Reinventing Operational Risk Regulation for a World of Climate Change, Cyberattacks, and Tech Glitches

Hilary J. Allen*

Around 30 years ago, banking regulators began to construct the concept of "operational risk," and devise rules to manage this newly created risk category. This "invention" of operational risk assembled a grab-bag of otherwise uncategorized risks associated with banking operations; this Article argues that the resulting operational risk regulation framework isn't very well suited to some of those risks. In particular, this Article demonstrates that the existing operational risk regulation framework is becoming an increasingly inadequate response to banks' exposure to operational losses following damage to their physical assets and business disruption and system failures. This is so for two reasons. First, the current iteration of operational risk regulation does not respond to the significant uncertainty affecting banking system operations, which is being exacerbated by increasing technological complexity, cyberattacks, and climate change. Second, existing regulation doesn't contemplate that operational risks can be transmitted to and from banks through technological and other non-financial channels, and so the potential for systemic contagion is underestimated.

This Article therefore sketches the beginnings of a "reinvented" approach to regulating for the operational threats of damage to physical assets and business disruption and system failures. The proposed framework places much less emphasis on risk-weighted capital regulation, favoring the alternative of simple buffers of equity that are more robust to uncertainty. In the absence of risk-weighted capital regulation, banking supervision will take on even greater importance. This Article therefore provides some guidance on what a "macro-operational" approach to banking supervision might look like, taking into account the possibility of technological and other forms of transmission of operational risk among banks. The Article concludes by recognizing that macro-operational supervision will not succeed in preventing all operational problems and therefore considers what new types of operations-specific emergency tools might need to be devised as a response.

---

* Professor of Law, American University Washington College of Law. Many thanks to Bryan Choi, Madison Condon, Thomas Eisenbach, Jordan Haedtler, and Alex Joel for reading and providing feedback on earlier drafts. This paper also benefitted enormously from comments and conversations during workshops at the Federal Reserve Bank, Reserve Bank of Australia, Banco de Portugal, the Fifth Conference on Law and Macroeconomics, and the Financial Institutions Section of the AALS Annual Meeting.

I. INTRODUCTION

Our economy depends on banks' continuing ability to make loans and process transactions, and so banking regulation has long sought to ensure that banks are prudently managing the credit and market risks associated with their lending and other activities.[1] Starting in the 1990s, however, banking regulators began to scrutinize "operational risk," a new category of risks that fell outside those traditional buckets of credit and market risks. In an article titled "The Invention of Operational Risk,"[2] Professor Michael Power demonstrated that this new category of "operational risk" was not an organic outgrowth of existing business practices, but was instead a newly constructed grab-bag of otherwise uncategorized risks associated with banking operations.[3] Thirty years later, as finance has become more technologically sophisticated (and therefore more vulnerable to both cyberattacks and accidents), and as climate events have become more frequent and more dire, it's time to *re*-invent how we think about and regulate operational risk.

The terms on which banks' operational risks are regulated, as well as the construction of the concept itself, have largely been established by the Basel Committee on Banking

1. RICHARD SCOTT CARNELL ET AL., THE LAW OF FINANCIAL INSTITUTIONS 100 (7th ed. 2021).
2. Michael Power, *The Invention of Operational Risk*, 12 REV. INT'L POL. ECON. 577 (2005).
3. *Id.* at 578–79.

Supervision (BCBS),[4] an international body comprised of financial regulators and central bankers drawn from advanced economies around the world.[5] The BCBS defines "operational risk" as "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events,"[6] and subdivides operational loss events into seven categories.[7] The most frequently occurring operational loss events tend to relate to fraud or mistakes made by human beings working within the bank[8]—operational risk is often seen as "the risk that someone will do something stupid or bad."[9] But some of the BCBS's categories of operational loss events are not like the others, and this Article argues that the existing operational risk regulation framework is becoming increasingly ill-suited to addressing operational loss events that fit into the categories of "damage to physical assets" and "business disruption and system failures." It argues further that these latter kinds of operational loss events should be managed primarily through banking supervision, instead of risk-weighted capital requirements.

The inadequacy of the current approach stems in large part from the uncertainty associated with these kinds of operational loss events, which are often the product of cascade failures within complex systems.[10] This Article relies heavily on the complex systems literature to explain how these kinds of events transpire, and also to explain that even though we understand the general dynamics of cascade failures, we can't predict precisely when they will occur or how they will transpire.[11] To use the framing of economist Frank Knight, these events are characterized by uncertainty, rather than risk.[12] Because of this uncertainty, any operational risk regulation framework that relies primarily on measuring amounts and probabilities of operational losses is a poor fit. And, as this Article will argue, the incidence of cascade failures impacting bank operations is likely to increase as a

4. *See* Peter Sands, Gordon Liao & Yueran Ma, *Rethinking Operational Risk Capital Requirements*, 4 J. FIN. REG. 1, 6 (2018) (detailing the BCBS's introduction of operational risk regulation following the 1995 collapse of Barings Bank).

5. *The Basel Committee - Overview*, BANK FOR INT'L SETTLEMENTS [BIS] (2024), https://www.bis.org/bcbs/ [https://perma.cc/25UK-GKV4].

6. *Revisions to the Principles for the Sound Management of Operational Risks*, BANK FOR INT'L SETTLEMENTS [BIS] 2 (2021), https://www.bis.org/bcbs/publ/d515.pdf [https://perma.cc/F52W-E4FY] [hereinafter *Revised PSMOR*].

7. These are (i) internal fraud; (ii) external fraud; (iii) employment practices and workplace safety; (iv) clients, products & business practices; (v) damage to physical assets; (vi) business disruption and system failures; and (vii) execution, delivery & process management. *QIS 2 - Operational Risk Loss Data*, BANK FOR INT'L SETTLEMENTS [BIS] 12–13 (2001), https://www.bis.org/bcbs/qisoprisknote.pdf [https://perma.cc/7H77-KDPY].

8. *See infra* notes 90–93 and accompanying text (explaining that the most common operational loss events in banking often stem from fraud or errors committed by human employees within the bank).

9. Victoria Guida (@vtg2), X (June 27, 2022), https://twitter.com/vtg2/status/1541537111291092993 [https://perma.cc/R5AU-P7KX].

10. *See infra* Part III.

11. The complexity science literature cited in this paper includes: David L. Alderson & John C. Doyle, *Contrasting Views of Complexity and Their Implications for Network-Centric Infrastructures*, 40 IEEE TRANSACTIONS ON SYS., MAN, & CYBERNETICS 839 (2010); SAMUEL ARBESMAN, OVERCOMPLICATED: TECHNOLOGY AT THE LIMITS OF COMPREHENSION (2016); Dirk Helbing, *Globally Networked Risks and How to Respond*, 497 NATURE 51 (2013); CHARLES PERROW, NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES 5 (1999); J.B. Ruhl, *Managing Systemic Risk in Legal Systems*, 89 IND. L.J. 559 (2014).

12. "There is a fundamental distinction between the reward for taking a known risk and that for assuming a risk whose value itself is not known." FRANK H. KNIGHT, RISK, UNCERTAINTY, AND PROFIT 43–44 (1921). Knight goes on to say that uncertainty is "not susceptible to measurement." *Id.* at 48.

consequence of both climate change and increasing reliance on increasingly complex information technology systems.

As the earth warms, the incidence of severe weather events is increasing, and these events may threaten banks' data centers or knock out electrical grids or telecommunications lines, compromising bank operations.[13] Banks' operations could similarly be compromised by a cyberattack that targets data centers, electrical grids, telecommunication lines, or other aspects of banks' information technology systems.[14] Although banks cannot predict when they will be targeted by a cyberattack, or what form the cyberattack will take, it is now almost an inevitability that a bank will be targeted in some way.[15] Even in the absence of any cyberattack, the increasing complexity of banks' information technological systems makes them more vulnerable to "normal accidents", where a seemingly small technological glitch can cascade into a much bigger problem with the system.[16]

We shouldn't assume that the impact of these kinds of cascade failures will be confined within a single bank—but the existing bank operational risk regulation framework tends to make this mistake, by and large. "Operational risk is usually perceived as idiosyncratic with limited systemic implications," and so operational risk regulation tends to leave banks to manage operational risk in isolation, within their own risk tolerances.[17] This Article will explore how operational risks might be transmitted among banks—not just because a bank experiencing an operational problem may default on their obligations to other banks or become insolvent (these kinds of transmission channels are contemplated by existing operational risk regulation), but also because operational problems might be transmitted directly from bank to bank through technological channels.[18] Cascade failures could also be transmitted through other non-financial connections within the broader social-economic-technological "system of systems" of which the financial system is a part, potentially impacting banks with a succession of compounding operational threats.[19]

It may be that, behind the scenes, financial regulators are starting to update their thinking on operational risk and recognize that it's not so idiosyncratic[20]—but no such shift is evident in the official statements or standards promulgated by the BCBS. Operational risk regulation should be formally updated, both to make operational risk regulation more robust to uncertainty, and to give it a more "macro" or systemic focus—at least with regard to the types of operational problems that lead to "damage to physical assets" and "business

13. *See infra* Part III.A.1.

14. *See infra* Part III.A.2.

15. *See* THOMAS M. EISENBACH, ANNA KOVNER & MICHAEL JUNHO LEE, CYBER RISK AND THE US FINANCIAL SYSTEM: A PRE-MORTEM ANALYSIS 1 (2020) ("Almost every financial stability survey includes cyber attacks among the top risks.").

16. *See infra* Part III.A.3.

17. Allen N. Berger et al., *Operational Risk is More Systemic than You Think: Evidence from U.S. Bank Holding Companies*, 143 J. BANKING & FIN. 1, 2 (2022) (citation omitted).

18. *See infra* Part III.A.1.

19. *See infra* Part III.A.2.

20. For example, the Acting Comptroller of the Currency (i.e. the primary regulator for national banks in the United States), said in a recent speech that "[w]e are building on the excellent work of staff over the last five years . . . related to IT and operational resilience supervision," suggesting that some of the issues discussed in this Article may already be on regulators' radars. Acting Comptroller of the Currency Michael J. Hsu, Safeguarding Trust in Banking: An Update, Remarks at the TCH + BPI Annual Conference 7 (Sept. 7, 2022), transcript available at https://occ.gov/news-issuances/speeches/2022/pub-speech-2022-106.pdf [https://perma.cc/NQ5R-KYP4].

disruption and system failures." After the 2008 financial crisis, there was "a simple recognition that the previous intellectual framework—focused on microprudential risk—was not fit for purpose."[21] Increased technological sophistication and interactive complexity, coupled with the impacts of climate change, should force a recognition that the current intellectual framework around operational risk is similarly unfit for purpose. In particular, as we look at this new generation of threats, historic losses become less relevant to the assessment of operational risk, and a more precautionary focus on near misses and potential losses must come to the fore.[22]

Practically speaking, this means that less emphasis should be placed on measurement, and more emphasis must necessarily be placed on skilled intuition and discretionary supervision. This Article will argue that the BCBS's risk-weighted capital framework is an inappropriate response to threats of "damage to physical assets" and "business disruption and system failures," and that it should be revised to require banks to simply fund their investments with more equity to cushion against uncertain events. If capital requirements are no longer being used to manage banks' preparation for and responses to these types of uncertain operational risks, then regulators' supervision of banks will become increasingly important. This Article sets out the beginnings of what a revised supervisory framework should look like for these kinds of operational risks.

The new supervisory framework should be principles-based and require banks to reckon with the increasing inevitability of major operational disruptions. In some instances, prescriptive minimum technical standards will be needed for banks' technological systems, but they should be a floor that banks are directed to build upon in light of evolving technologies and threats. To facilitate a better understanding of such evolving technologies and threats, a principles-based reporting regime around technological systems and operational problems (and near misses) is needed, as are exploratory scenario analysis exercises that generate insight into how new types of operational problems may spread and interact within the financial system—and within our broader social-economic-technological "system of systems".

After all, concerns about broader systems of systems are what motivated the adoption of banking regulation in the first place: banks are not ends in themselves but are instead important auxiliaries that facilitate economic growth through activities like extending credit and processing transactions.[23] As a complement to regulatory strategies designed to make banking operations more robust, we also need to develop new emergency response tools that can be applied if operational problems nonetheless threaten the functioning of the banking system. The emergency response tools we have now were designed to assist banks experiencing liquidity, rather than operational, problems[24]—relying on the complex

21. Hugues Chenet, Josh Ryan-Collins & Frank van Lerven, *Finance, Climate-Change and Radical Uncertainty: Towards a Precautionary Approach to Financial Policy*, 183 ECOLOGICAL ECON. 1, 7 (2021).

22. For elaboration on the argument for a more precautionary approach to financial stability regulation, see Hilary J. Allen, *A New Philosophy for Financial Stability Regulation*, 45 LOY. U. CHI. L.J. 173 (2013). On framing the distinction between historical losses on the one hand and near misses and potential losses on the other, see Power, *supra* note 2, at 586.

23. Although sometimes this is lost sight of. *See* Mehrsa Baradaran, *Banking and the Social Contract*, 89 NOTRE DAME L. REV. 1283, 1284 (2014).

24. For an overview of these "ex post" tools, see Iman Anabtawi & Steven L. Schwarcz, *Regulating Ex Post: How Law Can Address the Inevitability of Financial Failure*, 92 TEX. L. REV. 75, 102–22 (2013).

systems literature, this Article proposes new tools designed to ensure the continuity of the banking operations that our economy depends upon. Ultimately, this Article's proposals may result in a banking system that is less efficient in the short term, but in complex systems, some amount of efficiency will need to be sacrificed for a system to be robust in the long term.[25]

The remainder of this Article will proceed as follows. Part II will provide a brief history of how operational risk regulation came to be "invented" in the first place, and how it has evolved since that first invention. This provides context for Part III, which explores why the existing construct of operational risk is inadequate, both because it does not respond to the uncertainty around the operational impacts of climate change, cyberattacks, and technological glitches, and because it does not cater to the possibility of compounding failures or purely technological channels for transmitting operational risks from bank to bank. Part IV therefore proposes a reinvented operational risk regulation framework, with less emphasis on risk-weighted capital requirements and more emphasis on regulatory strategies that anticipate systemic interactions and are robust to uncertainty. Part V concludes.

II. A BRIEF HISTORY OF OPERATIONAL RISK REGULATION

When it comes to risk management, "operational risk" has never been the primary concern of banks, or of banking regulation—indeed, it is only relatively recently that any common framework for thinking about operational risks was formulated at all.[26] In contrast, banks have always been highly attuned to both market risk and credit risk as integral parts of their business model, and banking regulation has largely focused its attention on these kinds of risks as well.[27] Market risk relates to the many different kinds of changes that can happen in the marketplace and impact the value of an asset (for example, changes in interest rates will impact the value of a fixed-rate mortgage loan made by a bank).[28] Credit risk is the risk that a counterparty will not be able to deliver on its obligations (for example, the borrower may default on that mortgage loan).[29]

Banks have always been vulnerable to failure if they mismanaged their own credit and market risks; in the 1970s, regulators started to worry that the consequences of such mismanagement could spill over and have negative impacts on other banks—even in other countries. A consensus began to emerge among policymakers, particularly following the failure of the German Bankhaus Herstatt, that there needed to be more consistent supervision of banks' risk-taking across jurisdictions.[30] In response, a global group of central bankers known as the Basel Committee on Banking Supervision (the "BCBS") was formed

25. Ruhl, *supra* note 11, at 594.

26. "Although the term 'operations risk' existed in 1991 as a generic concept, the category of 'operational risk' did not acquire widespread currency until the mid to late 1990s." Power, *supra* note 2, at 579.

27. "Operational risk in the banking industry started life as a residual category, something left over from market and credit risk management practices . . . ." *Id.*

28. Erik F. Gerding, *Code, Crash, and Open Source: The Outsourcing of Financial Regulation to Risk Models and the Global Financial Crisis*, 84 WASH. L. REV. 127, 137–38 (2009).

29. *Id.* at 137.

30. DAVID ZARING, THE GLOBALIZED GOVERNANCE OF FINANCE 46 (2020).

and started to focus its attention on regulatory capital requirements as the centerpiece of bank regulation.[31]

Regulatory capital requirements are rules that require banks to fund their investments with more loss-absorbent equity, with the aim of improving both their own stability and the stability of domestic and global financial systems more broadly.[32] The BCBS issued its first accord on regulatory capital in 1988.[33] This accord, which subsequently became known as Basel I, focused primarily on credit risk.[34] Basel I made several mentions of the impact of market risk on asset pricing but did not mention the term "operational risk".[35] This omission is not surprising, as banks themselves did not regularly use the term "operational risk" at that time, at least not in any consistent way.[36] The conceptualization of "operational risk" as a distinct category of risk against which capital should be held was spurred in many ways by the failure of Barings Bank in 1995, following unauthorized trading by bank employee Nick Leeson.[37] Although the BCBS had already started looking at deficiencies in banks' internal controls and information systems before that time,[38] the Barings Bank failure helped crystallize the growing consensus that operational risk was no longer something that could simply be left to individual business units within the banks.[39] Under the new approach, banks' senior management needed to adopt an enterprise-wide approach to managing operational risks.[40]

To my knowledge, the first BCBS publication on operational risk was released in 1998: a short conceptual paper simply titled "Operational Risk Management".[41] The focus of this piece was on what it deemed "the most important types of operational risk": "breakdowns in internal controls and corporate governance."[42] While it was understood that credit and market risk often arose from things happening outside of the bank, most operational risk factors were viewed as "largely internal to the bank."[43] Technology failures and natural disasters were mentioned, but were described as "other aspects of operational risk."[44]

---

31. *History of the Basel Committee*, BANK FOR INT'L SETTLEMENTS, https://www.bis.org/bcbs/history.htm [https://perma.cc/FGF3-V73P].

32. JOHN ARMOUR ET AL., PRINCIPLES OF FINANCIAL REGULATION, 290–92 (2016).

33. *History of the Basel Committee*, *supra* note 31.

34. *International Convergence of Capital Measurement and Capital Standards*, BANK FOR INT'L SETTLEMENTS [BIS] 10 (1988), https://www.bis.org/publ/bcbs04a.pdf [https://perma.cc/2TRN-MCTL] "[C]redit risk . . . was the focus of the 1988 Accord." *History of the Basel Committee*, *supra* note 31.

35. *International Convergence of Capital Measurement and Capital Standards*, BANK FOR INT'L SETTLEMENTS [BIS] (1998), https://www.bis.org/publ/bcbsc111.pdf [https://perma.cc/DD9K-SF5H] (containing no instances of the phrase "operational risk").

36. "'[O]perational risk' scarcely existed as a category of practitioner thinking in the early 1990s." Power, *supra* note 2, at 579.

37. Gara Afonso, Filippo Curti & Atanas Mihov, *Coming to Terms with Operational Risk*, FED. RSRV. BANK N.Y. (Jan. 7, 2019), https://libertystreeteconomics.newyorkfed.org/2019/01/coming-to-terms-with-operational-risk [https:perma.cc/YR3F-AAE6].

38. Power, *supra* note 2, at 579.

39. Sands, Liao & Ma, *supra* note 4, at 6.

40. "The consensus among banks was that 'the primary responsibility for management of operational risk is the business unit'." *Id.*

41. *Operational Risk Management*, BANK FOR INT'L SETTLEMENTS [BIS] (1988), https://www.bis.org/publ/bcbs42.pdf [https://perma.cc/GU3V-ET5D].

42. *Id.* at 1.

43. *Id.*

44. *Id.*

In 2004, the BCBS substantially revised its regulatory capital requirements to make them more sensitive to credit, market, *and* operational risks, in a set of standards known as Basel II.[45] Basel II introduced a new "three pillar" approach to capital regulation. Pillar 1 refers to the updated version of Basel I's minimum regulatory capital requirements—since the adoption of Basel II, in calculating their risk-weighted assets, banks must consider the operational risks they are exposed to in addition to their credit and market risks.[46] Pillar 2 requires "supervisory review of an institution's capital adequacy and internal assessment process," while Pillar 3 requires "effective use of disclosure as a lever to strengthen market discipline and encourage sound banking practices."[47] Pillars 2 and 3 relate to operational risk, as well as credit and market risk.[48]

As a necessary part of these changes, Basel II included a definition of "operational risk" for the first time.[49] There was some back and forth on what should and should not be included,[50] but the definition the committee ultimately settled upon was: "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk."[51]

There are some pertinent things to note about how this definition has constructed the concept of operational risk. One is that it was *not* originally intended to include systemic risk: in an early Working Paper on the Regulatory Treatment of Operational Risk, the BCBS's Risk Management Group confirmed that their definition of operational risk "does not include systemic risk and the operational risk charge will be calibrated accordingly."[52] Another takeaway is that the Risk Management Group made clear that the causes of operational risk they were concerned about could be grouped into four categories—"people, processes, systems and external factors."[53] Ultimately, however, operational loss types were broken out into categories that aligned with the industry's "standardised business lines and 'event types'" to facilitate measurement and reporting.[54] The seven categories of relevant loss events that were ultimately adopted were: (i) internal fraud; (ii) external fraud; (iii) employment practices and workplace safety; (iv) clients, products & business

45. *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, BANK FOR INT'L SETTLEMENTS [BIS] (2004) [hereinafter *Basel II*], https://www.bis.org/publ/bcbs107.pdf [https://perma.cc/8JXC-V5TU]. This "Revised Framework" subsequently became known as "Basel II". *See The Application of Basel II to Trading Activities and the Treatment of Double Default Effects*, BANK FOR INT'L SETTLEMENTS [BIS] 1 (2005) [hereinafter *Application of Basel II*], https://www.bis.org/publ/bcbs116.pdf [https://perma.cc/6VKK-TTX4] ("The "Basel II" framework, or Revised Framework, as the new standard is frequently called . . . ."). On Basel II's increased risk sensitivity, *see* Jeremy C. Kress, *Banking's Climate Conundrum*, 59 AM. BUS. L.J. 679, 688–90 (2022).

