Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

International Review of Financial Analysis 72 (2020) 101587

Contents lists available at ScienceDirect

International Review of Financial Analysis

journal homepage: www.elsevier.com/locate/irfa

Does cyber tech spending matter for bank stability?☆

Md Hamid Uddin[a,*], Sabur Mollah[b], Md Hakim Ali[c]

[a] The University of Southampton - Malaysia Campus, Taylor's University, Malaysia
[b] Chair in Financial Management, Sheffield University Management School, The University of Sheffield, Sheffield, United Kingdom
[c] Taylor's University, Malaysia.

ARTICLE INFO

Keywords:
Bank stability
Risk-taking
CyberTech
Cybersecurity
FinTech

ABSTRACT

CyberTech has drawn academic attention in the aftermath of the global financial crisis (GFC) as banks were forced to embrace CyberTech more aggressively to cope with market competition after the crisis. Banks can improve their operational efficiency and quality of service by relying on CyberTech, but they become more vulnerable to cybersecurity. Thus, increasing investment in CyberTech becomes a strategic necessity for banks to combat cybersecurity hazards. The study investigates how disruptive digital transformation affects bank stability. In particular, it examines whether the law of diminishing marginal returns from overspending on CyberTech affects bank stability. Based on a global sample from 43 countries, we find that an increase in CyberTech spending above the threshold level adversely affects the stability of banks. The main reason behind the adverse effect of CyberTech spending on the stability of banks is that banks take more than the proportional risk for every dollar they spend on disruptive CyberTech after they cross a threshold level of spending. While results persist across sub-samples, our results indicate two important channels of technological regimes – a diminishing returns regime and an increasing returns regime. The diminishing returns regime improves bank stability through more aggressive spending on technology, and the increasing returns regime makes banks more unstable due to excess spending on disruptive CyberTech. The study has implications for cybersecurity and sustainable CyberTech spending for banks.

1. Introduction

Stability in the banking system is an important issue of interest for both regulators and policymakers. Academics, regulators, and policymakers are making efforts to understand the sources and dynamics of banking instability. The existing studies on banking stability address a wide variety of issues, such as governance problems (Anginer, Demirgüc-Kunt, & Mare, 2018), regulatory weakness (Ahamed & Mallick, 2017; Cabrera, & G. P., & Nieto, M. J., 2018), institutional supervisions (Bermpei, Kalyvas, & Nguyen, 2018; Shaddady & Moore, 2019), liquidity problems (Acharya & Mora, 2015), capital adequacy (Anginer, Demirgüc-Kunt, & Mare, 2018), bank concentration and competition (Clark, Radic, & Sharipova, 2018; Fu, Lin, & Molyneux, 2014; Goetz, 2018), and operational inefficiencies (Schaeck & Chiak, 2014). However, researchers have not yet adequately investigated whether the global digital revolution can affect banks' financial stability. Earlier studies suggest that the use of cyber technology (henceforth CyberTech) increases operational efficiency and reduces costs (Agyekum, Locke, & Hewa-Wellalage, 2016; Tchamyou, Erreygers, & Cassimon, 2019). Since excessive dependency on disruptive CyberTech[1] increases the likelihood of disruptions in banking operations through cybersecurity breaches (Basel Committee, 2010; Basel Committee, 2011), it is as yet unknown whether banks marginally gain from their CyberTech spending after crossing a threshold level.

However, disruptive CyberTech appears to be the leading source of hazard for banking operations in the digital environment. Nevertheless,

☆ This research is the output of Taylor's University's flagship research project # TUFR/2017/004/05: Cyber Risk and Bank Stability. Md Hamid Uddin is the leader, Sabur Mollah is the external collaborator, and Md Hakim Ali is working as a research scholar for this project. This paper was presented at Vietnam Symposium in Banking and Finance (VSBF2019) held at the Banking Academy of Vietnam and Malaysian Finance Association annual meeting 2019. We acknowledge data extraction assistance from M. Sawkat Hossain and Syed Rahman. We are grateful to two anonymous reviewers for insightful comments, which have helped to improve the overall exposition and significance of the paper. All comments should be sent to project leader Md Hamid Uddin.

* Corresponding author.
E-mail addresses: m.h.uddin@soton.ac.uk, iba_hu@yahoo.com (M.H. Uddin), s.mollah@sheffield.ac.uk (S. Mollah), mdhakimali@sd.taylors.edu.my (M.H. Ali).

[1] The industry practitioners often refer to cyber technology in normative term as 'disruptive cyber technology'. We use both 'CyberTech' and 'disruptive CyberTech' interchangeably as appropriate in the context.

https://doi.org/10.1016/j.irfa.2020.101587
Received 30 January 2020; Received in revised form 5 June 2020; Accepted 7 September 2020
Available online 12 September 2020
1057-5219/

increasing investment in CyberTech became a strategic necessity for banks after the global financial crisis because the innovations of financial technologies (hereafter FinTech) allowed FinTech firms to extend financial services at a much cheaper price and with greater convenience – affecting the earnings and market share of traditional banks (Buchak, Matvos, Piskorski, & Seru, 2018; Vives, 2019). Also, despite the concerns of cybersecurity hazards, the critical importance of relying on CyberTech is well observed during the COVID-19 pandemic as online communications and digital banking transactions have become a necessity in all spaces of social and economic life.

CyberTech spending and bank stability emerge as an important issue of research in banking. Due to the paradigm shift in FinTech in the banking industry, banks have few options but to increase CyberTech spending for their survival in the fast-changing FinTech era. As a result, banks increasingly offer more financial services and manage internal operations in a virtual environment that is enormously vulnerable to cybersecurity. However, they often need to allocate budget to digital infrastructure, even though these investments are not always profitable (Kauffman, Liu, & Ma, 2015). Also, in a competitive environment, banks have no choice but to continuously improve their electronic banking systems to enhance operational efficiency, performance, and service (Lages, 2016; Roth & Jackson-III, 1995).. According to a recent report, banks around the world have significantly increased their technology budgets and these are growing at an increasing rate (Greer, Lodge, Mazzini, & Yanagawa, 2019). Thus, it is important to investigate whether an increase in CyberTech spending by banks affects bank stability.

However, no prior study examined whether the excessive growth of cyber expenditure can affect a bank's stability. The existing studies find that the digitalization of financial services increases the productivity of banks due to the economies of scale that result from automated payment systems, which accelerates financial intermediation (Chemmanur, 2002; Esho & Sharpe, 1995; Frischtak, 1992; Hancock & Humphrey, 1997; Hancock, Humphrey, & Wilcox, 1999). As banks have invested more in CyberTech over the last few decades, the cybersecurity hazards are also becoming a new challenge for banks due to unpredictable security breaches by external and internal agents. *Cybercrime Magazine* predicts that cybercrime will cost around US$ 6 trillion annually by 2021 (https://cybersecurityventures.com). Therefore, the economies of scale for the use of CyberTech might be alarming due to the law of diminishing marginal returns (Koetter & Noth, 2013).

The diminishing returns of cyber investment is a matter of concern because of human interactions with technology. It is critical that humans have an inherent motive to cheat if there is an opportunity to gain materially (Dufwenberg & Dufwenberg, 2018). The absence of the effective control of human interactions with cyber systems leads to the rise in cybersecurity breaches. As the cybersecurity risk is a new operational problem and an effective control method is unknown, banks have no better option than to continuously upgrade their infrastructure with the latest secure technology without considering the marginal profitability of spending. These upgrades mean increases in cyber overheads that may cannibalize the marginal gains from cyber spending. Therefore, finding the optimal investment in technology with a positive net present value is always challenging.

In this paper, we investigate whether the law of diminishing returns from overspending on CyberTech affects bank stability. We analyze hand-collected CyberTech spending data for 354 banks from 43 countries for the period of 2008–2017. We find that a marginal increase in spending above the threshold contributes to a decline in the stability of a bank – indicating that banks take more than the proportional risk for every dollar they spend on disruptive CyberTech. The results show that spending on CyberTech has a significantly concave downward relationship with bank stability. These results indicate that bank stability can be improved due to CyberTech spending up to a certain threshold, but a further increase in CyberTech spending adversely affects the stability of banks. The subsample analysis shows that cyber spending has a similar effect on the financial stability of both small and large banks, and the effect is significantly noticeable during the FinTech revolution era. However, different results are observed in countries depending on their level of technological advancement. We find that CyberTech spending yields a significantly positive linear effect on the stability of banks in those countries where the level of technological advancement is still low, but the positive effect gradually wanes as the country becomes technologically mature. Overall, the study confirms that banks take more than the proportional risk for every dollar they spend on disruptive CyberTech subject to the technological regime of the country.

This study makes several contributions to the banking literature. First, to the best of our knowledge, this is the first research that provides empirical evidence on global data to show that a marginal increase in CyberTech spending exerts an incremental effect on bank instability after a threshold point. Although earlier studies found that efficiency in banking services increases through the effective implementation of e-banking operations (e.g. Chemmanur, 2002; Esho & Sharpe, 1995; Frischtak, 1992; Hancock et al., 1999; Hancock & Humphrey, 1997), this study sheds light on the incremental effect of CyberTech spending on bank instability, which adds new knowledge to the banking literature. Secondly, the study identifies two technological regimes globally for increasing and decreasing marginal returns from CyberTech spending, especially in that the same technological regime persists in both developed and developing countries. This suggests that the regime has a life-cycle, indicating that banks need to spend more aggressively to shorten the diminishing return stage and reap the gains from technology after reaching the threshold level. Thus, the technological regimes address an important question raised by Koetter and Noth (2013) on the economies of scale and the law of diminishing marginal returns for the use of CyberTech.

Thirdly, the study makes an important contribution by addressing some concerns raised in recent studies on bank market competition in the wake of FinTech innovations and Basel III capital requirements (e.g. Buchak et al., 2018; Vives, 2019). In particular, these studies emphasize that banks have fewer options left other than investing heavily in CyberTech for two reasons: First, banks are experiencing tougher competition in the wake of the FinTech era because FinTech firms can offer financial services at a much cheaper price and with greater convenience than banks; second, Basel III regulations tighten banks' lendings to maintain higher liquidity and more risk capital. Thus, examining the threshold level of CyberTech spending to maintain bank stability clearly helps to address the issues around bank market competition and Basel III capital requirements.

We divide the rest of the paper into the following sections: Section 2 provides the literature review and the theoretical discussion on how CyberTech spending affects the stability of banks. Section 3 describes the test methods and data. Section 4 presents the results and discussion. Finally, the last section offers the conclusion.

2. Literature and hypothesis

2.1. Banking stability puzzle

There is a plethora of research on banking stability, but most studies examine how credit and liquidity risks lead to financial instability for banks (Acharya & Mora, 2015; Acharya, Shin, & Yorulmazer, 2011; Acharya & Viswanatha, 2011; He & Xiong, 2012; Wagner, 2007). The literature also shows that credit and liquidity risks have independent effects on the probability of bank defaults (Imbierowicz & Rauch, 2014). Yet, the underlying reason for bank stability is still perplexing. This is because other studies find that the tightening of liquidity is unable to affect the credit risk of UK banks (Banerjee & Mio, 2018), and monetary policy has limited power to control the liquidity of US banks (Berger & Bouwman, 2017). Also, liquidity support in a crisis from the government does not help a bank if it has an existing solvency problem

(Boyson, Helwege, & Jindra, 2014). Hence, studies broadly accept that credit and liquidity risks primarily affect banks' financial soundness.

The research strand that focuses on the capital ratio and bank stability disagrees on the appropriate bank capital structure for various reasons (Allen, Carletti, & Marquez, 2011; Berger & Bouwman, 2013; Holmstrom & Tirole, 1997; Mehran & Thakor, 2011), but all generally agree that a higher capital ratio promotes bank stability because of a reduction in systemic risk (Anginer, Demirgüc-Kunt, & Mare, 2018b; Laeven, Ratnovski, & Tong, Bank size, capital, and systemic risk: Some international evidence, 2016. The research shows that the level of leverage in a bank affects its incentive to take risk (Dell'Ariccia, Laeven, & Marquez, 2014) and determines its ability to withstand economic shocks. Therefore, researchers have studied the underlying reasons why a bank would want to have more or less capital as a buffer, and regulators focus on the guidelines and rules that control the level of capital in banks to ensure the overall stability of the financial system. However, the outcomes are not always positive when regulators adjust the capital requirement for banks (Abou-El-Sood, 2016; Bandt, 2018) as the effect of this adjustment on loan growth is subject to the existing level of bank capital (Deli & Hasan, 2017). Therefore, another line of research explores whether the weakness in governance and regulation has a role in risk-taking and the stability of banks, but the results are mixed (Ahamed & Mallick, 2017; Cabrera, Gerald, & Nieto, 2018; Bermpei et al., 2018; Shaddady & Moore, 2019; Anginer, Demirguc-Kunt, Huizinga, & Ma, 2018a).

Another string of research examines the influence of concentration and competition on the risk-taking of banks and their financial stability. Again, the findings are inconsistent across countries. Some studies broadly find that competition improves bank stability in the US, the Commonwealth of Independent States (CIS), and 14 Asia-Pacific countries (Clark et al., 2018; Fu et al., 2014; Goetz, 2018). However, other studies find that more competition instead negatively affects bank stability in the Middle East and North African (MENA) countries and other economies where both Islamic and conventional banks work alongside each other (Albaity, Mallek, & Noman, 2019; Azmi, Ali, Arshad, & Rizvi, 2019). Overall, this brief literature review shows that researchers have found different reasons for the risk-taking by banks and their financial instability, but they are not adequately clear about the underlying reasons behind the problem: Why and how a bank takes on excess risk and falls into financial instability. Therefore, little academic research exists on the operational risk exposures and stability of banks.

The Basel Committee defines operational risk as the risk of direct or indirect loss from inadequate or failed internal processes, people, and systems or from external events (Basel Committee, 2010; Basel Committee, 2011). Operational risk usually occurs unwillingly due to matters that affect the internal operational processes, such as technology infrastructure, security system lapse, data loss, unexpected monetary loss, fraud, privacy protection, legal issues, operation shutdown, and environmental factors. Thus, operational risk exists as long as systems, processes, and people behave imperfectly. The broader definition of operational risk covers a myriad of risk factors, but the gravity of the threats that emerge from technology are well-recognized in the Basel guidelines for operational risk management as well as in the documents of the International Monetary Fund (IMF), World Bank, and Organization for Economic Cooperation and Development (OECD). Also, country-level regulators have issued policy guidelines for managing the operational risk that arises from CyberTech use.[2]

2.2. CyberTech and banks' financial stability

Technology enhances the efficiency of financial institutions, fosters financial development through global extension (Tchamyou et al., 2019), and allows banks to extend services cost-effectively (Agyekum et al., 2016). The speed of financial inclusion is manifested in the worldwide revolution of FinTech, which allows cyber payments, savings, and borrowing (Demirguc-Kunt, Klapper, Singer, Ansar, & Hess, 2018). The early research finds that the consequences of technological development in the banking sector increase the market power of a bank, thereby enhancing its profit buffers, which is useful to withstand adverse shocks. However, a bank increases its vulnerability to financial distress by choosing risky portfolios of assets and liabilities when competition increases (Koette & Poghosyan, 2009). This choice represents the complex relationship between bank competition and financial stability (Allen & Gale, 2004). Therefore, whether the widespread application of CyberTech is indeed helpful to banks remains unclear.

