Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 2, 2025

OBSTACLES AND HAZARDS IN THE IMPLEMENTATION OF CYBER FINANCIAL FRAUD UNDER PREVENTION OF ELECTRONIC CRIMES ACT, 2016

Rukhma Bibi[1], Hina Allauddin[*2]

[1]*LL.M Scholar, Law College, University of Peshawar*
[*2]*Lecturer, Co-Author & Supervisor, Law College, University of Peshawar*

Corresponding Author: *
Hina Allauddin

DOI: https://doi.org/ 10.5281/zenodo.15462608

Received	Revised	Accepted	Published
03 January, 2025	03 February, 2025	18 February, 2025	25 February, 2025

ABSTRACT

In Pakistan, cyber financial fraud has become more sophisticated and frequent, especially as online banking, digital wallets, and mobile commerce have expanded in popularity. The Prevention of Electronic Crimes Act (PECA), 2016, was introduced as a legal framework to address these digital threats. The implementation of PECA is still ineffective, nonetheless, according to data from institutional procedures and court case studies. This article critically analyzes the hurdles to its implementation, including lack of technical expertise, procedural ambiguities, jurisdictional overlaps, and low public awareness. The study draws attention to the discrepancies between legislative intent and actual conditions on the ground by using a qualitative content analysis of case law from District Court Peshawar (2023). The study also considers the shortcomings of PECA in addressing transnational crimes and suggests institutional and policy changes to improve the Act's effectiveness.

Keywords: *Cybercrime, Cyber Financial Fraud, Legal gaps, Jurisdictional challenges, Technological blockage, Enforcement Complexities.*

INTRODUCTION

Research Question

What are the main obstacles and hazards in the implementation of the Prevention of Electronic Crimes Act, 2016 in preventing and prosecuting Cyber Financial Fraud in the courts?

Methodology

This study uses a qualitative research methodology to investigate how the Prevention of Electronic Crimes Act, 2016 (PECA) is being implemented in regard to cyber financial fraud. Through the analysis of intricate social and institutional relationships, this methodological decision allows for a thorough knowledge of legal, enforcement, and technical difficulties. Through a thorough literature assessment that includes books, peer-reviewed publications, law journals, court decisions, magazines, and official government and institutional reports, the research is based on secondary data. To find important insights and reoccurring trends, these sources are thoroughly examined utilizing content analysis.

The study's main focus is a case study analysis of 10 court cases decided by the Court of Judicial Magistrate Peshawar in 2023. The challenges faced in implementing PECA, including legislative ambiguity, enforcement obstacles, and recurrent judicial interpretations, are practically demonstrated by these examples. In addition to their ability to reveal judicial trends and enforcement constraints, the chosen cases are examined for their applicability to cyber financial crimes.

To improve the precision and consistency of coding and interpretation, NVivo software is used for thematic analysis of data. Literary and legal textual data are categorized into themes like "technological blockades," "enforcement complexities," and "jurisdictional issues." Word frequency inquiries, text search queries, and matrix coding are some of the characteristics of NVivo that help find important themes, common legal phrases, and relational patterns among enforcement difficulties. This methodical study serves as the foundation for the development of practical suggestions meant to improve PECA's execution through improvements in technology, procedures, and policy.

Findings and Analysis

Enforcement Complexities

The incapacity of law enforcement to capture and hold suspects is a significant enforcement obstacle. The accused either avoided a court summons or fled before the trial started in more than half of the cases from the Judicial Magistrate Court in Peshawar that were reviewed. Courts were compelled to declare these people Proclaimed Offenders in accordance with Section 512 of the Criminal Procedure Code. However, because there is no cross-examination, rebuttal, or confrontation, in absentia trials seriously undermine prosecution efforts and give rise to substantial due process issues. Furthermore, suspects were able to destroy evidence, move money, or vanish completely due to procedural inefficiencies, such as insufficient follow-up with financial institutions, delays in issuing warrants, and a lack of cooperation among investigating agencies.