46. Sands, Liao & Ma, *supra* note 4, at 7–8.

47. *History of the Basel Committee*, *supra* note 31.

48. *Basel II*, *supra* note 45, at 160–61, 166, 168.

49. Afonso, Curti & Mihov, *supra* note 37.

50. *See* Power, *supra* note 2, at 584 ("[T]he project of defining operational risk is more than a simple matter of labelling; it involves work, often competitive work, to construct a concept in which different interests and ambitions can be represented.").

51. *Basel II*, *supra* note 45, at 137.

52. *Working Paper on the Regulatory Treatment of Operational Risk*, BANK FOR INT'L SETTLEMENTS [BIS] 2 (2001), https://www.bis.org/publ/bcbs_wp8.pdf. [https://perma.cc/B7PU-CXJZ]

53. *Id.*

54. *Id.* at 3.

practices; (v) damage to physical assets; (vi) business disruption and system failures; and (vii) execution, delivery & process management.[55]

The overall impression that one has from reading these materials is that the BCBS viewed the different kinds of operational risks as things that banks could measure and mitigate and that operational risk regulation should be designed to encourage banks to do so. However, measuring operational risk to determine the appropriate capital charge under Pillar 1 is challenging.[56] Because the measurement will impact the amount of capital a bank is required to fund its investments with, banks have incentives to minimize such measurements.[57] To quote an FDIC publication, "[c]onceptually, the operational risk capital estimate can be expressed as protection against expected and unexpected future losses at a selected confidence level, with some provisions for offsetting portions of this exposure through reserves or other permitted mitigation techniques (namely insurance)."[58] In practice, this entails using historical data available about past operational losses as well as information about the bank's current operations to come up with the number representing the bank's risk-weighted assets[59]—the lack of analytical rigor associated with this calculation has been criticized.[60]

Pillar 2 is more discretionary: if supervisors evaluating operational risk management detect deficiencies, they are directed to "use the tools most suited to the particular circumstances of banks and their operating environment."[61] To help guide supervisors and banks, the BCBS published the first version of its "Sound Practices for the Management and Supervision of Operational Risk" in 2003,[62] which outlined regulators' expectations for how banks should manage their operational risks with "appropriate internal processes, audit

---

55. *Id.* at 21–23.

56. For instance, Sands, Liao & Ma observe that when calculating risk-weighted assets ("RWA"):

> [T]here is significant variation in the percentage of a bank's total RWA contributed by operational RWA. Some of this variation can be explained by differences in strategy and business model (e.g. the fact that among the GSIBs, State Street and Bank of New York Mellon have the highest proportions of operational RWA reflects their focus on custody and settlement services rather than traditional lending), but many of the differences appear to reflect differences in the approach towards determining operational RWA across banks and regulatory jurisdictions, rather than differences in the underlying operational risk profile.

Sands, Liao & Ma, *supra* note 4, at 3.

57. For a discussion of banks' incentives to arbitrage regulatory capital requirements (which arise largely as a result of tax policy and government subsidies), see Hilary J. Allen, *Let's Talk About Tax: Fixing Bank Incentives to Sabotage Stability*, 18 FORDHAM J. CORP. & FIN. L. 821, 831–37 (2013).

58. FDIC, *Operational Risk Management: An Evolving Discipline*, 3 SUPERVISORY INSIGHTS 4, 9 (2006).

59. Christina Parajon Skinner, *Misconduct Risk*, 84 FORDHAM L. REV. 1559, 1592–93 (2016).

60. Sands, Liao & Ma, *supra* note 4, at 3; *see also* Francisco Covas et al., *A Modification to the Basel Committee's Standardized Approach to Operational Risk*, BANK POL'Y INST. (May 4, 2022), https://bpi.com/a-modification-to-the-basel-committees-standardized-approach-to-operational-risk/ [https://perma.cc/9A4U-TLZE] ("Although the Basel Committee defined the AMA operational-risk exposure as the 99.9th percentile of the distribution of aggregate operational-risk losses over a one-year horizon, making such an estimation with any degree of accuracy is impossible, so taking such estimates seriously is silly. In practice, banks could use various models including scenario analysis or extreme value theory to quantify operational risk.").

61. *Revised PSMOR*, *supra* note 6, at 19.

62. *Sound Practices for the Management and Supervision of Operational Risk*, BANK FOR INT'L SETTLEMENTS [BIS] (2003), https://www.bis.org/publ/bcbs96.pdf [https://perma.cc/R56P-KAXV].

programs, insurance protection, and other risk management tools."[63] As we will discuss shortly, these have been incrementally updated over the years, and are now embodied in a document titled "Principles for the Sound Management of Operational Risk" (often abbreviated to PSMOR).

Following the financial crisis of 2007–08, many parts of the Basel banking supervision framework underwent significant revision in what has come to be known as Basel III.[64] These updates reflect important lessons learned from the crisis, particularly that steps taken by individual institutions to manage their credit, market, and liquidity risks might protect those institutions from failure, but at the same time make the financial system as a whole more fragile.[65] The pre-crisis "microprudential" perspective, which was based on assumptions that systemic risk could be managed simply by making sure that individual banks had robust risk-management systems,[66] has been supplemented with some "macroprudential" measures, like regulatory capital "buffers" (these reduce the chance that banks will have to sell assets to stay in compliance with their regulatory capital requirements, which could potentially hurt other banks by depressing asset values).[67] Macroprudential regulation would certainly benefit from more thought and experimentation,[68] but the macroprudential mindset is an improvement over the pre-crisis status quo.

The regulatory treatment of operational risk regulation was not updated as part of the initial Basel III reform, however.[69] Later revisions to Basel III adopted in 2017 did make some changes to how operational risks affected the risk weighting of assets for Pillar 1,[70] but there was no fundamental rethinking or shift to a more "macro" approach.[71] With regard to Pillar 2, the Principles for the Sound Management of Operational Risk were updated in 2011 ("to reflect the enhanced sound operational risk management practices now in use by the industry"[72] as well as lessons from the crisis of 2007–08), and then revised again in 2021.[73] The 2021 Revisions to the Principles for the Sound Management of Operational Risk are intended to provide more guidance on how to implement the Principles in order to conform to the 2017 revisions to Basel III.[74] Also in 2021, the BCBS adopted new

63. FDIC, *supra* note 58, at 4.

64. *Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems*, BANK FOR INT'L SETTLEMENTS [BIS] (2010), http://www.bis.org/publ/bcbs189.pdf [https://perma.cc/CEE9-FLHG].

65. Samuel G. Hanson, Anil K. Kashyap & Jeremy C. Stein, *A Macroprudential Approach to Financial Regulation*, 25 J. ECON. PERSPS. 3, 5 (2011).

66. ARMOUR ET AL., *supra* note 32, at 409.

67. *Id.* at 417. It should be noted, however, there is some critique of whether these kinds of measures truly live up to the claim of being "macroprudential". *Id.* at 418; *see also* Jeremy C. Kress & Jeffrey Zhang, *The Macroprudential Myth*, 112 GEO. L.J. (forthcoming 2024).

68. Kress & Zhang, *supra* note 67, at 6–9.

69. Skinner, *supra* note 59, at 1592.

70. *Basel III: Finalising Post-Crisis Reforms*, BANK FOR INT'L SETTLEMENTS [BIS] 128–36 (2017), https://www.bis.org/bcbs/publ/d424.pdf [https://perma.cc//28FP-R8BE].

71. "Basel III's finalized regulatory standards will have less impact than was first assumed." Thomas Poppensieker et al., *Basel III: The Final Regulatory Standard*, 5 MCKINSEY ON RISK & RESILIENCE 3, 3 (2018) (on file with the *Journal of Corporation Law*).

72. *Principles for the Sound Management of Operational Risk*, BANK FOR INT'L SETTLEMENTS [BIS] 1 (2011), https://www.bis.org/publ/bcbs195.pdf [https://perma.cc/H72W-C3JF].

73. *Revised PSMOR*, *supra* note 6, at 1.

74. *Id.* at 1.

Principles of Operational Resilience in light of the increased frequency of natural disasters and technology failures, amongst other things.[75]

The latest version of the Principles for the Sound Management of Operational Risk includes twelve principles. Many of these relate to bank governance, calling for the establishment of policies relating to the identification and assessment of operational risks, and the development of monitoring, reporting, and mitigation mechanisms in accordance with those policies.[76] Principle 4, for example, provides that "[t]he board of directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk the bank is willing to assume."[77] Some principles are more specific to the kinds of operational risks discussed in this Article, including Principle 10 (which requires banks to implement a robust information and communication technology risk management program)[78], and Principle 11 (which requires banks to have "business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption").[79]

Principles 10 and 11 are very pertinent to this Article's discussion of operational risks arising from climate change and increased technological sophistication. So are the Principles for Operational Resilience, where the BCBS articulated its view that:

> [F]urther work is necessary to strengthen banks' ability to absorb operational risk-related events, such as pandemics, cyber incidents, technology failures and natural disasters, which could cause significant operational failures or wide-scale disruptions in financial markets. In light of the critical role that banks play in the operation of the global financial infrastructure, increasing their resilience would provide additional safeguards to the financial system.[80]

The BCBS recognizes that not all operational losses can be avoided, but these principles proceed from the position that "it is possible to improve the resilience of a bank's operations to such events."[81] These Principles for Operational Resilience require the development of business continuity plans for use in "severe but plausible scenarios" (Principle 3),[82] as well as incident response and recovery procedures (Principle 6).[83] Banks are also required to take steps to understand their dependencies on third-party vendors and others (Principles 4 and 5).[84] Principle 7 makes express reference to the need for banks' information and communication technology risk management programs to take cybersecurity into account.[85]

The recent adoption of the Principles for Operational Resilience, as well as the recent update of the Principles for the Sound Management of Operational Risk, are positive

---

75. *Principles for Operational Resilience*, BANK FOR INT'L SETTLEMENTS [BIS] 1 (2021), https://www.bis.org/bcbs/publ/d516.pdf [https://perma.cc/S69F-UT3E].

76. *Revised PSMOR*, *supra* note 6, at 5–18.

77. *Id.* at 8 (citation omitted).

78. *Id.* at 16.

79. *Id.* at 17.

80. *Principles for Operational Resilience*, *supra* note 75, at 1.

81. *Id.* at 2.

82. *Id.* at 5.

83. *Id.* at 7.

84. *Id.* at 6–7.

85. *Principles for Operational Resilience*, *supra* note 75, at 7–8.

developments. As the next Part will demonstrate, though, these do not go far enough in adjusting operational risk regulation to meet banking's new realities.

III. THE INADEQUACIES OF EXISTING OPERATIONAL RISK REGULATION

An important takeaway from the previous Part is that the concept of "operational risk" (at least as it applies in the banking sector) was intentionally constructed in the 1990s and early 2000s, as a catch-all category for risks that didn't fall easily into the more-established and intuitive buckets of credit and market risks.[86] There is some coherence to the concept of operational risk, to the extent that (unlike credit and market risks) banks don't affirmatively take on operational risk as a profit-making enterprise.[87] However, the various causes of operational loss diverge significantly and may need to be managed in very different ways. This Article argues that an unfortunate consequence of the way operational risk regulation has been constructed is that it puts more emphasis on the risks that can more easily be measured, notwithstanding that more uncertain events may be more consequential.[88] These more uncertain operational loss categories are not adequately served by the existing operational risk regulation framework.

Economists studying operational risk typically rely upon historical loss data that has been categorized to fit within the BCBS framework.[89] Using this data, Chernobai, Ozdagli & Wang indicate that operational risk is primarily "created by sources internal to the firm and is a result of control failures."[90] Aldasoro et al. state that "improper business practices . . . account for the lion's share of operational losses."[91] Of the seven categories of loss events determined by the BCBS, the most commonly occurring historically are: (i) internal fraud; (ii) external fraud; (iii) clients, products & business practices; and (iv) execution, delivery & process management.[92] Clients, products & business practices became a particularly significant source of operational losses as a result of lawsuits and fines levied against banks in the wake of the financial crisis of 2007–08, although losses in this category have become fewer in recent years.[93]

Historically, damage to physical assets and business disruption and system failures (the categories of loss events most clearly associated with natural disasters and technology problems) have been less frequent: [94] in many respects, these kinds of loss events are

86. Power, *supra* note 2, at 579. As the BCBS observed in 2003, "what is relatively new is the view of operational risk management as a comprehensive practice comparable to the management of credit and market risk in principle." *Sound Practices for the Management and Supervision of Operational Risk*, *supra* note 62, at 3.

87. *Sound Practices for the Management and Supervision of Operational Risk*, *supra* note 62, at 3.

88. *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions*, FIN. STABILITY BD. [FSB] 3 (2020), https://www.fsb.org/wp-content/uploads/P091020.pdf [https://perma.cc/Y8FS-A273].

89. Anna Chernobai, Ali Ozdagli & Jianlin Wang, *Business Complexity and Risk Management: Evidence from Operational Risk Events in U.S. Bank Holding Companies*, 117 J. MONETARY ECON. 418, 422–23 (2021). *See also* Berger et al., *supra* note 17; Iñaki Aldasoro et al., *Operational and Cyber Risks in the Financial Sector*, INT'L J. CENT. BANKING, Dec. 2023, at 341.

90. Chernobai, Ozdagli & Wang, *supra* note 89, at 419.

91. Aldasoro et al., *supra* note 89, at 345.

92. Chernobai, Ozdagli & Wang, *supra* note 89, at 422.

93. Aldasoro et al., *supra* note 89, at 342–43.

94. *Id.* at 356.

quintessential tail events—low probability, but potentially very high consequence.[95] Given their low probability, it is not surprising that we don't have that much data about these types of operational losses,[96] but their unexpected nature could prove very destabilizing for a financial institution, and the financial system more broadly.[97] As technological systems become more complex and natural disasters become more frequent, the operational risk categories of internal fraud, external fraud, clients, products & business practices, and execution, delivery & process management may not be the ones that matter most. In fact, the risks that matter most may not technically qualify as "risks" at all. Famed economist Frank Knight described "risk" as something that lends itself to measurement because it occurs with a known probability.[98] However, where the possible outcomes themselves—let alone their probabilities—are unknown, what we're dealing with is not so much risk as "uncertainty"[99] which cannot be accurately measured.

Much of the uncertainty around potential manifestations of damage to physical assets or business disruption and system failures arises because of complexity: interdependent components of complex systems interact and adapt in complex ways that can't be predicted simply by looking at the components in isolation, so we can't always predict cause and effect.[100] Instead, these systems are susceptible to what are known as "normal accidents"—debilitating problems that result from "cascade failures" that can be unexpectedly triggered by seemingly random and minor events.[101] When it comes to normal accidents, it is not the triggering event that should be the primary concern of those seeking to maintain the resilience of the system—the fragility created by the complexity of the system is the primary culprit and should be the focus of regulation.[102]

There are several complexity science concepts to unpack here. First is the term "complex adaptive system." I am using the term to describe a system where "large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing, and adaptation via learning or evolution."[103] These systems are often described as "robust yet fragile," as attempts to make their components more robust inadvertently add more complexity to the interactions among those components, making them more susceptible to normal accidents.[104] The term "normal accident" was coined by Charles Perrow to describe accidents that are produced when a seemingly minor problem is able to cascade through a system because of that system's interactive complexity and tight coupling.[105] In other words, problems are

95. *Id.* at 343 n.3.

96. For example, observe that "[d]ata on cyber incidents [is] scarce and thus quantitative analyses on the impact of cyber events is challenging." *Id.* at 347.

97. Berger et al., *supra* note 17, at 14.

98. KNIGHT, *supra* note 12, at 48.

99. *Id.*

100. Ruhl, *supra* note 11, at 567.

101. PERROW, *supra* note 11, at 5.

102. *See* ARBESMAN, *supra* note 11, at 12 (attributing infamous mechanical failures to the "system[s'] massive complexity").

103. MELANIE MITCHELL, COMPLEXITY: A GUIDED TOUR 13 (2009).

104. Ruhl, *supra* note 11, at 562.

105. PERROW, *supra* note 11, at 5.

transmitted as a result of often unexpected interactions between system components, with those interactions magnifying the problem as the failure cascades through the system.[106]

Within complex adaptive systems, cascade failures can happen like dominos knocking one another over, with the failure of each component successively causing the failure of linked components.[107] Cascade failures can also happen, though, in a way that leaves some components still standing and able to keep transmitting problems to other components elsewhere in the system (an illustration of the "robust yet fragile" dynamic).[108] These latter failures are sometimes referred to as "overload failures":

> [O]verload failures occur when the system responds to a perturbation . . . by rerouting network flow to the point that a node fails and immediately sheds the flow overload to other nodes, some of which fail and shed even more overload into the system. But not every node along the way fails—some manage to move the overload along without failing, and it is a node further along in the chain that next fails. The propagation of overload failure, therefore, is not necessarily a node-by-node line of failure along direct node-link pathways. Rather, a node fails in one network location, then in another potentially distant location, and so on in unpredictable patterns until the overload becomes a global drag on the system as a whole.[109]

The failure of the financial system in 2008 can be viewed in part as an overload cascade failure: banks that didn't fail nonetheless took steps to protect themselves (like fire sales of assets) that damaged the financial system as a whole.[110] Another classic example of an overload cascade failure in a complex system is a rolling power outage. There are any number of operational problems that a power transmission system can face, including unplanned surges in customer usage,[111] as well as problems with individual components, including "aging, fire, weather, poor maintenance, or incorrect design or operating settings."[112] As power flows are redistributed within the system following an operational problem, components of that system will "interact in new and unanticipated ways, and the more loaded the remaining components are, the stronger their interactions are likely to be."[113] If these interactions cause other system components to fail, the remaining components will become even more stressed and prone to failure themselves, potentially leading to a normal accident[114] —but the pathways of such cascade failure are challenging to predict in advance.

Bank technology systems, which are comprised of software, hardware, and human components, qualify as "complex adaptive systems" that are susceptible to cascade failures and normal accidents. The operation of these complex bank technology systems is also

---

106. Helbing, *supra* note 11 at 52.

107. J.B. Ruhl, *Governing Cascade Failures in Complex Social-Ecological-Technological Systems: Framing Context, Strategies and Challenges*, 22 VAND. J. ENT. & TECH. L. 407, 420–22 (2020).

108. *Id.* at 421.

109. *Id.*

110. Hanson, Kashyap & Stein, *supra* note 65, at 5–6.

111. Ian Dobson et al., *Complex Systems Analysis of Series of Blackouts: Cascading Failure, Critical Points, and Self-Organization*, 17 CHAOS 026103, 026103-2 (2007).

112. *Id.*

113. Hilary J. Allen, *Payments Failure*, 62 B.C. L. Rev. 453, 465 (2021).

114. Ruhl, *supra* note 107, at 421.

impacted by concentric circles of other complex and highly interconnected social, ecological, and technological systems.[115] Our ecosystem, for example, is a commonly cited example of a complex adaptive system,[116] and this Part will explore how the unexpected disruptions that the ecosystem is experiencing as a result of the phenomenon of climate change (which is itself an example of a cascade failure)[117] can damage physical assets in a way that has consequences for how banks' internal systems function.

A. Uncertain Threats

Banks cannot precisely forecast the operational problems that will damage their physical assets and lead to business disruption and system failures, and they certainly cannot predict the dollar amounts of losses that will ensue as a result. With that said, banks already know enough to understand the broad contours of some types of pertinent operational losses that are likely to arise, and they also know enough to reasonably expect that these kinds of operational losses will occur more frequently in the future.

Major operational risk losses associated with natural disasters and other environmental changes can reasonably be expected to become more frequent as climate change increasingly impacts the earth. In its Fourth National Climate Assessment issued in 2018, the U.S. Global Change Research Program (a joint project of thirteen federal agencies) found that: "[i]n the absence of significant global mitigation action and regional adaptation efforts, rising temperatures, sea level rise, and changes in extreme events are expected to increasingly disrupt and damage critical infrastructure and property, labor productivity, and the vitality of our communities."[118] This may very well be an understatement. Much of the research on the impacts of climate change ignores or minimizes worst-case outcomes, and climate-related events could become much more frequent and severe than anticipated.[119] Still, many kinds of climate-related events are already quite foreseeable—notwithstanding that we are sometimes ill-prepared for them.[120]

Major operational losses associated with technological problems are also likely to increase for several reasons. The most obvious is that the more banks move operations online, the more surface area there is for cyberattacks.[121] It is also true, though, that complex

115. For a discussion of social-ecological-technological systems, see *id.* at 411.

116. Simon A. Levin, *Ecosystems and the Biosphere as Complex Adaptive Systems*, 1 ECOSYSTEMS 431 (1998).

117. Ruhl, *supra* note 107, at 411.

118. U.S. GLOB. CHANGE RSCH. PROGRAM, FOURTH NATIONAL CLIMATE ASSESSMENT 25 (2018), https://nca2018.globalchange.gov/downloads/NCA4_2018_FullReport.pdf. [https://perma.cc/4TJHD-KK2A].

119. "Prudent risk management requires consideration of bad-to-worst-case scenarios. Yet, for climate change, such potential futures are poorly understood . . . . At present, this is a dangerously underexplored topic." Luke Kemp et al., *Climate Endgame: Explore Catastrophic Climate Change Scenarios*, PROC. NAT'L ACAD. SCIS., Aug. 23, 2022, at 1, https://www.pnas.org/doi/10.1073/pnas.2108146119 (on file with the *Journal of Corporation Law*).

120. As an example, see the discussion of the foreseeability of the 2021 Texas cold snap in James Doss-Gollin et al., *How Unprecedented was the February 2021 Texas Cold Snap?*, 16 ENV'T RSCH. LETTERS 064056 (2021).

121. *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions*, *supra* note 88, at 9.

systems are inherently fragile[122]—which suggests that as systems become more complex, they are more likely to fail even when they are not under attack.

To ground this Article's discussion of the operational risks associated with new technologies, I offer here some brief background on APIs, cloud computing, and machine learning technologies, which are increasingly being incorporated into banking business models.[123] It's also possible that, despite the limitations of blockchain technology,[124] banks may adopt it to some degree, so I provide some background on blockchains as well.

