Singapore Journal of Legal Studies
[2020] 35–62

TECHRISK

ROSS P **BUCKLEY***, DOUGLAS W **ARNER****, DIRK A **ZETZSCHE***** and ERIKS K **SELGA******

Fintech is now defined by a long-term, global process of digitisation of finance, increasingly combined with datafication and new technologies including cloud computing, blockchain, Big Data and artificial intelligence. Cybersecurity and technological risks are thus evolving into major threats to financial stability and national security. This trend has been magnified by the COVID-19 crisis which has heightened dependence on digital technologies and seen substantial parts of the population working from home through systems of questionable security. Additionally, the entry of BigTech firms brings two new issues. The first arises with new forms of potentially systemically important infrastructure. The second arises because data—like finance—benefits from economies of scope and scale and from network effects and—even more than finance—tends towards monopolistic or oligopolistic outcomes. This leads to potential systematic risk from new forms of "Too Big to Fail" and "Too Connected to Fail" phenomena. We suggest some basic principles about how to address this entire range of risks.

I. INTRODUCTION

Over the past five decades, finance has undergone a process of digital transformation, encompassing digitisation and datafication. Today, finance is not only the most

* KPMG Law and King & Wood Mallesons Chair of Disruptive Innovation, Scientia Professor, and Member, Centre for Law, Markets and Regulation, University of New South Wales Sydney. Professor Buckley chairs the Digital Finance Advisory Panel of the Australian Securities and Investment Commission ("ASIC"); however the views expressed herein are strictly his own, not those of ASIC.

** Kerry Holdings Professor in Law and Director, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong; and member, Advisory Board, Centre for Finance, Technology and Entrepreneurship.

*** Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Faculty of Law, Economics and Finance, University of Luxembourg, and Director, Centre for Business and Corporate Law, Heinrich-Heine-University, Düsseldorf, Germany.

**** Research Fellow, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong. This article extensively develops and expands ideas first raised in Douglas W Arner, Dirk A Zetzsche & Ross P Buckley, "FinTech, RegTech and Systemic Risk: The Rise of Global Technology Risk" in Arner *et al*, eds, *Systemic Risk in the Financial Sector: Ten Years after the Global Financial Crisis* (Ontario: CIGI Press, 2019). We would like to thank for support of this research the Australian Research Council as part of the project, "Regulating a Revolution: A New Regulatory Model for Digital Finance", the Hong Kong Research Grants Council Research Impact Fund and the Qatar National Research Fund National Priorities Research Programme. The authors are grateful for comments and remarks by participants of workshops and conferences at the Bank for International Settlements, the Financial Stability Board, Centre for International Governance Innovation, International Monetary Fund, and the National University of Singapore, among others.

globalised segment of the world's economy but also among the most digitised and datafied.[1]

This process can be seen across four major axes: the emergence of global wholesale markets, an explosion of financial technology ("FinTech") startups since 2008, an unprecedented digital financial transformation in developing countries (particularly China), and the increasing role of large technology and data companies ("BigTech") in financial services ("TechFin") as well as increasing real time interconnectivity between systems. This process of digital financial transformation brings structural changes. These changes have positive aspects but also negative ones, in the form of new risks. While finance and technology have always interacted and supported each other, over the period since the 2008 Global Financial Crisis, the changes have been unprecedented, particularly in terms of speed of change and extent of new entrants. Speed of change can be seen particularly in the role of new technologies, often summarised as the ABCD framework: artificial intelligence ("AI"), blockchain, cloud and data, which are co-evolving at an increasing rate with finance. Many would also add mobile internet and internet of things ("IoT") to this framework.

This long-term process of digitisation and datafication of finance has increasingly combined with related technologies including Big Data[2] and AI,[3] distributed ledgers and blockchain,[4] initial coin offerings ("ICOs"),[5] smart contracts,[6]

---

1 Prashant Gandhi, Somesh Khanna & Sree Ramaswamy, "Which Industries Are the Most Digital (and Why)?" (1 April 2016) *Harvard Business Review,* online: Harvard Business Review <https://hbr.org/2016/04/a-chart-that-shows-which-industries-are-the-most-digital-and-why>.

2 See generally, Solon Barocas & Andrew D Selbst, "Big Data's Disparate Impact" (2016) 104 CLR 671; Daniel Martin Katz, "Quantitative Legal Prediction – or – How I Learned to Stop Worrying and Start Preparing for the Data Driven Future of the Legal Services Industry" (2013) 62 Emory LJ 909; Omer Tene & Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) 11 Northwestern J Technology & Intellectual Property 239; Dirk A Zetzsche *et al*, "From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance" (2018) 14 New York UJ L & Business 393.

3 In computer science, Artificial Intelligence is defined as devices that perceive their environment and take actions that maximise their chance of successfully achieving their task. The base line of artificial intelligence is a computer mimicking human 'cognitive' functions such as 'learning' and 'problem solving'. Artificial intelligence today can be used to detect unexpected correlations in large data pools, test expected correlations for causation or determine an empirical probability of a predefined pattern. See David Lynton Poole, Alan K Mackworth & Randy Goebel, *Computational Intelligence: A Logical Approach* (New York: Oxford University Press, 1998); Stuart J Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3d ed (London: Prentice Hall, 2009).

4 See Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, Massachusetts: Harvard University Press, 2018); Usha Rodrigues, "Law and the Blockchain" (2018) 104 Iowa L Rev 679; Dirk A Zetzsche, Ross P Buckley & Douglas W Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain" (2018) U Ill L Rev 1361.

5 See Shaanan Cohney *et al*, "Coin-operated Capitalism", 119 Colum L Rev 591; Philipp Hacker & Chris Thomale, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law" (2018) ECFR 645; Dirk A Zetzsche *et al*, "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators" (2019) 60 Harv Intl LJ 305.

6 See Jeremy M Sklaroff, "Smart Contracts and the Cost of Inflexibility" (2017) 166 U Pa L Rev 263; Kevin Werbach & Nicolas Cornell, "Contracts Ex Machina" (2017) 67 Duke LJ 313; Max Raskin, "The Law and Legality of Smart Contracts" (2017) 1 Georgetown L Technology Rev 304.

regulatory technology ("RegTech")[7] and digital identity,[8] in a new era of FinTech.[9]

Two major trends stand out in the current period of FinTech development. The first is the speed of change driven by the commoditisation of technology, Big Data analytics, machine learning and AI. The second is the increasing number and variety of new entrants into the financial sector, including pre-existing technology and e-commerce companies. Most attention to date has focused on the general trajectory that technologised financial services will take[10] and how they will be regulated.[11] Special consideration has also been given to FinTech's impact on banks and the payment services sector,[12] including the disruptive effects of crowdfunding and crowdlending[13] on existing intermediaries. The darker side of digital financial transformation, however, can be unsettling as it raises many questions.[14] The recent COVID-19 coronavirus crisis in particular has highlighted the world's existential dependence

---

7 See Douglas W Arner, Janos Barberis & Ross P Buckley, "FinTech, RegTech and the Reconceptualisation of Financial Regulation" (2017) 37 Nw J Intl L & Bus 371; Lawrence G Baxter, "Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures" (2016) 66 Duke LJ 567 at 572 (arguing that technology assists banking regulators in updating regulation and keeping up with evolving markets); Dirk A Zetzsche *et al*, "The EU's Future of Data-driven Finance" (2020) Common Market L Rev in press.

8 Douglas W Arner *et al*, "The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities" (2019) 20 European Business Organisation L Rev 55.

9 *Cf* Douglas W Arner, Janos Barberis & Ross P Buckley, "The Evolution of FinTech: A New Post-Crisis Paradigm?" (2017) 47 Geo J Intl L 1271.

10 Arner, Barberis & Buckley, *supra* note 9 at 1276-1285.

11 See HJ Allen, "Regulatory Sandboxes" (2019) 87:3 Geo Wash L Rev 579; Chris Brummer, "Disruptive Technology and Securities Regulation" (2015) 84 Fordham L Rev 977; Chris Bummer & Yesha Yadav, "FinTech and the Innovation Trilemma" (2019) 107 Geo LJ 235; Kathryn Judge, "Investor-Driven Financial Innovation" (2018) 8 Harv Bus L Rev 291; ST Omarova, "New Tech v. New Deal: Fintech As A Systemic Phenomenon" (2019) 36 Yale J Reg 735; WJ Magnuson, "Regulating Fintech" (2018) 71 Vanderbilt L Rev 1168; Dirk A Zetzsche *et al*, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation" (2017) 23 Fordham J Corp & Fin L 31.

12 See Basel Committee on Banking Supervision, "Sound Practices: implications of fintech developments for banks and bank supervisors" (February 2018) *Bank for International Settlements ISBN 178-92-9259-128-1*, online: Bank for International Settlements <https://www.bis.org/bcbs/publ/d431.pdf>; U.S. Department of the Treasury, "A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation (Executive Order 13772 on Core Principles for Regulating the United States Financial System)" (31 July 2018), online: U.S. Department of the Treasury <https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities—Nonbank-Financials-Fintech-and-Innovation_0.pdf>; Lerong Lu, "Decoding Alipay: Mobile Payments, a Cashless Society and Regulatory Challenges" (2018) 33 Butterworths J International Banking & Financial L [forthcoming], online: Social Science Research Network <https://ssrn.com/abstract=3103751>.

13 See John Armour & Luca Enriques, "The Promise and Perils of Crowdfunding: Between Corporate Finance and Consumer Contracts" (2018) 81 Modern L Rev 51; Dirk Zetzsche & Christina Preiner, "Cross-Border Crowdfunding: Towards a Single Crowdlending and Crowdinvesting Market for Europe" (2018) 19 European Business & Organisation L Rev 217.

14 Financial Stability Board, "Decentralised Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications" (2019), online: Financial Stability Board <https://www.fsb.org/2019/06/decentralised-financial-technologies-report-on-financial-stability-regulatory-and-governance-implications/>.

on digital infrastructure.[15] The risks and challenges that arise are the focus of this article.