We observe outbreaks of cyber breaches in recent years that have caused unprecedented direct financial losses for banks globally and this reflects the vulnerability of CyberTech.[3] These breaches occur because there are countless ways to beat cybersecurity systems, such as malware, phishing, and targeted cyber-attacks as well as internal and external system abuses. Therefore, the risks of cyber breaches have become a systemic hazard that may happen without a signal and can create a major economic shock to the affected bank. This shock can also damage the financial system (Hurd, 2016; Johnson, 2015). Therefore, with the rise of cyber risk,[4] financial institutions have had to build a more resilient yet efficient global cyber infrastructure.

However, cybersecurity risk is becoming a common hazard of the online banking system because breaches are also increasing at the same pace with the advancement of technology. In this regard, Eling and Wirfs (2019) find that the primary source of cybersecurity risk is human behavior and not necessarily technology. This finding indicates that excess spending on CyberTech beyond an optimal level might not help to reduce the exposure to cybersecurity risk. However, Tang and Zannetos (1992) find that identifying the optimal level of technology investment is challenging because the technological and economic environments in which firms operate evolve continuously to different levels due to rapid technological changes and innovations. Further, banks have hardly any alternative but to increase their technology budgets to tackle the growing risk of cybersecurity. Therefore, banking institutions slowly enter into a vicious cycle of technological dependence (Ngonzi, 2016). That leads to more risk-taking through CyberTech. Banks pursue risky decisions on spending on CyberTech for their survival in the fast-changing market conditions as a result of technological innovations. This risk-taking is imperative for banks because, following the institutional theory (Meyer & Rowan, 1977; Roberts, 2004) as well as the stakeholder theory (Freeman, 1984; Schmidt,

[2] The Basel Committee identifies, describes, and compares the range of observed bank, regulatory, and supervisory cyber-resilience practices across jurisdictions (Basel Committee, 2018a). Also, Uddin, Ali, and M. H. (2018) provide a summary of the guidlines on cyber risk management by different international agencies and country-level reguators.

[3] A few examples of cybersecurity incidences: Tesco Bank lost 2.5 million pounds (Treanor, 2016), Bank of Russia lost around US$ 31 million in 2016 (Thomson Reuters, 2016). The Bangladesh Central Bank lost US$ 81 million in 2016 (Gopalakrishnan & Mogato, 2016), Vietnam's Tien Phong Bank lost US$ 1 million in 2015 (CNBC, 2016). Banco Del Austro in Ecuador had US$ 12 million financial loss in 2015 (Finch, 2016). A cyber-crime gang named Carbanak stole US$ 1 billion through several cyber-attacks in 2014 (Kaspersky, 2015). These are the tip of the iceberg in terms of cybersecurity problems in the financial industry around the world.

[4] The *Financial Times* reports that cyber-attacks on financial services in the UK rose fivefold in 2018 (Murgia & Megaw, 2019). An article in the *Harvard Business Review* indicates cyber-attacks could cause the next financial crisis because one might disrupt financial services, especially payment systems, around the world. Such an attack could drastically erode market confidence in the global financial system, which in turn could negatively affect the global economy (Mee & Schuermann, 2018)

2004), the attainment of business sustainability in tandem with changing environment is critically essential to serve human needs and protect the interests of diverse stakeholders without regard to the consequences of risk decision.

The banks' overall risk-taking became more complicated with the FinTech revolution, which changed the operational structure of the global financial market after the financial crisis. With the rise of the regulatory burden on traditional banks after the financial crisis, disruptive CyberTech created opportunities for FinTech firms to enter the shadow finance market, which contributed to the decline of traditional banks' market share (Buchak et al., 2018). The Basel Committee on bank supervision has identified that the nature and scope of banking risks as commonly understood significantly changed with the emergence of FinTech because new technologies affected the traditional banks' business models. This change led to the enhancement of strategic and profitability risks, operational risks, cyber risks, and compliance risks for the traditional banks (Basel Committee, 2018a). The strategic and profitability risks occur because FinTech leads to more competition among traditional banks, which affects the sustainability of their earnings.[5] Therefore, banks are increasingly adopting advanced cyber technologies or building partnerships with FinTech firms to deliver innovative financial products and services, which require more investment in technologies.

As banks' strategic focus shifts toward developing either an in-house technology infrastructure or a partnership with FinTech firms,[6] the operational risk also escalates due to increased technology interdependencies between the banks, and even between the banks and FinTech firms (Härle, Havas, & Samandar, 2016). Furthermore, the proliferation of innovative products and services based on advanced CyberTech and FinTech collaborations makes controlling the operational risks of the digital banking platform more difficult for traditional bank managers. The widespread technology adoption, big data analytics, and FinTech partnership or outsourcing could lead to compliance risk for data privacy (Basel Committee, 2018a; FSB, 2017). If a technology-based banking network allows customers to switch between different banks and FinTech firms to obtain a better return, the volatility in bank funding could add to credit and liquidity risk. Apart from these matters, increased interconnectivity between market players such as banks and FinTech firms can create benefits for the institutions and their customers, but cybersecurity risk also increases as the banking system becomes even more vulnerable to cyber threats. Overall, the FinTech revolution has further aggravated the technology-driven risk-taking of banks and has affected their stability.

2.3. Hypothesis

In the fast-changing market conditions as a result of technological innovations, both institutional (Meyer & Rowan, 1977; Roberts, 2004) and stakeholder theories (Freeman, 1984; Schmidt, 2004). Support the idea of disruptive CyberTech spending for the survival of banks. However, it is as yet unknown from the literature if banks' financial stability could be affected due to the law of diminishing marginal returns when CyberTech spending crosses a threshold level. In this subsection, we aim to provide the theoretical insights as well as propose a testable hypothesis to fill this critical research gap. Since CyberTech infrastructure is essential for banks in the digital era, the critical question is whether spending an extra dollar on CyberTech has a marginal benefit for stability. This pertinent research question needs to be answered because CyberTech per se cannot help unless other factors, such as banking regulations, governance, and supervision, cooperate in the changing environment. Therefore, if all other factors that affect bank stability cannot work in tandem,[7] then the increased use of CyberTech may succumb to the law of diminishing marginal returns.

Based on a sample of 737 European banks, Beccalli (2007) finds that higher technology spending has an apparent adverse effect on profit efficiency, with an unclear effect on the cost efficiency of European banks. However, Gupta (2018) uses a stochastic frontier analysis to find a similar profitability paradox with the increase of technology adoption in the Indian banking industry. Thus, it is apparent that in the digitalized environment, technology spending becomes a strategic necessity for banks without regard for the concern for profitability.

Moreover, banks have difficulty in identifying the level of necessity (threshold) due to the speed of changes and innovations in technology, FinTech revolutions and increased market competitions, pervasive operational risks of disruptive technologies influencing other risk drivers of banks, and the risks of cybersecurity breaches and system breakdowns (Buchak et al., 2018; Tang & Zannetos, 1992; Ngonzi, 2016; Basel Committee, 2018b; FSB, 2017). Therefore, conventional project assessment techniques, such as the net present value method, are less useful in analyzing strategic capital investments in technology (Gordon & Loeb, 2002; Shank, 1996); hence, banks have an incentive to allocate more budget to strategically remain at the forefront of technological changes and market competition as well as to maintain the resiliency of the technology infrastructure against cybersecurity hazards. As a result, banks take more business risks because of uncertainty in gaining marginal return from additional CyberTech spending. Based on the discussions above, we propose the following hypothesis:

H_A. *A marginal increase in CyberTech spending above what is necessary adversely affects the financial stability of a bank.*

3. Variables and test models

3.1. Dependent variable

This study examines whether spending on CyberTech affects the financial stability of a bank. We use *Z-score* as a stability proxy that captures the variability of net earnings and capital buffer of a bank. This proxy is appropriate in the context of our study because we argue that a bank takes more business risk from additional CyberTech spending. The *Z-score* is estimated as $(ROA + (Equity/Assets))/\sigma ROA$, which explicitly compares the risk buffers such as return on assets (ROA) and the capital ratio (equity to asset) of a bank with the volatility of asset returns. A higher *Z-score* means a lower probability of insolvency.

The *Z-score* is based on accounting data, which is the main point of the criticism of it as the accounting practices and audit quality matter for performance. However, Chiaramonte, Liu, Poli, and Zhou (2016) find that the *Z-score* can predict about 76% of bank failures in the US; thus, it is a well-accepted measure of risk-taking in the literature (Beck, Demirguc-Kunt, & Merrouche, 2013; Čihák & Hesse, 2010; Demirgüç-Kunt, Detragiache, & Tressel, 2008; Laeven & Levine, 2009). Since this *Z-score* uses the after-tax return on assets, we cannot exclude the

[5] A recent study finds that due to regulatory imperfection and supervision failure, FinTech-driven market competition becomes detrimental to bank stability because the development of shadow banking and unregulated banking activity pervasively affecting banks' risk-taking (Vives, 2019).

[6] As the traditional banks face challenges to innovate due to the lack of management focus and internal capabilities, cooperation with FinTech firms is a prominent option to foster banking innovations and maintain the market share during the period of technological revolution (Drasch, Schweizer, & Urbach, 2018).

[7] The synchronization between technological innovations and other factors is a challenging matter. For example, banks' personnel are supposedly experts in the banking business but not in CyberTech. Therefore, with the advancement of CyberTech, banks are increasingly relying on external technology firms or IT personnel to manage their cyber infrastructure. This means banks have less control over their operations due to the faster adoption of CyberTech. Also, banks were burdened with regulations after the financial crisis period, but the FinTech firms expanded their activities in the absence of adequate regulatory controls and supervision (Buchak et al., 2018).

contribution of the country's tax environment to the financial stability of a bank. Therefore, for robustness checking, we re-estimate it based on the income before taxes. The re-estimation leads to a better understanding of the managers' contribution to the financial stability of banks. In the literature, we find that researchers have used corporate risk-taking proxies based on the operating income instead of the net income after taxes (Boubakri, Cosset, & Saffar, 2013; Faccio, Marchica, & Mura, 2011).

3.2. Independent variables

We create two variables to capture the effect of CyberTech spending on bank stability. These are the natural log of the total CyberTech spending (*CyberTech-1*) and the total CyberTech spending as the percentage of non-interest operating expenses (*CyberTech-2*). The total CyberTech spending includes all kinds of costs related to software, hardware, data processing, outsourced technical support, and staff training. Of these, *CyberTech-1* is an aggregate measure transformed into the natural log, while *CyberTech-2* is the relative measure of CyberTech spending. Both measures have academic and practical significance. *CyberTech-1* provides an idea about the overall technology budget of a bank because it is a strategic budgetary allocation, while the *CyberTech-2* gives an idea about the bank's policy on technology versus non-technology expenses. Our hypothesis predicts a concave downward relationship between CyberTech spending and bank stability, which requires us to test non-linear models. Therefore, we also create squared variables: *CyberTech-1 squared* and *CyberTech-2 squared*.

3.3. Bank-level controls

Following the literature, we select (i) total assets, (ii) asset turnover, (iii) cost-to-income ratio, (iv) interest margin, (v) tier-1 capital ratio, (vi) equity-to-assets, and (vii) non-performing loans as the bank-level control variables for the empirical tests. *Total assets* is the common bank-level control that is used by studies because the financial soundness of banks varies with the size of their assets. Haan and Poghosyan (2012) provide a summary of the studies on the relation between the size and risk of banks. *Asset turnover* directly determines the return on assets through the Du-Pont identity and shows that the risks in asset choices of a bank affect their financial soundness (Wagner, 2007). The *Cost-to-income* ratio determines the level of bank efficiency that influences stability (Schaeck & Chiak, 2014). *Interest margin* determines the ability of a bank to manage interest rate risk to affect its profitability (Chaudron, 2018). The effect of the capital ratio on bank stability is well established in the literature, and Anginer et al. (2018b) find that capital is associated with a reduction in the systemic risk contribution of individual banks to system-wide fragility. Therefore, we include *tier-1* capital and *equity-to-asset* ratios as controls for capital. Finally, we take the percentage of *non-performing loans* as another important bank-level variable that directly affects the financial soundness of a bank. Nikolopoulos and Tsalas (2017) provide a review of the literature on loan performance and its effect on performance.

3.4. Country-level controls

As our sample includes global data, we identify a set of country-level controls that are relevant to this study. These include (i) cybersecurity commitment, (ii) corruption, (iii) financial freedom, (iv) gross domestic product, and (v) inflation. *Cybersecurity commitment* is the score awarded to a country by the International Telecommunication Union (ITU) based on the country-level policies and mandatory regulatory requirements to build up a resilient cyber society. Therefore, we assume that the level of a country's commitment to a cyber society affects a bank's budgetary allocation to CyberTech spending. The *Corruption* variable is the corruption perception score of a country as reported by Transparency International, which ranges from 0 (highly corrupt) to 100 (very clean). Regarding corruption in the country, the literature finds that banks extend credit without adequate risk assessment based on the political considerations, and such corrupt practices escalate loan defaults, which affects the stability of banks (Infante & Piazza, 2014)). *Financial freedom* is the financial freedom index of a country provided by Heritage.org. We use this variable because Chortareas, Girardone, and Ventouri (2013) find that higher financial freedom in the economy promotes the level of banking efficiency. *Gross domestic product* is the natural log of the real gross domestic product (GDP) per capita of the country, denominated in US$. Evidence shows that GDP influences bank performance through monetary policy shocks (Jiménez, Ongena, Peydró, & Saurina, 2012). *Inflation* is the annual rate of inflation of a country as measured by the consumer price index, and evidence shows that inflation affects the lending activities and financial market performance of a country (Boyd, Levine, & Smith, 2001).

3.5. Fixed effect control

As the study uses multi-country data over 10 years, we apply a country-year interaction (*Country*Year*) variable to capture the effects of unobservable country-level common factors on the performance of a bank in a particular year that operates in a country. In an earlier study on bank performance, Beck et al. (2013) have also used this interaction variable. We apply this variable to the ordinary least squares (OLS) estimation.

3.6. Test models and estimations

We specify the following base model for the empirical test:

$$Bank\ stability_{it} = \alpha + \beta_i CyberTech_{it} + \sum_{i=1}^{N} \gamma_i Controls_{it} + \varepsilon_i \quad (1)$$

where $Bank\ stability_{it}$ is the *Z-score* of bank *i* in year *t*. $CyberTech_{it}$ is the measure of CyberTech spending by bank *i* in year *t*. We test two alternative measures of CyberTech spending: *CyberTech-1* (the natural log of total CyberTech spending) and *CyberTech-2* (total CyberTech spending as the percentage of non-interest operating expenses). $Controls_{it}$ are the bank- and country-level control variables as well as the country and year interaction variables, as discussed above. The summary of all test variables is available in the appendix. We estimate this base model in three ways. First, we estimate the OLS models after correcting the standard errors for country and year clustering. Second, we test the dynamic system GMM models by adding the lag dependent variable to the model, which potentially corrects endogeneity issues and also provides more consistent estimates of the parameters. Third, we run fixed effect panel regression models that supposedly correct for omitted variable bias. Overall, we can draw a strong inference about our hypothesis if the findings of the base model are consistent across all estimation approaches.