An *API*, or *application programming interface* is essentially a type of computer software that allows two different information technology systems to communicate with one another.[125] In finance, APIs are increasingly being deployed to allow customer information to be shared between financial institutions; they are often developed by technology firms known as data aggregators.[126]

Cloud computing allows data to be stored on a network of servers, instead of on a local hard drive. This allows for greater volumes of data to be stored, and also provides some protective redundancy because if one server fails, others can pick up the slack.[127]

Machine learning algorithms are programmed to learn decision-making rules by deducing correlations in the data that is used to train them. This makes machine learning algorithms more autonomous (and also more unpredictable) than other computer programs, which execute according to the decision-making rules coded by a human software engineer.[128]

A *blockchain* is a kind of database where entries can only be added (not deleted), and where no centralized authority has the right to determine what is added to the database.[129] Crypto assets like tokens and coins are computer files stored on that database, and computer programs known as smart contracts can also run on the database, effecting transactions in tokens and coins in a way that is intended to be self-executing and self-enforcing.[130] With this background, we are in a position to explore new operational threats, and the uncertainty surrounding them, in more detail.

1. Climate Change

Financial regulators around the world recognize that climate change poses significant threats to individual banks, and to financial stability overall (although financial regulators

122. Ruhl, *supra* note 11, at 562.

123. *Fintech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*, FIN. STABILITY BD. [FSB] 6 (2019), https://www.fsb.org/wp-content/uploads/P140219.pdf [https://perma.cc/D7P6-7ZCF].

124. For a discussion of these limitations, see Hilary J. Allen, *DeFi: Shadow Banking 2.0?*, 64 WM. & MARY L. REV. 919, 960–63 (2023); Frederic Boissay et al., *Blockchain Scalability and the Fragmentation of Crypto*, BANK FOR INT'L SETTLEMENTS [BIS], BULLETIN NO. 56 (2022), https://www.bis.org/publ/bisbull56.pdf [https://perma.cc/B23P-92J8].

125. *Fintech and Market Structure in Financial Services*, *supra* note 123, at 6.

126. Dan Awrey & Joshua Macey, *The Promise and Perils of Open Finance*, 40 YALE J. ON REG. 1, 4–5 (2022).

127. *Fintech and Market Structure in Financial Services*, *supra* note 123, at 7.

128. For more background on machine learning, see David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653 (2017).

129. PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 2 (2018).

130. *Id.*

in the United States lag behind many of their international counterparts in this work).[131] These threats are commonly referred to as either "transition risks" or "physical risks."[132] Transition risks and physical risks might generate market, credit, liquidity, and operational risks for banks and other participants in the financial markets, but most research and regulatory attention has so far been directed at the associated credit risks.[133] Less research has been done, and limited data is available, about the operational risks associated with climate change.[134]

The Financial Stability Board, an influential international body that monitors threats to financial stability, characterizes transition risks as those relating "to the process of adjustment towards a low-carbon economy, including shifts in policies designed to mitigate and adapt to climate change, which would affect the value of financial assets and liabilities."[135] There are obvious market and credit risk concerns about investments in and loans to fossil fuel-related businesses, as these businesses are vulnerable to policy shifts regarding carbon-producing activities.[136] Market and credit risks could also arise from disruptions following the invention of a new and superior green technology that quickly renders existing industries obsolete, or from retail investors' increasing focus on environmental issues and rejection of carbon-intensive industries.[137] The impacts of transition risks on bank *operations* are not obvious, but it's possible there could be some impacts— when dealing with uncertainty, we are likely to be surprised by how some threats manifest. For example, it's possible that changing or inconsistent environmental policies across different jurisdictions could cause shortages or other supply chain issues that ultimately impair bank functioning.

The relationship between physical risk and operational risk is more obvious. The Financial Stability Board defines physical risk as "the possibility that the economic costs and financial losses from the increasing severity and frequency of extreme climate-change related weather events might erode the value of financial assets, and/or increase

131. Kress, *supra* note 45, at 711.

132. *Stocktake of Financial Authorities' Experience in Including Physical and Transition Climate Risks as Part of Their Financial Stability Monitoring*, FIN. STABILITY BD. [FSB] 2 (2020), https://www.fsb.org/wp-content/uploads/P220720.pdf [https://perma.cc/7P4Y-DV7C].

133. Patrizia Baudino & Jean-Philippe Svoronos, *Stress-testing Banks for Climate Change – A Comparison of Practices*, BANK FOR INT'L SETTLEMENTS [BIS] 23, FSI INSIGHTS ON POL'Y IMPLEMENTATION NO. 34 (2021), https://www.bis.org/fsi/publ/insights34.pdf [https://perma.cc/D2JK-NRBN].

134. "Climate change impacts on . . . operational risk remain largely unstudied." *Id.* at 23. "Existing studies suggest the potential for material operational climate losses on banks is small. However, this is based on modeling of idiosyncratic events and limited public information. . . . Further research on bank-relevant operational risks would therefore be valuable." *Climate-Related Risk Drivers and Their Transmission Channels*, BANK FOR INT'L SETTLEMENTS [BIS] 33 (2021), https://www.bis.org/bcbs/publ/d517.pdf [https://perma.cc/3DTQ-K22S].

135. *Stocktake of Financial Authorities' Experience*, *supra* note 132, at 2. "Carbon emissions have to decline by 45% from 2010 levels over the next decade in order to reach net zero by 2050. This requires a massive reallocation of capital. If some companies and industries fail to adjust to this new world, they will fail to exist." *Open Letter on Climate-Related Financial Risks*, BANK OF ENG. (Apr. 17, 2019), https://www.bankofengland.co.uk/news/2019/april/open-letter-on-climate-related-financial-risks [https://perma.cc/9J8D-72QH].

136. Graham S. Steele, *Confronting the 'Climate Lehman Moment': The Case for Macroprudential Climate Regulation*, 30 CORNELL J.L. & PUB. POL'Y 109, 126 (2020).

137. On the subject of changing investor preferences, see Michal Barzuza et al., *Shareholder Value(s): Index Fund ESG Activism and the New Millennial Corporate Governance*, 93 S. CAL. L. REV. 1243 (2020).

liabilities."[138] In the banking context, changes and events such as rising seas, fires, or hurricanes, could certainly threaten property that serves as collateral for loans, generating credit and market risks.[139] But these kinds of changes could also threaten data centers, force office closures, or knock out electrical grids or telecommunications lines that banks rely upon, causing operational risks that would fall into the categories of "damage to physical assets" and "business disruption and system failures." In the past, banks' operational capabilities have been compromised when natural disasters compromised telecommunications infrastructure.[140] These events are likely to become much more common in the future, but it is difficult to predict their exact contours.

In its 2021 report on climate and financial stability, the Financial Stability Oversight Council (a council of US financial regulators) acknowledged concerns about the ability of physical risks to compromise important infrastructure, observing that:

> The financial services sector relies upon critical infrastructure that is exposed to physical hazards, such as flood, fire, and extreme weather, which creates a risk of operational disruptions to core sector operations. These hazards impact the financial services sector directly through impacts to sector-operated critical infrastructure, and indirectly through cascading impacts to critical infrastructure upon which the financial sector relies, particularly energy and telecommunications infrastructure.[141]

The report also cites specific examples, such as the closure of stock trading for two days following Hurricane Sandy in October 2012, and disruptions to online banking for credit union customers nationwide after the servers of the third-party vendor Fiserv were shut down as a result of power outages during the Texas cold snap in February 2021.[142] Regulators generally recognize that climate-related risks may be challenging to quantify.[143] As one report from the BIS put it, "[a]s climate-related events are uncertain and likely to grow over time, their evolution will arguably involve non-linearities and tipping points. As a consequence, the largely backward-looking traditional approach based on historical loss experience will probably fail to capture the forward-looking elements of these risks."[144] There has therefore been significant interest in trying to manufacture data about climate-related financial risks (including operational risks) through stress tests and scenario analysis,[145] but the output of these exercises is unlikely to be truly predictive. Not only is there a paucity of data available about the likely operational impacts of climate-related

138. *Stocktake of Financial Authorities' Experience*, *supra* note 132, at 2.

139. *Id.* at 7.

140. *Climate-Related Risk Drivers and Their Transmission Channels*, *supra* note 134, at 19.

141. FIN. STABILITY OVERSIGHT COUNCIL, U.S. DEPT. TREASURY, REPORT ON CLIMATE-RELATED FINANCIAL RISK, 101 (2021), https://home.treasury.gov/system/files/261/FSOC-Climate-Report.pdf [https://perma.cc/Z5EN-2G5D].

142. *Id.* at 101–02.

143. *Id.* at 15.

144. *See, e.g.*, Rodrigo Coelho & Fernando Restoy, *The Regulatory Response to Climate Risks: Some Challenges*, BANK FOR INT'L SETTLEMENTS [BIS] 3, FSI BRIEFS NO. 16 (2022), https://www.bis.org/fsi/fsibriefs16.pdf. [https://perma.cc/L6E8-76HE].

145. Chenet, Ryan-Collins & van Lerven, *supra* note 21, at 3.

events,[146] the operational threats that banks are preparing for may occur further in the future than the three-to-five-year window that banks typically plan for.[147] Climate-related operational risks therefore require a different regulatory framework that caters to this uncertainty.

One way to respond to uncertainty is to take a precautionary approach, proactively adopting regulation that is likely—although not guaranteed—to address or mitigate uncertain outcomes, because failing to act proactively could result in harms that are irreversible and catastrophic.[148] However, attempts to adopt precautionary financial regulation in anticipation of a changing climate have met with staunch political opposition in the United States.[149] One curious aspect of this opposition is that precautionary climate-focused operational risk regulation would seek to protect banks from many of the same kinds of operational problems as would be caused by cyberattacks. Yet political attitudes to cyberattacks, as a type of national security threat, are very different in the United States and precautionary regulation is likely to be much less controversial.[150] We will turn to the operational risks associated with cyberattacks now.

2. Cyberattacks

In 2017, the G20 Finance Ministers and Central Bank Governors came together to state that "the malicious use of information and communication technologies . . . could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability".[151] This view is broadly shared, and concern has only increased in the intervening years—particularly regarding attacks on critically important third-party service providers that can cripple the activities of multiple financial institutions. For example, in January 2023, a ransomware attack on ION Markets disrupted derivatives brokers' ability to match and reconcile trades for several weeks.[152] In December 2023, sixty credit unions faced outages because their shared cloud computing provider was targeted in a ransomware attack.[153]

---

146. YEVGENY SHRAGO & DAVID ARKUSH, LOOKING OVER THE HORIZON: THE CASE FOR PRIORITZING CLIMATE-RELATED RISK SUPERVISION OF BANKS 8 (2022), https://rooseveltinstitute.org/wp-content/uploads/2022/06/RI_Climate-Related-Risk-Supervision_202206.pdf [https://perma.cc/HL4Q-EFGA].

147. *Id.*

148. Allen, *supra* note 22, at 178.

149. Kress, *supra* note 45 at 691. For a specific illustration of this dynamic, see Andrew Freedman, *Why Raskin's Climate Change Views Sank Her Fed Nomination*, AXIOS (Mar. 15, 2022), https://www.axios.com/2022/03/15/sarah-raskin-climate-change-views-sink-fed-nominee. [https://perma.cc/UK2N-N86K].

150. For a discussion of variations in US attitudes to precaution, see Jonathan B. Wiener, *Whose Precaution After All? A Comment on the Comparison and Evolution of Risk Regulatory Systems*, 13 DUKE J. COMP & INT'L L. 207, 210 (2003).

151. Communiqué, G20 Finance Ministers and Central Bank Governors, Statement from G-20 Meeting in Baden-Baden, (Mar. 17–18, 2017), http://www.g20.utoronto.ca/2017/170318-finance-en.pdf [https://perma.cc/655G-XQGH].

152. Nikou Asgari, *Derivatives Market Still Hit by Fallout From Ion Markets Cyber Attack*, FIN. TIMES (Feb. 20, 2023), https://www.ft.com/content/445ec6b7-50b6-4e8d-939b-6c321f4dc4ea [https://perma.cc/8M5R-ZTVX].

153. Jonathan Greig, *60 Credit Unions Facing Outages Due to Ransomware Attack on Popular Tech Provider*, RECORD (Dec. 1, 2023), https://therecord.media/credit-unions-facing-outages-due-to-ransomware [https://perma.cc/D2M8-6DGB].

Financial regulators and banks around the world consider cyberattacks to be a significant potential threat to both individual banks and the broader financial system.[154] Because they are so frequently targeted by cyberattacks, financial institutions have implemented some of the most sophisticated cybersecurity measures of any industry, but these are by no means impermeable.[155] Furthermore, insurance coverage is unlikely to make banks whole if any cyberattacks do occur, as "cyber insurers typically insist on setting policy limits that are well below policyholders' economic exposures to cyber risk."[156]

Cyberattacks target an information technology system's confidentiality, integrity, or availability (often abbreviated to CIA).[157] Data breaches undermining confidentiality are often discussed in the press, but while these can create reputational harms for banks (and may result in litigation or other operational losses that would probably fall into the operational risk category of "clients, products & business practices"), they are unlikely to disrupt a bank's business or cause its systems to fail.[158] Cyberattacks that seek to compromise system integrity and availability—in other words, to prevent a bank from performing its core activities—are most likely to result in business disruption and system failures, and they will be the focus of this Part.

A bank's operations could be compromised by a cyberattack that seeks to disable a bank's information technology systems, or by an attack that targets the data a bank uses to carry out its core functions.[159] One example of an attack type that compromises the information technology systems themselves is a "DOS" or "denial of service" attack that prevents authorized access to or delays the operations of a system—with the result that that system cannot perform its usual functions.[160] Data can also be targeted: the integrity of account data is critically important to the provision of banking services because it records "who owes what to whom at any moment . . . . An attack that destroyed or corrupted the accounts of a major financial institution could wreak devastating economic havoc unless those accounts could be quickly and reliably reconstituted."[161] This type of data corruption is particularly dangerous when it happens slowly and imperceptibly, as this allows the corrupted data to be backed up, replacing accurate backup copies that would otherwise be available to help repopulate the corrupted data once an attack is uncovered.[162]

---

154. Maziar Peihani, *Regulation of Cyber Risk in the Banking System: A Canadian Case Study*, 8 J. FIN. REG. 139, 141 (2022).

155. EISENBACH, KOVNER & LEE, *supra* note 15, at 1.

156. Kenneth S. Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of a Cyber Insurance Catastrophe*, 27 CONN. INS. L.J. 407, 460 (2021).

157. EISENBACH, KOVNER & LEE, *supra* note 15, at 6–7.

158. "While data breaches can lead to reputation, litigation, and other monetary costs, like most cyberattacks, they usually do not disrupt firms' operations." MATTEO CROSIGNANI, MARCO MACCHIAVELLI, & ANDRÉ F. SILVA, THE PROPAGATION OF CYBERATTACKS THROUGH FIRMS' SUPPLY CHAINS 3 (2021).

159. Anil K. Kashyap & Anne Wetherilt, *Some Principles for Regulating Cyber Risk*, 109 AM. ECON. ASS'N PAPERS & PROC. 482, 482 (2019).

160. *Cyber Lexicon*, FIN. STABILITY BD. [FSB] 10 (2018), https://www.fsb.org/wp-content/uploads/P121118-1.pdf [https://perma.cc/FVA2-DV8L].

161. Joel Brenner, *Keeping America Safe: Toward More Secure Networks for Critical Sectors*, MIT INTERNET POL'Y RSCH. INITIATIVE 33 (Mar. 2017), https://internetpolicy.mit.edu/reports/Report-IPRI-CIS-CriticalInfrastructure-2017-Brenner.pdf [https://perma.cc/29QP-JUFC]; *see also* Aldasoro et al., *supra* note 89, at 381 ("One key finding is that intentional data manipulation could be especially damaging, as it may erode confidence, triggering feedback loops, and require a prolonged recovery period.").

162. Brenner, *supra* note 161, at 33.

Difficulty in detecting "low and slow" cyberattacks contributes to the general uncertainty regarding banks' exposure to losses from cyberattacks.[163] Furthermore, when trying to plan for cyberattacks, it can be extremely challenging to predict whether other failures will cascade from the initial attack.[164] Because banks don't know in advance the probability of being the subject of a cyberattack, or whether they will be able to stop it from causing significant damage, this uncertainty undermines attempts to quantify the cyber risks that banks face.[165] Cyberattacks have appropriately been characterized as low-probability, but potentially high-consequence "tail events."[166] Although economists have begun to investigate the probabilities of cyberattacks on the financial industry and their likely costs,[167] this research is in its infancy, and data on "the costs, drivers and potential mitigating factors" is scarce[168] (and certainly more limited than data relating to more frequently occurring categories of operational loss events).[169] We do know that the financial industry is a frequent target of malicious cyberattacks, and some data suggest that better regulation and supervision reduce losses related to cyberattacks.[170] Beyond that, though, we are dealing with uncertainty, which cautions against relying on any historical data that suggest cyber-related losses will continue to be a small share of banks' operational losses.[171]

Banks and bank regulators are still developing best practices for resilience against cyberattacks,[172] and the possible types of attacks are evolving with new technologies. For example, banks are increasingly relying on machine learning for several functions, including internal risk management, borrower credit assessment, fraud and suspicious transaction detection, as well as to provide customer service.[173] Recent research has found that reliance on machine learning opens the user up to new kinds of attacks, including data poisoning attacks. Machine learning is only as good as its data, so nefarious agents can "corrupt and contaminate training data to compromise the system's performance".[174] In addition to simply flooding the algorithm with bad data, some computer scientists have explored the potential for "undetectable backdoors" to be added during the training of a machine learning algorithm that can be used to easily sabotage the output of the algorithm once it is

163. EISENBACH, KOVNER & LEE, *supra* note 15, at 8; Kashyap & Wetherilt, *supra* note 159, at 483.

164. Brenner, *supra* note 161, at 4.

165. "The traditional diffusion-based model of shock propagation, characteristic of credit and market risk models, fails to grasp the sense of purpose, intent and ingenuity that drives cyber attacks." José Ramón Martínez Resano, *Digital Resilience and Financial Stability: The Quest for Policy Tools in the Financial Sector*, 43 REVISTA DE ESTABILIDAD FINACERIERA 59, 66 (2022).

166. Iñaki Aldasoro et al., *The Drivers of Cyber Risk*, 60 J. FIN. STABILITY 1, 2 (2022).

167. *See, e.g.*, *id.* (identifying drivers in cyber risk and the cost of cyber incidents); EISENBACH, KOVNER & LEE, *supra* note 15 (exploring cyber risk on financial institutions).

168. Aldasoro et al., *supra* note 166, at 3.

169. Aldasoro et al., *supra* note 89, at 381–82.

170. *Id.* at 30.

171. Regarding this historical data, see Aldasoro et al., *supra* note 166, at 3–4.

172. *Cyber Resilience Practices – Executive Summary*, BANK FOR INT'L SETTLEMENTS [BIS] (2021), https://www.bis.org/fsi/fsisummaries/cyber_resilience.pdf [https://perma.cc/VW5D-SFRD].

173. *See* Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, 86 Fed. Reg. 16837 (Mar. 31, 2021).

174. *Id.* at 16841.

operational.[175] If the machine learning algorithm has been used to automate bank functions, there may be significant consequences if the algorithm is sabotaged.

Some banks (including, notably, JPMorgan) are also assessing the possibility of conducting transactions on permissionless blockchains.[176] A blockchain is considered "permissionless" if there is no trusted central intermediary that authorizes transactions on that blockchain–but a substitute mechanism is needed in the absence of any such intermediary to prevent people from copying their tokenized assets (which are essentially just computer files) and spending them multiple times.[177] The creators of permissionless blockchains have developed a variety of cryptography-based consensus mechanisms to determine which is the correct version of the blockchain (and therefore who is the owner of the various crypto assets hosted on that blockchain). These consensus mechanisms add inefficiency to transaction processing,[178] but their proponents argue that permissionless blockchains have the benefit of being more impervious to hacks.[179] A report commissioned by DARPA, however, found that permissionless blockchains are more dependent on centralized concentrations of power than they claim and that this centralization makes them more vulnerable to attacks than is widely appreciated.[180] Others have expressed concern that with the advent of quantum computing technologies, even truly decentralized permissionless blockchains could become targets for cyberattacks.[181]

3. Technological Glitches

To be clear, cyberattacks are not the only operational concern regarding blockchains, and more generally, not all technological problems are caused by malicious actors. Some technological problems are entirely unintentional–and by some calculations, the overall

175. This could be done by an internal bad actor involved in training the algorithm, but because a lot of machine learning training is outsourced, the authors of this research focus on the potential for a vendor to add the backdoor. They find that it would be very challenging for a bank to detect a "backdoor" that was built into a loan classifier algorithm by a vendor, and so the bank would be unaware that a bad actor has, for example, "the ability to change any user's profile (input) ever so slightly (into a backdoored input) so that the classifier always approves the loan." Shafi Goldwasser et al., *Planting Undetectable Backdoors in Machine Learning Models*, 63 IEEE ANN. SYMP. ON FOUNDS. COMPUT. SCI. 931, 932 (2022). Bad actors could profit from these kinds of backdoors in multiple ways; they could sell bank customers guarantees that their loans would always be approved, or they could engage in ransomware attacks where they demand payment from banks in exchange for not activating the back doors. *Id.* Undetectable backdoors could also be included at the behest of banks, though, allowing the bank to manipulate their risk management models in a way that is undetectable by regulators (in a way that is reminiscent of the Volkswagen scandal). For more on the Volkswagen scandal, see J.S. Nelson, *Disclosure Driven Crime*, 52 U.C. DAVIS L. REV. 1487 (2019).

176. Brayden Lindrea, *JPMorgan Executes First DeFi Trade on Public Blockchain*, COINTELEGRAPH (Nov. 3, 2022), https://cointelegraph.com/news/jp-morgan-executes-first-defi-trade-on-public-blockchain. [https://perma.cc/J7A2-UCFJ].