Legal flaws

Several legal flaws prevent PECA from being implemented. The primary one is the excessive dependence on circumstantial evidence, which includes CNIC data, SIM registrations, and bank transactions, without the backing of definitive digital forensics. In the absence of supporting documentation such as IP logs, CCTV footage, voice call records, or device forensic analysis, courts have routinely rejected such indirect links. For example, a lack of forensic evidence of actual usage created reasonable doubt and frequently led to acquittals, even in cases where the accused had registered the cellphone number used in fraud. Furthermore, in severe cybercrime cases, court settlements under Section 345 of the Cr.P.C., which allow for compromise between parties, were occasionally applied improperly, undermining the law's deterrent effect. In some instances, pardons were given out of religious or personal convictions, which further undermined official accountability systems.

Technological Blockades

Digital anonymity continues to be a significant obstacle to investigations into cybercrimes. Fraudsters frequently used impersonated social media profiles, untraceable or spoof email accounts, anonymous payment methods, and platforms hosted abroad. These factors made gathering evidence more difficult in addition to hiding the identify of the offender. Pakistani law enforcement also lacks the infrastructure for international cooperation and the digital forensics expertise required to track anonymous online activity or retrieve data from overseas sites. Further impeding the overall efficacy and efficiency of investigations were systematic technology deficiencies, including the lack of interagency databases, forensic tools, and centralized case management systems.

Procedure Inefficiencies

The investigation is hindered by inadequate interagency collaboration and bureaucratic hold-ups. The gathering of evidence from forensic labs, banks, telecom providers, and NADRA was frequently postponed because of misunderstandings or a lack of response. Important evidence in a number of cases was inadmissible because crucial forms, such as Form-31, which is required for forensic submission, were either absent from the trial record or never formally displayed. Case continuity was further interrupted by the transfers of investigation personnel, which frequently led to inadequate trial preparation and incomplete documents. Additionally, cops frequently handled complicated cases of digital fraud using antiquated manual techniques because they lacked specialized cybercrime training.

Victim Challenges

In addition to the initial money loss, victims of cyber financial fraud encounter many challenges. When victims have to submit extra petitions, such Superdari applications, to recover frozen cash, they frequently experience emotional distress and procedural weariness. This process puts a significant burden on already harmed parties by frequently requiring surety guarantees and navigating intricate legal regulations. A limited or no cash recovery was achievable in many cases, particularly when the fraudsters had no traceable assets or had taken money out rapidly. Legal settlements severely damaged victims' trust in the official court system because they were frequently seen as the sole way to receive financial compensation.

Institutional Defects

Cyber financial fraud persists in large part because to institutional failures, especially in banks and financial regulators. Banks were found to have failed to identify or respond to suspicious transactions in a number of occasions, including big withdrawals after dubious deposits. Unusual activity was frequently overlooked by compliance teams, which allowed fraud to continue unchecked. This suggests that Pakistan's banks supervision and anti-money laundering procedures have a wider flaw. Lack of interbank coordination and real-time monitoring makes the problem worse and lowers the likelihood of recovery or early action.

Introduction

Global dependence on technology in almost all aspects of international development and connectivity, i.e. from healthcare and education to communication and finance, at present, has risen to an extent that has never been seen before in the 21st century. The widespread reliance on technology has reshaped the fundamental structure of societies around the globe (Nations, 2024). Such dependency on the technological revolution is both a boon and a bane at the same time. But to a greater extent, the digital sphere is mostly a bane (Abro, 2013). Cyber financial fraud is one of the increasing cybercrimes, affecting both developed and developing countries (Wood, 2024).

The widespread incorporation of technology into many fields, has drastically changed connectedness and global development. Digital tools have improved patient care and operational efficiency in the healthcare industry, by enabling telemedicine and electronic health records (World Health Organization, 2021). Online learning platforms have transformed education by allowing access to knowledge beyond geographic borders. Instantaneous information interchange has been made possible by communication technologies, which have linked people globally. Online transactions and digital banking have simplified financial processes. But there are significant drawbacks to this heavy reliance on technology, especially in the area of cyber security. A serious issue that now affects both rich and developing countries is cyber financial fraud. For instance, in 2022, phishing attempts were five times higher in the financial services sector than in any other (National University, 2023).