4. Sample and data

As there is no regulatory requirement to disclose the cost of CyberTech as a separate item in income statements, the information is currently unavailable in the standard databases. Therefore, we manually collect the data on CyberTech spending by carefully reviewing the cost items reported in the financial statements of banks.[8] We gather the

[8] First, we check the income statement if the bank reports technology expenses under the heading of 'technology expense' or any related term, such as IT expense, ICT expense, etc. Second, we carefully review the detailed breakdown of the non-interest expense figures reported in the income statement that are available in the end-of-statement notes. We do this search to identify if any sub-item of the total non-interest expense relates to cyber technology spending. Third, we review the detailed breakdown of depreciations and amortizations for intangible assets to identify of any component of depreciations and amortizations related to hardware and software. Finally, we compile and reconcile the data collected from annual reports to construct two focused variables

annual reports from the banks in different countries following a systematic approach. First, we take countries that represent different regions of the world, such as North America, Europe, Latin America, Asia, Pacific, Middle East and North Africa (MENA), and the association of five major emerging national economies, namely Brazil, Russia, India, China and South Africa (BRICS). Second, we get the names of exchange-listed banks and then download their annual reports from their websites or those of the stock markets. We successfully downloaded the annual reports of 354 banks from 43 countries for the period from 2008 to 2017. We need to exclude many banks due to missing reports or because they are published in a non-English language. After reviewing all annual reports, we find that a total of 264 banks disclose cost information related to CyberTech for a minimum of three years. Therefore, we obtain a total of 2156 data observations for CyberTech spending by banks. Overall, the sample is widely distributed across the developed and developing countries as well as different regions. The US market has the highest number at 292 observations (13.49%), and Israel has the lowest number at 21 observations (0.97%). The sample distribution shows the US has the most banks at 30 (11.36%), while Chile, Finland, Japan, Mexico, Netherlands, Singapore, and the UAE have the least at 3 (1.14%). Therefore, the sample and data observations of CyberTech spending are globally representative. We collect the remaining data (other than CyberTech cost) from the Bloomberg database. Table 1 provides details of the distribution of our samples as well as their characteristics.

For example, Table 1 shows that banks globally doubled their spending on CyberTech from US$19,596 million in 2008 to US$ 41,684 in 2017. We observe that Chinese banks by far spend the highest amount on CyberTech throughout the sample period. However, if we carefully see the latest data for 2017, nine (9) banks in China spend the highest amount of US$9988 million followed by the USA (32 banks; US $3115 million), Spain (8 banks; US$2960 million), and Australia (6 banks; US$ 2319 million). On the other hand, 15 Bangladeshi banks spend merely US$ 13 million, followed by Egypt (9 banks; US$ 17 million), Tunisia (7 banks; US$ 29 million), and Argentina (7 banks; US $ 44 million). We also observe wide variations in the growth of CyberTech spending across countries.

The descriptive statistics in Table 2 show that the dependent variable *Z-score* varies from −1.719 to 48.795 with an average value of 7.511 and a standard deviation of 8.917. The *Z-score* (before tax), which is based on operating income before taxes, also shows a similar variation with a lower average of 6.438. The distributions of both *Z-scores* are skewed toward the right and are leptokurtic, which indicates outliers. We find that the distribution of *CyberTech-1* is relatively normal as its skewness (−0.318) is closer to zero, while kurtosis (2.983) is very close to 3. The distribution of *CyberTech-1 squared* is also slightly asymmetric as skewness (1.22) is marginally above 1, while kurtosis (3.861) is also marginally more than 3. The distribution of the other CyberTech spending variable, *CyberTech-2*, is skewed to the right side with a leptokurtic peak. Also, the distributions of bank-level control variables are generally skewed toward the right with leptokurtic peaks. However, the country-level controls are slightly skewed (− or +) from the symmetrical position with mostly platykurtic peaks. As a whole, the descriptive statistics show significant variation in the data observations with skewed distributions and leptokurtic or platykurtic peaks. These observations are typical of the real-life situation. Therefore, we winsorize the data observations at the 1% level on both sides of the distributions and rely on the robust *t-values* to test the statistical significance of the estimates of the model coefficients.

5. Results and discussion

5.1. Data visualization

We hypothesize that a marginal increase in CyberTech spending above what is necessary adversely affects the stability of a bank. Therefore, we expect a downward quadratic relation between CyberTech spending and bank stability. Hence, we first illustrate the scatter plots and polynomial regression splines of the test data in Fig. 1. Based on the scatter plot, Fig. 1.a shows a probable nonlinear relation between *CyberTech-1* and the *Z-score* as the scatter dots are less concentrated at the edges. The regression spline in Fig. 1.b confirms a concave downward relationship. Figs. 1.c and 1.d display a similar concave downward relationship between *CyberTech-2* and the *Z-score*. Overall, the data visualizations are consistent with the argument that a bank has no marginal benefit if it overspends on CyberTech even as technology and innovations advance at a much faster speed.

5.2. Baseline results

Table 3 presents the results from the OLS and dynamic system GMM of the base regression for both the linear and nonlinear effects of *CyberTech-1* on the *Z-score*. The findings of both the OLS (Model-2) and the GMM (Model-4) show that CyberTech spending has a statistically significant downward quadratic effect on a bank's risk-taking, and thereby affects its financial stability because both the OLS and GMM coefficients for *CyberTech-1* and *CyberTech-1 squared* are respectively positive and negative and are also statistically significant. The OLS coefficients of *CyberTech-1* and *CyberTech-1 squared* are 0.799 and − 0.107, respectively, which are significant at the 1% level. The corresponding GMM coefficients are 3.144 and − 0.372, respectively, which are significant at the 5% level. Overall, the nonlinear effect is consistent for both the OLS and GMM estimations. However, the linear tests provide inconsistent findings as the OLS (Model-1) coefficient for *CyberTech-1* is insignificant while that of the GMM (Model-3) estimate is marginally significant at the 10% level.

The findings overall support our hypothesis. Hence, the study confirms that overspending on CyberTech has no marginal gain and leads to high risk-taking. The baseline results suggest that banks should be cautious while investing in technology due to the existence of hype cycles in technological innovations (Dedehayir & Steinert, 2016; Lente, Spitters, & Peine, 2013). A bank could burden itself by quickly adopting new technology as the majority of technological innovations fail to sustain themselves in the long run due to the existence of shorter hype cycles. This is the case because the latest software and hardware could quickly become obsolete with the arrival of innovations before the current investment pays off. The risk of a cybersecurity breach or a system breakdown does not lessen by adding better technology, and customers might have difficulty frequently switching to new technologies. In a nutshell, we show that a 1% increase in CyberTech spending leads to more than a 1% increase in risk-taking by a bank.

As a bank takes more than the proportional risk for every dollar of cyber spending, an important question is whether banks should strike a balance between technology and non-technology spending. Therefore, we examine the effect of CyberTech spending as the percentage of non-interest operating costs (*CyberTech-2*) on the stability of a bank. In Table 4, we find a similar nonlinear downward quadratic effect on the *Z-score,* based on the results of OLS (Model-2) and GMM (Model-4) estimations. Both the OLS and GMM coefficients for *CyberTech-2* and *CyberTech-2 squared* are positive and negative, respectively. The OLS coefficients for *CyberTech-2* and *CyberTech-2 squared* are 0.171 and − 0.005, respectively, which are significant at the 5% level. However, the GMM estimates for *CyberTech-2* and *CyberTech-2 squared* are 0.557 and − 0.012, respectively, whereby the coefficient for *CyberTech-2* is significant at the 5% level while that of *CyberTech-2 squared* is significant at the 10% level. Hence, the results of both the OLS and GMM confirm that a concave downward relationship exists between *CyberTech-2* and the *Z-score* as well. We also find that the results of linear models (Model-1 and Model-3) are consistently significant for both the OLS and GMM estimations. Based on the linear and non-linear results in Table 4, we can conclude that banks should maintain an optimal balance in CyberTech spending as a part of their total non-

Table 1
Sample distribution.

No.	Country	Total banks	Banks reporting cyber spending data.	Total observations	Year-wise distribution of spending on CyberTech by banks across 43 countries (Figures in million $)									
					2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
1	Argentina	7	4	35	43	40	40	47	60	44	45	32	36	44
2	Australia	6	6	48	473	915	1420	1908	2441	2328	2143	2133	2299	2319
3	Bangladesh	18	14	101	1	2	2	8	32	35	42	50	13	13
4	Belgium	8	4	40	1040	1216	914	1069	894	878	779	683	767	978
5	Brazil	17	6	51	1304	2344	2604	2415	2459	2605	2443	1752	2308	2287
6	Canada	4	4	31	1059	1227	1277	1520	1626	1598	1666	1473	1640	1929
7	Chile	9	3	28	274	246	306	404	411	464	476	497	547	612
8	China	9	8	76	4265	4464	5132	6011	7949	8993	8751	8695	8205	9988
9	Denmark	7	4	27	282	204	175	188	175	185	183	194	269	328
10	Egypt	9	7	39	4	1	5	2	1	23	26	37	15	17
11	Finland	4	3	22	7	20	94	141	41	54	337	271	250	280
12	France	12	8	61	30	61	84	112	104	124	127	126	109	106
13	Germany	6	5	44	380	1067	1027	780	445	481	464	424	411	602
14	Greece	5	5	50	296	327	378	391	474	532	483	445	429	547
15	India	16	8	51	41	111	121	104	76	128	156	193	239	320
16	Indonesia	10	5	44	203	245	280	104	194	167	217	179	254	237
17	Israel	5	4	21	153	175	214	239	568	630	567	700	866	991
18	Italy	8	6	60	1197	569	1386	1285	1257	1139	1126	945	1042	1277
19	Japan	6	3	30	999	978	1725	1880	1850	1954	1440	1486	1591	1688
20	Jordan	8	8	71	36	40	34	43	48	54	68	72	61	64
21	Malaysia	9	9	87	293	408	498	509	589	672	694	588	575	682
22	Mexico	7	3	27	64	77	84	97	114	129	121	118	96	113
23	Netherland	3	3	23	1725	1888	1985	1946	1684	1684	1425	1379	1299	1473
24	New Zealand	4	4	34	77	186	215	212	241	243	250	269	321	264
25	Norway	9	9	69	4	35	54	65	82	78	66	61	67	75
26	Oman	6	5	37	59	68	25	28	78	73	46	54	101	330
27	Pakistan	8	7	66	17	16	19	32	39	46	50	42	50	50
28	Poland	9	9	77	591	685	548	458	653	845	834	615	716	821
29	Qatar	4	4	28	8	8	50	72	52	126	41	43	45	44
30	Russia	8	4	31	41	65	79	66	114	1126	1003	1000	1034	1203
31	Saudi Arabia	8	7	44	62	153	133	155	161	167	177	279	286	264
32	Singapore	3	3	22	267	261	361	387	962	1033	1138	1231	1279	1461
33	South Africa	7	4	40	233	329	414	360	314	271	269	217	327	411
34	South Korea	5	4	25	31	17	437	496	583	621	587	603	734	956
35	Spain	8	4	37	1655	1660	1628	2188	2555	2718	2360	2459	2444	2960
36	Sweden	4	4	33	18	28	51	75	60	69	71	70	64	85
37	Switzerland	13	9	56	69	72	75	112	106	99	96	124	99	108
38	Thailand	6	4	24	10	11	28	42	49	57	82	98	102	118
39	Tunisia	7	5	26	3	4	12	15	24	24	17	25	27	29
40	Turkey	10	9	77	206	312	369	387	533	566	688	578	605	651
41	UAE	4	3	30	6	8	13	19	31	35	44	55	79	105
42	UK	6	6	50	251	383	479	609	786	1549	1579	1858	1285	1736
43	USA	32	30	292	1822	2159	2223	2240	2348	2435	2589	2818	2913	3115
	Total	**354**	**264**	**2165**	**19,596**	**23,084**	**26,997**	**29,221**	**33,262**	**37,082**	**35,769**	**34,972**	**35,900**	**41,684**

Table 2
Variable descriptive statistics.

Variables	Obs.	Mean	Std.Dev.	Minimum	Maximum	Skewness	Kurtosis
Z-score	3237	7.511	8.917	−1.719	48.795	2.301	9.354
Z-score (before taxes)	3047	6.438	7.113	−1.695	38.437	2.221	9.041
CyberTech-1	2164	3.042	2.179	−2.989	7.476	−0.318	2.983
CyberTech-1 squared	2164	14.139	13.47	0.009	55.889	1.220	3.861
CyberTech − 2	2102	6.724	6.771	0.020	31.943	1.627	5.537
CyberTech-2 squared	2102	91.124	177.209	0.001	1020.36	3.274	14.793
Total asset	3341	9.843	1.922	5.749	14.484	0.337	2.609
Asset turnover	3307	0.048	0.036	0.007	0.214	2.595	10.777
Cost-to-income	3317	2.087	4.587	−17.612	25.931	1.270	16.214
Interest margin	3105	3.685	3.039	0.595	20.269	3.131	15.290
Tier-1 capital	2417	13.033	3.953	6.390	30.300	1.469	6.892
Equity-to-asset	3339	0.099	0.050	0.009	0.370	2.358	12.431
Non-performing loan	2270	3.920	4.915	0.133	30.738	3.001	14.129
Cybersecurity commitment	3540	0.592	0.184	0.176	0.919	−0.396	2.310
Corruption	3540	55.605	21.286	21.000	93.000	0.175	1.640
Financial freedom	3540	58.175	18.047	20.000	90.000	−0.294	2.219
Gross domestic product	3540	4.166	0.576	2.861	4.955	−0.676	2.380
Inflation	3540	4.113	5.593	−15.713	23.949	0.934	7.123

Z-score = (ROA + capital-asset ratio)/σROA. *CyberTech-1* is the natural log of the total CyberTech spending by sample bank. *CyberTech-1 squared* is the squared value of *CyberTech-1*. The minimum value of the natural log of the total CyberTech is negative because we extracted values in a million figures. So, a figure becomes a fraction when it is less than a million, and the log of a positive fraction can have a negative value. *CyberTech-2* is the CyberTech spending as a percent of non-interest operating costs. *CyberTech-2 squared* is the squared value of *CyberTech-2*. The *Z-score* (before taxes) is estimated by using the return on assets based on operating income (instead of net income). *Total Assets* are the natural log of the total bank assets. *Asset turnover* is the total revenue divided by the total assets of the bank. The *cost-to-income* is the ratio of operating expense to operating income. *Interest margin* is the spread between the average lending and deposit interest rates of the bank. *Tier-1* is the ratio of a bank's core capital to the risk-weighted asset. *Equity-to-asset* is the total equity of the bank divided by its total assets. The *non-performing loan* is the percentage of non-performing loans in the total loans of a bank. *Cybersecurity commitment* measures the commitment score of the country to cybersecurity as reported by International Telecommunication Union. *Corruption* is the corruption perception index of the country as reported by Transparency International. *Financial freedom* is the financial freedom index of a country provided by Heritage.org. *Gross domestic product* is the natural log of the real gross domestic product per capita of the country. *Inflation* is the annual rate of inflation of a country.

interest operating costs to achieve the maximum financial stability.