177. DE FILIPPI & WRIGHT, *supra* note 129, at 19–20.

178. Allen, *supra* note 124, at 960; Boissay et al., *supra* note 124, at 1.

179. V. Gerard Comizio, *The Cyber Threat Looming Over Virtual Currencies*, AM. BANKER (May 5, 2021), https://www.americanbanker.com/opinion/the-cyber-threat-looming-over-virtual-currencies [https://perma.cc/6WRM-WHVD].

180. EVAN SULTANIK ET AL., ARE BLOCKCHAINS DECENTRALIZED? UNINTENDED CENTRALITIES IN DISTRIBUTED LEDGERS 21 (2022), https://apps.dtic.mil/sti/pdfs/AD1172417.pdf. [https://perma.cc/PX6M-KA2H].

181. Comizio, *supra* note 179.

operational losses for firms associated with these unintentional events are greater than losses attributed to malicious attacks.[182] We will turn now to these unintentional technological glitches.

To cite just a few recent examples of banks experiencing operational problems as a result of unintentional technological glitches, Chase Bank mistakenly deposited $50 billion in a customer's account,[183] Santander UK accidentally made scheduled payments twice (resulting in an additional $175 million of payments made),[184] and 12,000 Bank of America customers were unable to access their accounts for hours on a day when many bill payments were due.[185] All of these examples relate to online banking: news of these kinds of problems is frequently shared on social media and then attracts media attention. However, banks undoubtedly experience technological glitches that are not publicly acknowledged: for example, a technological glitch in May 2020 prevented Citi from promptly posting the necessary margin for derivatives transactions; it was only publicly acknowledged in June of 2022 after a representative of ICE Clearinghouse alluded to the glitch.[186]

Ultimately, the impact of the problems just discussed seems to have been minimal. ICE Clearinghouse extended a little grace and refrained from liquidating Citi's derivatives position;[187] many of the erroneous online banking transactions discussed above were able to be reversed.[188] These kinds of friendly resolutions are not necessarily guaranteed, though. In a separate incident, Citi (in its capacity as lead arranger of a syndicated loan to Revlon) accidentally repaid lenders approximately $500 million of their principal (instead of just the expected interest payment).[189] Several recipients of the funds initially refused to return those payments to Citi, and it took an appeal to the Second Circuit to order repayment.[190] These kinds of events could be harbingers of future technology-related operational risks that could result in significant losses for banks.

In a thesis paper titled "*How Failures Cascade in Software Systems*," computer scientist Barbara Chamberlin applies the complexity science perspective to failures of

182. Aldasoro et al., *supra* note 166, at 2.

183. Alaa Elassar, *A Bank Accidentally Deposited $50Billion into a Louisiana Family's Account*, CNN (July 3, 2021), https://www.cnn.com/2021/07/03/us/50-billion-mistakenly-deposited-bank-account-louisiana/index.html [https://perma.cc/47LM-PSD7].

184. Stephen Jones, *A Bank Accidentally Paid Thousands of People More Than $175 Million on Christmas Day due to a Technical Glitch*, BUS. INSIDER (Dec. 31, 2021), https://www.businessinsider.com/santander-bank-accidentally-pays-people-175-million-christmas-day-2021-12 [https://perma.cc/W3FV-TLLC].

185. Taylor Raines, *Bank of America's Online Banking System Went Down Friday, Locking Thousands of Customers Out of Their Accounts*, BUS. INSIDER (Oct. 1, 2021), https://www.businessinsider.in/finance/news/bank-of-americas-online-banking-system-went-down-friday-locking-thousands-of-customers-out-of-their-accounts/articleshow/86687616.cms [https://perma.cc/F4CU-2T86].

186. Imani Moise et al., *Citi Suffered Tech Glitch During Height of Covid Market Stress*, FIN. TIMES (June 9, 2022), https://www.ft.com/content/e535658a-3fd5-46d2-8685-fc63be1cdfbd (on file with the *Journal of Corporation Law*).

187. *Id.*

188. Elassar, *supra* note 183; Jones, *supra* note 184; Raines, *supra* note 185.

189. Davide Scigliuzzo & Katherine Doherty, *Behind the Back-Office Blunder That Cost Citigroup $500 Million*, BLOOMBERG (Mar. 19, 2021), https://www.bloomberg.com/news/articles/2021-03-19/citigroup-c-and-revlon-behind-the-500-million-accidental-payment (on file with the *Journal of Corporation Law*).

190. Becky Yerak & Andrew Scurria, *Citi Wins Appeal on Errant $500 Million Revlon Loan Payment*, WALL ST. J. (Sept. 8, 2022), https://www.wsj.com/articles/citi-wins-appeal-on-errant-500-million-revlon-loan-payment-11662664035 (on file with the *Journal of Corporation Law*).

software systems.[191] She and her colleagues surveyed several publicly available postmortems of tech incidents to find what she terms "failure pairs" (being "two failures in distinct components, or the same component separated by time, where the first failure is described as being the cause of the second failure").[192] From her analysis of these failure pairs, Chamberlin identified three "themes" that described how many of the surveyed cascade failures had transpired (although she observes that sometimes, it is not possible to figure out why an initial error cascades into a full system outage).[193] These themes are ungraceful degradation ("one system component failing in some way and another component being unable to tolerate that failure"); automating failure ("when support systems or automation systems respond[] to an initial failure, and introduce an additional failure"); and ungraceful recovery (the failures that occur "as responders attempt to mitigate or resolve a failure, intentionally or unintentionally, leading to more failures").[194]

To give more context regarding the "ungraceful degradation" cascade failures identified by Chamberlin, an initial component failure sometimes starved other system components of resources (like computational resources, or access to databases).[195] One can envisage how an ungraceful degradation could interrupt a bank's ability to administer payments, for example, if data about customer account balances were unable to be used to validate and process any payment instructions. Attempts to reboot the servers storing customer account balance data after a failure might lead to an "ungraceful recovery". Chamberlin observed that one cascade failure started with the failure of a data server that was linked to other operative components of the system; once that happened, the restart process for the data server overloaded or otherwise threw off the other system components, causing them to fail.[196]

If the initial failure does not shut down a system component, but allows it to keep functioning in an error state, automating failures or ungraceful recovery may ensue (an excellent illustration of the overload failure, robust-yet-fragile dynamic).[197] For example, other components may fail as a result of interactions with the component that is in an error state: in a set of circumstances that is highly relevant for banks, Chamberlin observed that one initial failure "left a database with incorrect data (financial account balances set to 0) and the database in read-only mode," which resulted in a second failure where "the billing system began to repeatedly and erroneously charge customer credit cards because successful charges could not be recorded in the read-only database."[198]

Chamberlin did not restrict her focus to bank software, but bank software may be particularly vulnerable to these kinds of cascade failures. In large banks, new types of software are often grafted onto legacy technology systems, some of which were adopted as far back as the 1960s and '70s (and therefore rely on an old computer programming language

191. *See generally* Barbara W. Chamberlin, How Failures Cascade in Software Systems (Apr. 18, 2022) (M.S. thesis, Brigham Young University), https://scholarsarchive.byu.edu/etd/9474.

192. *Id.* at 4.

193. *Id.*

194. *Id.* at 10.

195. *Id.* at 7.

196. Chamberlin, *supra* note 191, at 7.

197. See *supra* notes 107–09 and accompanying text.

198. Chamberlin, *supra* note 191, at 8.

called COBOL that most contemporary software engineers never even learn).[199] The largest banks' technology systems are also complicated by the fact that most of them grew through mergers and acquisitions, and sometimes the merged or acquired bank keeps running on its old system. Deutsche Bank, for example, relied on 45 different operating systems as of 2015;[200] "Citigroup never integrated many of the operations [after its acquisition deals in the 1990s], leading to a hodgepodge of data systems and customer identification codes throughout the bank."[201]

It's not just the accretion of old systems that may generate operational risks; new technological innovations can also generate new ways in which technological operations can accidentally go awry. We've already discussed adversarial attacks on machine learning in the context of cyberattacks,[202] but the functioning of machine learning algorithms can also be impaired accidentally by poor choices made during training and tuning processes, and by poorly labeled or selected data.[203] New research suggests that not only does data quality matter but the order in which it is presented matters too. Machine learning algorithms may be impacted by an "initialization bias", where the data they learn from first will be more impactful than subsequent data.[204] Unintentionally ordering data incorrectly can therefore undermine the effectiveness of a machine learning tool (of course, poor data selection or data misordering could also be done on purpose to malicious ends, or as a form of regulatory arbitrage).[205]

Relying on smart contracts and other blockchain-related technologies to automate transactions could also generate new kinds of operational vulnerabilities for any banks that choose to rely upon them. Permissionless blockchains are vulnerable to "bugs, attacks, and uneven adoption of new releases, coupled with the governance problems that stem from [their] decentralized, open-source nature"—Angela Walch has therefore asserted that permissionless blockchains are "too unreliable to support financial market infrastructure."[206] Computer programs known as smart contracts that run on these blockchains also have operational vulnerabilities. Smart contracts are designed to self-execute, speedily and without

199. Tom Sullivan, *Looking for Job Security? Try Cobol*, N.Y. TIMES (Oct. 23, 2008), https://archive.nytimes.com/www.nytimes.com/external/idg/2008/10/23/23idg-Looking-for-job.html [https://perma.cc/X6EN-XDEM].

200. René M. Stulz, *FinTech, BigTech, and the Future of Banks*, 31 J. APPLIED CORP. FIN. 86, 93 (2019).

201. David Benoit, *Federal Reserve Wants Citigroup to Move Faster to Fix Problems With Its Risk Systems*, WALL ST. J. (Sept. 14, 2022), https://www.wsj.com/articles/regulators-want-citigroup-to-move-faster-to-fix-problems-with-its-risk-systems-11663172835 (on file with the *Journal of Corporation Law*).

202. See *supra* notes 174–76 and accompanying text.

203. For a discussion of human involvement in "the stages of machine learning" (where mistakes can be made), see Lehr & Ohm, *supra* note 128, at Part II.

204. Cory Doctorow, *Attacking Machine Learning Training by Re-Ordering Data*, MEDIUM (May 26, 2022), https://doctorow.medium.com/attacking-machine-learning-training-by-re-ordering-data-c59f7ec0f18e [https://perma.cc/VL8T-JR7F].

205. "Suppose for example a company or a country wanted to have a credit-scoring system that's secretly sexist, but still be able to pretend that its training was actually fair. Well, they could assemble a set of financial data that was representative of the whole population, but start the model's training on ten rich men and ten poor women drawn from that set – then let initialisation bias do the rest of the work." Ross Anderson, *Data Ordering Attacks*, LIGHT BLUE TOUCHPAPER (Apr. 23, 2021), https://www.lightbluetouchpaper.org/2021/04/23/data-ordering-attacks/ [https://perma.cc/6GPG-HJFB].

206. Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 893 (2015).

opportunity for human intervention.[207] Because the code is all there is to a smart contract, any flaw in that code becomes an operational liability, and yet code is never perfect[208] (although this is relatively new technology, there are already countless examples of flawed smart contract code causing significant problems).[209]

In sum, technological systems have been critical to the provision of banking services for a long time, but technological advances are ratcheting up the complexity of those systems, and that increased complexity is making the systems more fragile in some respects.[210] As banking becomes more technologically sophisticated, there is greater uncertainty about how that technology could fail, and about what the implications of cascade failures might be. We have long relied on human involvement to inject flexibility, judgment, and discretion into our systems when unanticipated events occur—perhaps without even realizing it.[211] As systems become more complex and more automated, they become more susceptible to normal accidents, and so we should expect to see banks suffer normal accidents more frequently in the future (particularly during unanticipated surges in usage).[212] As the BCBS recognized way back in 2003, "If not properly controlled, the greater use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks."[213] Or, to use a more colorful adage, to err is human but to really foul things up requires a computer.

B. Systemic Operational Interactions

The examples in the previous Part were largely portrayed as being idiosyncratic to the banks experiencing them. That framing reflects accepted understandings of operational risks as being individual to the banks experiencing them: an important takeaway from the BCBS's construction of operational risk is that it is by and large seen as idiosyncratic, with an individual bank's handling of operational risk having limited systemic implications.[214] A similar perspective was put forward at a workshop held at MIT, where senior financial industry personnel, government officials, and academics met to discuss cybersecurity. The report from that workshop noted that "[s]everal participants agreed that financial enterprises assume that in this space all parties are managing their own risks and that systemic

207. DE FILIPPI & WRIGHT, *supra* note 129, at 2.

208. Bryan H. Choi, *Software as a Profession*, 33 HARV. J.L. & TECH. 557, 566 (2020).

209. For a running catalog of these, see WEB3 IS GOING JUST GREAT, https://www.web3isgoinggreat.com/about [https://perma.cc/3Jl5-FS59] ("Web3 is Going Just Great is a project to track some examples of how things in the blockchains/crypto/web3 technology space aren't actually going as well as its proponents might like you to believe.").

210. Ruhl, *supra* note 107, at 410–11 ("The chief driver behind this quantum shift in failure speed and magnitude has been advancements in technology, specifically (1) the expanding reach and connections to the internet; (2) the ever-larger and more interconnected infrastructure systems; and (3) vast increases in computational capacity and speed, allowing rapid automation of system operations and decisions.").

211. On the importance of human ability to interrupt transactions, see Hilary J. Allen, *The SEC as Financial Stability Regulator*, 43 J. CORP. L. 715, 745 (2018). On the importance of flexibility and discretion with regard to enforcing financial arrangements more generally, see Katharina Pistor, *A Legal Theory of Finance*, 41 J. COMPAR. ECON. 315 (2013).

212. For a discussion of cascade failures during surges in usage, see *supra* notes 111–14 and accompanying text.

213. *Sound Practices for the Management and Supervision of Operational Risk*, *supra* note 62, at 1.

214. Berger et al., *supra* note 17, at 2.

risk is therefore also being managed through the sector".[215] This Part will explore why such a perspective is too limited, highlighting some ways in which operational problems might interact with one another, with systemic implications.

In a recent research paper, Berger et al. investigated the systemic risks associated with operational loss events and identified several channels for these kinds of losses to spill over into other institutions.[216] Many of these channels relate to ways that a bank's holding company could become more leveraged and therefore more vulnerable to failure (which can have domino effects for its counterparties).[217] In addition, the authors observe that "investors may fear that similar operational difficulties are present, but yet undiscovered, in comparable financial institutions," which could damage confidence in those other institutions.[218] Unsurprisingly, Berger et al. found that the likelihood of operational losses causing systemic problems increases when they occur in systemically important financial institutions.[219]

These are all important concerns, but the spillover channels identified by Berger et al. are modeled on historical understandings of how humans react to credit, market, and liquidity risks.[220] Spillover channels that are unique to operational risk might arise, though, that are independent of any human reaction to the operational problem. While ultimately, any operational spillovers will likely elicit human reactions and intertwine with market, credit, and liquidity risks,[221] it is important to anticipate that the spread of operational problems could have trajectories that are not anticipated by our previous experience of systemic risks.[222] For example, the impact of cascade failures resulting from problems with one bank's information technology systems may not stay contained within that bank—other banks' systems may be damaged as a result. The potential for these kinds of operational spillovers is likely to increase as banks' systems are made more interoperable, and they may be compounded by external events beyond the banks' control.

This Part of the Article will explore these types of contagion mechanisms, which are not really contemplated by the existing operational risk framework (at least, not explicitly).[223] The Principles for the Sound Management of Operational Risk, for example, are very focused on banks managing their own internal risks within their own internal tolerances and assume that as long as individual banks do so, then the system as a whole will

215. Brenner, *supra* note 161, at 34. It should be noted, though, that some participants doubted whether that underlying assumption would hold up. *Id.*

216. *See generally* Berger et al., *supra* note 17.

217. First, "through direct monetary losses related to operational risk events," second, through "loss of future business or productivity from reputational damage," and third, "public sell-off or short sales" that drive down value. *Id.* at 7.

218. Allen N. Berger et al., *Operational Risk is More Systemic than You Think: Evidence from U.S. Bank Holding Companies*, 143 J. BANKING & FIN. (forthcoming draft) (manuscript at 7), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3210808 [https://perma.cc/Y7M4-QAEB].

219. Berger et al., *supra* note 17, at 3.

220. For a summary of the traditional, credit channel perspective on financial system failure, see Allen, *supra* note 113, at 460–461.

221. *Id.* at 484.

222. Eisenbach, Kovner & Lee provide an example of a research project that gets this right, recognizing the possiblity for technological spillovers, as well as spillovers through the usual credit, market, and liquidity channels. *See generally* EISENBACH, KOVNER & LEE, *supra* note 15.

223. Referring specifically to the consequences of cyberattacks, Peihani has similarly noted that the existing operational risk regulation neglects technological transmission channels. Peihani, *supra* note 154, at 153.

be safe. One illustration of this is Principle 4, which provides that "[t]he board of directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk *the bank is willing to assume*".[224] Guidance on this Principle makes clear that risk tolerance should be formulated taking into account the interests of bank customers and shareholders,[225] but there is no direction to consider other banks who might be impacted if a bank's operational risk management failures have spillover effects. Principle 10 similarly gives broad discretion to banks' management to determine the best measures to implement to deal with cybersecurity risk "consistent with *the bank's* risk appetite . . . ."[226] In the Principles for Organizational Resilience, the BCBS says that:

> In considering its operational resilience, a bank should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption . . . [which is defined to mean] the level of disruption from any type of operational risk a bank is willing to accept given a range of severe but plausible scenarios.[227]

The steps that a bank takes to make itself more resilient, however, may sometimes undermine the resilience of other banks (and the financial system more broadly), and the Principles do not reference *their* risk appetite or willingness to accept operational risk.

1. Cascade Failures

We have already discussed how a problem could cascade within an individual bank's internal IT systems,[228] but there's no reason to think that cascade failures will respect that bank's organizational boundaries. Cascade failures can jump to interconnected systems as well,[229] and so this Part will explore how cascade failures could be a channel for bringing operational risks into the bank from outside (and vice versa)[230] (this concern is conceptually distinct from operational risks that multiple banks might experience simultaneously but independently—such as two banks being targeted in the same cyberattack—which we will return to shortly). The key takeaway from this Part is that the decisions that banks make about operational risk can impact other banks as well.

It is becoming increasingly well-recognized that banks are exposed to operational risks when they rely on systems provided by third parties (such as a cloud service provider,[231] or a data aggregator[232]). This is typically conceptualized as a type of domino failure: if the third-party provider stops operating, the bank may not be able to operate

224. *Revised PSMOR*, *supra* note 6, at 4 (emphasis added).

225. *Id.* at 8.

226. *Id.* at 16 (emphasis added).

227. *Principles for Operational Resilience*, *supra* note 75, at 3.

228. *See supra* Part III.A.

229. Ruhl, *supra* note 107, at 410.

230. This possibility has been noted in particular in the cyberattack context: "a virus or technical exploit may propagate through data and communications networks, through shared service providers or technological similarities." EISENBACH, KOVNER & LEE, *supra* note 15, at 9.

231. *See* THIRD-PARTY DEPENDENCIES IN CLOUD SERVICES: CONSIDERATIONS ON FINANCIAL STABILITY IMPLICATIONS, FIN. STABILITY BD. 12–13 (2019), https://www.fsb.org/wp-content/uploads/P091219-2.pdf [https://perma.cc/9SPG-F2Z8].

232. Awrey & Macey, *supra* note 126, at 5.

either.[233] It is less appreciated, though, that overload failures are also a possibility. A third-party provider may be suffering problems but remain operational, which could allow transmission of problems to banks' systems through their interoperable components.[234] It can be difficult for banks to manage these kinds of operational risks because they do not control their vendors (and the third-party vendors themselves may be compromised by failures cascading from problems with subcontractors, or otherwise within their supply chains).[235] Still, banks are expected to manage the risks associated with their reliance on third-party service providers.[236]

Banks relying on systems provided by third-party vendors may also be exposed to risks if a cascade failure begins at another bank that relies on a shared third-party system. The systemic implications are magnified the more banks rely on the same third-party provider, but in a recent FSB consultation, many of the financial institutions consulted expressed the view that "identifying, monitoring and managing systemic concentration risk in the provision of third-party services and other interdependencies is beyond the responsibility of individual financial institutions."[237] It is easy to have sympathy for this view, given that individual institutions "do not have access to data on other financial institutions' dependencies on specific third-party service providers,"[238] but that does not obviate the reality that operational failures at a bank can cascade into a third-party service provider and then back out into other banks.

Perhaps the strongest response we currently have to the systemic vulnerabilities associated with third parties is financial market infrastructure regulation. International regulatory bodies have developed Principles for Financial Market Infrastructure (the PFMIs), which apply to providers of critical financial "plumbing" services involved in processing payments and trades.[239] These PFMIs recognize that there will be systemic repercussions (with flow-on impact on the broader economy) if these central pieces of infrastructure are compromised, largely because of the lack of available substitutes.[240] While these PFMIs are important, they are not a complete response to the systemic implications of cascading operational failures.

---

233. Kotidis and Schreft document such a domino failure, where a cyberattack targeted a third-party service provider, and once it discovered this, "it took its computer systems offline to limit the damage done. In doing so, some bank customers of the [third-party service provider] . . . lost the ability to send payments over Fedwire using their usual processes." Antonis Kotidis & Stacey L. Schreft, *Cyberattacks and Financial Stability: Evidence from a Natural Experiment* 1, (FED. RSRV. BD., FIN. & ECON. DISCUSSION SERIES, No. 025, 2022) Regarding domino failures generally, see *supra* note 107 and accompanying text.

234. Regarding overload failures, see *supra* notes 108–09 and accompanying text.

235. *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Overview of Responses to the Public Consultation*, FIN. STABILITY BD. [FSB] 2 (2021), https://www.fsb.org/wp-content/uploads/P140621.pdf [https://perma.cc/LZE3-248M].

