“Comments on Eisenbach, Kovner, Lee”

July 8, 2020

Anil K Kashyap

I do not see how one can look at figures like these without seeing them representing possibilities. Is there some action a government of India could take that would lead the Indian economy to grow like Indonesia's or Egypt's? If so, what exactly? If not, what is it about the "nature of India" that makes it so? The consequences for human welfare involved in questions like these are simply staggering: **once one starts to think about them, it is hard to think about anything else.**

Robert E. Lucas, "On the Mechanics of Economic Development." Journal of Monetary Economics. 22 July, 1988

CHICAGO BOOTH
The University of Chicago Booth School of Business

Outline*

1. Brain candy: fascinating facts and findings

2. Their scenario

3. Bigger picture cyber issues

* These are my own views and not those of Bank of England Financial Policy Committee.

The Network

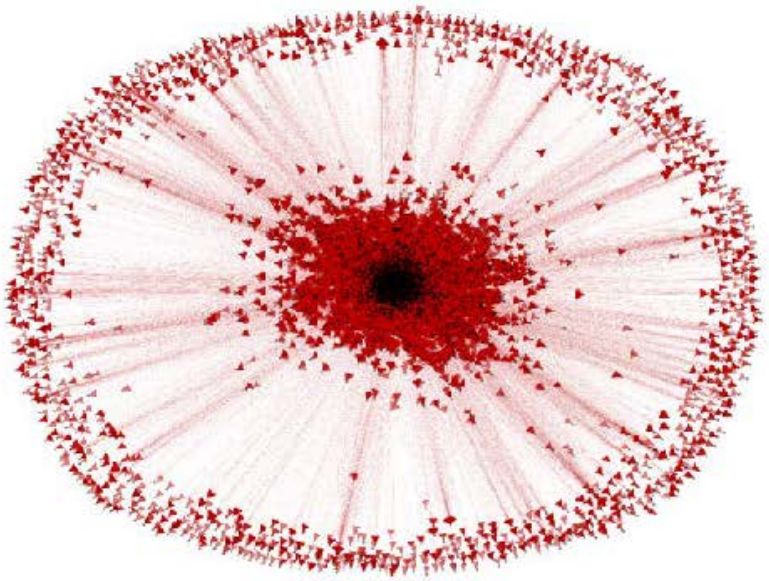
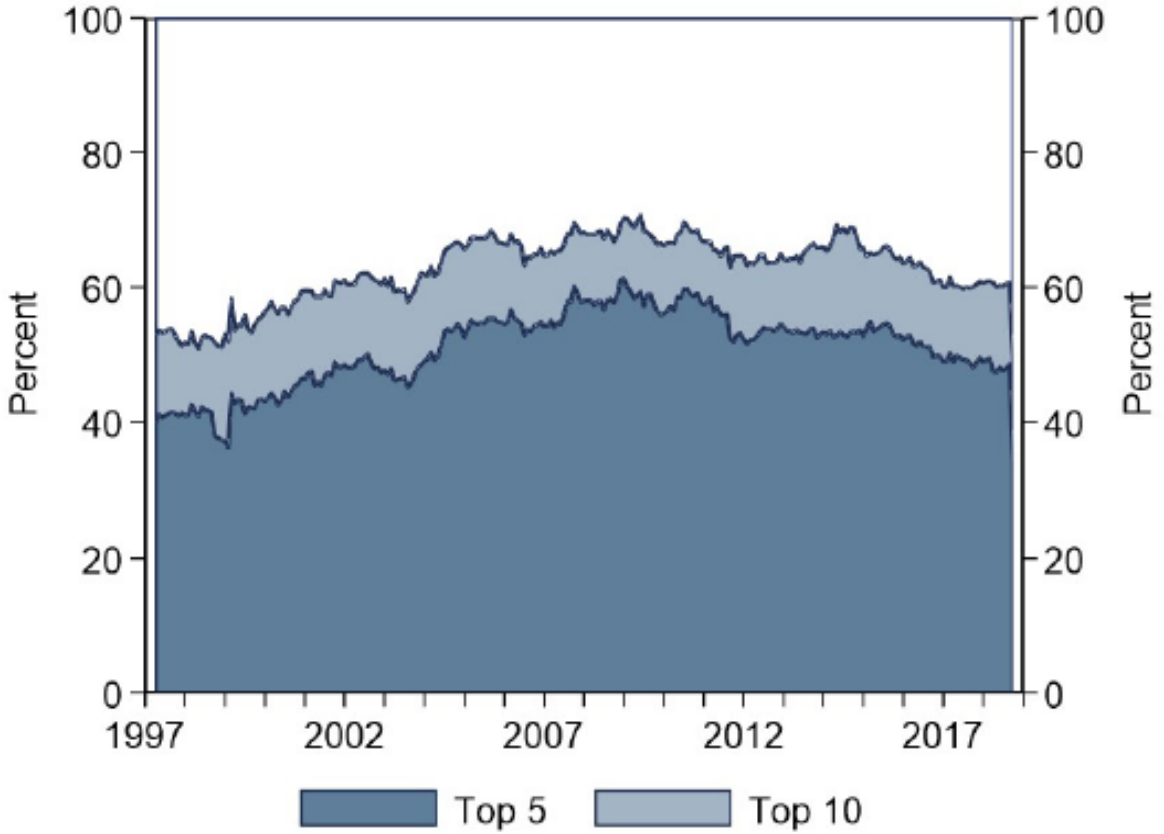


