (2025), WEF (2025).

### *Comparative vulnerability of emerging EU economies*

The cross-country picture is, as one might expect, uneven. ENISA's EU Cybersecurity Index for 2024 (European Union Agency for Cybersecurity, 2024) put the Union-wide average at 62.65 out of 100, with most member states clustered within about 10 points of that mean. On its face, this suggests a reassuring degree of convergence. But the CSI measures general cybersecurity posture; it does not capture the specific intersection of financial sector exposure and defensive capacity that matters for the question at hand. That is what the Cyber-Financial Vulnerability Index attempts to do.

**Table 2. Cyber-Financial Vulnerability Index (CFVI), selected EU economies, 2024**

| Country  | Cyber spend/<br>GDP (inv.) | Digital skills<br>(inv.) | Banking<br>conc. (HHI) | ICT import<br>dep. | EU-CSI<br>(inv.) | CFVI score |
|----------|----------------------------|--------------------------|------------------------|--------------------|------------------|------------|
| Romania  | 72                         | 68                       | 61                     | 74                 | 59               | 66.8       |
| Bulgaria | 78                         | 75                       | 65                     | 71                 | 64               | 70.6       |
| Poland   | 58                         | 55                       | 48                     | 52                 | 45               | 51.6       |
| Croatia  | 69                         | 62                       | 70                     | 66                 | 57               | 64.8       |
| Germany  | 32                         | 35                       | 38                     | 28                 | 30               | 32.6       |
| France   | 35                         | 38                       | 42                     | 31                 | 33               | 35.8       |

Source: Author's calculations based on ENISA EU-CSI (2024), Eurostat, IMF, World Bank data.

Note: All sub-indicators normalised to 0-100 scale. Higher values = greater vulnerability.

The gradient is stark. Bulgaria comes in at 70.6, Romania at 66.8, Croatia at 64.8. Poland, which benefits from a larger economy, a more diversified banking sector, and comparatively better digital skills investment, sits at 51.6 - still well above the Western European benchmarks of Germany (32.6) and France (35.8). In rough terms, the emerging economies face about twice the composite vulnerability of their established counterparts. That is a large gap, and it is not narrowing as quickly as one might hope.

The correlations flesh out the picture. CFVI scores correlate strongly and positively with banking concentration ( $r = 0.87$ ), which makes intuitive sense: a financial system dominated by a handful of large banks is, by definition, a system where a successful attack on any one of them can have outsized consequences. There is a moderate negative correlation with cybersecurity spending as a share of GDP ( $r = -0.72$ ), confirming that the investment gap is statistically associated with the vulnerability gap. And income level, proxied by GDP per capita, shows a strong negative correlation ( $r = -0.91$ ), though this needs to be interpreted with some care, as income explains a lot, but not everything.

Croatia is a case in point, as its GDP per capita exceeds Romania's, yet its CFVI score is only marginally lower (64.8 versus 66.8). The reason lies in Croatia's exceptionally concentrated banking sector and its limited domestic cybersecurity industry. Poland, by contrast, shows that deliberate investment and structural diversification can offset, at least partially, the disadvantages of emerging-economy status. Policy choices, in other words, are not irrelevant; a point worth underlining in any discussion that risks treating vulnerability as an inevitable function of income.

Geopolitics compounds the structural picture. ENISA's 2025 data (European Union Agency for Cybersecurity, 2025a) show that DDoS attacks on European financial entities spike around events connected to the Ukraine conflict and, more broadly, to the geopolitical tensions on the EU's Eastern Flank. Romania and Bulgaria sit squarely in that zone. State-aligned cyber groups tied to Russia, and to some extent China and Iran, continued targeting EU institutions and strategic industries throughout the reporting period. When you layer geopolitical exposure on top of the

structural vulnerabilities captured by the CFVI, what emerges is a compound threat environment; one in which the Eastern European members of the EU carry a disproportionate share of the burden.

### ***The Romanian case: a closer examination***

Romania warrants a closer look, partly because of its strategic importance on the Eastern Flank and partly because its trajectory encapsulates the tension between digital ambition and cybersecurity capacity. The country's Cybersecurity Strategy for 2022–2027 (Romanian Cybersecurity Strategy, 2022) is candid about the challenge: Romania faces both sophisticated attacks seeking strategic or financial gain and more routine intrusions that exploit well-known vulnerabilities. The institutional response has not been passive: the creation of the National Directorate of Cyber Security (DNSC) and the decision to host the EU's Cybersecurity Competence Centre in Bucharest signal real commitment.