236. "A banking organization is responsible for conducting its activities in compliance with applicable laws and regulations, including those activities involving third parties. The use of third parties does not abrogate these responsibilities." *Interagency Guidance on Third-Party Relationships: Risk Management*, 88 Fed. Reg. 37920, 37932 (June 9, 2023).

237. *Regulatory and Supervisory Issues*, *supra* note 235, at 3.

238. *Id.*

239. *Principles for Financial Market Infrastructures*, BANK FOR INT'L SETTLEMENTS 1 (2012), https://www.bis.org/cpmi/publ/d101a.pdf [https://perma.cc/G5WB-WXE5] [hereinafter *PFMIs*].

240. Aldasoro et al., *supra* note 89, at 381.

First, the PFMIs only cover a limited number of service providers that provide critical clearing, settlement, and payment infrastructure.[241] It is possible that smaller infrastructure providers, and providers of different kinds of infrastructure (like cloud providers and data aggregators), could also serve as bank-to-bank transmission mechanisms for operational problems.[242] Second, the primary goal of the PFMIs is to protect banks from credit and liquidity problems that arise in or are transmitted from other banks through financial market infrastructure.[243] They tend to neglect the possibility that one bank's operational problems could infect another bank through a third party's technology system components. Because of their focus on third parties, the PFMIs also do not address the possibility that operational risks might be transmitted directly between two banks (for example, if the information systems of two banks are made interoperable).

We can make these limitations of our existing approach to operational risk regulation more vivid by exploring some hypothetical illustrations of how operational problems at one bank might impact other banks, either directly or through third parties.

i. Disaster Recovery and Business Continuity Plans

Principle 11 of the Principles for the Sound Management of Operational Risk stipulates that "[b]anks should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption";[244] Principle 3 of the Principles for Operational Resilience similarly requires that "[b]anks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption."[245] These disruptions could result from the manifestation of a physical climate risk (like a fire, or a flood), or they could be the result of some kind of technological problem (whether malicious or unintentional).

A bank could try to repair the damaged internal systems following these kinds of disruptions, but if that takes too long, the resumption of services may require the use of backup services provided by a third party. If multiple banks rely on the same third-party provider, they may all need to use that provider's backup services at the same time (perhaps because of a common shock to their primary systems, like the flooding of all data centers in New Jersey or a coordinated cyberattack that targets multiple banks' account data). If the provider of backup services was not prepared for such heavy usage, it could be overloaded and end up being a channel for the transmission of operational problems because "as responders [at the backup service] work to restore the system to its normal state by resolving

241. *PFMIs*, *supra* note 239, at 7.

242. For a discussion of vulnerabilities associated with cloud providers, see *Regulatory and Supervisory Issues*, *supra* note 235. There have been some calls for dominant cloud providers to be designated as a financial markets utility that would be regulated pursuant to the PFMIs. *See, e.g.*, Press Release, Congresswoman Nydia Velázquez, Velazquez, Porter Urge FSOC to Oversee Tech Giants (Aug. 23, 2019), https://velazquez.house.gov/media-center/press-releases/velazquez-porter-urge-fsoc-oversee-tech-giants [https://perma.cc/9Z5F-QCEW].

243. "If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets." *PFMIs*, *supra* note 239, at 5.

244. *Revised PSMOR*, *supra* note 6, at 17.

245. *Principles for Operational Resilience*, *supra* note 75, at 5.

the initial failure and any cascading failures, their actions have the potential to introduce additional cascading failures as the system moves through unusual states on its way back to normal."[246] In an example of an overload failure, the third-party provider may not fail itself, but its atypical operations may cause problems that cascade into the systems of connected banks.[247]

Banks' business continuity plans are understandably kept confidential,[248] but one type of third party that such plans may rely upon is a cloud computing service that acts as a "data vault." Data vaulting is a practice that is intended to ensure that at least one encrypted backup of a firm's data is kept safe so that it can be accessed following a cyberattack, disaster, or hardware failure.[249] A data vault can be hosted at a remote data center maintained by a firm, but it can also be hosted in the cloud (which has the advantage of allowing the data to be stored on servers that are geographically remote from the bank's primary servers and backups).[250]

Banks cannot perform their critical functions without access to their data (for example, a bank cannot process a payment unless data is available that allows that bank to verify whether the payer has sufficient funds).[251] Data vaulting would be a useful recovery mechanism for any bank that has seen its primary data centers impacted by floods or had its data scrambled by a cyberattack. However, the cloud computing market is very concentrated[252] and if multiple banks rely on the same cloud provider to host their data vault and need to access their vaulted data at the same time, then it's possible that the cloud provider may not be able to fully support the enhanced load, and may propagate cascade failures as a result.

In particular, establishing links to a particular service can use up more capacity than maintaining existing service,[253] so even if the cloud provider can support all of the banks accessing backups once downloads begin, it may not be able to handle the stress of multiple banks connecting their restoration systems to the vaulted data at the same time. If a bank prepares its data recovery plans based on the assumption that it will be the only bank that will need to restore data hosted at a particular cloud provider at a particular moment in

246. Chamberlin, *supra* note 191, at 6.

247. "[S]upport systems are subject to failures just like other systems, and these failures can be cascading failures when they adversely affect the system they are supposed to be supporting." *Id.* at 11.

248. For example, JPMorgan's affiliated investment company JP Morgan Securities LLC disclosed to its clients that it had tested business continuity plans in place, but that "[t]he specific details of these plans are confidential for obvious security reasons." *Disclosure to Clients for Compliance with FINRA Rule 4370*, J.P. MORGAN, https://www.jpmorgan.com/content/dam/jpm/global/disclosures/by-business/JPMSI_Business_Continuity_Plan.pdf [https://perma.cc/EMS5-6QBY].

249. Margaret Rouse, *Data Vaulting*, TECHOPEDIA (Apr. 13, 2022), https://www.techopedia.com/definition/1071/data-vaulting [https://perma.cc/C6AG-H9UE].

250. *Id.*

251. David Mills et al., *Distributed Ledger Technology in Payments, Clearing, and Settlement* 5 (Fed. Rsrv. Bd., Working Paper No. 2016-095, 2016), https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf [https://perma.cc/M6VC-WPT8].

252. *Third-party Dependencies in Cloud Services: Considerations on Financial Stability Implications*, *supra* note 231, at 12.

253. Chamberlin, *supra* note 191, at 7.

time, it will miss the possibility that multiple banks may do so simultaneously[254] and that any failures the cloud provider experiences as a result of overload may cascade into and further compromise other banks' systems.

Ultimately, in an illustration of the "robust yet fragile" dynamic, the Principles' focus on quick restoration of service at individual banks may backfire. Delaying restoration of service at all banks, or sequencing restoration among banks, may be needed to protect the broader system.

ii. Open Banking Interoperability

In 2016, the European Systemic Risk Board prepared a report on the systemic risk implications of making central counterparties interoperable.[255] The ESRB identified many benefits of interoperability but also recognized that the "complexity and contagion in periods of stress" that come with interoperability were potential generators of systemic risk.[256] The report noted that "operational issues that limit the ability of a CCP to process cleared transactions will affect a linked CCP", and that the more entities are made interoperable, the more operational issues will increase.[257] These conclusions are consistent with our understanding of complex systems more generally and would apply equally to banks seeking to make their systems interoperable with the systems of other banks and third parties.

In other words, an operational problem originating in one bank could cascade through the systems of another bank that is directly interoperable with it (or is interoperable with a third party that is also interoperable with the first bank). These dynamics have already started to be scrutinized in the context of cyberattacks,[258] but as banks move to make their technology systems more directly interoperable to facilitate "open banking," more focus is needed on how that increased interoperability can increase both the number of contagion channels and the speed of contagion for operational problems (including cyberattacks,[259] but also normal accidents following technological glitches or natural disasters).

While there are many different approaches to "open banking," the Bank for International Settlements describes it as "the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services, such as those that provide real-time payments, greater financial transparency options for account holders, and marketing and cross-selling opportunities."[260] There are multiple ways of

254. Kashyap and Wetherilt note in the cyberattack context that "[i]f multiple firms are simultaneously attacked, each individual firm's assumptions about the availability of external resources may prove incorrect." Kashyap & Wetherilt, *supra* note 159, at 484. This would bear a resemblance to the inadequacies of living wills that assume that banks will only fail one at a time and not all together, and that there will therefore be other large banks available to buy them.

255. *ESRB Report to the European Commission on the Systemic Risk Implications of CCP Interoperability Arrangements*, EUR. SYSTEMIC RISK BD. [ESRB] (2016), https://www.esrb.europa.eu/pub/pdf/other/2016-01-14_Interoperability_report.pdf [https://perma.cc/6EWCG-8Y3G]

256. *Id.* at 15.

257. *Id.* at 20.

258. Kashyap & Wetherilt, *supra* note 159, at 483.

259. The BCBS has noted the "[c]hallenges of ensuring data and cyber security in an open banking framework." *Report on Open Banking and Application Programming Interfaces*, BANK FOR INT'L SETTLEMENTS [BIS] 6 (2019), https://www.bis.org/bcbs/publ/d486.pdf [https://perma.cc/85M2-2J6Q] [hereinafter *Report on Open Banking and APIs*].

260. *Id.* at 19.

implementing open banking, but APIs are high on the list:[261] Awrey and Macey have described APIs as "the technological backbone of an emerging financial market infrastructure designed to enhance data access, sharing, portability, and interoperability."[262]

APIs can prove an efficient way of sharing data between banks and non-banks; APIs can also be used to make systems interoperable to speed up payments.[263] Multiple banks might use APIs to connect their systems to those of a third party[264] (like a fintech firm that provides an app that allows customers to simultaneously see the balances they hold in different accounts with different banks, and make seamless transfers between them).[265] It is also possible that APIs could be used to connect bank systems directly. For example, before its failure, the global megabank Credit Suisse was reported to have adapted its open banking APIs to interbank transactions, with one spokesperson saying that "APIs enable innovative forms of collaboration and interoperability between banks," and that "[w]ith these solutions, we are supporting new forms for financial institutions to work together. The increased flexibility and efficiency benefit all parties and their end-clients."[266]

This increased flexibility and efficiency will be accompanied by new operational risks, however.[267] APIs are increasingly becoming an attack surface: vulnerabilities were recently detected in one fintech firm's APIs that would allow would-be attackers to "gain administrative access to the banking system using [its] platform."[268] In addition to being a target themselves, we should also consider whether APIs could also transmit problems among financial institutions. Complexity science suggests that "shortcuts" like APIs that allow data and funds to be transmitted more directly and quickly through the system will similarly allow technological problems to be transmitted among system components more directly and quickly.[269] Increased interoperability may, for example, provide channels that magnify the damage caused by a cyberattack—by targeting one bank that has made its technology systems interoperable with other systems, the attack could compromise multiple banks and third parties.

To demonstrate how a bank's defenses against business disruption and system failures may only be as strong as those of the weakest entity its systems interact with,[270] we can

261. *Fintech and Market Structure in Financial Services*, *supra* note 123, at 21. (defining "open banking" as a system reliant on APIs).

262. Awrey & Macey, *supra* note 126, at 4.

263. *Report on Open Banking and APIs*, *supra* note 259, at 6.

264. "Analysts at global investment bank Credit Suisse have estimated that the average U.S. bank account is now connected to more than 15 financial apps and other services." Awrey & Macey, *supra* note 126, at 45.

265. *Report on Open Banking and APIs*, *supra* note 259, at 9.

266. Andrew Saks-Mcleod, *Credit Suisse Applies Open Banking APIs to Interbank FX Transactions*, FIN. FEEDS (Nov. 24, 2020), https://financefeeds.com/credit-suisse-applies-open-banking-apis-interbank-fx-transactions [https://perma.cc/68P4-97HW].

267. These include "data breaches, misuse, falsification, denial of service attacks and un-encrypted login. Other types of identified risks include infrastructure malfunction, speed of execution and operations, man-in-the-middle attack, token compromise and IP address spoofing. An API gateway could also be a single point of failure if not designed to be resilient." *Report on Open Banking and APIs*, *supra* note 259, at 18.

268. SALT Labs, *API Threat Research: Server-Side Request Forgery on FinTech Platform Enabled Administrative Account Takeover*, SALT (Apr. 7, 2022), https://salt.security/blog/api-threat-research-server-side-request-forgery-on-fintech-platform-enabled-administrative-account-takeover [https://perma.cc/HBH3-7FLW].

269. Allen, *supra* note 113, at 466, 473. Regarding complexity, shortcuts, and systemic risk more generally, see Ruhl, *supra* note 107, at 417–19.

270. Resano, *supra* note 165, at 78.

look at the transmission of the NotPetya cyberattack (which did not involve APIs but was transmitted in part through networked computers). This cyberattack was the work of Russian military intelligence and was intended "to encrypt and paralyze the computer networks of Ukrainian banks, firms, and government"[271] (unlike a typical ransomware attack, this could not be reversed even if a ransom was paid—destruction was the end goal).[272] The NotPetya attack caused significant damage in Ukraine (including taking down the network of one large Ukrainian bank in 45 seconds), but it also spread beyond Ukraine, compromising several multinational firms and causing an estimated $10 billion in losses.[273] NotPetya "spread by opening email attachments of word documents,"[274] and once the virus infiltrated a system, it utilized a number of sophisticated mechanisms to jump to other networked computers[275]—including networked computers operating outside of Ukraine.[276] The important thing to note for our purposes is that computers that had downloaded the relevant security patch were protected from the initial download of the malware, but could still be infected by a linked computer that didn't have the security patch.[277] Cyberattacks like these are designed "to transit through weak spots both within and across borders of institutions."[278] Interoperability—achieved through APIs or otherwise—could therefore undermine a bank's defenses against cyberattacks, and their defenses against other business disruptions and system failures as well.

The use of substandard APIs may also facilitate the transmission of operational problems. "[B]uilding and maintaining public APIs can be time consuming and expensive for banks,"[279] and so resource pressures may result in APIs that lack the protections that are used to bolster the systems those APIs connect. APIs are sometimes the "weakest link" that

---

271. CROSIGNANI, MACCHIAVELLI & SILVA, *supra* note 158, at 5.

272. "It irreversibly encrypted computers' master boot records, the deep-seated part of a machine that tells it where to find its own operating system." Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [https://perma.cc/ZUX4-4FLH].

273. *Id.*

274. Natalia Zinets, *Ukraine Central Bank Warns of New Cyber-Attack Risk*, REUTERS (Aug. 18, 2017), https://www.reuters.com/article/idUSKCN1AY105 [https://perma.cc/G3FZ-DJTE].

275. A report on the NotPetya outlined that:

> NCCIC observed multiple methods used by NotPetya to propagate across a network. The first and—in most cases—most effective method, uses a modified version of the Mimikatz tool to steal the user's Windows credentials. The cyber threat actor can then use the stolen credentials, along with the native Windows Management Instrumentation Command Line (WMIC) tool or the Microsoft SysInternals utility, psexec.exe, to access other systems on the network. Another method for propagation uses the EternalBlue exploit tool to target unpatched systems running a vulnerable version of SMBv1. In this case, the malware attempts to identify other hosts on the network by checking the compromised system's IP physical address mapping table. Next, it scans for other systems that are vulnerable to the SMB exploit and installs the malicious payload. Refer to the malware report, MIFR-10130295, for more details on these methods.

Alert (TA17-181A): Petya Ransomware, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 15, 2018), https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware [https://perma.cc/XE88-WYRT].

276. Greenberg, *supra* note 272.

277. "You can infect computers that aren't patched, and then you can grab the passwords from those computers to infect other computers that *are* patched." *Id.*

278. Resano, *supra* note 165, at 67.

279. *Report on Open Banking and APIs*, *supra* note 259, at 9.

is most vulnerable to operational problems, which can then cascade into other linked systems. This has been demonstrated in the healthcare context, where APIs are widely used to facilitate sharing of sensitive patient data between different systems.[280] At the behest of a cybersecurity firm, one ethical hacker tried to hack the APIs used by 30 of the leading mobile health apps, and "discovered all were vulnerable to API attacks which could allow unauthorized individuals to gain access to full patient records."[281] The CEO of the cybersecurity firm concluded:

> The fact is that leading developers and their corporate and organizational customers consistently fail to recognize that APIs servicing remote clients such as mobile apps need a new and dedicated security paradigm. . . . Because so few organizations deploy protections for APIs that ensure only genuine mobile app instances can connect to backend servers, these APIs are an open door for threat actors and present a real nightmare for vulnerable organizations and their patients.[282]

Operational vulnerabilities have been particularly obvious in so-called "cross-chain bridges," APIs that link two blockchains together to make them interoperable.[283] Because of inherent limitations in their underlying technology, public permissionless blockchains do not scale very well.[284] The result is that in order to alleviate congestion and costs associated with processing crypto transactions, new alternative blockchains are being created—but a fragmented system depending on the use of multiple blockchains inhibits the "network externalities" (meaning a system becomes more valuable as more people use it) characteristic of financial infrastructure.[285] In an attempt to recapture these network externalities, APIs are being used to facilitate transactions across different blockchains,[286] making them interoperable.[287] However, the APIs used in these bridges are widely conceded to be some of the most vulnerable points for hacks and other operational problems.[288]

For another illustration, see financial regulatory agencies' plans to use APIs to facilitate information reporting by regulated financial institutions.[289] This could end up being

280. Steve Adler, *100% of Tested mHealth Apps Vulnerable to API Attacks*, HIPAA J. (Feb. 16, 2021), https://www.hipaajournal.com/100-of-tested-mhealth-apps-vulnerable-to-api-attacks [https://perma.cc/BUQ3-54J2].

281. *Id.*

282. *Id.*

283. Boissay et al., *supra* note 124, at 4.

284. *Id.*

285. *Id.* Network externalities refer to a system becoming more valuable as more people use it.

286. "Many blockchain bridges use APIs to initiate token transfers . . . ." Leeway Hertz, *Blockchain Bridge Between Ethereum and BSC*, MEDIUM (Dec. 9, 2021), https://medium.com/javarevisited/blockchain-bridge-between-ethereum-and-bsc-823baa2ffc5d [https://perma.cc/GK9Z-UWCG].

287. "To mitigate the problem of interoperability and allow for the transfer of coins across chains, "cross-chain bridges" have emerged. For example, a user can send 100 Ether to a centralized party (the bridge), where the Ether is stored. This transaction would be validated on the Ethereum blockchain. The bridge then mints new currency on another chain of equivalent value to the 100 Ether and transfers it to the user. This second transaction would be recorded on the other blockchain, not on Ethereum." Boissay et al., *supra* note 124, at 4.

288. Hertz, *supra* note 286; Samuel Haig, *Vitalik Sounds Alarm on Security of Cross-Chain Bridges*, DEFIANT (Jan. 11, 2022), https://thedefiant.io/vitalik-eth-cross-chain-bridges-security [https://perma.cc/8JPQ-X647].

289. Simone de Castri et al., *The Suptech Generations*, BANK FOR INT'L SETTLEMENTS [BIS] 4–5, FSI BRIEFS NO. 19 (2019), https://www.bis.org/fsi/publ/insights19.pdf [https://perma.cc/6LCP-KZMF].

another conduit for operational problems, because as I have discussed previously, "aspirations for interoperable reporting systems built on APIs that can ferry information back and forth between the systems of regulators and regulated entities could serve as shortcuts that inadvertently transmit technological problems from one system to the other."[290] The possibility of such an outcome (and attendant reputational damage) is something that regulators must keep in mind as they explore developing technology of their own.[291]

In sum, APIs have their own operational vulnerabilities and can be a channel capable of quickly transmitting cascading operational failures from one bank to another (directly, or through intermediaries).

2. Compound Risks

The previous Part explored how our current approach to existing operational risk regulation fails to anticipate that operational problems could ripple through technological contagion channels. Our current regulatory approach also underestimates the possibility that the kinds of events likely to cause damage to banks' physical assets or business disruption and system failures could follow one another in quick succession, amplifying the harm involved.

With these kinds of compound risks, the transmission channels are not within the banks, but entirely outside of the financial system—still, a quick succession of such events could prove challenging for individual banks, and perhaps the financial system more broadly, to withstand.[292] For example, a natural disaster that throws banks into chaos might result in those compromised banks becoming a particularly appealing target for a cyberattack, which would amplify the damage to banks that were already struggling. Or swift political action could come hard on the heels of the occurrence of a major natural disaster, perhaps requiring banks to divest immediately from all of their "dirty" investments.[293] An unusual volume of trade processing could tax banks' technological systems, potentially overloading them and causing them to shut down at a time when banks were already reeling from the fallout of the original disaster. It has also been surmised that "system-wide shocks may generate operational losses across several institutions as employees and managers may be distracted or desperate during systemic events."[294]

These kinds of compound risks can arise because banks' information technology systems are not just complex systems linked to other banks' complex systems; they operate in the context of a much larger and even more complex "system of systems" that has social

290. Hilary J. Allen, *Regulatory Innovation and Permission to Fail: The Case of Suptech*, 19 N.Y.U. J.L. & BUS. 237, 285 (2023).

291. *Id.*

292. For example, "natural hazards destroying socioeconomic infrastructures, such as hospitals, provide a fertile ground for pandemics to spread . . . ." Irene Monasterolo et al., *Financial Risk Assessment and Management in Times of Compounding Climate and Pandemic Shocks*, BROOKINGS (Oct. 22, 2021), https://www.brookings.edu/blog/future-development/2021/10/22/financial-risk-assessment-and-management-in-times-of-compounding-climate-and-pandemic-shocks [https://perma.ccMBP4-AZ7B].

293. *The Truth About Dirty Assets*, THE ECONOMIST (Feb. 12, 2022), https://www.economist.com/leaders/2022/02/12/the-truth-about-dirty-assets (on file with the *Journal of Corporation Law*).