The article proceeds, in Part II, with a framework of analysis for the consideration of risks, old and new, emerging from digital financial transformation so as to set the stage. This is followed by sections analysing key areas of concern: cybersecurity and data risks (Part III), BigTech / TechFin (Part IV), and new technological risks (Part V). Part VI then concludes, arguing for the need for coordinated approaches at both domestic and international levels and suggesting the basis of a set of principles which may serve as the basis of a framework to address these sorts of risks going forward.

II. Technology and Finance: Framework of Analysis

In 2019, Facebook announced it was leading a consortium to establish Libra. Libra is a new cryptocurrency to be created and to operate through a new global electronic payment system (effectively Facebook / WhatsApp / Instagram Pay), combined with a Facebook-led digital identification infrastructure. Principally, Facebook aims to create a new electronic payment system for its ecosystem of social media applications based on a new payment instrument linked to pools of fiat currencies (a "stablecoin"), allowing it to monetise the interactions of its approximately 3 billion users globally, particularly in developing countries lacking similar sorts of infrastructure.[16]

This proposal highlights many of the key areas of concern raised by digital financial transformation: What if Libra is hacked and destroyed? (cybersecurity risk) What if Facebook uses the data acquired for its own purposes? (data protection and privacy risk) What if user data is stolen? (data security risk) What if Facebook dominates the international financial system as a result of Libra? (new systemically important financial institution risk) What if Libra becomes the dominant international form of money? (technological infrastructure risk, threats to competition) All these concerns together help explain why Libra received a lukewarm response by regulators around the globe.[17]

These risks are key considerations for financial regulation. In looking at financial regulation, its objectives can be summarised in four major categories: 1) financial stability, 2) financial integrity, 3) customer protection, and 4) financial efficiency, development and inclusion ('financial market functioning'). Financial stability can be seen both negatively (as avoidance of crises) and positively (as appropriate functioning of the financial system). Financial integrity focuses on prevention of criminal activities and use of the financial markets for criminal activities, for instance in the

---

15 See on the importance of digital infrastructure and finance during the COVID-19 coronavirus crisis, Douglas W Arner *et al*, "Digital Finance & The COVID-19 Crisis", University of Hong Kong Faculty of Law Research Paper No 2020/017 (2020), online: Social Science Research Network <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3558889>.

16 See on Libra's set-up and regulation Dirk A Zetzsche, Ross P Buckley & Douglas W Arner, "Regulating Libra" (2020) Oxford J Leg Stud in press, available as EBI Working Paper (2019), online: Social Science Research Network <www.ssrn.com/abstract=3414401>.

17 See regarding the reaction of the United States, (Reuters, dpa, AP), "Mark Zuckerberg grilled by US Congress over Libra" *Deutsche Welle News* (23 October 2019), online: Deutsche Welle <https://www.dw.com/en/mark-zuckerberg-grilled-by-us-congress-over-libra/a-50957685>. For a summary of other countries' responses, see Zetzsche, Buckley & Arner, *supra* note 16.

context of money laundering, terrorist financing, international criminal organisations, and even state organised attacks. Customer protection focuses on systems to prevent abuses of users of financial services: consumers, savers and investors. Financial efficiency, development and inclusion focus on how to support and enhance the positive functioning and role of the financial system.

While FinTech raises concerns in all of these areas, our focus is in the context of financial stability, a core focus of regulators around the world particularly since 2008. Prior to 2008, the focus in terms of supporting financial stability and preventing crises was on the identification of major forms of risk and building appropriate regulatory and supervisory frameworks to address these, with the Basel II Capital Accord the state of art embodiment at an international level. Basel II and financial stability regulation in general focused on a "microprudential" approach prior to 2008, in which regulators and supervisors placed the greatest emphasis on the safety and soundness of individual financial institutions through prudential regulatory standards.

This approach focused on five major categories of risk: credit/counterparty risk, market risk, payment risk, operational risk, and legal risk. Basel II included capital charges and related regulatory standards for the first four of these (with relatively little attention paid to legal risk).

In this framework, risks relating to technological and data issues were incorporated into the operational risk framework, thus incurring a relatively small cost in terms of capital charges and related risk management and compliance systems. Since 2008, financial stability regulation has focused very heavily on addressing "macroprudential" risks: risks arising not just from the potential failure of individual institutions but risks arising from interdependencies in markets, which were at the heart of the 2008 financial crisis and thus have been central to post-crisis financial regulatory reform processes. Related analyses are now beginning to extend to a range of considerations and risks from FinTech.

We suggest that in the context of digital financial transformation, this treatment is no longer sufficient nor appropriate to capture the full range of risks faced by the financial system.

In looking at digital financial transformation, an appropriate framework of analysis encompasses: (1) new sources of traditional forms of risk; (2) new forms of risk; and (3) entirely new markets and systems, including for regulation (such as RegTech).

We develop this framework discussing a number of key areas of concern which have emerged during the process of digital financial transformation, in particular cybersecurity, data security and data privacy (see Part III, below), the emergence of new systemically important financial institutions (see Part IV, below) as well as the emergence of new financial market infrastructures and dependencies (see Part V, below).

III. Cybersecurity and Data Risks

Traditionally, issues relating to technology have been included in the context of operational risk, recognised as one key form of financial risk, along with credit risk, market risk and legal risk.[18] As a result of the emergence of digitisation and datafication,

[18] See Basel Committee on Banking Supervision, "Basel III: A global regulatory framework for more resilient banking systems"*Bank for International Settlements ISBN print: 92-9131-859-0* (December 2017), online: Bank for International Settlements <https://www.bis.org/publ/bcbs189.pdf>.

we suggest that technology risks (including risks relating to cybersecurity and data privacy) should be seen as a separate form of risk, beyond the traditional operational risk categorisation. Technology risks can arise in the context of individual institutions and in the interconnections among institutions. The technical difficulty in securing staff activity between proprietary and third-party networks and software during the coronavirus crisis is an apt example of such weaknesses. Even more fundamentally, technology risks have the potential to impact financial sector confidence and stability directly. As a result of digital financial transformation, cybersecurity has become one of the major sources of systemic risk in the financial system.

A. *Sources of Systemic Risk*

Before we give a detailed view of the new tech-induced threats, some background on systemic risk is required to contextualise our analysis.

Systemic risk[19] has long been a major focus in the evolution of financial regulation, particularly banking regulation. According to the Group of Twenty ("G20"):

> [S]ystemic financial risk is the risk that an event will trigger a loss of economic value or confidence in, and attendant increases in uncertainty about, a substantial portion of the financial system that is serious enough to quite probably have significant adverse effects on the real economy.[20]

Prior to the 2008 Global Financial Crisis ("GFC"), financial stability regulation had emerged as a core regulatory function, focusing on the identification, prevention and management of systemic risk.[21] The focus generally was in the context of banking—usually excluding non-bank financial institutions—and in particular in the context of size of individual institutions (the "too big to fail" ("TBTF") problem) and in the context of the payments system. Despite decades of experience and analysis, systemic risk was a core feature of the 2008 GFC, highlighting distinct failures in financial stability regulation.[22]

Following the 2008 GFC, there is a general consensus that systemic risk is usually the result of the financial intermediary's size (TBTF) or of interrelationships between

---

19 See the works by George G Kaufmann, an economist at the Federal Reserve *eg,* George G Kaufman, "Bank Failures, Systemic Risk, and Bank Regulation" (1996) 16 Cato Journal 16 at n 5 quoting Alan Greenspan, the former head of the US Federal Reserve; George G Kaufmann & Kenneth E Scott, "What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?" (2003) 7 The Independent Rev 371 at 371: "Systemic risk refers to the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, and is evidenced by comovements (correlation) among most or all the parts." Kaufmann and Scott refer to Kaufmann's earlier work in the 1990s; see also the contributions in Arner *et al*, *Systemic Risk in the Financial Sector: Ten Years after the Global Financial Crisis* (Ontario: CIGI Press, 2019).

20 Group of Ten, "Report on Consolidation in the Financial Sector" (25 January 2001) *International Monetary Fund*, online: International Monetary Fund <https://www.imf.org/external/np/g10/2001/01/eng/pdf/file3.pdf> at 126.

21 See Douglas W Arner, *Financial Stability, Economic Growth, and the Role of Law* (New York: Cambridge University Press, 2007).

22 See Steven L Schwarcz, "Systemic Risk" (2008) 97 Geo LJ 193. Schwarcz demands an integrated view on markets rather than institutions. His view indirectly supports the position presented herein that systemic risk is an established feature of the market governance objective of financial law.

intermediaries (Too Connected to Fail ("TCTF")). Both TBTF and TCTF are now seen as core aspects of financial stability regulation, both from the microprudential (TBTF) and the macroprudential (TCTF) standpoint.

Since the GFC, large volumes of research have sharpened the understanding of systemic risk. As a baseline, there is a common understanding that size of intermediaries and interconnectivity are core sources of systemic risk. As defined by former United States ("US") Federal Reserve Chair Ben Bernanke, a systemically important financial institution ("SIFI") "is one whose size, complexity, interconnectedness, and critical functions are such that, should the firm go unexpectedly into liquidation, the rest of the financial system and the economy would face severe adverse consequences."[23] SIFIs—particularly global SIFIs ("G-SIFIs")—have thus become a central focus of the G20 / Financial Stability Board ("FSB") post-crisis regulatory reform agenda, as well as a key focus of domestic and regional regulatory reforms over the past decade.