Cyber financial fraud includes phishing, identity theft, ransomware, and hacking—tools used to obtain sensitive financial information (McGuire & Dowling, 2013). By 2025, it is anticipated that cybercrime would cause $10.5 trillion in yearly damages worldwide, with financial institutions being especially vulnerable (Cyber Security Ventures, 2022). Globally, the average cost of data breaches increased from $4.45 million in 2023 to $4.88 million in 2024 (Morgan Lewis, 2024). As a result, businesses are advised to put robust cyber security safeguards in place, including multi-factor authentication, zero-trust architectures, and employee training (Financial Times, 2024). Pakistan's digital economy has grown rapidly, ranking 8th globally in online user growth with 132 million broadband users (PTA, 2024). Cybercrimes, particularly financial fraud, have increased, nevertheless. In 2021, the National Bank of Pakistan experienced a significant cyber attack, and in 2018, information from 22 Pakistani banks was made public on the dark web (Pro Pakistani, 2018).

Cyber financial fraud is one of the most common complaints that the Federal Investigation Agency (FIA) receives each year (Fareedi, 2023). Students made up 32% of complaints in 2021, with financial fraud accounting for 25% of those complaints. Only 222 convictions were reported

between 2020 and 2024, indicating a conviction rate of 3.16%, despite 7,020 arrests (Ali, 2025). The Prevention of Electronic Crimes Act (PECA), 2016, Pakistan's primary cyber security law, makes identity theft, unauthorized data access, and electronic fraud illegal (Shah, 2021). Empirical research, however, draws attention to its shortcomings. New risks like ransomware and digital identity theft are not sufficiently addressed by the law (Migration Letters, 2024). Effective prosecution is hampered by a lack of technical capability, unclear laws, and lax enforcement (Tribune, 2024). The repercussions of cybercrime are extensive. Significant financial losses result from a single Ponzi-style scam in Peshawar, which deceived an estimated Rs. 5.6 billion (Rauf, 2020). Since incidences of fraud and digital harassment are increasing, women and students are especially at risk (Awan & Qureshi, 2022). Pakistan has responded by considering the implementation of national firewalls to regulate threats and content, although detractors contend that such restrictions could impede internet freedom and hinder innovation (Hussain, 2023). Pakistan is at a crossroads in terms of technology. The PECA 2016 offers a fundamental legal foundation, but its application and breadth are inadequate to handle the changing nature of cyber financial fraud. Clearer statutory provisions, enhanced technical training for law enforcement, international collaboration, and public awareness initiatives are all necessary reforms. In order to safeguard Pakistan's digital economy and rebuild public confidence, strong cyber security regulations are necessary.

Literature Review

Cybercrime is the term used to describe illegal activities made possible by digital devices including computers, smartphones, and the internet (Smith & Grabosky, 2020). Ransomware, phishing, identity theft, hacking, and data breaches are some examples of these crimes. Cybercriminals have changed from launching sporadic attacks to launching highly coordinated, international operations that take advantage of systemic weaknesses as the digital economy has grown (Horan & Saiedian, 2021). Cyber financial fraud is a kind of cybercrime that focuses on using digital financial systems to get illegal profits. Among its strategies include phishing schemes, credit card fraud, illegal bank access, and crimes involving cryptocurrencies (Chua & Wareham, 2021). Because of the increased scope and complexity of these crimes due to technological advancements, they are more difficult to identify and prosecute.

Cybercrime evolved alongside technological advancement. In the 1970s and 1980s, hacking was often motivated by curiosity, as demonstrated by early malware like the Creeper virus (Hafner, 1996). By the late 1980s, incidents such as the Morris Worm caused widespread disruption, highlighting systemic vulnerabilities (Spafford, 1989). The 1990s witnessed a proliferation of financial cybercrimes with the emergence of email and online banking. Phishing emerged as a common fraud mechanism (Jakobsson & Myers, 2006), while email-based viruses like Melissa (1999) demonstrated the potential for widespread network disruption (CERT, 1999). The early 2000s saw more sophisticated worms like ILOVEYOU and Code Red, leading to billions in damages and exposing the inadequacies of existing cyber security defenses (Moore et al., 2002; Symantec, 2000).