But commitment and capacity are different things. The cybersecurity market, growing at 15 percent a year, is heavily concentrated in Bucharest, which accounts for about 63 percent of national revenue in the sector. Banking and financial services take up around 22 percent of cybersecurity spending, and these institutions now face the dual pressure of complying with DORA while simultaneously expanding digital banking services - each new mobile app or API endpoint being, in effect, a new surface to defend. An audit of 103 municipalities revealed sharp disparities in security readiness: smaller local governments sit on sensitive data with virtually no threat-monitoring capability. And the Electrica Group ransomware incident of December 2024 served as a reminder that even major infrastructure players remain exposed, prompting a wave of operational technology segmentation across both the energy and financial sectors.

What makes Romania's situation distinctive is the convergence of several factors that do not neatly separate. There are euro adoption aspirations, which require demonstrated institutional maturity. There is a financial sector in the middle of a rapid digital transition. There is deep integration into European payment and settlement systems. And there is a geographic position that places the country in the zone of most intense geopolitical cyber activity on the continent. Whether the pace of cybersecurity investment can keep up with both the AI-accelerated threat curve and the expanding attack surface is a question with direct bearing on Romania's broader convergence story, and not just a technical footnote.

### ***Economic cost estimation and fiscal exposure***

Putting a precise number on the cost of all this is, frankly, impossible. But rough estimation is better than none. Start with IBM's benchmark of about 6 million dollars per financial sector breach (IBM Security, 2025), apply it to the incident frequency ENISA reports for European financial entities, and add a correction for the underreporting that ENISA itself freely acknowledges. The result falls somewhere in the range of 3 to 5 billion euros per year for the EU financial sector as a whole in direct costs. Howden's broader estimate (Howden Group, 2025) of around 60 billion euros annually across Europe's four largest economies when indirect costs are included) gives a sense of the wider damage.

For the emerging economies, the proportional weight is heavier. Romania's cybersecurity market of 350 million euros amounts to roughly 0.11 percent of GDP, against 0.25 percent in Germany and 0.22 percent in France. The ECB's first-ever cyber resilience stress test, conducted in 2024 across 109 directly supervised banks (European Central Bank, 2024), found that response frameworks were broadly in place but flagged persistent weaknesses in two specific areas: the ability to estimate losses from a cyberattack (both direct and indirect), and the management of

dependencies on third-party ICT providers. These happen to be exactly the areas where emerging-economy banks are most stretched.

The fiscal transmission operates through multiple channels, some of them less obvious than others. Direct losses at state-owned or systemically important banks may necessitate public recapitalisation. Regulatory costs associated with implementing DORA fall disproportionately on smaller supervisory authorities with tight budgets. Disrupted financial intermediation means lost tax revenue. And reputational damage to a country's financial sector can, at the margin, push up sovereign borrowing costs; a mechanism that bites harder in countries outside the euro area, where the stabilising effect of ECB monetary policy transmission is absent.

### ***The regulatory landscape: DORA, NIS2, and the AI Act***

The EU has not been idle. The Digital Operational Resilience Act, in application since 17 January 2025 (European Insurance and Occupational Pensions Authority, 2025), is by any measure an ambitious piece of regulation. It imposes harmonised requirements on twenty categories of financial entity and their ICT providers: risk management, incident reporting, resilience testing, third-party oversight, information sharing. DORA is, in effect, the first cybersecurity rulebook designed specifically for finance at the European level, and it takes precedence over NIS2 in its domain.

The question, though, is implementation. DORA's threat-led penetration testing requirements, for instance, presuppose a mature market of certified testers and threat intelligence providers. That market exists in Frankfurt, Paris, and Amsterdam. It is considerably thinner in Bucharest, Sofia, or Zagreb. Compliance costs (several million euros per mid-sized bank, by some industry estimates) hit harder where margins are slimmer and regulatory budgets tighter. There is a genuine risk that DORA, for all its merits in harmonising standards, ends up producing a two-speed reality: effective resilience in the west, box-ticking compliance in the east. Nobody designing the regulation intended this outcome, but the structural asymmetries make it a plausible one.

The EU AI Act, which came into force in August 2024, adds another layer. Its transparency obligations and marking requirements for AI-generated content are relevant to the deepfake and synthetic fraud threats discussed here, even though the Act was not specifically designed with financial cybersecurity in mind. Enforcement is the weak link. The speed at which AI-enabled threats evolve outstrips the cadence of regulatory adaptation, and the capacity of national supervisors in smaller EU economies to monitor compliance with DORA, NIS2, and the AI Act all at once is, to put it diplomatically, an open question.

## **Conclusion**

The argument of this paper can be summarised in three propositions, none of them comfortable.

First, the threat taxonomy has undergone a genuine qualitative shift since 2023. Generative AI tools have lowered the cost of mounting sophisticated attacks, boosted their credibility, and enabled entirely new vectors; real-time deepfake fraud being the most dramatic example. The more-than-2,000-percent rise in deepfake incidents between 2022 and 2025 is not a statistical artefact; it reflects a structural change in the economics of cybercrime that has outrun most existing defences.