In the context of the TBTF paradigm, systemic significance follows from the size of a financial institution.[24] Under the TCTF paradigm, systemic importance follows from the fact that other financial intermediaries are engaged in business links with the intermediary which are crucial to the many intermediaries, while all of those intermediaries together are of critical importance for the financial system, and substitutes cannot be found for those links easily. The key post-crisis insight here is that interlinkages can take many forms, not just payment interlinkages, with a particular post-crisis focus on linkages from over-the-counter ("OTC") derivatives and the related counterparty risk. In addition, interlinkages are now seen as arising from common business models (*eg*, originate-to-distribute), contractual approaches (*eg*, standardised documentation such as those of the International Swaps and Derivatives Association) and commonalities across risk-management systems.

One consequence of systemic importance is that governments are pressed to provide support to systemically important financial institutions if they face financial problems.[25]

Much of the G20 / FSB post-crisis regulatory agenda thus focuses on prevention of systemic risk through a range of financial stability systems, including: (1) microprudential supervision of SIFIs, particularly G-SIFIs; (2) macroprudential supervision to identify interconnections and risks prior to any crisis trigger; and (3) strengthening core infrastructures, particularly in the context of systemically important infrastructures such as payment systems, securities settlement systems and central counterparties.[26] These have been undertaken through a wide range of efforts: domestic, regional and international, including regulatory changes and changes to

---

23 Ben Bernanke, "Causes of the Recent Financial and Economic Crisis" (Testimony delivered before the Financial Crisis Enquiry Commission, United States Congress, Washington D.C, 2 September 2010), online: The Federal Reserve <https://www.federalreserve.gov/newsevents/testimony/bernanke20100902a.htm>.

24 Luc Laeven, Lev Ratnovski & Hui Tong, "Bank Size and Systemic Risk" (May 2014) *(IMF Staff Discussion Note) No SDN/14/04*, online: International Monetary Fund <https://www.imf.org/external/pubs/ft/sdn/2014/sdn1404.pdf>.

25 See Bernanke, *supra* note 23.

26 See, for example, Kern Alexander & Steven L Schwarcz, "The Macroprudential Quandary: Unsystematic Efforts to Reform Financial Regulation" in Ross Buckley, Emilios Avgouleas & Douglas W Arner, eds, *Reconceptualising Global Finance and its Regulation* (New York: Cambridge University Press, 2016) 127.

the scope of regulatory mandates (in individual jurisdictions as well as through the FSB) and the creation of new systemic risk supervisory structures (such as the European Systemic Risk Board in the European Union ("EU") and the Financial Stability Oversight Council in the US).

B. *The Cyber Threat*

Cybersecurity has become one of the leading areas of attention of financial regulators around the world as well as of governments and financial and tech firms. We would suggest that cybersecurity is now the most significant source of systemic risk, as well as one of the more significant issues of national security. Cyberattacks are consistently increasing in severity and frequency, with 15% more firms reporting having experienced a cyber event in 2018, from the year before.[27] Cyber insurance premiums have tripled in the past two years and re-insurers are questioning the viability of the business.[28] The economic impact of cybercrime has risen fivefold in the past six years.[29] Espionage and service disruption continues to be a growing motive for hacking.[30] The technical chaos caused by the pandemic has also opened up a variety of new security gaps. Cybersecurity risk can thus be seen as a new source of traditional risk as well as an entirely new form of risk and one with potentially catastrophic consequences. The hacking of a Russian bank leading to the execution of $400 million in trades swung the USD/Ruble exchange rate by 15%. While the weight of the international risks is significant, addressing them at a cross-border level is particularly challenging due to not only financial stability issues but also national security issues.

From the standpoint of SIFIs which have almost entirely digitised their operations, hacking, cybertheft, cyberterrorism, cyberactivism and cyberattacks pose grave risks. While financial institutions have long focused on all forms of fraud and theft risk, digitisation and globalisation raise the potential for even simple fraud and theft to take on much greater scale: instead of robbing one account, office or firm, an attacker can potentially rob or attack all accounts and offices of multiple firms in multiple jurisdictions at the same time. The challenge here is greater provided the wide range of motivations for attackers.

While regulators—both in individual jurisdictions as well as internationally and regionally—are focusing attention on related issues, the wide range of actors and motivations are a challenge: though it is clearly appropriate and necessary for all financial institutions and infrastructure providers to focus significant resources and efforts on cybersecurity, the broad presence of state and state-supported actors involved highlights the difficulties of pushing the entire burden onto the financial

---

27 "Challenges to effective EU cybersecurity policy" (March 2019) *European Court of Auditors Briefing Paper*, online: European Court of Auditors <https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf>.

28 See *ibid* and Jeff Stone, "Demand for Cyber Insurance Grows as Volatility Scares off Some Providers" *CyberScoop* (29 July 2019), online: CyberScoop <https://www.cyberscoop.com/cyber-insurance-demand-cost-2019/>.

29 President Jean-Claude Juncker, "State of the Union 2017" (State of the Union Address 2017 delivered at the European Commission, 13 September 2017).

30 "Data Breach Investigations Report 2017" (2017) *Verizon Investigations Report*, online: Verizon <http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf>.

sector. Concurrently, the shift towards FinTech exacerbates certain cybersecurity threats that are unique to the financial system, and subsequently—financial stability. Vulnerabilities in the financial system stem from the high level of leverage, asset conversion chains, and procyclicality.[31] The growing dependence on complex digitalised information technology hubs without substitute, as illustrated by its lifeline role during the COVID-19 crisis, is contrasted by the growing amount of outwards facing FinTech, increasing cyber exposure.[32] Cyberattacks can exploit these security gaps to, for example, disrupt payment systems, corrupt data at custodian banks or central securities depositories, or cripple infrastructure on which the financial system relies.[33] While these are low-risk events, their occurrence will have high-impact consequences capable of snowballing into financial destabilisation if not contained.

As a result of the increased state presence in cyberactivities (including cyberwarfare), there is a clear need for states to take a leading role in building systems to monitor and support key sectors of the economy—such as the financial sector—in addition to private and regulatory attention to issues of cybersecurity.

We posit three factors that transform cybersecurity into a new form of risk, and one that is much more material to financial stability. These are: (1) the growing rate of technological development and adoption in finance, (2) the lag and divergence in international FinTech governance and (3) the erosion of trust from the conflation of national security and financial stability in the cyber domain.

1. *Risk from the growing rate of FinTech development*

The first layer of cyber risk stems from the high rate and typology of technological development and adoption of digital systems in finance. The growing transition to cloud infrastructure creates more concentrated data nodes, with less software diversity, requiring higher security measures.[34] Endogenous threats to such nodes stem from compromises of internal firm or client information, and unauthorised access to systems by or via users or employees.[35] Exogenous threats involve breaches from interfacing with other third-party systems, or using fraudulently acquired privileged accounts credentials to access data and perform transactions.[36] Both threats form several concentric layers of security risk by depending on the security of third-party software in the likes of (i) colocation centres holding primary server data, or

---

31 Martin Boer & Jaime Vazquez, "Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System" (2017) *Institute of International Finance*, online: Institute of International Finance <https://www.iif.com/Publications/ID/228/Cyber-Security-Financial-Stability-How-Cyber-attacks-Could-Materially-Impact-the-Global-Financial-System>.

32 Artie W Ng & Benny KB Kwok, "Emergence of Fintech and Cybersecurity in a Global Financial Centre" J Financial Regulation & Compliance (2017), online: Emerald Insight <https://www.emerald.com/insight/content/doi/10.1108/JFRC-01-2017-0013/full/html>.

33 Boer & Vazquez, *supra* note 31.

34 Centre for Risk Studies, "Cyber Risk Outlook 2019" (2019) *University of Cambridge Judge Business School*, online: University of Cambridge Judge Business School <https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyber-risk-outlook/cyber-risk-outlook-2019/>.

35 Polozov Y, "Trading Systems Manipulation: Metel/Corkow Trojan proof-of-concept attack" (2016) Wapack Labs, FS-ISAC.

36 Benton E Gup, *The Most Important Concepts in Finance* (Cheltenham: Edward Elgar Publishing, 2017) at 43.

(ii) employee mobile and other IoT devices.[37] For example, in 2016 criminals stole $81 million from the central bank of Bangladesh, by infecting a SWIFT server with malware.[38] With more interconnected and digitised technology, cyber security is only as strong as the weakest link in the network.

New FinTech, like distributed ledger technologies (*eg*, blockchain), or stablecoins come with their own set of threats. While their novel methods of centralisation (or decentralisation) provide unique value to their users, they still tend to be based on traditional or cloud based infrastructure.[39] For example, a theft of 7000 bitcoins, stolen from one of the world's largest cryptocurrency exchanges through the use of phishing and viruses to gain user data, led to the value of bitcoin falling by about 3 percent.[40] Further examples include the hacks of Mt. Gox and The DAO.[41] Depending on the level of centralisation and 'chain'-related status, updating the infrastructure of the technology can also be difficult. With no clear contingency mechanism, a security breach can instantly disrupt such networks, which are increasingly important for channelling resources, thus risking access to vital resources for ever growing numbers of people.

2. *Risk from lagging and divergent international FinTech governance*

The second layer of risk stems from lag and divergence in cyber governance in different countries. While cyberspace is a high-speed, frictionless global network, its regulation is fragmented, with at best, significant gaps, and at worst, normative clashes between various actors. At national levels, particularly less mature regulatory environments, severe discrepancies leave smaller private and public entities vulnerable, opening the wider system to cascading effects from breached entities.[42] Attempts to lessen such sectoral discrepancies are nascent and as yet untested for their impact.

The US, for example, has embraced public-private partnerships, with the *Cybersecurity Information Sharing Act*[43] of 2015 inviting private entities and certain government agencies to share information on threats with federal agencies. The National Institute of Standards and Technology and the Financial Industry Regulatory Authority collect, identify, assess and respond to risks between public and private entities, exchanging best practices. However, these are largely soft measures with varying membership across sectors and size. Hard measures generating systemic protection are rare and divergent. New York recently implemented comprehensive cybersecurity rules requiring financial service firms to appoint chief information

---

37 *Ibid* at 45.