In Table 5, we present results based on fixed-effect panel regressions that reconfirm the existence of a highly significant downward quadratic relationship between both measures of CyberTech spending (*CyberTech-1* and *CyberTech-2*) and bank stability (*Z-score*) due to the more than proportional increase in risk-taking for a one-dollar additional spending on CyberTech. The nonlinear Model-2 shows that the coefficients for *CyberTech-1* and *CyberTech-1 squared* are positive and negative, respectively, and both coefficients are significant at the less than 1% level. Likewise, Model-4 shows that the coefficients for *CyberTech-2* and *CyberTech-2 squared* are also positive and negative, respectively, with a level of significance similarly at less than 1%. As expected, the results of the linear regressions (Model-1 and Model-3) are statistically insignificant, but the nonlinear results (Model-2 and Model 4) are highly significant. Therefore, the findings of the OLS, GMM, and fixed-effect panel regressions reported in Tables 3, 4, and 5 provide clear global evidence to support our hypothesis. Hence, the empirical tests prove that a marginal increase in CyberTech spending above what is necessary adversely affects the stability of a bank.

5.2.1. Bank sizes and financial stability

The technology policies and strategies of small banks could differ subject to the availability of resources, and industry analysts find that retail banks struggle to find resources to face the challenges of the digital era. However, large banks can dedicate more funds to developing their digital infrastructure to combat cybersecurity threats and compete with FinTech firms. Furthermore, studies find that banks' stability varies with their size and market share (Kim, Park, & Song, 2016; Pawlowska, 2016). Hence, we examine if the CyberTech spending by small and large banks has different effects on their financial stability. Small banks are those with total assets below the median value, while large banks are those with asset values above the median. The regression results in Table 6 generally show that CyberTech spending has a significant nonlinear quadratic effect on the stability of both small and large banks as the results of the nonlinear models (Model-2 and Model-4) are significant while those of the linear models (Model-1 and Model-3) are insignificant. These findings indicate the pervasiveness of technology risks as they adversely affect the stability of all banks irrespective of their size. Hence, our results differ from earlier studies that find that banks' riskiness varies with their size (Laeven, Ratnovski, & Tong, 2016; Varotto & Zhao, 2018).

5.2.2. Technological advancement and financial stability

We assume that the country-level development of CyberTech and the maintenance of a resilient cyber infrastructure could play a role in banks' decision-making in terms of spending on technology. If the country has a strong commitment to the technological transformation of its society, then banks need to comply with regulatory requirements concerning technology adoption and maintaining their cyber infrastructure (Crisanto & Prenio, 2017). The International Telecommunication Union (ITU) periodically assesses[9] the commitment level of a country to build a cyber-resilient nation. It measures this level with an aggregate score based on several criteria, such as ICT regulations, technical infrastructure, organizational implementation of ICT initiatives, level of capacity to build programs, and cooperation with local and international agencies. Based on the ITU scores, we classify sample countries into three groups: (i) initiating level, (ii) maturing level, (iii) leading level. The countries at the initiating level are those with a cyber resiliency commitment score below the 33rd percentile, the countries at the maturing level are those with a score between the 34th and 67th percentiles, and the countries at the leading level are those with a score above the 67th percentile. The empirical findings in Table 7 show that the marginal benefit of CyberTech for banking stability gradually wanes as the country gradually moves from the initiating level and to the maturity level of cyber resiliency.

Table 7 shows that the coefficient for *CyberTech-1* in the linear

[9] Its first report was published in 2015 and was based on the prior years' data. Subsequent reports were published in 2017 and 2019.

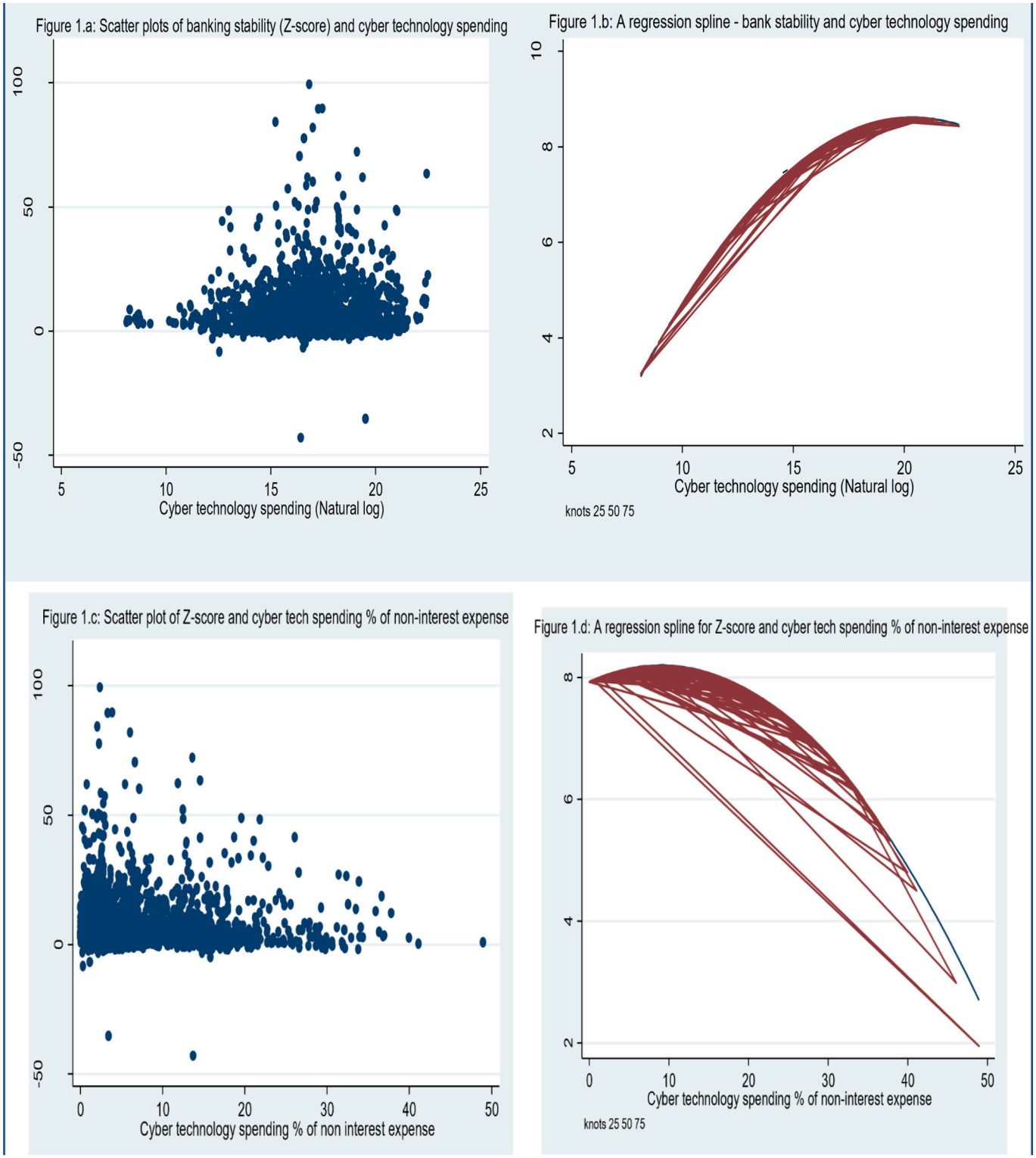

Fig. 1. Pattern of relationship between banking stability and CyberTech spending.

model (Model-1) is significantly positive in the initiating level countries, which indicates that the banks of these countries can improve performance by spending more on cyber technology. The coefficients for the nonlinear equations (Model-2) are insignificant and confirm the finding in Model-1. This finding is because substituting technology for the manual process helps these countries reduce their operational costs while their technology risks are still low as the cyber penetration is negligible. In the maturing level countries, the coefficient for *CyberTech-1* in the linear model (Model-3) is still significantly positive, while the coefficients of *CyberTech-1* and *CyberTech-1 squared* in the nonlinear model (Model-4) are significantly positive and negative, respectively. These coefficients indicate that the pervasive technology risks gradually take a toll on bank performance, which leads to more risk-taking. When a country reaches the leading level of technological advancement, we find that a marginal increase in CyberTech spending only adversely affects the stability of a bank. The coefficient for

Table 3
Regression findings of banking stability and CyberTech spending measured as the natural log.

Variables		OLS estimation		GMM estimation	
		Model 1 Linear Model	Model 2 Non-linear Model	Model 3 Linear Model	Model 4 Non-linear Model
Lag variable	*Z-score*$_{t-1}$			0.577***	0.564***
				(10.276)	(9.821)
Focused variables	*CyberTech-1*	0.166	0.799***	0.874*	3.144**
		(1.259)	(5.382)	(1.837)	(2.243)
	CyberTech-1 squared		−0.107***		−0.372**
			(−5.584)		(−2.047)
Bank-level controls	*Total asset*	0.467**	0.578***	0.285	0.420
		(2.349)	(2.684)	(0.603)	(0.708)
	Asset turnover	−18.424	−15.286	−10.500	7.384
		(−0.871)	(−0.729)	(−0.305)	(0.190)
	Cost to income	−0.113**	−0.114**	0.088	0.114
		(−2.225)	(−2.305)	(0.933)	(1.183)
	Interest margin	0.357	0.332	0.286	−0.104
		(1.268)	(1.202)	(0.662)	(−0.198)
	Tier-1 capital	0.145	0.144	0.020	0.024
		(1.371)	(1.342)	(0.174)	(0.195)
	Equity-to-asset	28.729***	27.926***	38.075	33.397
		(3.432)	(3.358)	(1.570)	(1.362)
	Non-performing loan	−0.529***	−0.529***	−0.233*	−0.286**
		(−11.460)	(−11.296)	(−1.894)	(−2.101)
Country-level controls	*Cybersecurity commitment*	1.760	1.853	−1.033	−2.338
		(0.693)	(0.717)	(−0.276)	(−0.588)
	Corruption	0.052	0.058	−0.006	−0.007
		(1.454)	(1.654)	(−0.082)	(−0.001)
	Financial freedom	−0.072**	−0.076**	0.106	0.116
		(−2.139)	(−2.423)	(1.468)	(1.500)
	Gross domestic product	−4.664***	−4.641***	−5.140**	−5.955**
		(−4.990)	(−4.802)	(−2.175)	(−2.233)
	Inflation	−0.298***	−0.298***	−0.015	−0.051
		(−3.215)	(−3.265)	(−0.111)	(−0.354)
Fixed effect	*Country and Year*	−0.000***	−0.000***	*See note*	*See note*
		(−3.665)	(−4.539)		
	Constant	22.211***	20.463***	10.407	11.665
		(3.310)	(2.958)	(1.130)	(1.149)
	Observations	1356	1356	1256	1256
	F-Value (OLS)/Wald χ^2 (GMM)	28.210	27.340	386.090	350.520
	R-squared	0.185	0.189		

We estimate $Zscore_{it} = \alpha_i + \beta_i CyberTech1_{it} + \Sigma_{i=1}{}^{n}\Upsilon Control_{it} + \varepsilon_{it}$ by using an OLS and a dynamic panel of system GMM. We include $Zscore_{it-1}$ as a lag variable in the GMM model. *Z-score* is the proxy for banking stability calculated as (ROA + capital-asset ratio)/σROA; where ROA equals the ratio of net income to total assets. *CyberTech-1* is the natural log of the total CyberTech spending of the bank. *Controls* are vectors of control variables defined in the appendix. The country and year interaction variable is used in the OLS estimation based on the literature (Beck et al., 2013) but is not applied to the system GMM as supporting literature is unavailable. The values within parenthesis are robust *t-stats* adjusted for heteroscedasticity. The asterisks ***, **, and * denote significance at less than 1%, 5%, and 10% levels.

CyberTech-1 in the linear model (Model-5) confirms the finding as it is significantly negative for the banks operating in technologically leading countries. For the nonlinear model (Model-6), we find that the coefficients for both *CyberTech-1* and *CyberTech-1 squared* are negative, whereby *CyberTech-1 squared* is significantly negative at the less than 1% level.

5.2.3. The FinTech era and financial stability

The technological transformation in the banking sector started many years ago, but the rise of FinTech firms and shadow banking after the global financial crisis changed the operational structure and market players of the global financial market over the decade. Therefore, banks have had no choice but to aggressively adopt advanced technologies or build partnerships with FinTech firms to retain market share and survive. Hence, we separately check the effect of CyberTech spending on the banks' risk-taking and stability during the pre-FinTech and FinTech periods. In Table 8, the results of the linear tests (Model-1 and Model-3) are insignificant for both periods, but the nonlinear tests (Model-2 and Model-4) identify a significantly downward quadratic relationship between CyberTech spending and the banks' stability during the FinTech period. The nonlinear coefficients for *CyberTech-1* and *CyberTech-1 squared* are positive and negative, respectively, and both are significant at less than the 1% level. The significantly positive coefficient for *CyberTech-1* in the FinTech period indicates that banks took advantage of CyberTech to stay competitive in the market and to overcome FinTech challenges. However, overspending on technology leads a bank to take more risks, which negatively affects its stability. The quadratic effect of technology spending on bank stability is also evident in the pre-FinTech period, but the coefficient for *CyberTech-1* is insignificantly positive, which indicates that the financial crisis meltdown took away any technological gains as well. The adverse effect of overspending on technology is clearly noticeable in the FinTech era as *CyberTech-1 squared* is significantly negative.

5.3. Robustness checks

In the above analysis, we use after-tax ROA to estimate the *Z-score*. Thus, our bank stability measure may be driven by the tax regulations of a country. Therefore, we re-estimate the base model by applying a *Z-score* that is before taxes to eliminate any effect of the country's tax environment on the financial stability of a bank. We test both linear and nonlinear models to check if the effect of CyberTech spending on the

Table 4
Regression findings of banking stability and CyberTech spending measured as the percentage of non-interest expense.