Second, the Cyber-Financial Vulnerability Index developed here confirms that the emerging economies of the EU face roughly double the composite vulnerability of their established counterparts. This is not simply a reflection of lower income. It is driven by a specific combination of underinvestment in cybersecurity, concentrated banking systems, heavy dependence on imported

ICT services, and lower scores on EU-wide maturity indices. These factors interact in ways that multiply risk: a concentrated financial system that relies on foreign IT providers and spends comparatively little on defence is, simultaneously, a more attractive target and a less capable one.

Third, the EU's regulatory response (anchored by DORA and NIS2) provides necessary harmonisation but does not resolve, on its own, the implementation gap between Western and Eastern European economies. The fiscal exposure of converging economies to AI-enabled cyber risk, running through direct losses, compliance costs, and sovereign risk premia, ought to be embedded more deliberately in macroeconomic surveillance, including the European Semester and the convergence assessments that govern euro area accession.

Emerging economies would benefit from EU-funded technical assistance specifically targeting DORA implementation in smaller financial institutions. Shared regional cybersecurity operations centres, pooling scarce expertise across borders, would address the thin-market problem that makes penetration testing and threat intelligence costly. And the conditionality frameworks attached to EU structural and convergence funds could usefully incorporate cyber resilience metrics. For Romania in particular, the presence of the European Cybersecurity Competence Centre in Bucharest represents an opportunity that should be exploited not just for research but as a springboard for building domestic capacity in financial sector cyber defence.

The limitations of this study should be acknowledged openly. The CFVI uses equal weighting across its six components; a sensitivity analysis with alternative weighting schemes would strengthen confidence in the results. The cost figures are rough, inevitably so given the opacity of existing data. Future work might usefully pursue dynamic modelling of cyber-financial contagion in concentrated banking systems, track how DORA implementation actually unfolds across different EU jurisdictions, and develop early-warning indicators that integrate the pace of AI threat evolution into macroprudential monitoring. The challenge is large, and this paper is, at best, a step toward framing it in the right terms.

## Acknowledgments

During the preparation of this work, the author used Perplexity as a language-editing aid to improve clarity, refine phrasing, and review the manuscript for stylistic consistency in English. The conceptualisation, research design, data collection, analysis, construction of the Cyber-Financial Vulnerability Index, and all substantive arguments are the author's own. Following the use of this tool, the author thoroughly reviewed and revised the content and assumes full responsibility for the final version of the publication.

## References

- Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE*, 19(4), e0297312. <https://doi.org/10.1371/journal.pone.0297312>
- Deloitte Center for Financial Services. (2025). Deepfake banking and AI fraud risk. Deloitte Insights. Retrieved from <https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html>
- Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access*, 11, 125138–125158.
- Entrust. (2024). 2025 Identity Fraud Report. Retrieved from <https://www.entrust.com/company/newsroom/deepfake-attacks-strike-every-five-minutes>

- European Central Bank. (2024). ECB concludes cyber resilience stress test. Press release, 26, July 2024. Retrieved from <https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html>
- European Insurance and Occupational Pensions Authority. (2025). Digital Operational Resilience Act (DORA). Retrieved from [https://www.eiopa.europa.eu/digital-operational-resilience-act-dora\\_en](https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en)
- European Union Agency for Cybersecurity. (2025a). ENISA Threat Landscape 2025. ENISA, Athens. Retrieved from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- European Union Agency for Cybersecurity. (2025b). ENISA Threat Landscape: Finance Sector (January 2023 to June 2024). ENISA, Athens. Retrieved from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector>
- European Union Agency for Cybersecurity. (2024). The EU Cybersecurity Index 2024. ENISA, Athens. Retrieved from <https://www.enisa.europa.eu/publications/the-eu-cybersecurity-index-2024>
- Howden. (2025). Rebooting growth: Howden's 2025 cyber insurance report. London: Howden Group Holdings. Retrieved from <https://www.howdengroupholdings.com/reports/2025-cyber-report>
- IBM Security. (2025). *Cost of a Data Breach Report 2025*. IBM Corporation.
- Institute for Financial Integrity. (2025). Deepfake deep dive: AI-enabled fraud and financial institutions. Retrieved from <https://finintegrity.org/deepfake-deep-dive/>
- Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, 13(10), 5875.
- Romanian Government. (2022). *Romania Cybersecurity Strategy 2022–2027*. Ministry of Research, Innovation, and Digitalization.
- World Bank. (2024). A review of the economic costs of cyber incidents. *Digital Economy Papers*, World Bank Group, Washington, DC.
- World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. Geneva: World Economic Forum.
- Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modelling for supply chain organizational environments. *Future Internet*, 11(3), 63.