38 Emanuel Kopp, Lincoln Kaffenberger & Christopher Wilson, "Cyber Risk, Market Failures, and Financial Stability" (2017) International Monetary Fund Working Paper No 17/185, online: International Monetary Fund <https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104>.

39 Financial Stability Board, *supra* note 14.

40 Eric Lam, "Hackers Steal $40 Million Worth of Bitcoin From Binance Exchange" *Bloomberg* (8 May 2019), online: Bloomberg <https://www.bloomberg.com/news/articles/2019-05-08/crypto-exchange-giant-binance-reports-a-hack-of-7-000-bitcoin>.

41 See for a list of major hacks through 2018: Zetzsche, Buckley & Arner, *supra* note 4 at 1367-1369.

42 "Challenges to effective EU cybersecurity policy", *supra* note 27.

43 Pub L No 114-113, div N, tit I, 129 Stat 2936 (2015) (codified as amended at 6 USC § 1501 *et seq*).

security officers and to conduct periodic risk assessments and protect sensitive data.[44] California, for example, avoids prescriptive requirements in favour of risk-based security centred on consumer data protection.[45]

Likewise, the EU Network and Information Security Directive adopted in 2016 sets a minimum level of harmonisation among Member States, setting a single point of contact and creating computer security incident response teams ("CSIRTs").[46] Yet, Latvia has 8 sectoral competent authorities, Estonia has one, and Spain splits them by public and private sectors.[47] In case an incident is recorded, cooperation among law enforcement is difficult, granted the number of jurisdictions involved and the inefficiencies persisting in cross-border collaboration.[48] These differences are capable of placing additional burdens on attempts at cooperation, facilitating hackers' business, and extending cyber incident contagion.[49]

3. *Risk from conflating national security and financial stability*

The third layer of risk is tied to the convergence of national security and financial stability in the cyber domain. Where cybersecurity has conventionally been understood as a state responsibility, aimed at protecting internal critical infrastructure and cyberspace from national security incidents,[50] increasingly interconnected data and transaction flows necessitate broadening the mandate. However, the defence origins of cybersecurity can lead to vastly varying approaches to transnational cybersecurity cooperation, which may hamper the intelligence pooling necessary to effectively prevent cyber incidents. Recent challenges for CSIRTs—the national cyber incident first responder teams—are a representative microcosm.

Hundreds of CSIRTs across the world perform similar primary functions in both the public and private sectors, they: (i) coordinate prevention efforts against cyber-threats, (ii) disseminate information regarding cybersecurity practices and incidents, (iii) remediate damage by securing breached data, and (iv) recover public and private systems after a cyber-attack on national infrastructure.[51] To disseminate and

---

44 *Cybersecurity Requirements for Financial Service Companies*, 23 NYCRR tit 23 § 500.00 (2017).

45 US, AB 375, *California Consumer Privacy Act*, 2017-2018, Reg Sess, Cal, 2018 (enacted).

46 EU, *Commission Directive 2016/1148 of 6 July 2016 the European Parliament and of the Council of concerning measures for a high common level of security of network and information systems across the Union* [2016] OJ, L 194/1.

47 See Sabrina Galli, "NYDFS Cybersecurity Regulations: A Blueprint for Uniform State Statute" (2018) 22 NC Banking Inst 235 and John Ogle, "Identities Lost: Enacting Federal Law Mandating Disclosure & Notice after a Data Security Breach" (2019) 72 Ark L Rev 221.

48 *Ibid.*

49 See Loretta J Mester, "Perspectives on Cybersecurity, the Financial System, and the Federal Reserve" (2019) *Ohio Division of Financial Institutions, Columbus, OH*, online: Federal Reserve Bank of Cleveland <https://www.clevelandfed.org/newsroom-and-events/speeches/sp-20190404-perspectives-on-cybersecurity-the-financial-system-and-the-federal-reserve>.

50 For example, major cybersecurity mobilisation took place among international organisations after cyberattack experienced by Estonia in 2007, which disrupted its communication capabilities through denial of service attacks, when an Iranian nuclear facility was destroyed by a virus, or when the US financial sector experienced DDOS attacks between 2011 and 2013. For more, see: Christopher S Yoo, "Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures" (2016) University of Pennsylvania, Public Law Research Paper No 15-3.

51 Yoo, *supra* note 50.

develop intelligence and best practices among themselves, various informal cybersecurity networks were established connecting CSIRTs to one another aiming to foster collective cybersecurity.[52] Such 'walled-gardens' remain the main vehicles of best practice, toolset, and communication exchange between CSIRTs, mitigating the asymmetry of capacity between various teams.[53]

As CSIRT functions evolve to meet the demands of their respective governments, their duties can expand to include law enforcement or intelligence activity. This can alter their ability to reveal vulnerabilities or raise the suspicion of network members to the use of received information for political purposes. Through no fault of their own, CSIRTs risk being isolated from the "web of trust", cutting them off from access to the latest vulnerabilities and leaving them in an information vacuum.[54] CSIRT groupings can create significantly more cyber-resilience than individual units.[55] As these networks are comprised of both public and private sector teams, limiting the access of one team to information can disable cybersecurity capacity, increasing financial destabilisation risk.

Similar misalignments are present at higher policy levels. For instance, the US strategy labels certain private sector firms as a subset of critical infrastructure with catastrophic national effects on economic security. However, as of recently, the US cybersecurity policy has pivoted from defence to deterrence.[56] The Financial Systemic Analysis and Resilience Center established in 2016 by the heads of eight large US financial service providers, launched a pilot project together with the US government to share threat data on nation-state actors that may pose threats to US national security.[57] The shift towards increasing the role played by major financial players in the context of US intelligence is a challenge for other in implementing their own approaches, including taking similar approaches themselves.[58] States must now carefully consider the extent to which US financial services providers with branches in their jurisdictions collect and transfer information, which may deter some from information sharing. As other states adopt similar approaches, risks of

---

52 The largest network, FIRST was established in 1990. Membership has grown from a handful of CSIRTs in North America in the year of formation, to over 490 from 92 countries all over the world by 2019. Samantha Bradshaw, "Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity" (2015) Global Commission on Internet Governance Paper Series, Paper No 23.

53 Isabel Skierka *et al*, "CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams" (2015) Global Public Policy Institute Working Paper, online: Global Public Policy Institute <www.gppi.net/publications/global-internet-politics/article/csirtbasics-for-policy-makers> at 8.

54 Jaco Robertson, Marthie Lessing & Simon Nare, "Preparedness and Response to Cyber Threats Require a CSIRT" (2008) International Federation for Information Processing.

55 Joseph S Nye, "The Regime complex for managing global cyber activities. Global Commission on Internet Governance" (2014) Global Commission on Internet Governance Paper Series No 1, online: Centre for International Governance Innovation <https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf>.

56 *Ibid*.

57 Chris Bing, "Project Indigo: The Quiet Info-Sharing Program between Banks and U.S. Cyber Command" *CyberScoop* (21 May 2018), online: CyberScoop <https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/>.

58 Gil Baram *et al*, "Strategic Trends in the Global Cyber Conflict" [2018] 2:3 Cyber Security: A Peer-Reviewed Journal 238, online: Ingenta <https://www.ingentaconnect.com/content/hsp/jcs/2018/00000002/00000003/art00006>.

fragmentation increase. A final challenge arises from adversary regimes intentionally and surreptitiously utilising cyberspace against their rivals, in which case cooperation in cyber for the purpose of financial stability can be wholly precluded. However, in such cases states and regions tend to have separate, mutually independent, FinTech networks.

4. *Risk from Cyber-Monoculture*

One additional cyberrisk comes from the lack of cyberdiversity, that is: where most large institutions use the same IT features (software, infrastructure, cloud computing), cyberrisks increase since cyberattacks against one institution could also succeed against another institution that is running similar IT systems. The COVID-19 pandemic exemplifies the risks of the hasty transition to digital solutions, especially to facilitate remote working, which may not be wholly secure. Hence, not only the tech use, but the uniformity of tech applications (which are inherent in the tech economy) create new risks.

5. *Addressing the new Cybersecurity threat*

Cybersecurity is generally considered mature where concerned with traditional critical infrastructure,[59] but the growth of data and money flows enabled by FinTech may create a dangerous interdependence that tends to avert stakeholder attention away from cyber-resilience. To address the aforementioned risks, we suggest expanding the breadth of cyber incident scenarios internationally, involving a variety of FinTechs to not only assess system weaknesses and costs, but to clarify liability assignment, which may be instrumental to reduce uncertainty in case of a cyber-caused crisis and aid in promoting a common legal framework. Such tests may also highlight the problems associated with moral hazard and TBTF and TCTF.

Considering national security concerns, we also suggest a comprehensive regulatory effort founded on already established grassroots operational initiatives with experience in pooling preventative, reactive, and proactive cybersecurity efforts. Careful examination should identify entities vulnerable to cyber breaches and capable of impacting financial stability, and relevant intelligence should be shared with other stakeholders at an international level. Policy differences are capable of inhibiting trust between stakeholders, so an apolitical mechanism may be appropriate. The International Committee of the Red Cross offers a model for a confidential and impartial coordinator entity working with independent national sub-structures, capable of tracking threats of contagion internationally. Such a model may be especially important to implement to allow a minimum level of cooperation during times of upheaval.

At the domestic level, there is a clear need for a multi-tiered approach, with coordination efforts at the national level (for national security issues), at the sectoral level (for instance the financial sector, for financial stability issues), and at the industry

[59] Basel Committee on Banking Supervision, "Cyber-Resilience: Range of Practices" (December 2018) *Bank for International Settlements ISBN 978-92-9259-228-8*, online: Bank for International Settlements <https://www.bis.org/bcbs/publ/d454.htm>.

level, internally and externally, in the context of the so-called "three lines of defence" (management control, risk control and compliance controls, independent assurance) at both individual institutions and across the financial industry.