294. Berger et al., *supra* note 17, at 18–19.

and ecological as well as technological components.[295] The result can be simultaneous or successive problems in multiple systems, which will compound the difficulty of coping with problems in individual systems. Compound failures are particularly salient in the context of climate change, where the damage wrought can cascade through the system of systems in a truly unpredictable manner.[296] Given their scale, compound failures can easily impact multiple banks simultaneously. For example, five of the seven biggest US banks, as well as five of the eight most critical providers of financial market infrastructure, are located in the New York City Metro area,[297] and a natural disaster affecting New York could affect all of those entities at the same time.

Under our existing regulatory regime, banks make plans to mitigate operational problems, particularly through the use of insurance.[298] However, insurance coverage and other mitigation measures associated with natural disasters, business disruptions, and system failures may prove inadequate because of the uncertainty associated with those kinds of "known unknowns", and are particularly likely to be inadequate in the context of compounding failures generating "unknown unknowns".[299] Situations where multiple banks are experiencing the same shock at the same time have been analogized to "'crowded trades,' where individual banks overestimate the liquidity that will be available when they want to unwind a position" because they fail to appreciate that other banks will also be trying to unwind at the same time.[300] The bandwidth of the broader system of systems to absorb bank operational failures will be reduced if similarly situated banks are suffering the same problem at the same time. For example, if a bank suffers multiple large and successive operational losses, the insurance coverage may be exhausted; the insurer may also be unable to pay out if it insures multiple similarly situated banks that were not expected to all claim at the same time.[301]

To be clear, the compound risk scenarios contemplated here are not even the worst-case scenarios. "[C]limate events are expected to continue to play out with compounded, permanent adverse consequences unless action is taken on a global level,"[302] and those compounded consequences may include pandemics, mass starvation, mass migration, war, and other geopolitical and social instability.[303] If the situation becomes dire enough, then bank operational risk regulation will be rendered irrelevant by the scale of calamity. In a

295. "[A]lthough we often compartmentalize social, ecological, and technological systems as distinct, it is becoming difficult to disaggregate them in operation, as automated online systems increasingly run infrastructure systems, expanding infrastructure systems increasingly degrade ecological systems, and degraded ecological systems diminish the resilience of human social and economic systems." Ruhl, *supra* note 107, at 411.

296. Monasterolo et al., *supra* note 292; Kemp, et al., *supra* note 119.

297. FIN. STABILITY OVERSIGHT COUNCIL, *supra* note 141, at 102.

298. *Working Paper on the Regulatory Treatment of Operational Risk*, *supra* note 52.

299. On insurers' potential unwillingness to insure uncertain events, see Abraham & Schwarcz, *supra* note 156, at 463.

300. EISENBACH, KOVNER & LEE, *supra* note 15, at 10.

301. In the context of cyberattacks, Abraham & Schwarcz have observed that "[w]hile insurers are well equipped to cover risks that are likely to impact a discrete number of policyholders at any given time, they have much more difficulty covering correlated risks that could produce massive aggregate losses." Abraham & Schwarcz, *supra* note 156 at 409–10.

302. Nahiomy Alvarez, Alessandro Cocco & Ketan B. Patel, *A New Framework for Assessing Climate Change Risk in Financial Markets*, FED. RSRV. BANK CHI. (Nov. 2020), https://www.chicagofed.org/publications/chicago-fed-letter/2020/448 [https://perma.cc/XCS5-CGWX].

303. Kemp et al., *supra* note 119, at 3.

more hopeful scenario, though, those extreme outcomes can be averted, and we can consider how operational risk regulation should be revamped to more accurately reflect the uncertainty that banks face.

IV. REINVENTED OPERATIONAL RISK REGULATION

To state the obvious, operational risk regulation can only do so much—it can't stop climate change or cyberattacks, nor can it fix the uncertainty inherent in complex systems.[304] Operational risk regulation can be improved, though. The previous Part explored two broad reasons why the existing operational risk framework for banks is inadequate. First, it is not responsive to the uncertainty surrounding operational problems that can lead to physical asset damage, business disruption, and system failures (and these kinds of problems have become more salient with climate change and banks' reliance on increasingly sophisticated information technology systems). Second, it does not embrace the possibility of technological and other non-financial contagion channels among banks. This Part will explore how operational risk regulation can be reinvented to address these inadequacies.

As a first step, how "operational risk" is constructed matters for how we think about it.[305] As currently constructed, "operational risk" is not particularly conceptually coherent. Operational risk regulation would benefit from not putting all operational risks in the same bucket. While the original definition of operational risk was purposefully capacious, to focus senior management attention on risks other than credit, market, and liquidity,[306] the threats of "damage to physical assets" and "business disruption and system failures" demand very different responses from bank management than operational risks like "individual credit card fraud, teller errors, employee expense fraud, or data entry errors, which are characterized by a relatively large number of events and relatively small losses per event."[307] "Damage to physical assets" and "business disruption and system failures" should be carved out of the existing framework for operational risk regulation.

We need not be precious about disturbing the concept of "operational risk", which was always a somewhat artificial and conflicted rhetorical construct, and one that was relatively recently constructed at that.[308] Even in 1998, the BCBS recognized that there was a distinction between "frequent, smaller operational losses such as those caused by occasional human errors are seen as common in many businesses" and "major operational risk losses [which] were seen to have low probabilities, but an impact that could be very large, and perhaps exceed those of market or credit risks."[309] The BCBS's first foray into defining operational risk also noted that while some banks understood technological risk to be a form of operational risk, others thought technological risk should be separated and treated

304. Peihani makes this point with regard to cyberattacks specifically. Peihani, *supra* note 154, at 161.

305. "[C]ategories such as 'operational risk' . . . provid[e] tentative maps for the reordering of practice and new languages and ideas for change agents at the organizational level." Power, *supra* note 2, at 578.

306. "In short, definitions of operational risk embody, intentionally or otherwise, intuitions about responsibilities." *Id.* at 585.

307. Sands, Liao & Ma, *supra* note 4, at 10–11.

308. *See supra* Part II (explaining BCBS and their development of Operational Risk Management Theory).

309. *Operational Risk Management*, *supra* note 41, at 4.

as a standalone risk category.[310] More recently, it has been acknowledged that the risk of cyberattacks does not fit easily within existing approaches to operational risk regulation.[311]

This Part will therefore propose the outlines of a new regulatory framework for "damage to physical assets" and "business disruption and system failures" under Pillars 1 and 2 of the Basel framework. This Article does not make any recommendations about how to best regulate the more common categories of operational risk (i.e. internal fraud; external fraud; employment practices and workplace safety; clients, products & business practices; and execution, delivery & process management).[312]

A. A Macro-Operational Approach

When it comes to "damage to physical assets" and "business disruption and system failures," the application of Pillars 1 and 2 needs to be revised in ways that are much more robust to uncertainty. While it is possible to simply "wait and see" in the face of uncertainty, that kind of approach is dangerous in situations where failing to act could result in outcomes that are both irreversible and catastrophic. As I have explored in previous work, major financial system failures cause irreversible and catastrophic harm to society, and this harm is not exclusively economic—financial crises can result in physical harm and even death.[313] Furthermore, the brunt of financial system failure tends to be borne by the most vulnerable members of society[314] (who are also likely to be the ones who suffer most from the more direct environmental consequences of climate change).[315] In the face of uncertainty, banking regulators should err on the side of caution and take steps to prevent financial crises.[316]

We tend to think of financial crises through the prism of historical experience, as events that prevent banks from performing their traditional role as credit providers for the broader economy.[317] Widespread operational problems at banks could certainly prevent banks from lending, but a massive operational failure of the financial system might also impact the broader economy in ways that are more direct and immediate than disrupted credit channels.[318] Imagine, for example, that a cascade failure inspired by a technological glitch incapacitates multiple banks' abilities to process retail payments. Presumably, a long and widespread payment outage could cause irreversible and catastrophic harm to the

310. *Id.* at 3.

311. "While cyber risks are superficially similar to other operational risks, they differ importantly in the form they take and the impact they can have." Kashyap & Wetherilt, *supra* note 159, at 486.

312. Aldasoro et al., *supra* note 89, at 356.

313. HILARY J. ALLEN, DRIVERLESS FINANCE: FINTECH'S IMPACT ON FINANCIAL STABILITY 30 (2022).

314. *Id.* at 24.

315. On the groups affected by climate change the most, David Arkush et al. finds that:

> Communities of color and low-income or low-wealth, indigenous, rural, and rustbelt communities are more likely to be impacted by floods, storms, drought, food and water insecurity, increased diseases, faltering infrastructure, increased violence, and most other climate harms. These same communities often have the fewest economic resources with which to respond.

DAVID ARKUSH ET AL., CLIMATE ROADMAP FOR U.S. FINANCIAL REGULATION iv (2021), https://www.citizen.org/wp-content/uploads/Climate-Financial-Reg-Report.pdf [https://perma.cc/9QRA-ZDG5].

316. Allen, *supra* note 22, at 198.

317. Allen, *supra* note 113, at 460–62.

318. *Id.* at 463.

broader economy (the Kenyan economy registered impacts from outages of the popular payment system M-Pesa that were only a few hours long).[319] At the more micro level, the inability to access funds even for a few days would prevent people from making time-critical payments for things like food, gas, medication, and shelter, which could quickly spiral into significant social problems.

Emergency measures like discount window lending and central bank guarantees, which are typically deployed to mitigate financial system failure once it begins, are often unable to fully contain the damage of a financial crisis.[320] It is also important to note that these types of emergency measures have been developed to address credit, market, and liquidity problems[321]—by and large, central banks and financial regulators have yet to design emergency interventions that could respond directly to operational problems.

A more precautionary approach is needed, to make banks more robust to damage to physical assets, business disruption, and system failures while there is still time to avoid some of their harms. Even though regulators don't have precise data or probabilities regarding these kinds of operational problems, that doesn't mean we have no idea how to respond to them: "[b]eing rational in a world of radical uncertainty involves ignoring information that is of little help, using experience (rather than data) and discretion, developing coping strategies and thinking about the future in qualitative terms."[322] A precautionary approach to these kinds of operational risks might perhaps be an easier political "sell" than a precautionary approach to other kinds of financial risks, because (unlike credit and market risks) banks aren't affirmatively trying to take on operational risks as a profit-making enterprise.

Past experience and creative thinking about the future should prompt regulators to adopt a more "macro-operational" perspective on operational risk regulation.[323] It became clear during the 2008 crisis that when individual banks sold assets to protect their own solvency they depressed the market prices of those assets, which ultimately threatened the solvency of other financial institutions that had invested in similar assets.[324] The hard-earned lesson was that we cannot assume that the whole financial system will be safe just because individual banks are managing their own credit, market, and liquidity risks—any regulatory regime predicated on that assumption will be inadequate. And yet that same inadequate "micro" perspective continues to govern operational risk regulation.[325] An update is required which recognizes that sometimes the steps taken by individual banks to

319. *Id.* at 470–71; *see also* Kotidis & Schreft, *supra* note 233, at 2 (explaining the risks that cyberattacks pose to financial security).

320. *Addressing Climate as Systemic Risk: The Need to Build Resilience within Our Banking and Financial System: Hybrid Hearing Before the Subcomm. on Consumer Prot. and Fin. Inst. of the H. Comm. on Fin. Services*, 117th Cong. 6–7 (2021) (prepared statement of Hilary J. Allen, Associate Professor of Law, American University Washington College of Law) [hereinafter *Addressing Climate*]. For discussions of the economic costs of financial crises, see U.S. GOV'T ACCOUNTABILITY OFF., GAO-13-180, FINANCIAL CRISIS LOSSES AND POTENTIAL IMPACTS OF THE DODD- FRANK ACT (2013).

321. *See supra* note 24 and accompanying text (providing an explanation of "ex post" tools).

322. Chenet, Ryan-Collins & van Lerven, *supra* note 21, at 10.

323. For another call for more macroprudential approaches to operational risk, see Jermy Prenio & Fernando Restoy, *Safeguarding Operational Resilience: The Macroprudential Perspective*, BANK FOR INT'L SETTLEMENTS [BIS], FSI BRIEFS NO. 17 (2022), https://www.bis.org/fsi/fsibriefs17.pdf [https://perma.cc/4TKF-YLTV].

324. Hanson, Kashyap & Stein, *supra* note 65, at 5–6.

325. *See supra* notes 223–27 and accompanying text.

make themselves more operationally robust may result in a more fragile system overall. In particular, overload cascade failures may become more frequent as banks take steps to strengthen their individual operational resilience because this will allow banks to continue operating at some level of capacity even during operational problems—and therefore be able to transmit their operational problems to the information technology systems of other banks.[326]

Complexity science teaches us, however, that systems can be made more robust to catastrophic failures by building in sensors, feedback mechanisms, and redundancies.[327] Redundancy is largely self-explanatory. Sensors can be designed to "detect internal and external changes that may pose threats to the continued functioning of the system," while "feedback protocols can be established to act on the input of those sensors, allowing the system to grow and evolve."[328] This Part will propose incorporating some new types of sensors, feedback mechanisms, and redundancies into the regulatory framework to improve operational robustness. This Part will also propose some measures to improve the reliability of some components of the banking system, but these proposals come with the caveat that focusing exclusively on component reliability and not enough on component interactions can make the system more susceptible to overload failures and therefore more fragile.[329]

To be clear, the project of addressing the operational risks identified in this Article cannot fall entirely on the shoulders of banks and banking regulatory agencies. A "whole of government" approach is needed, especially because of the importance of the electrical grid and telecommunications infrastructure to the provision of financial services.[330] Useful forums for collaboration on these issues include the Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection and the Financial and Banking Information Infrastructure Committee, which are already working on tools for "data collection, modeling, and visualization platform to identify the operational links among financial institutions and supporting infrastructure (e.g., energy and telecommunications)."[331] This Part, however, will restrict its focus to the piece of the puzzle which is improving operational risk regulation for banks.

B. Pillar 1

The main goal of Pillar 1's regulatory capital requirements is to ensure that a cushion of funding is available to allow banks to better absorb losses on their investments.[332] If a bank's cushion is too small and it experiences losses on its investments, there is a greater chance that that bank's repayment obligations will end up exceeding the value of its investments and that the bank could ultimately become insolvent.[333] Pillar 1 therefore forces

326. Regarding overload failures, see *supra* notes 108–09 and accompanying text.

327. Ruhl, *supra* note 11, at 594.

328. Allen, *supra* note 113, at 468. *See also* Ruhl, *supra* note 11, at 594.

329. Allen, *supra* note 113, at 467.

330. FIN. STABILITY OVERSIGHT COUNCIL, *supra* note 141, at 101–03.

331. *Id.*; *see also* Exec. Order No. 14030, 86 Fed. Reg. 27967 (May 25, 2021) (entitled "A Roadmap to Build a Climate-Resilient Economy").

332. For further explanation of regulatory capital requirements, see CARNELL ET AL., *supra* note 1, at 209–15.

333. *Id.* at 129.

banks to fund a minimum percentage of their investments with a cushion of funding that does not need to be repaid.[334] Banks otherwise have strong incentives, particularly under the tax code, to fund their investments with more borrowed money.[335] The most important requirement under Pillar 1 is the risk-based capital ratio: the numerator of the ratio is the cushion of funding (i.e. the capital itself) and the denominator is a number that represents the bank's "risk-weighted assets."[336]

The BCBS chose to risk-weight the denominator of this capital ratio because it wanted capital requirements to increase as a bank's asset portfolio became riskier: this risk sensitivity was intended to make it easier to detect banks' vulnerability to quantifiable risks.[337] Risk sensitivity can also be deployed to discourage banks from making certain types of highly risky investments. However, risk-weighting is much more complicated than a simple leverage ratio would be (in a leverage ratio, the denominator is simply the total assets of the bank),[338] as it requires a bank to calculate the likely losses associated with its portfolio of assets using highly sophisticated risk management models.[339] The price of heightened risk sensitivity is heightened complexity in the regulatory regime.

A bank's market and credit risk exposures are central to the calculation of its risk-weighted assets, but operational risk is also included in the calculation.[340] Until recently, Pillar 1 provided three different methods for calculating the operational risk component of risk-weighted assets,[341] all of which used some permutation of historical loss data and information about business conditions and internal controls.[342] On January 1, 2023, the BCBS's 2017 revisions to Pillar 1 became effective, and these stipulate one standardized approach to calculating the operational risk component of risk-weighted assets using information about business indicators and historical loss data over a ten-year time period.[343] This change was motivated by a desire for increased comparability and simplicity, but "the mathematics of the calculation turn out to be remarkably complex given the issues around defining loss and different types of income."[344]

---

334. Some capital must take the form of common equity, other capital may take the form of certain kinds of hybrid instruments that have features of debt and equity. Allen, *supra* note 57, at 830–31.

335. *Id.* at 839–44.

336. CARNELL ET AL., *supra* note 1, at 212.

337. Andrew G. Haldane, Exec. Dir. of Fin. Sec., Bank of Eng. & Vasileios Madouros, Economist, Bank of Eng., The Dog and the Frisbee, Speech at the Federal Reserve Bank of Kansas City's 366th Economic Policy Symposium 10 (Aug. 31, 2012), transcript available at https://www.bis.org/review/r120905a.pdf [https://perma.cc/6HNW-YBNY].

338. CARNELL ET AL., *supra* note 1, at 215.

339. "[C]apital requirements are usually calibrated on the basis of an implicit value at risk (or similar) methodology, with a view to measuring losses for specific exposures in contingent scenarios occurring with a predetermined probability." Coelho & Restoy, *supra* note 144, at 4.

340. Sands, Liao & Ma, *supra* note 4, at 2.

341. *Id.* at 7–8. There was significant variation in calculation methodologies between countries and banks as a result of this choice. *Id.* at 3.

342. Skinner, *supra* note 59, at 1592–93.

343. "The new SA calculates capital requirements according to a regulatory formula that uses as inputs income and expense items from banks' financial statements as well as banks' historical operational losses." Marco Migueis, *Regulatory Arbitrage in the Use of Insurance in the New Standardized Approach for Operational Risk Capital*, FED. RSRV. SYS. (Mar. 30, 2020), https://www.federalreserve.gov/econres/notes/feds-notes/regulatory-arbitrage-in-the-use-of-insurance-in-the-new-standardized-approach-for-operational-risk-capital-20200330.html [https://perma.cc/N34F-8EM8].

344. Sands, Liao & Ma, *supra* note 4, at 9.

National authorities must take steps to implement the revisions to the BCBS's standards in their home jurisdictions: the proposal for United States implementation, which is colloquially known as the "Basel III Endgame," is expected to increase banks' operational risk-related capital requirements and has met with fierce industry opposition as a result.[345] Putting bank profitability aside, though, risk-based capital regulation has also been criticized for inadequately serving the public interest.[346] This is due, in part, to its complexity.[347]

Haldane and Madouros have argued that simple decision-making rules are likely to be more robust to an uncertain future than more fine-grained and complex rules that depend on accurate assessments of future probabilities for their efficacy.[348] There are also those who more specifically criticize the use of risk weightings to address *operational* risk: as problematic as modeling credit and market risk exposures can be, we have more data about the probabilities associated with those exposures than we do for operational risks.[349] A bank also has less ability to reduce its operational risks, when compared with its ability to control the credit and market risks associated with its investments, and so risk-weightings are less effective in discouraging risk-taking behavior in this instance.[350] Another critique is that banks' internal models aim to calculate the losses that the *bank itself* is likely to incur and that regulators should not focus so heavily on a measure that neglects the costs that a bank's operational problems might have for others.[351]

Many of these critiques become more trenchant when dealing with the types of operational problems that result in damage to physical assets, business disruptions, and system failures. Predicting risk exposures becomes more challenging in environments that are largely devoid of relevant historical data,[352] and the complexity of information technology systems and the severity of climate events have no historical precedent. Risk management models are unlikely to be predictive when we are dealing with the types of "unknown unknowns" discussed in Part III of this Article, where probabilities cannot be estimated in any meaningful way.[353] For example, Eisenbach, Kovner & Lee have suggested that risk-

345. *See* David Wessel, *What is Bank Capital? What is the Basel III Endgame?*, BROOKINGS (Mar. 7, 2024), https://www.brookings.edu/articles/what-is-bank-capital-what-is-the-basel-iii-endgame [https://perma.cc/HQG7-UZKZ] (explaining the nature and origin of the Basel III Endgame regulations); Claire Williams & Kyle Campbell, *'Unprecedented': Banks' Lobbying Blitz Against Capital Rules*, AM. BANKER (Nov. 20, 2023), https://www.americanbanker.com/news/unprecedented-banks-lobbying-blitz-against-capital-rules [https://perma.cc/5AN7-NRPF] (highlighting the opposition to the Basel III Endgame regulations).

346. *See, e.g.*, Haldane & Madouros, *supra* note 337; Anat Admati et al., *Fallacies, Irrelevant Facts, and Myths in the Discussion of Capital Regulation: Why Bank Equity is Not Socially Expensive* 59–60 (Stan. Univ. Graduate Sch. of Bus., Working Paper No. 161, 2013) ("[H]igh leverage makes banking institutions highly *inefficient* and exposes the public to unnecessary risk and harm.").

347. Haldane & Madouros, *supra* note 337, at 19.

348. *Id*. at 2, 5.

349. Sands, Liao & Ma, *supra* note 4, at 11–13.

350. "The implication of this is that whereas credit and market RWA are powerful influences on management behaviour, operational RWA has very limited, if any, influence." *Id.* at 17.

351. "[T]he scale of the loss to the bank might not be the best measure of societal impact, and therefore of regulatory concern." *Id.* at 15.

352. "[O]perational risks are constantly evolving and the drivers of the biggest losses defy mechanistic prediction from historical data." *Id.* at 3.