Globalization of the internet also enabled cross-border scams, notably the 419 Nigerian scams and the rise of Russian cybercrime syndicates, which orchestrated massive financial heists (Anderson et al., 2013). Cybercrime evolved into organized criminal enterprises, with underground marketplaces like Shadowcrew offering hacking tools and stolen data (Brenner, 2010). Global legal frameworks have developed in response to growing cyber threats. The Computer Fraud and Abuse Act (1986) in the U.S. and the UK's Computer Misuse Act (1990) were among the earliest statutes addressing digital crimes (Goodman, 2015). The Budapest Convention on Cybercrime (2001) became the first international treaty to standardize cybercrime legislation and encourage global cooperation (Council of Europe, 2001). The General Data Protection Regulation (GDPR) of the EU (2018) further bolstered privacy rights and security compliance across jurisdictions, influencing similar legislation worldwide (Voigt & Bussche, 2017). Pakistan's first digital legislation, the Electronic Transactions Ordinance (ETO) 2002, legalized digital documents and signatures but did not address

criminal liabilities or cyber security threats (Ahmed & Waqar, 2019). Its limitations became clear with the rise of cybercrime in the 2000s. The Prevention of Electronic Crimes Ordinance (PECO) 2007 criminalized cyber offenses like hacking and cyber terrorism, but it lapsed without parliamentary approval (Malik, 2017). PECO's temporary nature, lack of procedural safeguards, and absence of data protection laws were heavily criticized (Ali, 2020). In response to growing cyber threats, Pakistan enacted the Prevention of Electronic Crimes Act (PECA) 2016, which remains the country's central cybercrime law. PECA criminalizes a wide range of activities including electronic fraud (Section 14), forgery (Section 13), and unauthorized use of identity information (Section 16) (Government of Pakistan, 2016). The FIA Cyber Crime Wing, PTA, and NR3C were given powers to investigate and regulate cyber offenses (Raza & Hussain, 2023).

However, scholars have noted that PECA's implementation suffers from weak enforcement, vague definitions, and lack of alignment with global conventions such as the Budapest Convention (Ahmed, 2019). PECA also lacks real-time investigative capabilities and adequate procedural safeguards, which are central to the Budapest Convention's approach (Council of Europe, 2023). Judicial interpretations of PECA and its relationship with the Pakistan Penal Code (PPC) continue to evolve. In the Sheraz Khan case (2021), the Lahore High Court ruled that although PECA is a standalone law, certain non-conflicting provisions of the PPC could be applied in conjunction. The case emphasized the need for clearer legislative boundaries and better coordination between PECA and traditional legal frameworks. Compared to international frameworks, PECA remains underdeveloped. The Budapest Convention emphasizes global cooperation, real-time data collection, and harmonized investigative procedures—areas in which PECA is lacking (Gercke, 2012). Pakistan's exclusion from this treaty is driven by geopolitical concerns, such as the presence of Israel among the signatories and fears of compromising data sovereignty (Dawn, 2020).

Recommendations

Strengthening International Cooperation and Cross-Border Jurisdiction

Pakistan needs to improve international collaboration and cross-border jurisdiction in order to solve the jurisdictional issues that continuously impede the prosecution of cyber financial fraud. Cybercriminals frequently use platforms housed on foreign servers or operate from outside the nation. Due to the lack of mutual legal assistance treaties (MLATs), demands for user data or supporting documentation from multinational IT companies were frequently ignored in the cases under consideration. Pakistan should formally enter into bilateral and multilateral treaties with other governments and digital service providers in order to get past this. Furthermore, PECA must to be modified to make clear the extraterritorial scope of its provisions, allowing investigators and judges to track down criminals wherever they may be. Additionally, the establishment of a national cybercrime body would facilitate cooperation between domestic and foreign organizations, improving uniformity and prosecution of transnational crimes.