C. *Data Security and Privacy Risk*

In addition to cybersecurity, the increasingly central role of data in the financial sector highlights the second major area of concern: data protection. Different policies are being developed in different economies, in part representative of fundamentally different societal approaches, with the US, China and EU being the leading examples of legal approaches to use, ownership and protection of data. Most notably, the EU's General Data Protection Regulation ("GDPR") may be understood as the most ambitious, harmonised legal approach to date reflecting concerns for an individual's privacy (and in turn establishing a user's rights *vis-à-vis* the data comptroller);[60] The US has so far generally taken a business friendly approach based on limited regulation and full transferability with nuances of the data governance issues only through federal agencies such as the Federal Trade Commission.[61] This characterisation and approach however are in the process of changing rapidly, with the enactment of new legislation in California not dissimilar in many ways to GDPR and with both political parties and most major technology companies now agreed on the need for new federal legislation in the area. China has largely followed a US style laissez-faire approach to data markets but with a very high level of comfort in state collection and use of data.[62] These variations undergird major questions about the role of data in digitised and datafied societies and economies: who owns and controls data, and what does ownership and control entail?

In looking at related issues, it is important to distinguish between data security or protection risks (about the protection of data, which often overlaps with cyber security risks), with data privacy risks (which is about the collection and use of personal data, particularly in jurisdictions with extensive privacy protections such as GDPR).

As dissimilitude in national legal approaches and capacities tend to heighten data security and privacy TechRisks,[63] we identify three data security and privacy risks in particular: (1) data manipulation uncertainty risk, (2) FinTech systemic integration risk, and (3) RegTech intervention and capacity risk.

---

60 See, for a short description on the GDPR as well as on the GDPR's impact on data-driven finance, Zetzsche *et al*, *supra* note 7.

61 See for instance, on Facebook's Cambridge Analytica scandal, Federal Trade Commission, Press Release, "FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer - FTC alleges they deceived Facebook users about data collection" (24 July 2019), online: Federal Trade Commission <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer>.

62 See the overview provided by Susan Ning & Han Wu, *China: Data Protection 2019*, online: International Comparative Legal Guide <https://iclg.com/practice-areas/data-protection-laws-and-regulations/china>.

63 World Bank, "World Development Report 2020: Trading for Development in the Age of Global Value Chains" (2019), online: World Bank <http://elibrary.worldbank.org/doi/book/10.1596/978-1-4648-1457-0> at 245.

1. *Data manipulation uncertainty risk*

The compound effects of increasingly concentrated data nodes with more levels and forms of analysis and subsequent use are yet unclear.[64] Given the current tendency towards 'evidence based policy' building so as not to unduly limit growth—legal frameworks are generally not constructed to take into account macroprudential data risks.[65] The principle of precaution for data and privacy is thus still nascent. Impact assessments tests required by data controllers under the EU's GDPR, for example, remain "abstract or imprecise".[66] Regulators lack a clear understanding of harm caused from bad faith or negligent data interfacing and transfers across jurisdictions.[67]

To avoid misconstruing data risks by setting narrow goal-based rules, a regulatory shift is taking place towards increasing the accountability of data manipulators by scrutinising the technical construction of algorithms and the auditability of their data analytics.[68] While helpful in retrospective investigations, these factors do not work well in mitigating or preventing loss.

2. *FinTech systemic integration risk*

In 2018, Carstens highlighted the risks associated with FinTech expansion into financial intermediation or 'online money market funds'.[69] The size of certain FinTechs is cause for credit and liquidity, and cascading investor run, risks.[70] Traditional banks will combine small deposits into large loans, while FinTech relies on a mixture of internal sources, syndicated loans and onselling originated credit.[71] The use of proprietary or second-hand non-traditional banking data to evaluate credit risk may import different levels of risk depending on the size of the data samples available, thereby precluding one-size fits all regulatory solutions. China, for instance, established *sui generis* norms for BigTech companies (explored later), requiring reserves on custodial accounts and for payments to be channelled through an authorised clearing house.

---

64 Arvind Narayanan, Joanna Huey & Edward Felten, "A Precautionary Approach to Big Data Privacy" (2016).

65 Andrew Stirling, "Precaution in the governance of technology" (July 2016), University of Sussex, Science Policy Research Unit Working Paper Series SWPS 2016–14.

66 Amir Shayan Ahmadian *et al*, "Supporting Privacy Impact Assessment by Model-Based Privacy Analysis" (2018) Proceedings of the 33rd Annual ACM Symposium on Applied Computing, online: Association for Computing Machinery <http://doi.acm.org/10.1145/3167132.3167288>.

67 Luiz Costa, "Privacy and the Precautionary Principle" (2012) 28 CLS Rev 14.

68 Paulette Lacroix, "Big Data Privacy and Ethical Challenges" in Mowafa Househ, Andre W Kushniruk & Elizabeth M Borycki, eds, *Big Data, Big Challenges: A Healthcare Perspective: Background, Issues, Solutions and Research Directions* (Berlin: Springer International Publishing 2019), online: Springer Link <https://doi.org/10.1007/978-3-030-06109-8_9>.

69 Agustín Carstens, "Big Tech in Finance and New Challenges for Public Policy" (Keynote address delivered at the FT Banking Summit, London, 4 December 2018), online: Bank for International Settlements <https://www.bis.org/speeches/sp181205.htm>. See also "FinTech and Banks. Friends or Foes?" *European Economy*, online: European Economy <https://european-economy.eu/book/fintech-and-banks-friends-or-foes/>

70 Carstens, *supra* note 69.

71 *Ibid*.

The compound network effects enjoyed by firms with access to large data panels allows for pattern recognition unreachable to new entrants, thereby dampening competition.[72] Even if policy attempts to remedy such imbalances by restricting data collection and retention, the incumbent data provides a plethora of derivative readings and forms of analysis capable of avoiding traditional compliance, which can continuously challenge regulators.[73] Firms with access to high amounts of data also benefit from a high symmetry of information in its operating markets—any attempts to galvanise the firm in a certain direction will necessarily face international challenges, exacerbated by fragmented regulatory frameworks.

3. *RegTech monitoring and intervention capacity risk*

If data risks are shared between the public and private sectors, regulators will require sufficient legal and technical capacity to effectively assess and impact the data-driven economy. In this regard, three data attributes create particular challenges:[74] (1) the strain placed on resources by the vastly varying data that needs to be monitored for a holistic investigation, (2) the vast variety of data structures running through proprietary systems that may need to be transposed into a form that meets regulatory standards, and (3) data quality assessment that requires understanding and comparing to upstream and vertical data origins and points, thereby exponentiating the investigative burden. Data investigation difficulties are also particularly strained by cross-jurisdictional coordination burdens, like heterogenous methodological approaches and investigative mandates and capacities.

Globally, standardisation initiatives, such as legal entity identifiers ("LEIs"), have great potential to assist with data alignment, but they are slow and offer limited macroprudential entry points.[75] However, data access sharing is scarce, and even contentious. For example, the US *Clarifying Lawful Overseas Use of Data Act*[76] obligates cloud providers like Google and Amazon to submit data to law enforcement under warrant or subpoena, even if the data is in another country. EU authorities report that the act clashes with the EU's GDPR, highlighting an "urgent" need for updates to Mutual Legal Assistance Treaties encompassing principles of proportionality and data minimisation.[77] For companies to comply with both, they may need to fully

---

72 Financial Stability Board, "FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications - Financial Stability Board" (2019), online: Financial Stability Board <https://www.fsb.org/2019/02/fintech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability-implications/>.

73 See, for example, the discovery of profitability bias in Amazon's algorithms in Dana Mattioli, "WSJ News Exclusive | Amazon Changed Search Algorithm in Ways That Boost Its Own Products" *The Wall Street Journal* (16 September 2019), online: The Wall Street Journal <https://www.wsj.com/articles/amazon-changed-search-algorithm-in-ways-that-boost-its-own- products-11568645345>.

74 Mark Flood, HV Jagadish & L Raschid, "Big Data Challenges and Opportunities in Financial Stability Monitoring" (2016) 20 Financial Stability Rev 129.

75 *Ibid*.

76 Pub L No 115-141, div V, 132 Stat 1213 (2018).

77 Email from EDPB and EDPS to Mr. Lopez Aguilar (Brussels, 10 July 2019), online: European Data Protection Board <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_response_us_cloudact_coverletter.pdf> or <https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en>.

segment their network, relegating vulnerabilities to divested branches. If data access remains an uneven playing field, the asymmetry of information will limit preventative and reactive risk management.

4. *Addressing data security and privacy risks*

Data security and privacy risks differ from cybersecurity by relating to the collection as well as the utilisation and veracity of collected data, instead of its protection. Consequently, regulators should consistently canvas the public sector for weaknesses in its integrity, risks of re-identification, *etc*. This demands sufficient resources and mandates to investigate the complex data streams. Once investigated, legal risk management frameworks can be created and updated. To effectively follow data trails, regulation should be harmonised internationally.

Similar to cyberactivity, the most effective way to advance more effective data assessments is through networks of data specialists exchanging best practices.[78] We posit supporting already existing initiatives, and reinforcing public private partnerships to better understand technical risks and events capable of drawing opprobrium from stakeholders, especially firms with potential impact on cross-jurisdictional institutional trust.

IV. FinTech, TechFin, Size and Connectivity

Beyond cybersecurity and data protection, the involvement of new financial participants such as FinTechs and BigTech raises potential concerns.[79]

From a systemic risk perspective, we do not believe that the risk stems from FinTechs as such. FinTechs are problem-driven firms, and though trying to become big, tend to start small.[80] Most FinTechs do not seek to disrupt the existing intermediaries; rather they want to collaborate and seek intermediaries as clients. It is here where the true FinTech innovation takes place—and at a rapid pace. As such, balanced proportional approaches to regulation are most appropriate, as we have analysed in detail elsewhere.[81]

However, the involvement of BigTech in financial matters is a reason for concern, especially given their increasingly essential role in the functioning of market supply-chains, as the current pandemic has shown.[82]

---

78 Konstantina Vemou & Maria Karyda, "Evaluating Privacy Impact Assessment Methods: Guidelines and Best Practice" (2019) *Information & Computer Security*, online: Emerald Insight <https://www.emerald.com/insight/content/doi/10.1108/ICS-04-2019-0047/full/html>.