353. Power, *supra* note 2, at 587–88 (claiming "data for operational risk management is most needed where it is both thin and conceptually problematic, i.e. for rare, high-impact possibilities").

based capital requirements may not be as effective against cyberattacks because of the general uncertainty surrounding such attacks.[354] Researchers at the Bank for International Settlements have similarly argued that Pillar 1 is not well suited to addressing climate-related risks to the financial system, because of the longer timeline and uncertainty associated with those risks.[355]

In short, it is not possible to estimate with precision the probability of the types of operational problems discussed in this Article, or the likely cost of such problems for a bank—or those outside of the bank. When it comes to damage to physical assets, business disruptions, and system failures, the BCBS should adopt a simpler approach to capital regulation that is more robust to uncertainty. Sands, Liao & Ma proposed removing operational risks entirely from the calculation of risk-weighted assets, and instead dealing with the risks by requiring an extra buffer of equity funding expressed as a percentage of market and credit risk-weighted assets.[356] A narrower and potentially simpler intervention would be to entirely dispense with the risk-weightings associated with damage to physical assets and business disruption and system failures but require banks to fund themselves with more of a buffer of equity capital, expressed as a percentage of the bank's total assets.[357]

Alternatively, adding a buffer of extra equity to existing risk-based capital requirements would provide a cushion to absorb miscalculations of risk weightings,[358] which would serve as a type of redundancy that could help absorb any kind of low-probability but potentially high-consequence events. This kind of approach could be deployed immediately, within the confines of the BCBS's existing capital regime. Regulators already have the authority to implement a countercyclical buffer that requires banks to fund up to an additional 2.5% of their risk-weighted assets with equity capital.[359] As an alternative or a supplement to the countercyclical buffer, regulators already have the authority to require the largest banks to fund their investments with higher percentages of equity capital[360]—current percentages could be increased to provide more cushion to absorb uncertainties about damage to physical assets and business disruption and system failures. Because a significant portion of banks' required capital is currently attributable to operational risk,[361] the implementation of larger buffers may be needed in any event to ensure that this Article's proposals to simplify capital regulation don't inadvertently reduce banks' capital requirements overall.

C. Pillar 2

If Pillar 1 is to be made less sensitive to certain kinds of operational risk as the previous Part proposes, the burden will fall more heavily on Pillar 2 to manage those kinds of

354. EISENBACH, KOVNER & LEE, *supra* note 15, at 10.

355. Coelho & Restoy, *supra* note 144, at 1.

356. Sands, Liao & Ma, *supra* note 4, at 24.

357. The simplest measure of a bank's capital position is "the market value of equity relative to unweighted assets." Haldane & Madouros, *supra* note 337, at 11.

358. For further discussion of the benefits of increased equity funding for banks, see Anat Admati et al., *Healthy Banking System Is the Goal, Not Profitable Banks*, FIN. TIMES (Nov. 9, 2010), https://www.ft.com/content/63fa6b9e-eb8e-11df-bbb5-00144feab49a (on file with the *Journal of Corporation Law*).

359. CARNELL ET AL., *supra* note 1, at 224.

360. *Id.* at 224–25.

361. Afonso, Curti & Mihov, *supra* note 37.

risk.[362] Pillar 2 is intended to ensure that banks "develop and use better risk management techniques in monitoring and managing" their risks, and also sets out a framework for the regulators supervising banks to "evaluate how well banks assess their capital needs relative to their risks and take measures, where appropriate."[363] Where "excessive risks, insufficient capital or deficiencies are identified, prompt and decisive action can be taken to reduce risk, address deficiencies or restore capital."[364]

Increased reliance on Pillar 2 is well suited to dealing with "damage to physical assets" and "business disruption and system failures," because Pillar 2 requirements are principles-based.[365] In a principles-based regime, broad principles are elaborated that "express the fundamental obligations that all should observe,"[366] and then banks are expected to comply with "the spirit of a regulation" rather than simply "box-ticking."[367] While principles-based regulation can devolve into *de*regulation if regulators defer too heavily to the industry and forego necessary enforcement,[368] this need not be the case. A principles-based regulatory framework where banks face real consequences for not living up to the principles provides flexibility that is well suited to dealing with uncertainty.[369] It is also more robust to threats that are rapidly evolving. For example, financial institutions have suffered cyberattacks even when their systems conform to applicable cybersecurity standards.[370] Enshrining the specifics of those standards in formal accords or rules would ensure that regulation rapidly becomes obsolete as the climate changes and technology evolves. In contrast, a flexible principles-based approach would allow new supervisory standards to be implemented as needed to adapt to changing operational realities, without legislation or rulemaking.[371]

Kashyap & Wetherilt have suggested some principles for regulating cyber risks that can be adapted for regulating uncertain operational risks more broadly.[372] First, a principle should be adopted that requires banks to operate with the presumption that a major disruption to their operations is inevitable.[373] Second, a principle should "[i]nsist that firms plan for prolonged and system-wide disruption, with particular attention to resourcing for

362. Haldane & Madouros have also called for increased focus on Pillar 2, advocating for "a rebalancing away from prescriptive rules," which "provides greater scope for supervisory judgment." Haldane & Madouros, *supra* note 337, at 16.

363. *Overview of Pillar 2 Supervisory Review Practices and Approaches*, BANK FOR INT'L SETTLEMENTS [BIS] 1 (2019), https://bis.org/bcbs/publ/d465.pdf [https://perma.cc/HS2M-P79S].

364. *Id.*

365. *See Pillar 2 Framework – Executive Summary*, BANK FOR INT'L SETTLEMENTS [BIS] 1 (2019), https://www.bis.org/fsi/fsisummaries/pillar2.htm [https://perma.cc/7Z5E-NWH5] ("[Pillar 2] is a principles-based standard premised on sound supervisory judgment . . . .").

366. Julia Black, Martyn Hopper & Christa Band, *Making a Success of Principles-Based Regulation*, 1 LAW & FIN. MKTS. REV. 191, 192 (2007).

367. Douglas W. Arner, Jànos Barberis & Ross P. Buckley, *The Evolution of FinTech: A New Post-Crisis Paradigm?*, 47 GEO. J. INT'L L. 1271, 1311–12 (2016).

368. Saule T. Omarova, *Wall Street As Community of Fate: Toward Financial Industry Self-Regulation*, 159 U. PA. L. REV. 411, 423 (2011).

369. Coelho & Restoy, *supra* note 144, at 4.

370. Brenner, *supra* note 161, at 37.

371. Black, Hopper & Band, *supra* note 366, at 193.

372. Kashyap & Wetherilt, *supra* note 159, at 484.

373. *Id.*

response and recovery."[374] Third, the principles adopted should "[a]im for a two-way dialogue between firms and supervisors as part of a wider collaborative approach to recovery objectives."[375] To these, we can add more specific principles relating to technical standards, reporting, and scenario analysis. Kashyap & Wetherilt recognize that regulation that focuses solely on how individual banks manage their exposure to these operational risks will be insufficient, and perhaps even counterproductive.[376] A more "macro" perspective is needed, and so the framework offered here is often "macro-operational" in orientation. This proposal for macro-operational regulation will inevitably need to be expanded and refined, but it is a start.

1. Technical Standards

There is currently a vibrant debate over whether regulation should be "technology neutral." This is a preference that is often expressed: for example, in a recent speech on the regulation of digital assets, Treasury Secretary Janet Yellen said, "[w]herever possible, regulation should be 'tech neutral.'"[377] Technological neutrality can have different meanings in different contexts, though.[378] Many have argued that issuers of securities should not be able to evade securities regulation simply by making the security a digital asset that lives on a blockchain, for example[379] – this type of tech neutrality makes sense. However, when it comes to banks' operational risks, these risks will vary significantly depending on the technology used to deliver financial services, and so the regulation of those risks should be different too. In short, operational risk regulation should not be technology neutral.

Regulators overseeing "other industries in which operational risk events can generate significant negative externalities—such as aviation, shipping, pharmaceuticals or nuclear— tend not to use capital requirements as a regulatory instrument, but instead put more reliance on standards, reporting, inspection, and accountability."[380] Right now, the principles regarding the quality of banks' information technology systems are expressed at an extremely high level. Principle ten of the Principles for the Sound Management of Operational Risk, for example, simply states that "Banks should implement a robust [information and communication technology] risk management programme in alignment with their operational risk management framework."[381] If Pillar 2 is to become the primary way in which regulators force banks to prepare for business disruption and system failures, then

374. *Id.*

375. *Id.* at 485.

376. Kashyap & Wetherilt, *supra* note 159, at 485.

377. Janet L. Yellen, Sec'y of the Treasury, Remarks on Digit. Assets at American University Kogod Sch. Bus. Ctr. for Innovation (Apr. 7, 2022), available at https://home.treasury.gov/news/press-releases/jy0706 [https://perma.cc/36HP-CS3H].

378. Chris Hoofnagle, *Should Regulation Be "Technology Neutral"?*, CHRIS HOOFNAGLE (Feb. 2, 2018), https://hoofnagle.berkeley.edu/2018/02/02/should-regulation-be-technology-neutral [https://perma.cc/YL69-BF7A].

379. *See, e.g.*, Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n, Kennedy and Crypto, Remarks at SEC Speaks (Sept. 8, 2022), available at https://www.sec.gov/news/speech/gensler-sec-speaks-090822 [https://perma.cc/P7B7-S3U6] ("The core principles from [the securities] statutes apply to all corners of the securities markets. That includes securities and intermediaries in the crypto market.").

380. Sands, Liao & Ma, *supra* note 4, at 16.

381. *Revised PSMOR*, *supra* note 6, at 16.

technological standards for banks' information technology systems should set a more prescriptive floor for supervisory expectations.

Bank information technology systems have many different components—they depend on some combination of hardware, software, data, and people, and their functioning will depend to some extent on the environment in which they operate.[382] This Part will focus primarily on standards for software (but that should not be interpreted as dismissing the importance of data, hardware, governance, or environmental conditions).[383] Such standards might stipulate minimum expectations about the choice of code libraries that will be used by the software engineers, the types of diagnostic tests that will be run, and the quality of data used to train any machine learning algorithm.[384] The National Institute of Standards and Technology has also formulated a Cybersecurity Framework, which has recently been updated[385]—compliance with these standards should also be expected. A principle should then be adopted that requires banks to monitor their technology and go beyond these prescriptive floors as technology, circumstances, and threats evolve—to ensure that the technology can discharge the function it was designed for, can do so reliably even under anticipated conditions of stress, and is resilient to attack.

Looking first at the minimum standards, special standards have been formulated for certain types of software that are considered "safety-critical" (including software deployed in "automotive vehicles, medical devices, and nuclear power plants").[386] While the failure of financial services is often characterized as financial harm, rather than as a matter of "life or limb", financial system failure *can* result in physical harm, and even its economic harm can be irreversible and catastrophic.[387] Certain banking software systems should therefore be considered "safety-critical," although they are not currently.[388]

Minimum standards for safety-critical software are roughly modeled on software standard DO-178, which was developed for the aviation industry.[389] DO-178 requires certain kinds of steps to be taken to avoid mistakes in the software development process, including mandating "code 'traceability,'" meaning that every requirement in the design document must be traced to the actual lines of code implementing that requirement.[390] Vice

382. "Information and communication technology" refers to the underlying physical and logical design of information and communication systems, the individual hardware and software components, data, and the operating environments." *Id.* at 16 n. 25.

383. For example, as machine learning becomes increasingly integral to banking operations, emerging standards about data quality and explainability may become relevant to operational risk regulation. For a discussion of these issues, see ALLEN, *supra* note 313, at 55–56.

384. *See id.* (regarding data quality); Choi, *supra* note 209, at 632 (regarding some of the quality checks used by software engineers).

385. NAT'L INST. STANDARDS & TECH., THE NIST CYBERSECURITY FRAMEWORK 2.0 (2024), available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

386. Choi, *supra* note 208, at 581.

387. Similarly, software developers have often escaped liability on the grounds that the loss they occasioned is "pure economic loss." *Id.* at 587.

388. For a comparative discussion of attitudes towards financial infrastructure compared with infrastructure relating to nuclear powerplants and airplanes, see Emery Roe & Paul Schulman, *When Critical Infrastructures are Interconnected: Lessons for Financial Services*, EUR. FIN. REV. (Jan. 2, 2017), https://www.europeanfinancialreview.com/when-critical-infrastructures-are-interconnected-lessons-for-financial-services/ [https://perma.cc/35LH-EH6Z].

389. Choi, *supra* note 208, at 581.

390. *Id.* at 577.

versa, every line of code must be traced back to a requirement in the design document, to avoid risks caused by "dead code" or "orphan code."[391] As a result, the processes of developers of safety-critical software—including in choosing the libraries of code they will use, and the diagnostic tests they will run—are very different from the processes of those developing, say, a social media app for a cellphone.[392] There may also be a need for standards particular to the banking industry, to focus the attention of software engineers on features of their programs that they may otherwise neglect, like "how numbers get stored and rounded when performing calculations . . . ."[393]

To be clear, software errors are inevitable to some degree: "[t]he uniform consensus of experts in the field is that software developers cannot avoid producing bad code as a matter of ordinary course."[394] While standards can and should be adopted to minimize unnecessary complexity and accidental mistakes, software cannot achieve its core purpose without a baseline level of complexity that makes it impossible to eliminate all cascade failures.[395] With so many possible permutations and combinations of code and data involved in creating even a relatively simple piece of computer software, there are an exponential number of ways in which the software could operate.[396] Standards mandating testing of more of these pathways will improve the quality of the software, but it's simply not practicable to test all pathways (and it will not always be clear at the outset which pathways to focus testing on). Testing opportunities may also be limited by circumstance: where a software engineer is developing code to repair an initial failure, they may not have time to follow usual procedures regarding testing, and so the code they produce is more likely to be flawed[397] (and may even trigger further failures, in the vein of Chamberlin's "ungraceful recovery").[398] Furthermore, as with any complex system, tradeoffs must be made when designing software: for example, steps taken to maximize cybersecurity may undermine reliability in non-attack conditions, and vice versa.[399]

Software errors should therefore be expected (in other words, software components of banks' operational systems can never be made perfectly reliable). As such, in addition to minimum technical standards, principles should be adopted that not only require banks to deal with software errors through continuing and ongoing refining and debugging[400] but also to deploy some combination of redundancies and backstops that limit the consequences of inevitable software errors.[401] One explanation that has been offered for why there have not been more airplane accidents, notwithstanding the imperfections of aviation-related software, is that "extraneous factors—such as pilot 'airmanship' or the safety design of non-software elements—have tended to save avionics software from itself."[402] This

391. *Id.* at 579.
392. *Id.* at 625, 632.
393. ARBESMAN, *supra* note 11, at 97.
394. Choi, *supra* note 208, at 566.
395. *Id.* at 571–73.
396. *Id.* at 572.
397. Chamberlin, *supra* note 191, at 9.
398. *Id.* at 11.
399. Choi, *supra* note 208, at 585.
400. *Id.* at 625.
401. *Id.* at 623 ("[T]he prospect of physical injuries and deaths caused by bad code is still uncommon, but that "safety" record is attributable to the modesty with which software is deployed.").
402. *Id.* at 580.

explanation is consistent with the general findings of complexity science, that redundancy makes systems more robust.[403]

Part III demonstrated that the operational resilience of one bank will sometimes depend, in part, on the operational resilience of other banks, and so systemic risks will be created if banks shirk investing in the robustness of their own infrastructure.[404] Standards and principles developed to ensure robustness for the sake of the public good will inevitably be costly and inefficient for individual banks, though, creating a collective action problem that needs to be solved by regulation.[405] When significant costs are involved, banks will sometimes try to skirt regulation,[406] and may deploy technology to avoid or outright violate regulation in sophisticated ways. For example, in a non-financial context, Volkswagen infamously deployed software in its cars that illegally enabled "VW vehicles to identify when they were being tested by regulators and perform differently under those conditions than when being driven by consumers on the road."[407] If there are going to be minimum standards for bank technology systems and principles that build on those standards, bank regulators will need to be able to assess compliance with them (so, for that matter, will senior bank managers). Financial regulators will therefore need expertise in complex systems, computer science, data science, and climate science to regulate the operational risks discussed in this Article. This expertise is not currently well-represented among banking regulators and will need to be built up either internally, or in other government agencies with which the banking agencies have a relationship.[408]

2. Reporting

Expertise comes from domain knowledge, but also from experience,[409] and banking regulators have had limited experience with climate and technology-inspired operational problems. Regulatory expertise can be improved, however, by requiring reporting of operational problems occurring across the banking industry.[410] As noted by Eisenbach, Kovner & Lee in the context of cyberattacks, "requirements to disclose to regulators even minor cyber events or to share with other banks information on threat assessments and contingency plans could increase resilience by reducing uncertainty and improving collective learning."[411] Concerning climate-related risks, one BIS report noted that relevant publicly available information about operational risks "is scarcer than for other risk types", and that

403. Ruhl, *supra* note 11, at 594.

404. Brenner, *supra* note 161, at 34.

405. "Individual firms have fewer incentives to internalize concerns about how an incident at their firm might affect overall confidence in the financial system (or potentially the overall functioning of the system if they provide a critical service)." Kashyap & Wetherilt, *supra* note 159, at 484.

406. This practice is often referred to as "regulatory arbitrage." For more on regulatory arbitrage, see generally Victor Fleischer, *Regulatory Arbitrage*, 89 TEX. L. REV. 227 (2010).

407. Nelson, *supra* note 175, at 1494.

408. For one proposal on how to achieve this, see Hilary J. Allen, *Resurrecting the OFR*, 47 J. CORP. L. 1 (2021). Alternatively, Mulligan and Bamberger have called for the reinstatement of the Office of Technology Assessment (which was defunded during the Gingrich era). Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance by Design*, 106 CAL. L. REV. 697, 734 (2018).

409. John Crawford, *Wargaming Financial Crises: The Problem of (In)Experience and Regulator Expertise*, 34 REV. BANKING & FIN. L.111, 126 (2015).

410. Power, *supra* note 2, at 589.

411. EISENBACH, KOVNER & LEE, *supra* note 15, at 10.

"[r]elevant information [about damage to physical assets and business disruption and system failures] is most likely to be held by the banks themselves."[412] It is critical that banks report these events to the regulators, and that they be broken out from data reported about other kinds of operational losses that might otherwise camouflage these events.

Banks have many incentives not to share such information, though, and may actively take measures to avoid disclosure.[413] If this Article's recommendations were adopted, banks' capital requirements would not be affected by losses arising from damage to physical assets or business disruption and system failures, and so bank personnel might have fewer concerns about reporting such operational problems.[414] However, banks (and even internal units in a bank) may still be discouraged from reporting operational problems because of reputational concerns.[415] Letting the public know about such problems could also cause panic among a bank's depositors or other creditors—from a financial stability perspective, this is undesirable.[416] Furthermore, such disclosure could make the compromised bank an attractive target for cyberattacks,[417] and attempts to disseminate information about cyberattacks in particular may conflict with national security objectives.[418]

Public reporting of these kinds of operational issues will therefore often be ill-advised, but reporting *to banking regulators* should be a critically important "sensor," detecting changes that constitute threats to the continued functioning of the financial system.[419] In November 2021, the U.S. banking regulators took a step in this direction. They adopted a rule that requires banks to report certain incidents that result in actual harm to the bank's information systems or information within 36 hours in order to allow regulators to "have early awareness of emerging threats to banking organizations and the broader financial system" (amongst other things).[420] However, this rule could be improved upon. Based on comments from the industry, the agencies narrowed their original proposal (which would have required notification of incidents that could potentially cause harm) to a rule where only notification of actual harm was required.[421] Given that the propagation of cyber incidents (both attacks and glitches) can be latent for some time, it can be hard in the moment to determine whether actual harm has occurred. Similarly, the limitation of notification requirements to situations where there is a "reasonable likelihood of materially disrupting

412. *Climate-Related Risk Drivers and Their Transmission Channels*, *supra* note 134, at 19.

413. For a discussion of how regulated firms may rely upon lawyers and attorney-client privilege to avoid disclosing information about cyberattacks to regulators, see Daniel Schwarcz, Josephine Wolff & Daniel W. Woods, *How Privilege Undermines Cybersecurity*, 36 HARV. J.L. & TECH. 421, 468–69 (2023).

414. Power, *supra* note 2, at 588. "A positive culture towards cyber incident handling can enable an organisation to shift its focus from trying to suppress incidents towards using these incidents to improve the organisation and enhance its readiness." *Effective Practices for Cyber Incident Response and Recovery: Final Report*, FIN. STABILITY BD. [FSB] 6 (2020), https://www.fsb.org/wp-content/uploads/P191020-1.pdf [https://perma.cc/CL9K-AL2V].

415. Kashyap & Wetherilt, *supra* note 160, at 484.

416. Christina Parajon Skinner, *Bank Disclosure of Cyber Exposure*, 105 IOWA L. REV. 239, 272 (2019).

417. *Id.* at 242.

418. Peihani, *supra* note 154, at 159–160.

419. For example, Kotidis and Schreft were able to use confidential data regarding a cyberattack that was only available to the Federal Reserve to explore the financial stability implications of cyberattacks. Kotidis & Schreft, *supra* note 233, at 11. On sensors, see *supra* notes 327–29 and accompanying text.

420. Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424, 66425 (Nov. 23, 2021) (to be codified at 12 C.F.R. pts. 53, 225, 304).

421. *Id.* at 66426.

or degrading the banking organization or its operations"[422] assumes that probabilities of harm can be calculated, which is inconsistent with the uncertainty surrounding cyberattacks. Reporting should therefore be expanded, not only to cover cyber incidents where the level of disruption or harm is uncertain, but also to cover other kinds of triggers for operational problems, like natural disasters.