Figure 1: Fedwire payment network. Network representation of the Fedwire payment system. Lines represent payment flows between participant on Fedwire. Distance between pairs represents value of payment flows.

Five staggering facts/findings

5. Concentration importance of the top 5 banks (about 50%)



(a) Concentration of payments

Five staggering facts/findings

4. Seasonality in the vulnerability

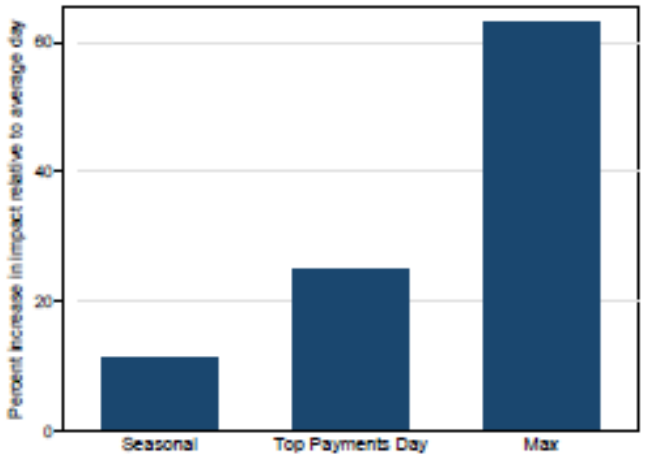


Figure 7: Network impact conditional on attacker's information set. The figure shows how much higher the network impact of an attack on a top-5 institution is on particular days relative to an average day. From left to right, bars show the percent increase in the average weighted share of institutions that become impaired if the attack occurs on a seasonal day, on a top payment day, and on the day of maximum impact, respectively.

Table 1: Summary statistics. The table shows summary statistics of payments in Fedwire.

	Avg.	St. dev.	p1	p25	p50	p75	p99
Total sent$_{i,t}$ (millions)	519.94	9588.86	0.00	0.00	0.37	3.16	7242.90
Avg. by institution i (millions)	508.75	9318.75	0.00	0.15	0.86	4.29	7818.85
Total on day t (trillions)	2.85	0.32	2.32	2.63	2.81	3.02	3.73

Five staggering facts/findings

3. Importance of the Foreign Branches

Table 4: Summary statistics of reverse scenario including FBOs. The table reports the distribution for the reverse scenario of $|U_{Nt}^{\min}|$ for entities under \$10 billion in asset size, $N = 10$, and entities between \$10 and \$50 billion in asset size, $N = 50$, including branches of FBOs. "Days with Impairment" indicates the number of days for which there existed at least one set of banks in U_N for which a top-5 institution would become impaired.