79 See Jon Frost *et al*, "BigTech and the Changing Structure of Financial Intermediation" (April 2019) BIS Working Papers No. 779.

80 Daniel Drummer *et al*, "Fintech – Challenges and Opportunities" (May 2016) *McKinsey & Company*, online: McKinsey & Company <*https://www.mckinsey.de/files/160525_fintech_english.pdf*>.

81 Zetzsche *et al*, *supra* note 11.

82 Current regulatory attention focuses on the systemic risk dimension of technology firms. The BIS/BCBS has entered into a global consultation, in particular, on the role of 'BigTech'. See Basel Committee on Banking Supervision, *supra* note 12 at 15.

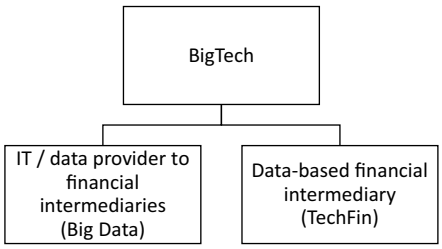

Fig. 1. BigTech's Function in Finance.

A. *BigTech*

According to the Basel Committee on Banking Supervision:

> BigTech refers to large globally active technology firms with a relative advantage in digital technology. Bigtech firms usually provide web services (search engines, social networks, e-commerce etc) to end users over the internet and/or IT platforms or they maintain infrastructure (data storage and processing capabilities) on which other companies can provide products or service.[83]

These BigTechs are linked to financial markets in two ways. First, they can function as third party providers to financial intermediaries. Use cases include the cloud services provided by Amazon and others, or data feeds to banks and asset managers which are used to inform risk models and calculations. Second, BigTech firms can move more directly into the provision of financial services, initially serving as conduits linking the financial service providers with the customers that the BigTech typically already has, and over time potentially beginning to provide the financial service itself directly to customers: as TechFins.[84]

Both BigTech business models—be it third-party IT services (Big Data) or TechFin-like provision of financial services—have the potential to create systemic risk, albeit in different ways.

As to TBTF, we highlight the rapid build-up of size drawing on the example of **TechFins** (data giants moving into financial services, such as Amazon and Alibaba). Large tech firms are increasingly moving into finance, often benefiting from: (a) regulatory gaps and/or disparities in treatment with traditional financial institutions, (b) economies of scope and scale, and (c) network effects (*ie* a tendency towards concentration in both data and finance). This combination suggests that TechFins may in fact potentially increase TBTF risks, in addition to raising concerns about competition and data protection.

As to TCTF, we argue that in a world of digitised finance, all is connected via the data feed, and such connectivity creates systemic risk. In particular, traditional bank-owned and bank-run infrastructure is replaced by new systemically important

---

83 BIS/BCBS, "Sound Practices: Implications of fintech developments for banks and bank supervisors", Consultative Document, (2017) at 15.

84 Dirk A Zetzsche *et al*, "From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance" (2018) 14 NYUJ L & Bus 393.

infrastructure owned by someone else and that someone else is potentially not a financial intermediary in the traditional sense, *ie* not regulated at all and not subject to measures we associate with systemic risk (bail-in/bail-out, segregation of critical infrastructure *etc*). Examples include market concentration in data feeds, cloud services (non-financial firm providing data and hosting services for financial firms and regulators), and others. In addition, cybersecurity risks arise dramatically across all aspects of finance.

We argue that BigTech's involvement in finance pairs size with connectivity—a combination which creates sizable potential systemic risks. The lack of transparency and the potential to build up (further) size in financial services very rapidly complete a story that suggests strongly that regulatory action with regard to BigTech should be on regulatory agendas.

B. *TechFin*

In contrast to FinTechs, TechFins—BigTech firms entering into finance—are often very significant firms beyond financial services prior to stepping into the financial sector. Due to their scale TechFins are connected to many institutions from the moment they enter the financial services market by, for example, functioning as a conduit to licensed institutions. Moreover, because of their data power, TechFins exercise influence over connected financial institutions from their moment of entry, and may often quickly control whole market segments when they finally begin to provide regulated financial services.

The governance and disclosure frameworks for financial services are not designed to accommodate Techfins: Financial intermediaries should be experts in processing financial information so as to channel cash flows to their most efficient use, in terms of expected risk-return ratios. This paradigm is challenged by TechFins. If TechFins have better data than traditional financial institutions, TechFins may provide the financial intermediary function more effectively. However, TechFins, at least today, operate for the most part in an unregulated environment. Until rather late in their journey into financial services, when they apply for a financial services licence, TechFins will not be subject to client/customer/investor protection rules nor to measures that ensure the functioning of financial markets and prevent the build-up of systemic risk.[85]

Moreover, from the perspective of incumbent licensed financial intermediaries, TechFins provide unbalanced, and arguably unfair, competition. The fixed costs of an initial licence and the ongoing costs of supervision and related reviews by advisors *etc*, will mean licensed intermediaries bear higher costs than unlicensed ones. In the long run, licensed intermediaries are doomed to lose these contests, given their higher cost-base and limited flexibility to respond to competitive challenges. Such an uneven playing field clearly raises risks of regulatory arbitrage as well as unfair competition.

---

[85] *Cf* Dirk Zetzsche, "Investment Law as Financial Law: From Fund Governance over Market Governance to Stakeholder Governance?" in Hanne S Birkmose, Mette Neville & Karsten Engsig Sørensen, eds, *The European Financial Market in Transition* (London: Kluwer Law International, 2012) at 339-343.

Risks arise from the potential for very rapid scaling in the TechFin context, something we have previously highlighted in the context of the speed with which a firm or product can now move from "too small to care" to TBTF—a core feature of the FinTech era which has emerged over the past decade.[86] For instance, Ant Financial runs a wealth management platform named Yu'e Bao. In its first ten months of operation Yu'e Bao[87] became the fourth largest money market fund in the world, which led to a swift, restrictive response from Chinese regulators.[88] In April 2017, after China's regulators had lifted the shackles, and only four years after its creation, Yu'e Bao assumed the top spot among all money market funds globally.[89] Alibaba's decision to separate Ant into a separate licensed financial services holding company—albeit under its continued control—by renaming its subsidiary Alipay in October 2014 was the direct result of regulators' fears over possible systemic risk arising from both Alipay and Yu'e Bao, and resulted in China's decision to build a regulatory system to address FinTech.[90] In a similar way, mobile money platforms such as M-Pesa have assumed systemic importance in some African countries,[91] as well as MercadoLibre (with payments and financial subsidiaries) and Russian financial platform provider Tinkoff in their respective home markets.

While arguably bringing important consumer benefits, the emergence of TechFins highlights the emergence of large new firms which must be carefully considered form the standpoint of their potential risks, arising from their size, interconnectivity and their roles in providing systemically important infrastructure. Often in the past trust and control of important market segments in financial services being in the hands of the few has led to major financial crises. Examples include the early-2000s accounting frauds[92] and of the credit ratings agencies in the 2008 crisis[93] as well as the roles of SIFIs in many crises, not just the most recent.[94] Accounting firms and rating agencies are mere data providers linked to the system (similar to early stage

---

86 Arner, Barberis & Buckley, *supra* note 9.

87 Jamil Anderlini, "Explosive Growth pushes Alibaba online fund up global rankings" *Financial Times* (10 March 2014), online: Financial Times <https://www.ft.com/content/748a0cd8-a843-11e3-8ce1-00144feab7de>.

88 Zhou Weihuan, Douglas W Arner & Ross P Buckley, "Regulation of Digital Financial Services in China: Last Mover Advantage" (2015) 8 Tsinghua China L Rev 25.

89 See Yifan Xie & Chuin-Wei Yap, "Meet the Earth's Largest Money-Market Fund" *The Wall Street Journal* (13 September 2017), online: The Wall Street Journal <https://www.wsj.com/articles/how-an-alibaba-spinoff-created-the-worlds-largest-money-market-fund-1505295000>.

90 *Ibid.*

91 See *eg*, Kiarie Njoroge, "Report: This is What Would Happen to Kenya's Economy if M-Pesa was to Collapse" *Nairobi News* (30 November 2016), online: Nairobi News <http://nairobinews.nation.co.ke/news/treasury-report-reveals-fears-m-pesas-critical-role-economy/>; Frank Jacob, "The Role of M-Pesa in Kenya's Economic and Political Development" in Falola T & Heaton M M, eds, *African Histories and Modernities* (New York: Palgrave MacMillan, 2016) 89.

92 See *eg*, Sean Farrell, "The world's biggest accounting scandals" *The Guardian* (22 July 2015), online: The Guardian <https://www.theguardian.com/business/2015/jul/21/the-worlds-biggest-accounting-scandals-toshiba-enron-olympus>; C William Thomas, "The Rise and Fall of Enron" (2002) 193:4 J Accountancy 41.

93 Amanda J Bahena, "What Role Did Credit Rating Agencies Play in the Credit Crisis?" (March 2010), online: <http://www.spaeth.ru/HS20152016/artikel_16.pdf>.

94 Financial System Inquiry, "Too-big-to-fail and moral hazard" (7 December 2014), online: The Treasury <https://treasury.gov.au/sites/default/files/2019-03/p2014-FSI-01Final-Report.pdf>.