Real-time reporting of operational incidents would be preferable, and it is possible that that could become technologically and economically feasible in the future.[423] In the meantime, however, it might make sense to lessen the regulatory burden on banks by allowing more time to deliver reports of smaller incidents (for example, a quarterly report detailing all such events in the previous three months might be sufficient). Again, with smaller incidents, it may also make sense to allow banks to report anonymously.[424]

Incident reporting should not be the only focus of reporting, however. As we will explore in the next Part, regulators should also try to understand fragilities even before a problem occurs by engaging in scenario analysis. Before they can do that, though, regulators will need banks to report certain information about their technological systems, as well as their relationships with other banks and third-party vendors. I have previously called for banks to regularly provide their regulators with a report known as "Form T":

> [Form T] would require regulated financial institutions to disclose all of the technological systems that they rely upon to deliver financial services. This Form T should require disclosure of any technology that forms the backbone of a particular financial product offered by the institution, as well as any technological system used by an institution to manage its operations internally (for example, machine learning systems used for institutional risk assessment, or cloud computing for data storage). Form T should also require disclosure of the technological qualifications held by members of the institution's board of directors and senior management, to give regulators insight into whether the financial institution is capable of overseeing its own use of technology.[425]

This Form T would provide insight into the vulnerabilities of an individual bank's technological systems, but it is also important to think about how such vulnerabilities could cascade into other banks. One approach might require banks to disclose to regulators all of their third-party relationships and technological connections[426] (including those that will only arise during a disaster) so that regulators can "map" shared dependencies and get a sense of the networks through which shocks could pass.[427] At the very least, bank regulators should consider doing a sweep exam of banks' business continuity and disaster recovery plans to get a sense of where overloads might occur in the future. Knowing that

---

422. *Id.* at 66430.

423. For a discussion of technological innovations in regulatory reporting, see Allen, *supra* note 290.

424. Anonymized data can still be helpful in understanding the types of operational problems experienced. Skinner, *supra* note 416, at 276.

425. ALLEN, *supra* note 313, at 164.

426. *Regulatory and Supervisory Issues*, *supra* note 235, at 6.

427. *Id.*; Peihani, *supra* note 154, at 153. Current US supervisory guidance already recommends that banks maintain "[a] current inventory of all third-party relationships (and, as appropriate to the risk presented, related subcontractors) that clearly identifies those relationships associated with higher-risk activities, including critical activities." *Interagency Guidance on Third-Party Relationships: Risk Management*, 88 Fed. Reg. 37920, 37936 (June 9, 2023).

regulators are focused on this issue in their examinations will hopefully encourage banks to be proactive in addressing any obvious vulnerabilities.[428]

In addition to gathering more information from banks about their operational dependencies and vulnerabilities, it would be helpful for bank regulators to obtain similar information directly from the third-party service providers the banks rely upon. Regulators' ability to do so will depend, however, on the boundaries of their jurisdiction. Some bank regulators do have direct oversight over some third-party service providers, but more typically, regulators only have the authority to supervise banks' handling of their third-party relationships, not to supervise the third parties directly.[429] Macro-operational regulation would certainly benefit from giving banking regulators more oversight over the third-party providers banks rely upon or are otherwise interoperable with, but the associated jurisdictional issues are beyond the scope of this Article.

3. Scenario Analysis

Historically, stress tests have been used to test banks' ability to remain solvent in specified hypothetical stressed scenarios–and poor performance on the stress tests has often resulted in requirements for banks to increase cushions of regulatory capital.[430] However, regulators and central banks have been reluctant to tie capital requirements to banks' ability to withstand hypothetical climate change scenarios, because of the level of uncertainty associated with climate change.[431] As a result, there has been significant interest in engaging in "scenario analysis," which is a similar process to stress testing, but with a different outcome. While banks are still assessed against hypothetical stressed scenarios, the results do not have immediate ramifications for banks' capital levels.[432] This kind of approach is well-suited to *all* operational risks associated with damage to physical assets, business disruptions, and system failures.

While stress tests are designed to test for a particular outcome, scenario analysis can be used to find out "what would happen if . . . ", which can be particularly useful in uncertain contexts.[433] The idea is not to predict exactly what will happen in the future, but to use scenario analysis to build a "skilled intuition" that can help banks and their regulators plan for these kinds of operational problems, and guide them when they eventuate.[434] A high-

428. "Examinations are conducted in accordance with published procedures and guidance, which lay out what examiners are looking for and put banks on notice of supervisory expectations." SHRAGO & ARKUSH, *supra* note 146, at 4.

429. *Report on Open Banking and APIs*, *supra* note 259, at 13. For a discussion on monitoring banks' handling of third party relationships, see *Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships: Discussion Paper*, FIN. STABILITY BD. [FSB] 5 (2020), https://www.fsb.org/wp-content/uploads/P091120.pdf [https://perma.cc/YN3H-ZVVT] ("All supervisory authorities rely primarily on [financial institutions] to manage the risks in their outsourcing and third-party relationships. They do so through regulatory requirements and supervisory expectations regarding how FIs should oversee these relationships, with a particular focus on those that are critical or important to financial stability; the safety and soundness of FIs; or the provision of critical or important functions.").

430. Baudino & Svoronos, *supra* note 133, at 2.

431. *Id.*

432. *Id.*

433. *Addressing Climate*, *supra* note 320, at 6–7.

434. Regarding fighting financial crises with "skilled intuition", see Crawford, *supra* note 409, at 141.

level principle should therefore be adopted that requires banks to engage in scenario analysis around significant operational failures.

When a particular type of event only occurs infrequently, there are few opportunities for banks and regulators to learn, practice, and refine their risk management approaches: in these circumstances, the use of imagination and experiments is critical.[435] In their paper on the potential financial stability implications of a cyberattack, Eisenbach, Kovner & Lee note that when rare events are involved, "[r]ather than wait to perform a post-mortem analysis", it is helpful to "conduct a pre-mortem analysis to uncover ways that attacks may be amplified."[436] The banking industry is already doing some of this on its own[437]—for example, SIFMA recently coordinated "a massive cross-industry cyber security drill that aims to ensure Wall Street knows how to respond in the event of a ransomware attack that threatens to disrupt a range of financial services."[438] However, banks sometimes have incentives to minimize or underplay the cyber threats they face[439] and are generally focused more on their own institutional interests than the interests of the financial system as a whole.[440] There is therefore an important role for regulators to play not only in supervising banks to ensure that they are engaging in scenario analysis but also in developing scenarios to highlight systemic vulnerabilities. The outcomes of these exercises (a type of sensor) can then guide regulators in their supervisory discussions with banks—which serve as a type of feedback mechanism.[441]

Scenario analysis methodology will need to be adapted, however, to address technological transmission channels. The methodologies typically used for stress testing and scenario analysis are focused on modeling the impacts of economic shocks, [442] rather than the transmission of technological problems. These existing methodologies will be useful for considering the impact of operational problems that intertwine with credit, market, and liquidity problems, but they won't be complete as they don't anticipate the types of cascade failures identified in Part III. Banking regulators should turn to other fields for inspiration on how to construct hypotheticals that highlight the impact of these types of failures.

Some technology firms engage in what is known as "chaos engineering": recognizing the likelihood of normal accidents, chaos engineering purposely shuts down random parts of a system at random times, driving software engineers to design systems that are robust to those disruptions.[443] This kind of practice can also identify when interventions following

435. *Id.* at 160.

436. EISENBACH, KOVNER & LEE, *supra* note 15, at 2.

437. "Organisations' plans and playbooks include severe but plausible cyber scenarios and stress tests that are based on high-impact, low-probability events and scenarios led by cyber threat intelligence that may result in service failure." *Effective Practices for Cyber Incident Response and Recovery: Final Report*, *supra* note 414, at 8.

438. Pete Schroeder, *Banks Ordered to Promptly Flag Cybersecurity Incidents Under New U.S. Rule*, REUTERS (Nov. 18, 2021), https://www.reuters.com/business/finance/banks-ordered-promptly-flag-cybersecurity-incidents-under-new-rule-2021-11-18/ [https://perma.cc/5S7M-8BXX].

439. Kashyap & Wetherilt, *supra* note 159, at 484.

440. ALLEN, *supra* note 313, at 20.

441. Baudino & Svoronos, *supra* note 133, at 2.

442. The focus is on "assess[ing] future exposures and potential losses." *Id.* at 4.

443. *See* ARBESMAN, *supra* note 11, at 10.

an operational problem could cause more harm than good in the long run.[444] Banks probably won't want to start shutting down their systems randomly, but *simulations* of what happens when shutdowns occur and interventions are taken could be very instructive. These simulations could be achieved with the assistance of artificial intelligence: many different machine learning approaches are being applied to stress testing electrical grids, for example,[445] and bank regulators could do the same. These simulations can be run over and over with slight tweaks and their output can then be worked into scenarios that are applied to banks (in uncertain environments, the more scenarios that can be constructed, the better).[446] To account for compound risks, scenarios should be devised that include more than one operational problem in succession.[447]

Scenarios should also have a "macro" dimension to ensure that the systemic dimensions of operational risk are not disregarded. For example, scenarios that only test individual banks' disaster recovery and business continuity plans in isolation may miss faulty underlying assumptions that only become clear when multiple banks are trying to recover at the same time and usage shifts to alternative infrastructures. When coordinated scenario analysis or "war games" are carried out, they are more likely to "identify the extent to which firms' plans for recovery are jointly realistic."[448] In a similar vein, scenarios could be made more severe when banks rely on shared infrastructure,[449] or when their systems are interoperable with the systems of other firms (banks and non-banks).

A group of central bankers and financial regulators known as the Network for Greening the Financial System ("NGFS") has been at the forefront of efforts to use scenario analysis to make banks more robust to climate change.[450] This is a positive development, but more varied climate scenarios are needed. There does not seem to be much content in the NGFS scenarios relating to operational risks – and there appears to be complete neglect of the possibility of technological transmission mechanisms of operational problems following climate events. The NGFS scenarios do, however, clearly anticipate compound risks as "macro" transmission channels.[451] The NGFS recognizes that their assumptions about how these macro transmission channels might function may turn out to be inaccurate given the underlying uncertainty,[452] but these scenarios can nonetheless help in the development of supervisory practices. Even if it is not appropriate for this kind of scenario analysis to be tied to the feedback mechanism of capital adjustments, other feedback mechanisms may be appropriate. For example, regulators may insist on geographical readjustments for some aspects of bank operations to promote diversification against the increased threat of severe weather events arising from climate change. Or regulators might

444. Chamberlin identified "actions taken by responders, in response to an initial failure, as unintentionally leading to a cascading failure." Chamberlin, *supra* note 191, at 9.

445. *See generally* Matteo Rizzato et al., *Stress Testing Electrical Grids: Generative Adversarial Networks for Load Scenario Generation*, 9 ENERGY & AI 100177 (2022).

446. Baudino & Svoronos, *supra* note 133, at 6.

447. For a discussion of compound risks, see *supra* Part III.B.2.

448. Kashyap & Wetherilt, *supra* note 159, at 485.

449. *Id.* at 486.

450. *NGFS Climate Scenarios for Central Banks and Supervisors*, NETWORK FOR GREENING FIN. SYS. [NGFS] 9 (2020), https://www.ngfs.net/sites/default/files/medias/documents/820184_ngfs_scenarios_final_version_v6_0.pdf [https://perma.ccR47E-6ATV].

451. *Id.*

452. *Id.* at 30.

insist that banks reduce their reliance on outdated legacy systems and rationalize the many different operating systems they rely upon.[453]

D. Pillar 3

Pillar 3 is supposed to "encourage market discipline by way of meaningful disclosure,"[454] but market discipline is unlikely to be particularly helpful in managing banks' exposure to damage to physical assets, business disruptions, and system failures. While it's possible that some market participants may be interested in disclosures about the robustness of a bank's policies and preparedness protections against operational risk,[455] market discipline has a fairly poor track record of reining in risky behavior by banks, with self-interested private actors typically having limited incentives to exercise any discipline until it is too late for that discipline to do anything other than cause panic.[456] More specifically, when it comes to the operational threats discussed in this Article, there is also an uncertainty problem to compound the incentive problem. As Part III.A explored, banks don't affirmatively take on the risk of natural disasters or system failures, and banks cannot predict with any precision the losses that will occur if they are passively condemned to experience during such an event. Given this uncertainty, it is unsurprising that some banks' disclosures relating to operational risk have been described as only "cursory."[457] Market discipline will presumably be less effective when market participants cannot assess if and when operational problems will transpire, and what the ripple effects of such problems will be.[458] Pillar 3 is therefore unlikely to be very effective in managing banks' exposure to damage to physical assets, business disruptions, and system failures. This underscores the importance of Pillar 2 in managing these kinds of operational threats.

E. Emergency Response Playbook

The regulatory approaches outlined so far in this Part are *ex ante* regulation, in the sense that they try to preemptively make banks more robust to operational problems that might occur.[459] Although there is often a sense of inevitability about cascade failures occurring in complex systems—that is why Charles Perrow chose the term "normal accidents" to describe the results of cascade failures in complex systems[460] —*ex ante* efforts can be effective to some degree. Some data suggest that better regulation and supervision

453. *See supra* notes 200–02 and accompanying text.

454. *Pillar 3 Framework – Executive Summary*, BANK FOR INT'L SETTLEMENTS [BIS] 1 (2019), https://www.bis.org/fsi/fsisummaries/pillar3_framework.htm [https://perma.cc/U2Q5-NB8Y].

455. Skinner, *supra* note 416, at 275.

456. As David Min argues, bank shareholders may often benefit from the bank's risk-taking in the short-term, and many of the bank's creditors (including depositors) do not wish to expend the effort needed to monitor the bank's risk-taking until it is too late. David Min, *Understanding the Failures of Market Discipline*, 92 WASH. U. L. REV. 1421, 1470 (2015).

457. Sands, Liao & Ma, *supra* note 4, at 17.

458. For example, Madison Condon has observed that, in general, "markets are not accurately assessing and pricing climate change-related risks." Madison Condon, *Market Myopia's Climate Bubble*, 2022 UTAH L. REV. 63, 65.

459. For a discussion of the difference between *ex ante* and *ex post* financial stability regulation, see Hilary J. Allen, *Putting the "Financial Stability" in Financial Stability Oversight Council*, 76 OHIO ST. L.J. 1087 (2015).

460. PERROW, *supra* note 11, at 5.

reduce losses related to cyberattacks[461] and reduce operational losses overall,[462] and the stakes are such that regulators should do what they can to make the banking system more operationally robust. As one report on cybersecurity put it, "[t]otal security is not achievable. But a materially improved security environment for the infrastructure on which virtually all economic and social activity depend can be created with sufficient resources and political will."[463]

Still, *ex ante* regulation is not perfect, and it does not seem wise to put all our eggs in that one basket. Much of the literature on normal accidents assumes that no steps will be taken to intervene once the cascade failure starts, but in reality, there are often opportunities for intervention once it begins.[464] We should therefore look to the literature on sensors, feedback mechanisms, and redundancies for guidance on how to address or mitigate cascade failures once they start.[465]

Complexity scientist Dirk Helbing has argued that it is necessary to "prepare and exercise contingency plans for all sorts of possible failure cascades" in order to facilitate recovery and repair.[466] Currently, preparation for cascading operational problems is left primarily to banks to manage internally.[467] In particular, banks are already subject to principles that direct them to develop disaster recovery and business continuity plans.[468] However, as this Article has already explored, the banking system as a whole may suffer as a result of the interactions of multiple banks simultaneously following their own individual disaster recovery and business continuity plans. Particularly if banks resume operations before they're truly ready to do so, that might set off an overload failure that compromises other banks. Regulators should therefore be wary of judging banks' disaster recovery and business continuity plans by how quickly they allow banks to resume operations.

Of course, there aren't just regulatory pressures to resume services once a cascade failure starts: banks will also have commercial motivations to resume services as quickly as possible. Where slower recovery and resumption of services are critical to making the overall banking system more robust, sensors and feedback mechanisms will be needed to allow regulators to pause bank operations where necessary. Similarly, where interoperability between bank systems has the potential to serve as a conduit for the transmission of disabling operational problems, regulators may also need to pause certain bank operations. We should therefore consider how regulators might apply circuit breakers in response to operational problems: "generalised circuit breakers are intended as 'time-out' rules aimed at pausing the normal course of intermediaries' business in situations where cyber incidents [or other operational problems] may put financial stability at risk."[469]

If real-time reporting of operational problems becomes technologically feasible, such reports could serve as sensors that alert regulators to operational problems, and then

461. Aldasoro et al., *supra* note 89, at 30.

462. *Id.* at 4.

463. Brenner, *supra* note 161, at 5.

464. Roe & Schulman, *supra* note 388.

465. "[S]ome degree of systemic risk is inherent in any complex adaptive system—but the balance between robustness and fragility is something we can hope to influence." Ruhl, *supra* note 11, at 565.

466. Helbing, *supra* note 11, at 55. *See also* Ruhl, *supra* note 11, at 565.

467. *See* notes 223–27 and accompanying text.

468. *See* notes 244–45 and accompanying text.

469. Resano, *supra* note 165, at 64.

regulators can deploy a kind of circuit breaker.[470] Thought needs to be given, though, as to how regulators might practically prevent banks from resuming operations and how dire the situation needs to be before they do so. One idea might involve temporarily shutting down access to the Federal Reserve Master Accounts needed for payment processing.[471] There are already difficult transparency and accountability issues associated with more traditional emergency playbooks, like central banks extending credit to banks experiencing liquidity problems as "lenders of last resort".[472] At least with lender-of-last-resort facilities, banks are receiving funds rather than having their operations suspended. There will be extremely challenging accountability and distributional questions associated with unelected regulators suspending banking operations (which would presumably entail suspending bank customers' rights to transact) in situations where there's unlikely to be any time for judicial review of the regulator's decision. Because of these challenges, there may be a temptation to avoid thinking about this kind of regulatory intervention, but that would be shortsighted.

Climate change is already forcing energy authorities to make difficult determinations about shutting down energy services.[473] Moreover, energy authorities are being forced to make these decisions during the "fog of war"; banking regulation would benefit from some forethought on these matters. Forethought should also be given to the redundancies that can be preemptively built into the system to make it more robust should a problem occur. For example, an *ex ante* rule may be needed that prevents banks from relying on certain kinds of shared infrastructure. Even if banks' local data centers individually tend to have more operational vulnerabilities than, say, a widely used cloud provider, from a systemic perspective, a cloud failure could be much more harmful than regular but scattered local outages.

Sometimes, the redundancy will need to be provided by a public authority. Traditionally, central banks have provided a type of redundancy through their lender-of-last-resort function, lending to illiquid banks when no other market participant will.[474] However, this type of redundancy will not be effective when problems in delivering banking services are purely or primarily operational. The Federal Reserve has experimented with other emergency responses that are more tailored to operational problems, like extending processing time for payments.[475] Consideration of other responses in this vein would be helpful, but it should be noted that central banks' own systems can also experience technical outages.[476]

---

470. EISENBACH, KOVNER & LEE, *supra* note 15, at 10.

471. For further exploration of this idea, see Hilary J. Allen, *Digital Bank Holidays*, YALE J. ON REG. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4756871 (on file with the *Journal of Corporation Law*).

472. "Most commentators agree that the anger engendered by emergency lending around the world during the Financial Crisis shows the need for a regime that is more accountable and responsive to democratic checks." MICHAEL S. BARR, HOWELL E. JACKSON & MARGARET E. TAHYAR, FINANCIAL REGULATION: LAW AND POLICY 884–85 (2016).

473. "[T]here was a significant controversy when PG&E selectively shut off power for some of its customers during the 2019 California wildfires, for example." ALLEN, *supra* note 313, at 180–81. *See also* Annie Lowrey, *Alone in the Dark in the Bay Area*, ATLANTIC (Oct. 12, 2019), https://www.theatlantic.com/ideas/archive/2019/10/californias-power-outage/599935/ [https://perma.cc/T8XS-YNAT].

474. ARMOUR ET AL., *supra* note 32, at 78.

475. Kotidis & Schreft, *supra* note 233, at 23.

476. Jeff Cox, *The Fed's System that Allows Banks to Send Money Back and Forth Went Down for Several Hours*, CNBC (Feb. 24, 2021), https://www.cnbc.com/2021/02/24/the-feds-system-that-allows-banks-to-send-money-back-and-forth-is-down.html [https://perma.cc/VGZ3-Q4QA3].

The most obvious—and low-tech—way to ensure that there is some slack during systemic operational problems is to preserve the viability of cash, which is currently under threat in some areas.[477] Given the possibility of an increased need for physical cash as natural disasters, cyberattacks, and other technological problems compromise our banking infrastructure,[478] public investment in cash infrastructure is critical.

V. CONCLUSION

Banking regulation is generally considered the province of economists, lawyers, and accountants, and it tends to neglect the possibility of operational risks that could arise as a result of systemic interactions best understood by scientists. This Article has brought the work of some of these scientists—work on climate change, complex systems, and computer science—into conversation with the BCBS's operational risk regulation framework. In doing so, this Article has demonstrated that that framework, as it pertains to potential losses resulting from damage to physical assets and business disruption and system failures, is inadequate. This Article has also made the case that the existing framework will only become more inadequate as banks adopt increasingly sophisticated information technology systems and natural disasters become more frequent. There is an unfortunate tendency to maintain status quo banking regulation until a crisis erupts to showcase its inadequacies, but this Article urges the BCBS and other policymakers to be more proactive in adopting a macro-operational risk regulation framework that is more robust to the growing uncertainty banks face.

477. "As the variable revenues associated with operating a cash infrastructure fall below the fixed costs, maintaining the cash infrastructure becomes untenable." Geoffrey Goodell & Hazem Danny Al-Nakib, The Development of Central Bank Digital Currency in China: An Analysis 2 (Oct. 26, 2021) (unpublished manuscript), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3906358. For an overview of the arguments for keeping cash as a payment mechanism, see BRETT SCOTT, CLOUDMONEY: CASH, CARDS, CRYPTO, AND THE WAR FOR OUR WALLETS (2022).

478. For example, when ice movement near Alaska cut the subsea fiber network in June 2023, several rural Alaskan towns lost all internet access, and businesses were forced to pivot to cash transactions. Alena Naiden, *Residents Hit by Rural Alaska Fiber Network Outage Turn to Satellite Internet, Analog Operations*, ANCHORAGE DAILY NEWS (June 15, 2023), https://www.adn.com/alaska-news/rural-alaska/2023/06/15/residents-hit-by-rural-alaska-fiber-network-outage-turn-to-satellite-internet-analog-operations/ [https://perma.cc/C588-LGKX].