Variables		OLS estimation		GMM estimation	
		Model 1 Linear Model	Model 2 Non-Linear Model	Model 3 Linear Model	Model 4 Non-linear Model
Lag variable	*Z-score*$_{t-1}$			−0.150***	−0.151***
				[−4.874)	(−3.420)
Focused variables	*CyberTech-2*	0.060**	0.171**	0.170*	0.557**
		(2.398)	(2.720)	(1.940)	(2.114)
	CyberTech-2 squared		−0.005**		−0.012*
			(−2.240)		(−1.788)
Bank-level controls	*Total asset*	0.647***	0.639***	1.346	1.183
		(3.442)	(3.500)	(0.915)	(0.885)
	Asset turnover	−18.021	−16.283	71.358	78.728*
		(−0.856)	(−0.770)	(1.437)	(1.940)
	Cost to income	−0.111**	−0.111*	−0.008	−0.009
		(−2.183)	(−2.170)	(−0.199)	(−0.666)
	Interest margin	0.382	0.364	1.156**	1.169**
		(1.345)	(1.280)	(2.275)	(2.539)
	Tier1 capital	0.144	0.148	−0.186	−0.198
		(1.393)	(1.400)	(−1.189)	(−1.552)
	Equity-to-asset	28.845***	27.508**	7.766	8.386
		(3.495)	(3.180)	(0.360)	(0.473)
	Non-performing loan	−0.526***	−0.524***	−0.188	−0.199*
		(−11.106)	(−11.180)	(−1.454)	(−1.657)
Country-level controls	*Cybersecurity commitment*	1.760	1.654	−16.687***	−17.197**
		(0.691)	(0.660)	(−3.959)	(−2.226)
	Corruption	0.050	0.512	0.099	0.096
		(1.381)	(1.410)	(1.444)	(1.260)
	Financial freedom	−0.071**	−0.074*	−0.025	−0.022
		(−2.046)	(−2.160)	(−0.365)	(−0.353)
	Gross domestic product	−4.644***	−4.707***	37.507***	36.991**
		(−5.051)	(−5.070)	(3.212)	(2.481)
	Inflation	−0.296***	−0.297***	−0.128**	−0.135*
		(−3.192)	(−3.230)	(−2.342)	(−1.729)
Fixed effect	*Country and Year*	−0.000***	−0.000***	*See note*	*See note*
		(−3.446)	(−3.390)		
	Constant	20.287***	20.420**	−165.218***	−162.854**
		(2.744)	(2.770)	(−3.799)	(−2.436)
	Observations	1356	1356	1041	1041
	F-Value (OLS)/Wald χ^2 (GMM)	27.940***	26.390***	74.81***	71.49***
	R-squared	0.189	0.187		

We estimate $Zscore_{it} = \alpha_i + \beta_i CyberTech2_{it} + \Sigma_{i=1}{}^{n} YControl_{it} + \varepsilon_{it}$by using an OLS and a dynamic panel of the system GMM. We include $Zscore_{it-1}$ as a lag variable in the GMM model. *Z-score* is the proxy for banking stability calculated as (ROA + capital-asset ratio)/σROA; where ROA equals the ratio of net income to total assets. *CyberTech-2* is the CyberTech spending as the percentage of non-interest spending of the bank. *Controls* are vectors of control variables defined in the appendix. The country and year interaction variable is used in the OLS estimation based on the literature (Beck et al., 2013) but is not applied to the system GMM as supporting literature is unavailable. The values within parenthesis are robust *t-stats* adjusted for heteroscedasticity. The asterisks ***, **, and * denote significance at less than 1%, 5%, and 10% levels.

before-tax *Z-score* is consistent with that of the after-tax *Z-score*. The results in Table 9 (Panel A) show that both measures of CyberTech spending (*CyberTech-1* and *CyberTech-2*) have a similar nonlinear downward quadratic effect on the before-tax *Z-score*. Overall, the results are consistent with those based on the after-tax Z-score. Therefore, our robustness tests confirm that the effect of CyberTech spending on bank stability is not sensitive to the differences in the tax policies across countries.

In earlier regressions, we tested *CyberTech-1* and *CyberTech-2* as alternative proxy measures for the CyberTech spending of banks. The results show that a 1% increase in CyberTech expenditure leads to more than proportional risk-taking by banks and that banks take more risk and become unstable if they spend more on cyber technology. These findings suggest that banks that overspend on CyberTech are more unstable than those spending less on technology. Therefore, we split the samples into three groups based on their annual spending on cyber technology. The high technology spending banks ($CyberTech_{High}$) are those with a total yearly spending amount that is greater than the 75th percentile. The low technology spending banks ($CyberTech_{Low}$) are those with an annual total spending amount that is lower than the 25th percentile. The banks with technology spending between the 25th and 75th percentiles are considered the base group. Then, we change the base regression by replacing the continuous measures of CyberTech spending with two dummy variables:

$$Bank\ stability_{it} = \alpha + \beta_1 CyberTech_{High} + \beta_2 CyberTech_{Low} + \sum_{i=1}^{n} YControl_{it} + +\varepsilon_{it} \quad (2)$$

In this test, $CyberTech_{High}$ and $CyberTech_{Low}$ show the variation in bank stability relative to the base group. Table 9 (Panel B) shows that the coefficient for $CyberTech_{High}$ is significantly negative for both after-tax and before-tax *Z-scores*. This coefficient indicates that a bank that overspends on CyberTech is less stable than the base group. We find that the coefficient for $CyberTech_{Low}$ is positive for both measures of the *Z-score*, but they are insignificant. This coefficient means that spending less on technology is not marginally better than spending moderately. Overall, the robustness tests with dummy specifications revalidate our earlier findings that overspending on CyberTech leads to higher risk-taking and more instability in banks and that maintaining an optimal balance between technology and non-technology expenditures is essential.

Table 5
Fixed effect (FE) panel regression findings of banking stability and CyberTech spending.

Variables		FE panel regressions for the natural log of CyberTech spending.		FE panel regressions for the CyberTech spending as the percentage of non-interest expense.	
		Model 1 Linear	Model 2 Non-linear	Model 3 Linear	Model 4 Non-linear
Focused variables	*CyberTech-1*	−0.502	0.629***		
		(−0.39)	(3.68)		
	CyberTech-1 squared		−0.113***		
			(−5.19)		
	CyberTech-2			0.007	0.136***
				(0.30)	(2.63)
	CuberTech-2 squared				−0.005***
					(−2.91)
Bank-level controls	*Total asset*	0.617***	0.734***	0.579***	0.575***
		(3.07)	(3.48)	(3.30)	(3.36)
	Asset turnover	−20.556	−17.935	−21.869	−20.096
		(−0.78)	(−0.68)	(−0.81)	(−0.75)
	Cost to income	−0.135***	−0.136***	−0.135***	−0.135**
		(−2.61)	(−2.67)	(−2.62)	(−2.62)
	Interest margin	0.514	0.493	0.519	0.501
		(1.63)	(1.57)	(1.63)	(1.57)
	Tier1 capital	−0.013	−0.189	−0.006	−0.000
		(−0.12)	(−0.18)	(−0.06)	(−0.00)
	Equity-to-asset	20.493***	18.979***	20.37***	19.118***
		(2.99)	(2.92)	(2.94)	(2.67)
	Non-performing loan	−0.561***	−0.559***	−0.562***	−0.560***
		(−12.89)	(−12.80)	(−12.43)	(−12.58)
Country-level controls	*Cybersecurity commitment*	−1.170	−1.316	−1.20	−1.367
		(−0.69)	(−0.79)	(−0.67)	(−0.79)
	Corruption	0.059*	0.067**	0.058*	0.059*
		(1.98)	(2.42)	(1.95)	(1.97)
	Financial freedom	−0.080*	−0.843**	−0.80*	−0.084**
		(1.99)	(−2.26)	(−1.98)	(−2.07)
	Gross domestic product	−4.514***	−4.529***	−4.482***	−4.502***
		(−3.95)	(−3.90)	(−3.97)	(−3.95)
	Inflation	−0.381***	−0.370***	−0.375***	−0.371***
		(3.32)	(−3.06)	(−3.34)	(−3.29)
	Constant	24.241***	22.544***	24.359***	24.267***
		(3.32)	(2.99)	(3.09)	(3.10)
	Observations	1356	1356	1356	1356
	F-Value	22.70	21.72***	22.70***	21.22***
	R-squared	0.181	0.186	0.182	0.182

We estimate the base model $Zscore_{it} = \alpha_i + \beta_i CyberTech_{it} + \Sigma_{i=1}{}^{n}\Upsilon Control_{it} + \varepsilon_{it}$ as a fixed effect panel regression. We apply the *Z-score* as the proxy for banking stability calculated as (ROA + capital-asset ratio)/σROA. In this estimation, ROA equals the ratio of net income to total assets. We test two proxies for CyberTech spending: *CyberTech-1* is the natural log of total CyberTech spending, and *CyberTech-2* is the CyberTech spending as the percentage of non-interest expense. *Controls* are vectors of bank- and country-level variables defined in the appendix. The values in parenthesis are robust *t-stats* adjusted for heteroscedasticity. The asterisks ***, **, and * denote significance at less than 1%, 5%, and 10% levels.

5.4. Findings by region and country

In this subsection, we provide more insights into the above findings by presenting the results for regions and countries. We test the base regression for every country and region separately by using the alternative measures of the dependent and independent variables. As the findings are generally consistent, we only discuss the results for the before-tax *Z-score* and *CyberTech-2*. Table 10 shows that CyberTech spending has a nonlinear but quadratic downward effect on bank stability in all regions of the world; however, the effect is significant mainly in North America, Europe, and MENA. This effect means that these parts of the world are maturating in technology use; thus, the marginal benefit from technology spending is waning due to the economic law of diminishing returns. However, the country-level findings show the different nature of the relationship between technology spending and banking stability. We find a wide variation in the country-level results. For example, banks in Germany, Greece, Netherlands, Finland, Denmark, Bangladesh, Turkey, and Argentina seem to be able to overcome the diminishing returns by more aggressively spending on technology as *CyberTech-2* is negative but *CyberTech-2 squared* is significantly positive. In countries such as Canada, France, Belgium, Italy, Switzerland, Sweden, Indonesia, Singapore, New Zealand, Brazil, and Saudi Arabia, banks can benefit from spending more on cyber technology, yet the marginal gain is not enough to resist the law of diminishing returns. In these countries, *CyberTech-2* is negative and *CyberTech-2 squared* is positive but insignificant. In the remaining countries, including the US, an increase in technology spending by banks still yields a positive result up to a point, but spending more than the threshold adversely affects the banks as *CyberTech-2* and *CyberTech-2 squared* are positive and negative, respectively, in these counties.

Overall, in 19 countries, the stability of banks declines to a certain point with every dollar of technology spending, followed by an improvement in stability with a further increase in technology expenditure. However, in the remaining 24 countries, an additional dollar of technology expense improves bank stability initially up to a threshold level, followed by a decline in stability with more technology spending beyond the threshold. Therefore, we find two global technological regimes for banks' risk-taking and stability across both developed and developing countries. In one technological regime, banks require more aggressive spending on technology to further improve their performance and overcome the diminishing returns of cyber technology. In the other regime, banks need to be more cautious in

Table 6
Bank stability and CyberTech spending by bank size.

Variables		Small banks		Large banks	
		Model 1 Linear	Model 2 Non-linear	Model 3 Linear	Model 4 Non-linear
Focused variables	*CyberTech-1*	0.055	0.199	0.174	1.118*
		(0.181)	(0.794)	(1.225)	(2.063)
	CyberTech-1 squared		−0.124*		−0.128*
			(−2.206)		(−2.041)
Bank-specific variables	*Total asset*	1.875***	1.965***	−0.016	0.235
		(4.984)	(4.781)	(−0.081)	(1.000)
	Asset turnover	2.337	8.417	−53.551	−46.870
		(0.042)	(0.154)	(−1.643)	(−1.469)
	Cost to income	−0.075	−0.070	−0.125**	−0.126**
		(−1.669)	(−1.511)	(−2.528)	(−2.603)
	Interest margin	0.172	0.155	0.881*	0.854*
		(0.304)	(0.277)	(2.008)	(1.986)
	Tier 1 capital	0.090	0.098	0.262**	0.245**
		(0.497)	(0.536)	(2.750)	(2.564)
	Equity to asset	24.588*	22.034	22.650**	23.646**
		(1.868)	(1.664)	(2.485)	(2.604)
	Non-performing loan	−0.375***	−0.367***	−0.538***	−0.542***
		(−3.643)	(−3.573)	(−10.991)	(−10.965)
Country-specific variables	*Cybersecurity commitment*	−3.164	−2.467	3.025	3.063
		(−0.647)	(−0.498)	(1.084)	(1.091)
	Corruption	0.142***	0.158***	0.034	0.032
		(5.305)	(5.512)	(0.768)	(0.741)
	Financial freedom	−0.083	−0.088	−0.053	−0.052
		(−1.637)	(−1.721)	(−1.601)	(−1.564)
	Gross domestic product	−2.810*	−2.931**	−5.863***	−5.729**
		(−2.152)	(−2.335)	(−3.264)	(−3.102)
	Inflation	−0.079	−0.088	−0.403***	−0.405***
		(−0.854)	(−0.946)	(−3.423)	(−3.502)
Fixed effects	*Country and Year*	−0.000	−0.000	−0.000**	−0.000**
		(−1.366)	(−1.572)	(−2.637)	(−2.494)
	Constant	0.164	−0.330	31.711***	26.745**
		(0.022)	(−0.040)	(3.527)	(2.481)
	Observations	393	393	963	963
	F-value	8.380	7.980	14.850	14.830
	R-square	0.149	0.153	0.208	0.210

We estimate $Bank\ stability_{it} = \alpha + \beta CyberTech1_{it} + \Upsilon Controls_{it} + \varepsilon_{it}$. We classify the sample into two size groups based on the median value of the log of total assets. The small banks are those below the median value while the large banks are those above the median. *CyberTech-1* is the explanatory variable that is the natural log of total cyber tech spending as absolute value, and the *Z-score* is the proxy for bank stability. Values in parenthesis are robust *t-stats* adjusted for heteroscedasticity in the data. The asterisks ***, **, and * denote significance at less than 1%, 5%, and 10% levels.

increasing technology spending because excess spending may quickly lead to diminishing returns.

However, the country-level results show that the same technological regime can exist for both developed and developing countries. For example, banks in the developed countries like Germany, the Netherlands, Finland, and Denmark overcome the diminishing return stage with aggressive spending on new technology. We find a similar situation in developing countries like Argentina, Bangladesh, Oman, and Thailand, where banks spend heavily on technology to exert a positive effect on the stability of banks. While future research will perform a more in-depth study of this anomaly, we can assume that there is a life-cycle for the technological regime. Perhaps some advanced countries moved to the next cycle of technological innovation while the developing countries remain at the beginning stage of the technology regime.

5.5. Additional analysis

To further substantiate our main findings in the earlier sections, we undertake several additional tests across different dimensions, which we report in Appendix 2. First, the data visualization and non-parametric spline regression findings in Fig. 1 show a non-linear effect of CyberTech spending on the financial stability of banks. We confirm a similar non-linear impact in the parametric univariate test results presented in Panel A, validating the underlying premise of all test models applied in this study. Second, while the study finds that there is a threshold level for cyber spending, one may argue that financially stronger banks can afford more CyberTech costs than weaker ones. This means that the threshold might differ between the weaker and stronger banks. Therefore, we run a quantile regression at 25th, 50th, 75th, and 99th quantiles of our dataset and report the results in Panel B. As we expect, the findings show a consistently significant non-linear effect of cyber technology spending on bank stability at different quantiles, with a few exceptions. However, the variation in the threshold for different quantiles is evident for the coefficients of both *CyberTech-1* and *CyberTech-1 squared*. Importantly, the coefficients are higher for the banks at the upper quintiles than those at the lower quintiles.