Establishing Investigative Capacity and Specialized Cybercrime Courts

Establishing specialist cybercrime courts and enhancing investigative capabilities are crucial for enforcement. The majority of judges and law enforcement officers do not now possess the technical skills required to manage intricate digital evidence. Due to circumstantial evidence not meeting the legal standard for conviction, this has resulted in a number of acquittals. The establishment of specialized cybercrime courts with staff members educated in digital forensics, cyber law, and admissibility of evidence is necessary to close these enforcement gaps. To increase productivity and transparency, these courts ought to use digital case management tools. The investigation, collection, and preservation of electronic evidence in accordance with legal requirements should be supported by continuous training and resources for law enforcement authorities. To prevent evidence loss and delays in investigations, interagency collaboration must also be strengthened,

especially between the police, FIA, NADRA, telecom firms, and financial institutions.

Modifying and Modernizing Cybercrime Laws

In terms of legislation, Pakistan has to amend and modify PECA to take into account the realities of cybercrime today. Despite being a first step, the current law's definitions and application are nonetheless out of date. Deepfakes, AI-enabled schemes, and cryptocurrency-based fraud are examples of more recent concerns that it does not adequately handle. PECA should be updated to incorporate more expansive and up-to-date definitions of cyber financial fraud in order to fill in these legal gaps. To reduce procedural errors, the admissibility requirements for digital evidence should also be tightened. To maintain the deterrent value of the law, significant financial fraud cases should limit the frequent application of Section 345 of the Criminal Procedure Code, which permits compromise and acquittal in specific circumstances. A victim-centered strategy is also required, one that supports individuals impacted by cybercrime by offering legal assistance, prompt compensation, and streamlined complaint procedures.

Advanced Technology Integration and Digital Infrastructure Strengthening

Lastly, to get over technological obstacles, integrating cutting-edge technology and fortifying digital infrastructure must be given top priority. Modern forensic tools like mobile field investigation kits, blockchain analytics platforms, and encrypted data recovery systems are essential for law enforcement agencies to have access to. These technologies are essential for gathering reliable, useful digital evidence instantly. Additionally, banks, ISPs, and telecom companies should be legally obligated to swiftly share data with investigative authorities, especially in cases of ongoing financial fraud. Proactive threat detection can be greatly improved by utilizing deepfake detection tools, automated monitoring systems, and analytics driven by artificial intelligence. Equally crucial is public awareness. People can identify and report cyber scams with the use of nationwide initiatives that promote cyber hygiene, bilingual materials, and round-the-clock helplines. Building a robust digital society requires educating the public and providing support networks.

Conclusion

In order for the Prevention of Electronic Crimes Act (PECA), 2016 to be effectively enforced, systemic reform in the areas of law, institutions, technology, and international interactions is necessary in addition to its legislative presence. PECA will continue to fail to achieve its intended impact in the absence of specialized courts, updated legislation, improved international cooperation, and contemporary investigation tools, according to an examination of cyber financial crime cases. Pakistan needs to make investments in a comprehensive, forward-thinking strategy that adapts its legal and enforcement frameworks to the changing landscape of cybercrime in order to guarantee justice for victims and responsibility for perpetrators.

REFERENCES

Abro, W. (2013, April 26). Is technology boon or bane? *Dawn*. https://www.dawn.com/news/1025334/is-technology-boon-or-bane

Ahmed, A., & Waqar, M. (2019). Evolution of Cyber Laws in Pakistan: A Legal Overview. *Cyber security Journal of Pakistan*, 4(1), 67-85.

Ahmed, S. (2019). *Cybercrime and its Legal Framework in Pakistan: A Review of PECA 2016*. Journal of Cyber security Studies.

Ali, F. (2020). "Cybercrime Laws in Pakistan: Evolution and Challenges." *Journal of Cyber Law*, 6(2), 45-59.

Ali, K. (2025, January 15). Cybercrime conviction rate 'very low'. *Dawn* Retrieved from https://www.dawn.com/news/1885210

Anderson, R., Barton, C., Bohme, R., et al. (2013). Measuring the Cost of Cybercrime. *ACM Transactions on Information and System Security*.

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. ABC-CLIO.

CERT. (1999). Melissa Virus Incident Report. Retrieved from https://www.cert.org.