TechFins), while SIFIs are typically very large (like TechFins that offer regulated services).[95] All three, unlike the TechFins, are at last strictly regulated today.[96]

Yet TechFins are by no means risk free. Without experience and monitoring, **we simply do not know all the risks created by technology since information flow to financial regulators is not mandatory as long as TechFins are beyond the scope of monitoring or supervision**. We will only experience the outcome if the service is not performed properly, with often surprising results. This will be particularly so as Artificial Intelligence and Machine Learning ("AI/ML") applications to large/novel data sets become more prevalent in financial services, because the underlying algorithms are very complex, almost opaque, and the behaviour of the self-learning algorithms becomes impossible to predict. Further, we lack experience with AI/ML based pricing models over a full business cycle.

If financial law does not apply, potential systemic risk may build up unobserved, unmitigated and uncontrolled, and, looking longer-term, the next global financial crisis may well come from weaknesses in TechFins rather than authorised financial institutions. Such concerns led to the decision in China to classify Ant Financial as a SIFI in late 2018.

C. *Addressing Tech Risk*

While the cause of systemic risk in case of BigTechs is increased by connectivity, a connectivity could be diversified away, but at some cost, the systemic risk perspective of TechFins rests on the assumption of **size and connectivity**, so diversification does not help.

At the core of our concern is the TechFin's conduit function in their early stage when they stand between the financial intermediary and its clients. One could respond that the early stage TechFin conduit function is merely one of data delivery; and data delivery is not a special activity warranting regulation.

Yet data provision in a highly concentrated market has prompted regulators to require financial institutions to diversify their data sources. The difference with TechFins is that data delivery is a back-end function, while TechFins also provide front-end, overlay services to the financial institutions, framed as a financial ecosystem or platform technology. TechFins' conduit function cannot be addressed by diversification requirements since the financial institution cannot readily change the 'service provider' as it can a back-end relationship—terminating the cooperation with the TechFin would cost the financial institution the link to its most precious asset: its clients.

For that reason, we have proposed elsewhere to regulate data gathering and analytics by virtue of a moderate regulatory intervention, along the business evolution

---

95 Mustafa Yuksel, "Identifying Global Systemically Important Financial Institutions" *Reserve Bank of Australia December Quarter 2014* (December 2014), online: Reserve Bank of Australia <https://www.rba.gov.au/publications/bulletin/2014/dec/pdf/bu-1214-8.pdf>.

96 See *eg*, Siegfried Utzig, "The Financial Crisis and the Regulation of Credit Rating Agencies: A European Banking Perspective" (January 2010) Asian Development Bank Institute Working Paper No 188.

from (1) too small to care, to (2) too large to ignore and then to (3) too big to fail (TBTF).[97]

As TechFins often do not seek access to client funds directly, many established financial regulatory thresholds based on balance sheet size, exposures or assets under management will fail to be triggered. In order to set appropriate thresholds, regulators must develop new criteria. These could include an overall number of data points, or holding data on a significant share of a population in the reference market, or other measures that reflect a very substantial data set.

If financial data gathering and analytics becomes a regulated activity, systemic risk measures will apply as soon as TechFins become essential to financial stability, and this will be determined by the TBTF or too complex / too connected to fail (TCTF) tests. If the TechFin is the main client channel for one important bank or for many banks which together are of systemic importance, the importance of the TechFin becomes like that of a new chief executive officer ("CEO") or a new business model rather than merely that of infrastructure. To the same extent that a new bank CEO and other key staff would be subject to regulatory scrutiny, we would ask the TechFin to meet the 'fit and proper' requirement, and ask for adequate resources to maintain that function on the side of the TechFin. This is where a systemic risk perspective indicates a case for regulation of TechFins.

Once regulators come to the conclusion that the TechFin is of **systemic importance**, for instance once TechFin data is essential for a systemically significant financial institution, or the TechFin provides the main client access for several financial institutions which together are of systemic significance, we recommend measures to control and limit systemic risk. In the first case this could require the significant financial institution to diversify its data sources. In the second case we recommend (a) structural requirements for TechFins (quarantine provisions as to 'Fin' with respect to entity, IT, capital; minimum capital for maintenance and clean-up; and country-by-country, or market-by-market, respectively, segregation of activities, the price to pay may be an increase in costs for the consumers), (b) empowering regulators to shut down the activity (while preserving customer data), or (c) to appoint a commissioner to run the quarantined TechFin part of the business in the public interest. As part of the resolution scheme regulators must ask the service provider how to ensure access to essential facilities in times of a crisis. In the case of data driven business models such as those of a TechFin, the resolution plan must lay out how continued access to data is ensured even if the financial business is bankrupt. For instance, we would ask data intensive financial firms to provide for licensing contracts with their data-driven mother subsidiaries that ensure business continuity (*ie* further data feeds) even if the financial firm itself is bankrupt for a certain period of time. Since without the data the whole firm will be threatened, and rarely will the TechFin arm of a BigData firm have full ownership of the data it is supplying.

Systemic risk intervention could go even one step further. Since running a crucial data provider in the public interest is not a long-term solution, mandating an open data policy under certain circumstances, as a particular systemic risk measure for data driven financial services, may reduce the need for additional regulatory intervention long-term. Note that, in contrast to open banking proponents, we do not argue for

---

[97] *Ibid*.

open data policies in all cases, but only as a specific crisis measure imposed on very large data driven financial services firms.

V. New Forms of Financial Infrastructure

In addition to new risks from the digital environment (particularly relating to cybersecurity and data protection and privacy) and from new financial institutions (particularly scale and network effects), new risks also arise from the evolution of new forms of digital financial infrastructure. BigTech has played a particularly salient role in this development. In China, for example, BigTech mobile payments reached 16% of Gross Domestic Product ("GDP") in 2017, providing services to more than half of the overall population through the use of proprietary payment services without dependence on traditional banks.[98] The activities of these firms are rapidly expanding into credit provision, insurance, and investment services, creating complex interconnected webs across several sectors.[99] The situation is similar in Kenya, India and Russia, among an increasing range of other countries.

While in regions where incumbent bank-based payments are dominant, like the US or Europe, new payment services are still underpinned by traditional bank infrastructure—the growing market share of FinTech would foresee a convergence of traditional banking into a new infrastructure.[100] The rate and scope of such change, as exemplified by China, can cause tectonic shifts in financial structure.

Concerns about financial infrastructure are by no means new, with financial regulation focusing on payment systems since the failure of Bankhaus Herstatt in 1974 and on securities clearing and settlement systems particularly since the failure of the Hong Kong stock and futures exchanges in 1987, with both addressed by the Bank for International Settlements ("BIS") Committee on Payment and Settlement Systems and the International Organisation of Securities Commissions ("IOSCO"). Since 2008, concerns about and focus on "financial market infrastructures" ("FMIs") have increased dramatically, with leadership taken by the FSB and the renamed joint BIS-IOSCO Committee on Payment and Market Infrastructures. Since 2008, there has been an ongoing debate about risks in central clearing houses and whether the benefits in terms of reducing counterparty risk are exceeded by new risks of concentration and systemic reliance. The COVID-19 crisis has also highlighted the acute need to upgrade digital financial frameworks.[101]

Clearly, cybersecurity issues relate directly to derivatives central counterparties ("CCPs") and similar infrastructures. There are also TBTF/TCTF concerns, particularly as new entrants using new technologies such as blockchain or stablecoins try to disrupt existing markets and participants.

However, beyond these, we have also seen the emergence of new forms of digital financial infrastructure, particularly in the context of cloud services. Cloud services and cloud service providers are taking an increasing role in the financial sector. This

---

98 Jon Frost *et al*, "BigTech and the Changing Structure of Financial Intermediation" (2019) Bank for International Settlements Working Paper No 779, online: Bank for International Settlements <https://www.bis.org/publ/work779.htm> at 6.

99 *Ibid* at 7.

100 *Ibid* at 6; Carstens, *supra* note 69 at 3.

101 Arner *et al*, "Digital Finance & The COVID-19 Crisis", *supra* note 15.

is particularly the case with new FinTechs which are often cloud natives, with often their entire business being cloud based—an example of the extent to which digitisation and datafication have evolved. At the same time, traditional financial institutions are increasingly using cloud services to not only provide backup to existing systems but also to build new systems and in an increasing number of cases to replace existing outdated core systems (often based on old mainframes running seriously out-of-date software).

In the case of IT/data provision to financial intermediaries, the intermediaries are exposed to operational, in particular cyber, risks from those third-party service providers. For instance, when Amazon's cloud computing data centre in Hong Kong failed, the website of the US Securities and Exchange Commission ("SEC"), plus many consumer-oriented services, such as Netflix, went down.[102] We can also allocate here the development of large IT service platforms to which many financial intermediaries outsource core functions. For instance, Aladdin—the back-office software platform developed by Blackrock, the world's largest asset manager[103]—is relied on by approximately 25,000 investment professionals[104] around the world and is used to manage approximately 7 percent of the world's financial assets, including the assets of other top ten asset managers.[105]

Financial supervision typically does not apply to the Big Data providers. IT/data providers usually fall outside the scope of financial regulation: financial regulators lack information regarding such firms and their potential roles in interconnectivity across the financial sector as well as tools of supervision or regulation.

Financial law usually responds to risks created by non-supervised firms by imposing **strict outsourcing requirements** on financial firms. In particular, the financial firm needs to ensure systemic stability at all times, regardless of the outsourcing of information technology. But how should a bank (even a JP Morgan or Goldman Sachs) ensure that a major tech company (for example Amazon, Apple, Google or Microsoft) provide appropriate service? Banks cannot police firms whose market value is a multiple of that of their own (if worst came to worst, Apple could buy Deutsche Bank with its pocket cash), nor can they apply controls that ensure that BigTech's cloud centres work.

Such issues in the context of cloud services are leading to increasing discussion of whether such firms should be regarded as systemically important infrastructure providers and regulated accordingly, in the same way as certain payment systems or securities/CCPs. Related discussions are also taking place about whether or not cloud services are in fact a form of utility and need to be separated from other tech businesses.