Our results suggest that banks are more unstable due to overspending on cyber technology, which implies that banks' earnings performance may suffer as they often need to spend more on technology without a due diligence analysis of the cost and benefits. Therefore, Panel C shows that a marginal increase in CyberTech spending by banks has a significantly negative effect on their return on assets and return

Table 7
Bank stability and CyberTech spending across different levels of CyberTech advancement in the country.

Variables		Initiating level		Maturing level		Leading level	
		Model 1 Linear	Model 2 Non-linear	Model 3 Linear	Model 4 Non-linear	Model 5 Linear	Model 6 Non-linear
Focused variables	*CyberTech-1*	0.977*	0.254	0.647***	1.697**	−0.843**	−0.112
		(1.903)	(0.380)	(3.707)	(2.532)	(−2.446)	(−0.756)
	CyberTech-1 square		0.120		−0.151*		−0.169***
			(1.041)		(−2.007)		(−5.395)
Bank-level variables	*Total asset*	0.883	0.805	−0.420	−0.284	1.361***	1.807***
		(1.827)	(1.575)	(−1.305)	(−0.834)	(3.792)	(5.072)
	Asset turnover	32.587	25.390	−39.219	−39.590	20.590	42.582
		(0.330)	(0.246)	(−1.395)	(−1.430)	(0.551)	(1.104)
	Cost to income	−0.163*	−0.164*	−0.063	−0.071	−0.090*	−0.085*
		(−2.251)	(−2.092)	(−1.130)	(−1.220)	(−2.009)	(−1.958)
	Interest margin	−0.035	0.044	0.557*	0.575*	−0.286	−0.450
		(−0.035)	(0.040)	(1.937)	(1.997)	(−0.808)	(−1.340)
	Tier 1 capital	−0.016	−0.013	0.612***	0.598***	0.210	0.217
		(−0.113)	(−0.087)	(5.479)	(5.466)	(1.506)	(1.682)
	Equity to asset	37.575**	38.215**	5.313	3.311	−3.683	−3.575
		(2.997)	(2.950)	(0.517)	(0.343)	(−0.209)	(−0.214)
	Non-performing loan	−0.432***	−0.435***	−0.528***	−0.54***	−1.073***	−1.047***
		(−3.849)	(−3.825)	(−10.923)	(−12.69)	(−5.610)	(−5.495)
Country-level variables	*Cybersecurity Commit*	−10.00***	−9.902***	−16.675*	−13.733	45.142***	44.286***
		(−3.537)	(−3.742)	(−2.144)	(−1.833)	(4.533)	(4.338)
	Corruption	0.152***	0.140**	−0.030	−0.037	0.058	0.049
		(3.494)	(3.204)	(−1.259)	(−1.447)	(0.922)	(0.798)
	Financial freedom	−0.149***	−0.140***	−0.024	−0.029	−0.046	−0.061**
		(−3.754)	(−3.732)	(−0.602)	(−0.789)	(−1.604)	(−2.523)
	Gross domestic product	−6.384***	−5.982***	−5.731***	−5.351**	−6.648**	−4.923*
		(−5.323)	(−5.515)	(−3.462)	(−3.151)	(−2.609)	(−2.056)
	Inflation	−0.349**	−0.344**	−0.348**	−0.348**	−0.132	−0.128
		(−2.353)	(−2.335)	(−2.298)	(−2.303)	(−1.224)	(−1.165)
Fixed effects	*Country and Year*	0.000	0.000	−0.000	−0.000	−0.000***	−0.000***
		(1.612)	(1.585)	(−1.474)	(−1.292)	(−3.773)	(−4.808)
	Constant	23.703**	23.412**	43.157***	37.93***	−7.520	−17.199
		(2.538)	(2.528)	(4.452)	(3.780)	(−0.541)	(−1.253)
	Observations	368	368	372	372	616	616
	F-value	11.460	10.790	7.970	7.890	13.640	14.810
	R-square	0.283	0.285	0.305	0.310	0.189	0.201

We estimate $Bank\ stability_{it} = \alpha + \beta CyberTech1_{it} + \Upsilon Controls_{it} + \varepsilon_{it}$. We sort the sample banks into three classes based on the level of CyberTech advancement in the country as determined by International Telecommunication Union (ITU). The initiating-level countries are those with a score below the 33th percentile, the maturing level countries are those with a score between the 33th and 67th percentiles, and the leading countries are those with a score above the 67th percentile. *CyberTech-1* is the explanatory variable that is the natural log of total cyber tech spending as the absolute value, and the *Z-score* is the proxy for bank stability. Values in parenthesis are robust *t-stats* adjusted for heteroscedasticity in the data. The asterisks ***, **, and * denote significance at less than 1%, 5%, and 10% levels.

on equity. We reexamine CyberTech spending by testing a growth model, which tests the impact of yearly variation in gross cyber spending on bank stability. As the effects of technology investment persist after the current period, we examine the lag effect in another model. The results in Panel D overall confirm that banks become more unstable when they significantly increase current spending as compared to the previous year. The results also show that technology spending has a persistent effect beyond the current year. These new findings provide additional support to our key argument that overspending on CyberTech does matter for bank stability.

Finally, Panel E presents the results for before and after Basel III and across high and low growth economies. It shows that overspending on CyberTech has a significantly adverse effect on banking stability after the Basel III regulation. This could be because banks with more liquidity and regulatory capital requirements need to increase business income by expanding their financial services in reliance on more advanced technology. Finally, we test our models for high and low growth economics separately. The findings in Panel E show that the adverse effect of excess CyberTech spending on bank stability is insignificantly noticeable in high growth economies. It indicates that technology plays a critical role in increasing marginal productivity when the economy is at the high growth stage and the diminishing return stage is yet to come.

6. Conclusion

The fast development of CyberTech has changed the paradigm of the global banking system over the last few years. The speed of operations and the quality of banking services have improved significantly in recent years for a wider application of CyberTech, but banks are exposed to more operational risks than ever before due to cybersecurity hazards and unexpected system breakdowns. Indeed, CyberTech creates enormous opportunities for FinTech firms to enter the shadow finance market, which creates a further challenge for banking operations. This study investigates whether bank stability is affected by CyberTech spending. To answer this question, we focus on the law of diminishing marginal returns because an optimal technology investment with a positive net present value is a challenging task for the banks since the

Table 8
Bank stability and CyberTech spending in pre-FinTech and FinTech era.

Variables		Pre-FinTech era		FinTech era	
		Linear	Non-linear	Linear	Non-linear
Focused variables	*CyberTech-1*	0.054	0.306	0.086	0.782***
		(0.155)	(1.280)	(0.788)	(8.362)
	CyberTech-1 square		−0.040		−0.119***
			(−2.601)		(−6.462)
Bank-specific variables	*Total asset*	−0.235	−0.199	0.638**	0.766**
		(−1.484)	(−1.281)	(3.097)	(3.430)
	Asset turnover	47.354	47.490	−20.987	−17.086
		(0.888)	(0.870)	(−0.933)	(−0.759)
	Cost to income	0.019	0.016	−0.151**	−0.150**
		(0.762)	(0.680)	(−2.907)	(−2.966)
	Interest margin	−0.403	−0.402	0.538	0.506
		(−0.819)	(−0.789)	(1.892)	(1.801)
	Tier 1 capital	−0.247**	−0.244***	0.077	0.074
		(−44.802)	(−220.143)	(0.661)	(0.630)
	Equity to asset	13.867**	13.832**	31.025**	29.795**
		(50.709)	(44.241)	(3.179)	(3.023)
	Non-performing loan	−0.658	−0.651	−0.529***	−0.530***
		(−3.324)	(−3.254)	(−9.155)	(−9.148)
Country-specific variables	*Cybersecurity*	−2.797	−2.881	0.997	1.134
		(−1.153)	(−1.193)	(0.333)	(0.374)
	Corruption	0.027	0.029	0.075*	0.082*
		(0.418)	(0.467)	(1.934)	(2.156)
	Financial freedom	−0.081	−0.082	−0.075	−0.080*
		(−1.370)	(−1.386)	(−1.680)	(−1.933)
	Gross domestic product	−3.031*	−3.013*	−5.299***	−5.276***
		(−11.319)	(−7.991)	(−5.453)	(−5.171)
	Inflation	−0.146	−0.144	−0.365**	−0.367**
		(−3.249)	(−2.930)	(−3.353)	(−3.398)
Fixed effects	*Country and Year*	0.000	0.000	−0.000***	−0.000***
		(0.723)	(0.727)	(−3.033)	(−4.047)
	Constant	28.002***	27.197***	23.689**	21.859**
		(66.366)	(127.039)	(2.942)	(2.650)
	Observations	200	200	1156	1156
	F-value	4.530**	4.320**	19.040***	19.350***
	R-square	0.173	0.172	0.199	0.203

We estimate $Bank\ stability_{it} = \alpha + \beta CyberTech1_{it} + \Upsilon Controls_{it} + \varepsilon_{it}$. We classify the sample into two sub-sets: the pre-FinTech period (2008–9) and the FinTech period (2010–2017). *CyberTech-1* is the explanatory variable that is the natural log of total cyber tech spending as the absolute value, and the *Z-score* is the proxy for bank stability. Values in parenthesis are robust *t-stats* adjusted for heteroscedasticity in the data. The asterisks ***, **, and * denote significance at less than 1%, 5%, and 10% levels.

cost of CyberTech and cybersecurity hazards may drain the marginal returns of CyberTech spending.

The empirical study shows that a marginal increase in CyberTech spending above a threshold level adversely affects the stability of a bank. The results are robust after implementing different estimation methods and alternative proxies of bank stability. While the technology risk to the stability of banks is pervasive across small and large banks, the effect is more noticeable in the technologically advanced countries and during the FinTech era. Further, the results show two technological regimes for bank stability across both developed and developing countries. In one regime, banks are likely to overcome diminishing returns with more aggressive spending on technology to improve their stability. In the other regime, aggressive CyberTech spending might lead to diminishing returns, which adversely affects the stability of banks.

This study has both theoretical and practical implications for cybersecurity and sustainable CyberTech spending for banks. The results shed a different light on the argument that technology can defy the law of diminishing returns. Thus, the study opens up a new avenue for theoretical researchers as the positive effects of CyberTech spending on the stability of banks diminish after a certain threshold. This finding may spur banking researchers to think about the optimal threshold for technology spending in the future. Policymakers, regulators, and bank managers can gain insights from this empirical study. For example, when a country advances toward the developed stage, its policymakers and regulators need to focus more on governance mechanisms for cybersecurity rather than enforcing technology solutions. As it is now evident that overspending on CyberTech adversely affects banks' stability, managers should as much as possible conduct a careful cost-benefit analysis before committing to increasing CyberTech budgets.

Due to the unavailability of data, we couldn't conduct a more in-depth analysis of the country-specific differences in CyberTech spending and bank stability. Thus, future research can investigate whether the same technological regime persists in both developed and developing countries due to the cyclicity of technological regimes, which we suggest as a possible reason because earlier literature shows

Table 9
Robustness tests with alternative measures of dependent and independent variables.

Focused Variables	Panel A: Tests with Z-score (before taxes) as the dependent variable $Bank\ stability_{it} = \alpha_i + \beta_1 CyberTech_{it} + \Sigma_{i=1}{}^{n} \Upsilon Control_{it} + \varepsilon_{it}$ The appendix provides details of the test variables. In the nonlinear estimations, we apply *CyberTech squared* as an additional variable.				Panel B: Tests with a different measure of focused explanatory variable $Bank\ stability_{it} = \alpha + \beta_1 CyberTech_{High} + \beta_2 CyberTech_{Low} + \Sigma_{i=1}{}^{n} \Upsilon Control_{it} + \ + \varepsilon_{it}$, See notes at the bottom of this table:	
	Linear	Non-linear	Linear	Non-linear	Z-score	Before-tax Z-score
CyberTech-1	−0.059	0.456***				
	(−0.822)	(2.615)				
CyberTech-1 squared		−0.087***				
		(−3.561)				
CyberTech-2			0.036**	0.129**		
			(2.122)	(2.299)		
CuberTech-2 squared				−0.004*		
				(−1.784)		
$CyberTech_{High}$					−1.396***	−1.480***
					(−3.360)	(−3.870)
$CyberTech_{Low}$					0.296	0.708
					(0.46)	(1.14)
Controls	Yes	Yes	Yes	Yes	Yes	Yes
Country and year effect	−0.000***	−0.000***	−0.000***	−0.000***	−0.000	−0.000*
	(−3.281)	(−4.043)	(−2.954)	(−3.360)	(−1.46)	(−1.69)
Constant	10.601**	9.060*	10.516**	20.204***	17.510***	8.270***
	(2.063)	(1.668)	(2.002)	(2.735)	(5.530)	(2.630)
Observations	1309	1309	1356	1356	1827	1738
F-value	33.180***	32.060***	32.450***	26.240***	16.53***	17.410***
R-squared	0.194	0.198	0.200	0.187	0.178	0.200

$CyberTech_{High}$ = 1 if the natural log of total CyberTech spending is greater than the 75th percentile, otherwise 0. $CyberTech_{Low}$ = 1 if the natural log of total CyberTech spending is less than the 25th percentile, otherwise 0. The banks with CyberTech spending between the 25th and 75th percentiles are considered the base group. Other variables are the same as those in the earlier tables. For both panels, we rechecked them with fixed effect models, but the significance levels do not change. The values in parenthesis are robust *t-stats* with standard errors clustered by country and year. We cannot report control variable results here due to space limitation. The asterisks ***, **, and * denote significance at less than 1, 5, and 10% levels in both panels.

Table 10
Findings by region and country.