Chua, C. E. H., & Wareham, J. (2021). Fighting cyber financial fraud: The role of organizational and technological strategies. *Journal of Cyber security Research*, 17(3), 45–62.

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Council of Europe. (2023). *Current State of Signatories to the Budapest Convention.* Retrieved from https://www.coe.int/en/web/cybercrime/signatories.

Cybersecurity Ventures. (2022). *Cybercrime to cost the world $8 trillion annually in 2023*. Retrieved from https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Dawn. (2020). Why Pakistan is not joining global forum on cybercrime. Retrieved from https://www.dawn.com/news/1531734

Fareedi, T. (2023, November 15). Digital fraud cause long probes. *Express Tribune*. https://tribune.com.pk/story/2446414/digital-frauds-cause-long-probes

Financial Times. (2024). *Technology and cybercrime: how to keep out the bad guys*. Retrieved from https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bf

Gercke, M. (2012). *Understanding Cybercrime: Phenomena, Challenges, and Legal Response.* International Telecommunication Union.

Goodman, M. (2015). *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World.* Anchor Books.

Hafner, K. (1996). Cyberpunks: A New Generation of Computer Crime. *Time Magazine.*

Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *Journal of Cyber security and Privacy*, 1(4), 580-596.

https://www.who.int/publications/i/item/9789240020924

Hussain, F. (2023). *Regulating the internet in Pakistan: The case for and against national firewalls*. Cyber Policy Review, 28(3), 89-105.

Jakobsson, M., & Myers, S. (2006). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley.

Malik, H. (2017). "Cyber Terrorism and National Security: A Legal Perspective." *Security Review Quarterly*, 9(1), 33-48.

McGuire, M., & Dowling, S. (2013). *Cybercrime: A review of the evidence research report 75.* Home office. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5e089b9bac3cdba577724cf0cd23f648a4f952d9

Moore, D., Shannon, C., & Claffy, K. (2002). Code Red: A case study on the spread and victims of an Internet worm. *ACM Internet Measurement Workshop*.

Morgan Lewis. (2024). *Study finds average cost of data breaches continued to rise in 2023*. Retrieved from https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023

National University. (2023). *101 cybersecurity statistics and trends for 2024*. Retrieved from https://www.nu.edu/blog/cybersecurity-statistics/

Nations, U. (2024). *The Impact of digital technologies.* Retrieved November 30, 2024, from https://www.un.org/en/un75/impact-digital-technologies

Pakistan Telecommunication Authority (PTA) report, (2024). Retrieved on May 22, 2024, from https://www.pta.gov.pk/en/telecom-indicators

Propakistani. (2018, October 29). BankIslami customers lose over $6 million in biggest security breach in Pakistan's history. Retrieved from https://propakistani.pk

Rauf, A. (2020, December 24). Scammers rob Rs5.6 billion in online investment funds in Pakistan northwest. *Arab News.* https://www.arabnews.pk/node/1782216/Pakistan

Raza, H., & Hussain, T. (2023). *Challenges in Cybercrime Prosecution in Pakistan*. Journal of Legal Studies, 5(3), 77-98.

Shah, N. (2021). *Legal framework for cybercrime in Pakistan*. *The Express Tribune*.

Migration Letters. (2024). Weaknesses in Pakistan's cybercrime legislation: A critical analysis. *Migration Letters*. Retrieved from https://migrationletters.com/index.php/ml/article/view/10352

Smith, R. G., & Grabosky, P. N. (2020). Cybercrime: Conceptual issues for law enforcement and crime prevention. *Crime, Law and Social Change*, 74(3), 259-275.

Spafford, E. H. (1989). The Morris Worm: A lesson learned. IEEE Software, 6(3), 24-29.

Tribune India. (2024). Cybercrime conviction rate in Pakistan remains low. *The Tribune*. Retrieved from https://www.tribuneindia.com/news/world/cybercrime-conviction-rate

Voigt, P., & Bussche, A. V. D. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

Wood, J. (2024, September 04). *Rising cyber threats pose serious concerns for financial stability*. IMF. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

World Health Organization. (2021). Global strategy on digital health 2020–2025. World Health Organization.