The alternative to control over the service provider is **diversification**. For instance, financial law could require that any financial firm must have mirror cloud servers at three different providers, and that these providers be unrelated to each other. While

---

102 Elaine Ou, "Can't Stream Netflix: The Cloud May Be to Blame" *Bloomberg* (3 March 2017), online: Bloomberg <https://www.bloomberg.com/view/articles/2017-03-02/can-t-stream-netflix-the-cloud-may-be-to-blame>.

103 See Aladdin by BlackRock, online: BlackRock <https://www.blackrock.com/aladdin>.

104 Aladdin Platform Overview, online: BlackRock <https://www.blackrock.com/aladdin/offerings/aladdin-overview>.

105 "The monolith and the markets" *The Economist* (7 December 2013), online: The Economist <https://www.economist.com/briefing/2013/12/07/the-monolith-and-the-markets>.

mandatory diversification ensures some additional security and also has some positive effects on market structure in the provider market, it also comes with increased costs and other problems.

The first other problem is **cybersecurity**. The more providers hold the intermediaries' financial data, the greater is the risk of data corruption (stealing, manipulation or abuse) from the inside or a cyberattack from the outside. Second, mandatory diversification of data streams and server space **takes away some of the benefits of datafication**. It slows down IT processes and creates risk of confusion: If data are stored on a blockchain comprising many different cloud providers the storing of data on a blockchain itself costs time and resources. If a brokerage system runs on three different data streams simultaneously, and one of the streams shows different data from the other two, which of the three datasets is correct, and on which should the broker base a multi-billion USD transaction? These risks are exacerbated by the fact that the market for cloud storage and related analytics as well as data provision for financial markets is highly concentrated.[106] Financial intermediaries have little choice, and cyberattacks have easy targets.

Other examples come from reliance on a small number of data providers, which in turn raises risks of interconnections due to similarities of business models (as occurred with securitisation prior to 2008) as well as to concentration and reliance risks.

VI. The New Risk Paradigm: IT and Model Risk as Drivers of Systemic Risk

We do not believe that systemic risk will be created so large as to warrant intervention from new forms of tech investments into tech products, be it blockchain, cryptocurrencies or token sales. While the growth of initial coin offering volumes has been impressive indeed,[107] we lack evidence of significant involvement of regulated financial intermediaries in such products. Given the public statements by bank CEOs quite the opposite seems to be true.[108] However, this may change and first indicators of such a change may be found in the apparently growing numbers of so-called crypto hedge funds and regulated investment funds getting involved in those markets.[109] Given the rapid growth of the ICO markets, regulators are well advised to

---

106 See Zetzsche *et al*, *supra* note 7 at 31. See Douglas W Arner, Dirk A Zetzsche & Ross P Buckley, "FinTech, RegTech and Systemic Risk: The Rise of Global Technology Risk", in Arner *et al*, eds, *Systemic Risk in the Financial Sector: Ten Years after the Global Financial Crisis* (Ontario: CIGI Press, 2019).

107 See Zetzsche *et al*, *supra* note 5.

108 See *eg*, Anthony Cuthbertson, "Bitcoin trading comes to Goldman Sachs after investment bank hires first cryptocurrency trader" *The Independent* (3 May 2018), online: The Independent <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-trading-latest-goldman-sachs-digital-asset-trader-investment-banks-a8334171.html>; Tae Kim, "Jamie Dimon says he regrets calling bitcoin a fraud and believes in the technology behind it" *CNBC Markets* (9 January 2018), online: CNBC <https://www.cnbc.com/2018/01/09/jamie-dimon-says-he-regrets-calling-bitcoin-a-fraud.html>.

109 See Jemima Kelly & Maiya Keidan, "Bitcoin boom failing to attract big name investors" *The Independent* (23 October 2017) online: The Independent <https://www.independent.co.uk/news/business/news/bitcoin-investers-crypto-currencies-hedge-funds-a8014666.html>, citing Autonomous NEXT, *Crypto Fund List* (05 April 2010) online: Autonomous <https://next.autonomous.com/cryptofundlist/>.

enforce existing laws strictly, monitor developments closely and cooperate globally to ensure that systemic risk is kept under control.[110]

Rather, the clear risk of digitisation—a process which in many cases covers entire businesses—is that of security, namely cybersecurity and data protection. Even if policy makers and regulators follow our recommendations one thing does not change and cannot be changed: the dependence on technology and the exposure to tech and human failures. At the same time, financial risks have not been reduced. Cyber-risks, data risks, technological risks and financial risks accumulate. This new type of risk, tech risk, now comprises another major form of risk, alongside the other traditional categories of financial risks. Digitisation / datafication, cybersecurity and TBTF/TCTF considerations together create a world where the financial system is more vulnerable than before. At the same time, as the current pandemic has shown, digitisation is becoming ever more critical to the functioning of modern society.[111] Where tech risks are new drivers of instability, regulators are well advised to focus on these new forms of risk both independently and in terms of their connections to other forms of risk.

In a sense, many of the characteristics of the international financial system and its participants can be transposed to the international cyber networks and their participants—in particular, TechFins. Both concern large concentrated, relatively frictionless movements, necessitating increased transparency and control. Both are undergoing discussions regarding the merits of international centralisation, or regionalisation—except instead of currency, it is data. Both are now scrutinised for their potential volatility, risk susceptibility, and contagion effects. Both have demanded structural attention. It is therefore unsurprising that TechFins, through their growing roles in several concurrent fields—including finance—would require prudential regulation and supervision, for which previous experience can be a helpful compass.

To conclude, we present some basic principles of how cybersecurity and tech risks can be regulated and monitored, but also outline the deficiencies of existing / traditional approaches. The deficiencies in the regulatory system with regard to technology risks are similar to those that we experienced with respect to macroprudential risks prior to the 2008 GFC. Those deficiencies include lack of understanding, deficiencies in mandates, loopholes in regulation, lack of coordination among regulators, information asymmetries, lack of expertise on the part of financial intermediaries and regulators *etc*. We encourage a new risk agenda that responds to technology risks proactively.

In terms of importance, cybersecurity and tech risk, as categories of operational risk, have complemented (traditional) financial risks. Rather than market developments, we believe that tech risk functions as a new driver of potential instability, and that regulators are well advised to focus on this new risk category.

How should regulators respond to this new reality? The deficiencies in the regulatory system with regard to global technology risks are similar to those that we experienced with regard to other new forms of systemic risk prior to the GFC. Those deficiencies include loopholes in regulation, lack of coordination among regulators,

---

110 See Zetzsche *et al*, *supra* note 5.

111 Arner *et al*, "Digital Finance & The COVID-19 Crisis", *supra* note 15.

information asymmetry, lack of expertise on the side of financial intermediaries and regulators, and lack of awareness or investment on the side of intermediaries.

We encourage a new risk agenda that responds to global technology risks proactively. It should take into account insights from the COVID-19 epidemic, including that strategies should seek to support policy coordination and action in using digital channels to better direct resources, and that these channels must work well in times of disruption. Such an agenda must include, from a regulatory perspective, seven steps.[112]

First, regulators must **prioritise tech risks**, and this prioritisation must take place both internally and externally. The result of this prioritisation is that tech risks should play an equally important role as financial risks. This is particularly important in the context of monitoring these new sorts of risk and collecting non-traditional forms of information. This could be done by appointing a Chief Technology Risk Officer ("CTRO") for the supervisory authority or creating a similar role at board level in order to emphasise the significance of these sorts of risks. At the same time, financial intermediaries should be required to appoint CTROs or equivalent senior management officers responsible for cyber, technology and data risks, as a main contact point, with board monitoring, perhaps at the least in the context of any firm's risk committee. Further, the CTRO's report on cyberrisk should be a core agenda item at all meetings of the authorities' as well as of intermediaries' senior management.

Second, regulators need to **strengthen in-house tech expertise** to understand the sources of these new exposures of the ecosystems which they monitor and supervise, and to be able to discuss tech matters with intermediaries. We encourage, in particular, tech councils and tech expert groups at global policy bodies such as the FSB, IOSCO and others.

Third, regulators must continue to **enhance reporting requirements** with regard to details on the intermediaries' tech risk management strategies and the budget invested into and human resources devoted to systemic stability and cybersecurity. These reports should include tech details, and be read by the supervisor's tech department.

Fourth, **regulators must prioritise** these sorts of risks in the context of both on- and off-site supervision to understand whether intermediaries have understood those risks and how they address them; when they visit they need to speak to tech people rather than upper management or the legal department. Of course, on the authorities' side, technology and regulatory experts should be present as well.

Fifth, regulators must strive to **depoliticise** cybersecurity where related to financial stability, to foster the development of intergovernmental or sectoral networks capable of preventing and defending against cyber incidents, especially considering the growing financial interconnectedness. An isolated cybersecurity island that is still connected to the datafied financial network poses increasing risks of contagion.

Sixth, regulators will have to **make use of new technologies themselves**, since only the user understands the issues with the application. This can be part of a major RegTech strategy which—in many instances—is overdue anyway, in order to respond to the enormous data streams regulators receive in response to GFC-related additional reporting requirements. We admit that regulators may also suffer from

---

[112] We have advanced this agenda before in Arner, Buckley & Zetzsche, *supra* note 106 at 69.

the failures of technology, but if they do they will also learn to handle large tech projects—and know what they have to ask for from the intermediaries.

Seventh, regulators should continually seek to **harmonise** normative cyber and data policies to avoid friction and uncertainty, and not allow rules with potential impacts on financial stability to entrench themselves in the long run. This may prevent races to the bottom that can intensify destabilising behaviour.

The world has become riskier with tech risk becoming a prime driver of risk levels as a result of FinTech. The new tech risk will translate into financial risk sooner or later. A regulatory system that waits until financial risks have materialised as long-term impacts of tech risk has failed in its core function. Regulators need to face rather than fear the unknown and develop a degree of tech expertise matched only by the large—yet entirely unregulated—data driven firms. This is a very demanding challenge for all regulators and academics, but not one they can avoid.