Country and region	Linear Model	Non-linear Model		Country and region	Linear Model	Non-linear Model		Country and region	Linear Model	Non-linear Model	
	CyberTech	*CyberTech*	*CyberTech Squared*		*CyberTech*	*CyberTech*	*CyberTech Squared*		*CyberTech*	*CyberTech*	*CyberTech Squared*
USA	0.052	0.508*	−0.018**	Bangladesh	−0.032	−0.597**	0.0183**	Egypt	−0.040	0.246	−0.013
Canada	−0.004	−2.398	0.144	China	0.144	0.891	−0.036	Israel	1.164**	0.988	0.005
North America	**−0.163****	**0.215**	**−0.016****	India	−0.792	3.308	−0.562	Jordan	0.374	1.446*	−0.047
				Pakistan	0.630**	2.937**	−0.387**	Oman	−0.368***	−1.351***	0.028**
				Thailand	−0.339	−2.329***	0.198**	Qatar	−0.178	1.769	−0.097
UK	−0.081**	0.082	−0.005	Indonesia	−0.324**	−0.915	0.021	Saudi	0.240	−0.401	0.0456
Germany	−1.103***	−4.947***	0.236***	Malaysia	−0.030	0.127	−0.004	Tunisia	0.073	0.735*	−0.026*
France	0.129	0.005	0.006	Singapore	−1.588***	−7.327*	0.246	Turkey	−0.276***	−1.127**	0.053**
Belgium	−0.494***	−0.902	0.020	Japan	−0.095	0.529	−0.017	UAE	1.289	6.150*	−1.279*
Italy	−1.229***	−2.448***	0.229	Korea	−1.420**	1.258	−0.256*	**MENA**	**0.133**	**0.768****	**−0.023****
Greece	−0.005	0.094	−0.002	**Asia**	**−0.085**	**0.080**	**−0.008**				
Spain	0.529**	1.915	−0.085					Russia	−0.013	0.056	−0.002
Poland	0.054	1.205***	−0.030***					South Africa	−0.552	2.403	−0.473*
Switzerland	−0.040	1.606*	−0.093	Australia	0.126*	0.192	−0.0024	**Others**	**1.787**	**1.799****	**−1.999****
Netherland	0.139	−0.962	0.092*	New Zealand	−0.295	−17.650	4.068				
Finland	−0.111	−1.883***	0.087***	**Asia Pacific**	**−0.010**	**0.672**	**−0.025**	The base model is: $Bank\ stability_{it} = \alpha + \beta CyberTech_{it} + \Upsilon Controls_{it} + \varepsilon_{it}$. We test both *CyberTech-1* and *CyberTech-2* as different measures of CyberTech spending. We add *CyberTech-1 squared* and *CyberTech-2 squared* as the additional variables. As results are consistent for both estimations of CyberTech spending, we report here only those based on *CyberTech-2* due to space limitation. Asterisks ***, **, and * denote significance at the less than one, five, and 10% levels.			
Denmark	−0.191**	−0.722***	0.018***								
Norway	−0.047	0.291***	−0.012***	Argentina	0.029	−3.387**	0.6227**				
Sweden	−0.521***	−1.935*	0.140	Brazil	−0.327***	−0.465**	0.005				
Europe	**0.262**	**0.519****	**−0.043***	Chile	0.056	0.166	−0.004				
				Mexico	0.100	8.628***	−1.269***				
				Latin America	**0.016**	**0.436**	**−0.014**				

technological innovation follows a hype cycle. Also, further research can investigate whether country-specific regulatory differences matter for CyberTech spending and bank stability.

Author statement

Md Hamid Uddin: Idea Conceptualization, Literature Review, Theory and Argument Building, Hypothesis, Project Preparation and Funding Application, Methodology Selection, Variable Selection, Data Analysis and Software, Paper Drafting, Knowledge Contribution and Presentation.

Sabur Mollah: Ideas Conceptualization, Hypothesis Development Project Preparation and Funding Application Methodology Selection, Theory and Argument Building, Analysis and Knowledge Contribution.

Md Hakim Ali: Literature Review and Hypothesis and Concept Building, Data Extraction from Annual Reports and Bloomberg Database, Data Curating and Validation, Variable Construction, Running Software, Data Analysis, Drafting and Editing.

Acknowledgements

This research is the output of Taylor's University's flagship research project # TUFR/2017/004/05: Cyber Risk and Bank Stability. Md Hamid Uddin is the leader, Sabur Mollah is the external collaborator, and Md Hakim Ali is working as a research scholar for this project. This paper was presented at Vietnam Symposium in Banking and Finance (VSBF2019) held at the Banking Academy of Vietnam and Malaysian Finance Association annual meeting 2019. We acknowledge data extraction assistance from M. Sawkat Hossain and Syed Rahman. We are grateful to two anonymous reviewers for insightful comments, which have helped to improve the overall exposition and significance of the paper.

Appendix 1: Variables description

Dependent variables			
Variables	Descriptions	Source	References
Z-score	*Z-score* = (ROA + capital-asset ratio)/σROA, which measures the financial stability of banks.	Authors' calculation	Demirgüç-Kunt et al. (2008); Laeven and Levine (2009); Čihák and Hesse (2010); Beck et al. (2013); Chiaramonte et al. (2016);
Z-score (before taxes)	*Z-score (before taxes)* is estimated by using the ROA based on operating income before taxes. Prior researchers measured risk proxies (σROA) based on the operating income instead of the net income after taxes.	Authors' calculation	Boubakri et al. (2013); Faccio et al. (2011)
Focused independent variables			
CyberTech-1	*CyberTech-1* is the natural log of CyberTech spending in the bank. The total cost covers the data processing, third-party security providing services, computer and software development, and IT personnel training in the income statement and current year amortization of software and computer expenses in separate notes to the financial statement.	Manual collection form annual report	Our study
CyberTech-1 squared	*CyberTech-1 squared* refers to the squared value of *CyberTech-1*	Authors' calculation	Our study
CyberTech-2	*CyberTech-2* is the percentage of total non-interest operating expenses.	Manual collection form annual report	Our study
CyberTech-2 squared	*CyberTech-2 squared* refers to the squared value of *CyberTech-2*	Authors' calculation	Our study
$CyberTech_{High}$	$CyberTech_{High}$ = 1 if the natural log of total CyberTech spending is greater than the 75th percentile, otherwise 0.	Authors' calculation	Our study
$CyberTech_{Low}$	$CyberTech_{Low}$ = 1 if the natural log of total CyberTech spending is less than the 25th percentile, otherwise 0	Authors' calculation	Our study
Bank-level control variables			
Total assets	*Total assets* is the average of the beginning balance and ending balance of the balance sheet	Bloomberg	Haan and Poghosyan (2012)
Asset turnover	*Asset turnover* is the total revenue divided by total assets	Authors' calculation	Wagner (2007)
Cost to income	The *cost-to-income* is the ratio of operating expense to operating income.	Bloomberg	Schaeck and Chiak (2014)
Interest margin	*Net interest margin* in percentage is a performance metric that examines how successful a firm's investment decisions are compared to its debt. A negative value denotes that the firm did not make an optimal decision, because interest expenses were greater than the amount of returns generated by investments.	Bloomberg	Chaudron (2018)
Tier-1 capital	*Tier-1* is the ratio of a bank's core capital to the risk-weighted asset in %. In Europe it is referred to as the BIS ratio, the European Solvency ratio, or the Cooke ratio as the Cooke committee established it	Bloomberg	Anginer, Demirgüc-Kunt, and Mare (2018)
Equity-to-asset	*Equity-to-asset* is the total equity of the bank divided by its total assets. Average Total Common Equity is the average of the beginning balance and ending balance and Total asset is the average of the beginning balance and ending balance in the balance sheet	Authors' calculation	Anginer, Demirgüc-Kunt, and Mare (2018)
Non-performing loan	The *non-performing loan* is the non-performing loan as the percentage of the total loan of a bank. Total loan is the sum of short-and long-term loans	Authors' calculation	Nikolopoulos and Tsalas (2017). Review paper.
Country-level control variables			
Cybersecurity	*Cybersecurity commitment* measures the commitment score of the country to cybersecurity protection.	International Telecommunication Union	Our study
Corruption	*The Corruption* Perceptions Index measures the perceived levels of public sector corruption in countries worldwide, the score ranging from 0 (highly corrupt) to 100 (very clean).	Transparency International	Infante and Piazza (2014)

Financial freedom	This is the financial freedom index of a country provided by Heritage.org. We use this variable because studies find that higher financial freedom in the economy promotes banking efficiency.	The Heritage Foundation	Chortareas et al. (2013)
Gross domestic product	*Gross domestic product* is the natural log of the real gross domestic product (GDP) per capita of the country denominated in USD. Evidence shows that GDP influences banking performance through monetary policy shocks	World Bank	Jiménez et al., 2012)
Inflation	*Inflation* is the consumer price index of a country.	World Bank	Boyd et al. (2001)
Fixed effect control			
*Country * year*	*Country*time* is an interaction between country and year to capture the heterogeneity of country and year fixed effects.	Authors' calculation	Beck et al. (2013)

Appendix 2: Additional tests

Panel A: Univariate effect of CyberTech spending on bank stability

Focused variables	***Z score 1***	***Z score 2***
CyberTech-1	0.522***	0.401***
	(4.000)	(3.780)
CyberTech − 1 squared	−0.0447***	−0.021*
	(−5.520)	(−1.880)
F Value	16.170	7.310
R squared	0.010	0.010

We estimate model:$Z\ score_{it} = \alpha + \Upsilon CyberTech1_{it} + \varepsilon_{it}$. All variables are defined in Appendix 1.

We also test the model by using *CyberTech-2*, and results are consistent. The values within parenthesis are robust *t-stats* adjusted for heteroscedasticity. Asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels.

Panel B: Quantile regression findings

Quantiles	Focused variables	*Z-Score*
25th percentile	*CyberTech-1*	0.178
	CyberTech-1 squared	−0.056**
50th percentile	*Cybertech-1*	0.146
	CyberTech-1 squared	−0.066**
75th percentile	*CyberTech-1*	0.318
	CyberTech-1 squared	−0.107*
99th percentile	*CyberTech-1*	3.170***
	CyberTech-1 squared	−0.269**

The generic model is: $Zscore_{it} = \alpha + \beta CyberTech1_{it} + \Upsilon Controls_{it} + \delta Country_j * Year_t + \varepsilon_{it}$.We apply quantile regression tests at 25Th, 50th, 75th, and 99th percentiles of data set based on the *Z-Score*. The quantiles regressions are non-parametric tests that do not rely on the data normality assumption. The explanatory variables are same as those in the earlier tables. We also test the quantile regression model for *CyberTech-2* and Z-score 2; results are consistent to those we report in this table. The values within parenthesis are robust *t-stats* adjusted for heteroscedasticity. Asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels. We did not report control variables results to save space.

Panel C: Effect of CyberTech spending on the financial performance of banks

Variables		OLS estimates				GMM estimates			
		ROA	ROA	ROE	ROE	ROA	ROA	ROE	ROE
Lag dependent variable						0.13	0.16	0.08	0.12
						(0.82)	(1.05)	(0.39)	(0.64)
Focused variables	*CyberTech-1*	−0.07***		−0.73***		−0.18**		−2.30*	
		(−5.46)		(−4.38)		(−2.25)		(−1.76)	
	CyberTech-2		−0.01*		−0.02		−0.02*		−0.58*
			(−1.87)		(−0.61)		(−1.77)		(−1.81)
Constant		0.08	0.66***	23.01***	28.19***	−1.50	0.01	−20.69	−6.23
		(0.33)	(2.66)	(7.11)	(9.13)	(−1.64)	(0.01)	(−1.01)	(−0.38)
Observations		1360	1360	1346	1346	1259	1259	1240	1240
F-Value/ Wald χ2 (GMM)		138.45	133.83	61.92	61.03	350.82	360.95	184.81	159.90
R-squared		0.62	0.62	0.47	0.46				

We estimate $Performance_{it} = \alpha_i + \beta_i CyberTech_{it} + \Sigma_{i=1}{}^{n} \Upsilon Controls_{it} + \varepsilon_{it}$ using OLS and dynamic system GMM. We use return on asset (ROA) and return on equity (ROE) as two proxies for the *performance* variable. *Controls* are as defined in Appendix-1. The values within parenthesis are robust *t-stats* adjusted for heteroscedasticity. Asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels. We did not report control variables results to save space.

Panel D: Annual cyber spending growth and lag effects on bank stability

Variables	Model 1 Effect of cyber spending growth	Model 2 Lag effect of cyber spending
CyberTech - growth	1.347* (1.662)	
CyberTech – growth squared	−0.253*** (−3.209)	

CyberTech – Lag (−1)		0.537**
		(2.704)
CyberTech – Lag (−1) squared		−0.075**
		(−2.700)
Constant	20.923***	23.753***
	(5.056)	(3.794)
Observations	1229	1241
F-Value	15.27	
R-squared	0.188	0.190

Model 1: $Zscore_{it} = \alpha_i + \beta_i CyberTech - Growth_{it} + \beta_i CyberTech - Growth\ squared_{it} + \Sigma_{i=1}{}^{n}\Upsilon Controls_{it} + \varepsilon_{it}$

Model 2: $Zscore_{it} = \alpha_i + \beta_i CyberTech_{it-1} + \beta_i CyberTech - Growth\ squared_{it-1} + \Sigma_{i=1}{}^{n}\Upsilon Controls_{it} + \varepsilon_{it}$

For Model 1, $CyberTech - Growth_{it} = \frac{CyberTech_t - CyberTech_{t-1}}{CyberTech_{t-1}}$.

In the both models, we apply same controls that are used in main tests. The values within parenthesis are robust *t-stats* adjusted for heteroscedasticity. Asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels. We did not report control variables results to save space.

Panel E: Variations of results after Basel III and across high and low growth economies

Focused variable	Basel regulation		Economic growth	
	Basel II 2008–14	Basel III 2015–17	High growth	Low growth
CyberTech	0.386	0.768***	0.581	0.706*
	(0.757)	(2.864)	(1.336)	(1.788)
CyberTech squared	−0.050	−0.137***	−0.071	−0.093**
	(−0.677)	(−3.333)	(−0.881)	(−2.424)
Constant	33.708***	3.380	24.628***	25.085***
	(6.505)	(0.531)	3.722	3.241
Observations	862	494	710	646
F-Value	16.63	16.94	7.26	9.92
R-squared	0.222	0.207	0.1747	0.197

We test the base model: $Zscore_{it} = \alpha_i + \beta_i CyberTech1_{it} + \beta_i CyberTech1\ square_{it} + \Sigma_{i=1}{}^{n}\Upsilon Controls_{it} + \varepsilon_{it}$ for split-sample set for before and after Basel III as well as high and low growth countries. Also, we split the sample countries into high and low growth countries based on the median GDP growth rate of our sample. The countries above the median are classified as 'High growth,' and those below the median are 'Low growth.' All variables are as defined in Appendix 1. The values within parenthesis are robust *t-stats* adjusted for heteroscedasticity. Asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels. We did not report control variables results to save space.

References

Abou-El-Sood, H. (2016). Are regulatory capital adequacy ratios good indicators of bank failure? Evidence from US banks. *International Review of Financial Analysis, 48*, 292–303.

Acharya, V. V., & Mora, N. (2015). A crisis of banks as liquidity providers. *The Journal of Finance, 70*(1), 1–43.

Acharya, V. V., Shin, H. S., & Yorulmazer, T. (2011). Crisis resolution and Bank liquidity. *The Review of Financial Studies, 24*(6), 2166–2205.

Acharya, V. V., & Viswanatha, S. (2011). Leverage, moral Hazard, and liquidity. *The Journal of Finance, 66*(1), 99–138.

Agyekum, F., Locke, S., & Hewa-Wellalage, N. (2016). *Financial inclusion and digital financial services: Empirical evidence from Ghana. MPRA paper 82885*Germany: University Library of Munich.

Ahamed, M. M., & Mallick, S. (2017). Does regulatory forbearance matter for bank stability? Evidence from creditors' perspective. *Journal of Financial Stability, 28*, 163–180.

Albaity, M., Mallek, R. S., & Noman, A. H. (2019). Competition and bank stability in the MENA region: The moderating effect of Islamic versus conventional banks. *Emerging Markets Review, 38*, 310–325.

Allen, F., Carletti, E., & Marquez, R. (2011). Credit market competition and capital regulation. *The Review of Financial Studies, 24*(4), 983–1018.

Allen, F., & Gale, D. (2004). Competition and financial stability. *Journal of Money, Credit and Banking, 36*(3), 453–480.

Anginer, D., Demirguc-Kunt, A., Huizinga, H., & Ma, K. (2018a). Corporate governance of banks and financial stability. *Journal of Financial Economics, 130*(2), 327–346.

Anginer, D., Demirgüc-Kunt, A., & Mare, D. S. (2018b). Bank capital, institutional environment and systemic stability. *Journal of Financial Stability, 37*, 97–106.

Azmi, W., Ali, M., Arshad, S., & Rizvi, S. A. (2019). Intricacies of competition, stability, and diversification: Evidence from dual banking economies. *Economic Modelling, 83*, 111–126 (In press).

Bandt, O. D. (2018). Optimal capital, regulatory requirements and bank performance in times of crisis: Evidence from France. *Journal of Financial Stability, 39*, 175–186.

Banerjee, R. N., & Mio, H. (2018). The impact of liquidity regulation on banks. *Journal of Financial Intermediation, 35*, 30–44.

Beccalli, E. (2007). Does IT investment improve bank performance? *Evidence from Europe. 31*(7), 2205–2230.

Beck, T., Demirguc-Kunt, A., & Merrouche, O. (2013). Islamic vs. conventional banking model: Business model, efficicency and stability. *Journal of Banking & Finance, 37*(2), 433–447.

Berger, A. N., & Bouwman, C. H. (2013). How does capital affect bank performance during financial crises? *Journal of Financial Economics, 109*(1), 146–176.

Berger, A. N., & Bouwman, C. H. (2017). Bank liquidity creation, monetary policy, and financial crises. *Journal of Financial Stability, 30*, 139–155.

Bermpei, T., Kalyvas, A., & Nguyen, T. C. (2018). Does institutional quality condition the effect of bank regulations and supervision on bank stability? Evidence from emerging and developing economies. *International Review of Financial Analysis, 59*, 255–275.

Boubakri, N., Cosset, J.-C., & Saffar, W. (2013). The role of state and foreign owners in corporate risk-taking: Evidence from privatization. *Journal of Financial Economics, 108*, 641–658.

Boyd, J. H., Levine, R., & Smith, B. D. (2001). The impact of inflation on financial sector performance. *Journal of Monetary Economics, 47*(2), 221–248.

Boyson, N., Helwege, J., & Jindra, J. (2014). Crises, liquidity shocks, and fire sales at commercial banks. *Financial Management, 43*(4), 857–884.

Buchak, G., Matvos, G., Piskorski, T., & Seru, A. (2018). Fintech, regulatory arbitrage, and the rise of shadow banks. *Journal of Financial Economics, 130*(3), 453–483.

Cabrera, M., & G. P., & Nieto, M. J. (2018). The G-20's regulatory agenda and banks' risk. *Journal of Financial Stability, 39*, 66–78.

Chaudron, R. F. (2018). Bank's interest rate risk and profitability in a prolonged environment of low interest rates. *Journal of Banking & Finance, 89*, 94–104.

Chemmanur, T. J. (2002). New technologies, financial innovation, and intermediation. *Journal of Financial Intermediation, 11*(1), 2–8.

Chiaramonte, L., Liu, F. H., Poli, F., & Zhou, M. (2016). How accurately can Z-score predict Bank failure? *Financial Markets. Institutions & Instruments, 25*(5), 333–360.

Chortareas, G. E., Girardone, C., & Ventouri, A. (2013). Financial freedom and bank efficiency: Evidence from the European Union. *Journal of Banking & Finance, 37*(4), 1223–1231.

Čihák, M., & Hesse, H. (2010). Islamic banks and financial stability: An empirical analysis. *Journal of Financial Services Research, 38*(2–3), 95–113.

Clark, E., Radic, N., & Sharipova, A. (2018). Bank competition and stability in the CIS markets. *Journal of International Financial Markets, Institutions & Money, 54*, 190–203.

CNBC (2016, May 15). *Vietnam's Tien Phong Bank says it was second bank hit by SWIFT cyberattack.* CNBC: Tech - Cybersecurity. Retrieved from https://www.cnbc.com/2016/05/15/vietnams-tien-phong-bank-says-it-was-second-bank-hit-by-swift-cyber-attack.html.

Basel Committee (2010). *Sound practices for the management and supervision of operational risk.* Basel, Switzerland: Bank for International Settlements. Retrieved from https://www.bis.org/publ/bcbs183.pdf.

Basel Committee (2011). *Principles for the sound.* Basel, Switzerland: Bank for International Settlements. Retrieved from https://www.bis.org/publ/bcbs195.pdf.

Basel Committee (2018a). *Cyber-resilience: Range of practices.* Basel, Switzerland: Bank for Internattional Settlements. Retrieved from https://www.bis.org/bcbs/publ/d454.pdf.

Basel Committee (2018b). *Sound practices: Fintech implications for banks and supervisors.* Basel, Switzerland: Bank for International Settlements. Retrieved from https://www.bis.org/bcbs/publ/d431.pdf.

Crisanto, J. C., & Prenio, J. (2017). *FSI insights on policy implementation No 2: Regulatory approaches to enhance banks' cyber-security frameworks.* Basel, Switzerland: Financial Stability Institute - Bank for International Settlements.

Dedehayir, O., & Steinert, M. (2016). The hype cycle model: A review and future directions. *Technological Forecasting and Social Change, 108*, 28–41.

Deli, Y. D., & Hasan, I. (2017). Real effects of bank capital regulations: Global evidence. *Journal of Banking and Finance, 82*, 217–228.

Dell'Ariccia, G., Laeven, L., & Marquez, R. (2014). Real interest rates, leverage, and bank risk-taking. *Journal of Economic Theory, 149*, 65–99.

Demirgüç-Kunt, A., Detragiache, E., & Tressel, T. (2008). Banking on the principles: Compliance with Basel Core principles and bank soundness. *Journal of Financial Intermediation, 17*(4), 511–542.

Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. R. (2018). *The Global Findex Database 2017 : Measuring Financial Inclusion and the Fintech Revolution (English).* Washington, D.C.: World Bank Group.

Drasch, B. J., Schweizer, A., & Urbach, N. (2018). Integrating the "Troublemakers": A taxonomy for cooperation between banks and fintechs. *Journal of Economics and Business, 100*, 26–42.

Dufwenberg, M., & Dufwenberg, M. A. (2018). Lies in disguise – A theoretical analysis of cheating. *Journal of Economic Theory, 175*, 248–264.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(3), 1109–1119.

Esho, N., & Sharpe, I. G. (1995). Long-run estimates of technological change and scale economies in a dynamic framework: Australian permanent building societies, 1974–1990. *Journal of Banking & Finance, 19*(7), 1135–1157.

Faccio, M., Marchica, M. T., & Mura, R. (2011). Large shareholder diversification and corporate risk-taking. *The Review of Financial Studies, 24*(11), 3601–3641.

Finch, G. (2016, May 20). *Ecuador Bank Says It Lost $12 Million in Swift 2015 Cyber Hack.* Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2016-05-20/ecuador-bank-says-it-lost-12-million-in-swift-2015-cyber-hack.

Freeman, R. E. (1984). *Strategic management: A stakeholder perspective.* New Jersey: Prentice-Hall.

Frischtak, C. (1992). Banking automation and productivity change: The Brazilian experience. *World Development. 20*(12), 1769–1784.

FSB (2017). *Financial stability implications from FinTech: Supervisory and regulatory issues that merit Authorities' attention.* Basel, Switzerland: Financial Stability Board. Retrieved from http://www.fsb.org/wp-content/uploads/R270617.pdf.

Fu, X. M., Lin, Y. R., & Molyneux, P. (2014). Bank competition and financial stability in Asia Pacific. *Journal of Banking & Finance, 38*, 64–77.

Goetz, M. R. (2018). Competition and bank stability. *Journal of Financial Intermediation, 35*(Part A), 57–69.

Gopalakrishnan, R., & Mogato, M. (2016, May 19). *Bangladesh Bank official's computer was hacked to carry out $81 million heist: Diplomat.* Reuters: Business News. Thomson Reuters. Retrieved from https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH.

Gordon, L. A., & Loeb, M. P. (2002). Return on information security investments, myths vs realities. *Strategic Finance, 84*(5), 26–31.

Greer, S., Lodge, G., Mazzini, J., & Yanagawa, E. (2019). *Global tech spending forecast: Banking edition, 2019.* (CELENT).

Gupta, S. D. (2018). Information technology and profitability: Evidence from Indian banking sector. *International Journal of Emerging Markets, 13*(5), 1070–1087.

Haan, J.d., & Poghosyan, T. (2012). Size and earnings volatility of US bank holding companies. *Journal of Banking and Finance, 36*(11), 3008–3016.

Hancock, D., & Humphrey, D. B. (1997). Payment transactions, instruments, and systems: A survey. *Journal of Banking & Finance, 21*, 1573–1624.

Hancock, D., Humphrey, D. B., & Wilcox, J. A. (1999). Cost reductions in electronic payments: The roles of consolidation, economies of scale, and technical change. *Journal of Banking & Finance, 23*, 391–421.

Härle, P., Havas, A., & Samandar, H. (2016, July). The future of bank risk management. *McKinsey working papers on risk*. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management.

He, Z., & Xiong, W. (2012). Dynamic Debt Runs. *The Review of Financial Studies, 25*(6), 1799–1843.

Holmstrom, B., & Tirole, J. (1997). Financial intermediation, loanable funds, and the real sector. *The Quarterly Journal of Economics, 112*(3), 663–691.

Hurd, T. R. (2016). *Contagion! Systemic Risk in Financial Networks.* Springer International Publishing.

Imbierowicz, B., & Rauch, C. (2014). The relationship between liquidity risk and credit risk in banks. *Journal of Banking & Finance, 40*, 242–256.

Infante, L., & Piazza, M. (2014). Political connections and preferential lending at local level: Some evidence from the Italian credit market. *Journal of Corporate Finance, 29*, 246–262.

Jiménez, G., Ongena, S., Peydró, J.-L., & Saurina, J. (2012). Credit supply and monetary policy: Identifying the Bank balance-Sheet Channel with loan applications. *American Economic Review, 102*(5), 2301–2326.

Johnson, K. N. (2015). Managing Cyber Risk. *Georgia Law Review, 50*(2), 548–592.

Kaspersky (2015, February 16). The greatest heist of the century: Hackers stole $1 bln. Kaspersky lab daily. Retrieved from https://www.kaspersky.com/blog/billion-dollar-apt-carbanak/7519/.

Kauffman, R. J., Liu, J., & Ma, D. (2015). Technology investment decision-making under uncertainty. *Information Technology and Management, 16*(2), 153–172.

Kim, H., Park, K., & Song, S. (2016). Banking market size structure and financial stability: Evidence from eight Asian countries. *Emerging Markets Finance and Trade, 52*(4), 975–990.

Koette, M., & Poghosyan, T. (2009). The identification of technology regimes in banking: Implications for the market power-fragility nexus. *Journal of Banking & Finance, 33*(8), 1413–1422.

Koetter, M., & Noth, F. (2013). IT use, productivity, and market power in banking. *Journal of Financial Stability, 9*(4), 695–704.

Laeven, L., & Levine, R. (2009). Bank governance, regulation and risk taking. *Journal of Financial Economics, 93*(2), 259–275.

Laeven, L., Ratnovski, L., & Tong, H. (2016). Bank size, capital, and systemic risk: Some international evidence. Journal of Banking & Finance, 69 (Supplement 1), S25–S34.

Lages, L. F. (2016). VCW-value creation wheel: Innovation, technology, business, and society. *Journal of Business Research, 69*, 4849–4855.

Lente, H.v., Spitters, C., & Peine, A. (2013). Comparing technological hype cycles: Towards a theory. *Technological Forecasting and Social Change, 80*(8), 1615–1628.

Mee, P., & Schuermann, T. (2018). *How a Cyber Attack Could Cause the Next Financial Crisis.* Harvard Business Review September 18.

Mehran, H., & Thakor, A. (2011). Bank capital and value in the cross-section. *The Review of Financial Studies, 24*(4), 1019–1067.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340–363.

Murgia, M., & Megaw, N. (2019). Cyber attacks on financial services sector rise fivefold in 2018. *Financial times.* , February 25. Retrieved from https://www.ft.com/content/6a2d9d76-3692-11e9-bd3a-8b2a211d90d5.

Ngonzi, T. T. (2016). *Theorizing ICT-based social innovation on development in the context of developing countries of Africa.* Captown: University of Cape Town.

Nikolopoulos, K. I., & Tsalas, A. I. (2017). Non-performing loans: A review of the literature and the international experience. In P. Monokroussos, & C. Gortsos (Eds.). *Non-Performing Loans and Resolving Private Sector Insolvency. Palgrave Macmillan Studies in Banking and Financial Institutions*. Palgrave Macmillan.

Pawlowska, M. (2016). Does the size and market structure of the banking sector have an effect on the financial stability of the European Union? *The Journal of Economic Asymmetries, 14*(Part A), 112–127.

Reuters, T. (2016, December 2). *Russian central bank, private banks lose $31 mln in cyber attacks.* Reuters: Technology News. Retrieved from https://www.reuters.com/article/us-russia-cenbank-cyberattack-idUSKBN13R1TO.

Roberts, J. (2004). *The modern firm: Organizational Design for Performance and Growth.* Oxford: Oxford University Press.

Roth, A. V., & Jackson-III, W. E. (1995). Strategic determinants of service quality and performance: Evidence from the banking industry. *Management Science, 41*(11), 1720–1733.

Schaeck, K., & Chiak, M. (2014). Competition, efficiency, and stability in banking. *Financial Management, 43*(1), 215–241.

Schmidt, R. H. (2004). Corporate governance in Germany: An economic perspective. In J. P. Krahnen, & R. H. Schmidt (Eds.). *The German financial system* (pp. 386–424). Oxford: Oxford University Press.

Shaddady, A., & Moore, T. (2019). Investigation of the effects of financial regulation and supervision on bank stability: The application of CAMELS-DEA to quantile regressions. *Journal of International Financial Markets, Institutions & Money, 58*, 96–116.

Shank, J. K. (1996). Analysing technology investments—From NPV to strategic cost management (SCM). *Management Accounting Research, 7*(2), 185–197.

Tang, M.-J., & Zannetos, Z. S. (1992). Competition under continuous technological change. *Managerial and Decision Economics, 13*, 135–148.

Tchamyou, V. S., Erreygers, G., & Cassimon, D. (2019). Inequality. *ICT and financial access in Africa. 139*, 169–184.

Treanor, J. (2016, November 8). Tesco Bank cyber-thieves stole £2.5m from 9,000 people. The Guardian. Retrieved from https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m.

Uddin, M. H., Ali, H., & M. H. (2018). Cybersecurity risk and banking stability - a thematic review. *Proceding (abstarct), 9th Annual Financial Market Liquidity Conference 15–16 November 2018 (p. 10)*. Budapest: Corvinus University.

Varotto, S., & Zhao, L. (2018). Systemic risk and bank size. *Journal of International Money and Finance, 82*, 45–70.

Vives, X. (2019). Competition and stability in modern banking: A post-crisis perspective. *International Journal of Industrial Organization, 64*, 55–69 (In press).

Wagner, W. (2007). The liquidity of bank assets and banking stability. *Journal of Banking & Finance, 31*(1), 121–139.