Impairment	p1	p25	p50	p75	p99	Mean	SD	Days with Impairment
U_{10}	1	1	2	6	381	11	43	180 of 250
U_{50}	1	1	1	1	6	1	1	250 of 250

Five staggering facts/findings

2. Shared technological risk, part 1

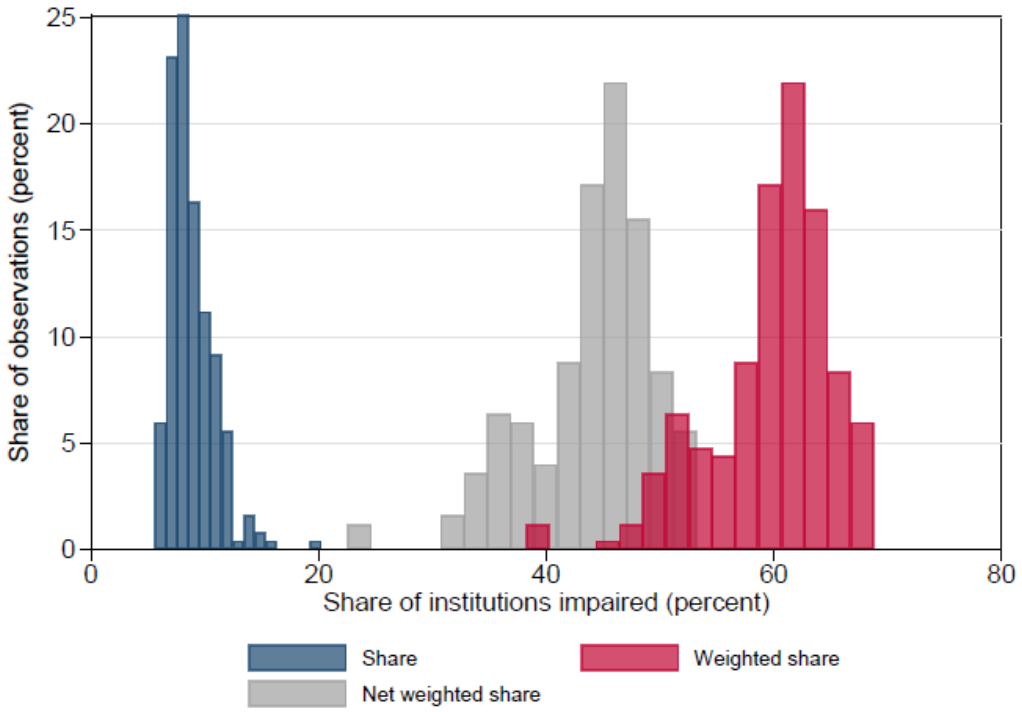
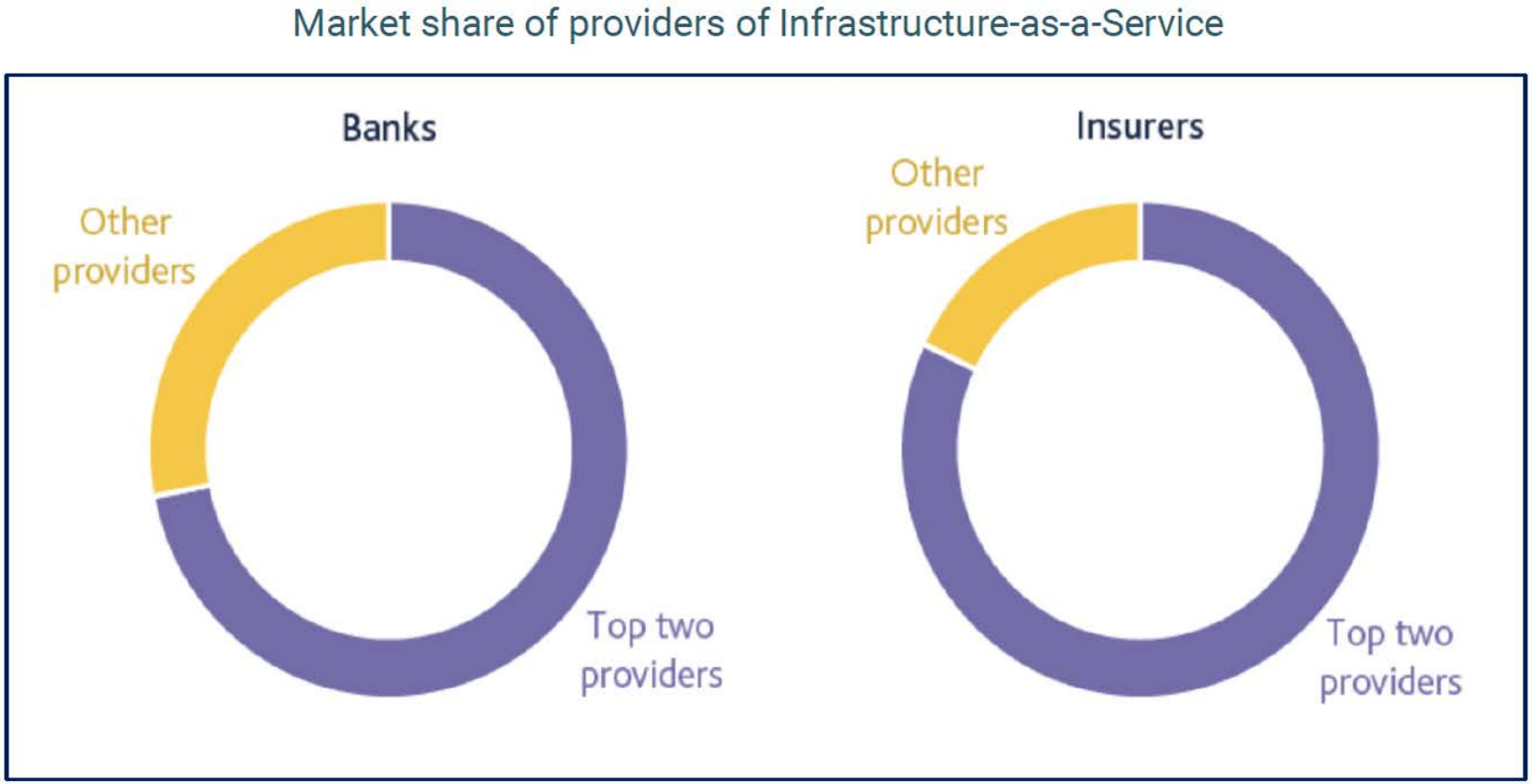


Figure 14: Cyber vulnerability through a third-party service provider. The figure shows the distribution of the network impact for the scenario with a disruption originating from a third-party service provider. "Share" represents the unweighted percent of institutions that become impaired. "Weighted share" represents the percent of institutions that become impaired, weighted by asset size. "Net weighted share" refers to the percent of institutions that become impaired, net of the shocked institutions.

Five staggering facts/findings

2. Shared technological risk, part 2



'CLOUD CONCENTRATION RISK II: WHAT HAS CHANGED IN THE PAST TWO YEARS?' *Cloudera White Paper*, 2020 10.13140/RG.2.2.31023.15524

Five staggering facts/findings

1. Data Integrity Risks (buried in footnote 2!)

Dwell time: the time from first evidence of compromise to detection

https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

The one day liquidity black hole

Very natural case to consider, though perhaps it is not a particularly worrisome case because:

i) almost all business continuity planning involves recovery in one day, so banks need to worry about this

ii) central bank is particularly well-positioned to offset this kind of a shock because the bank was solvent at t-1 and you know which payments showed up during the day.

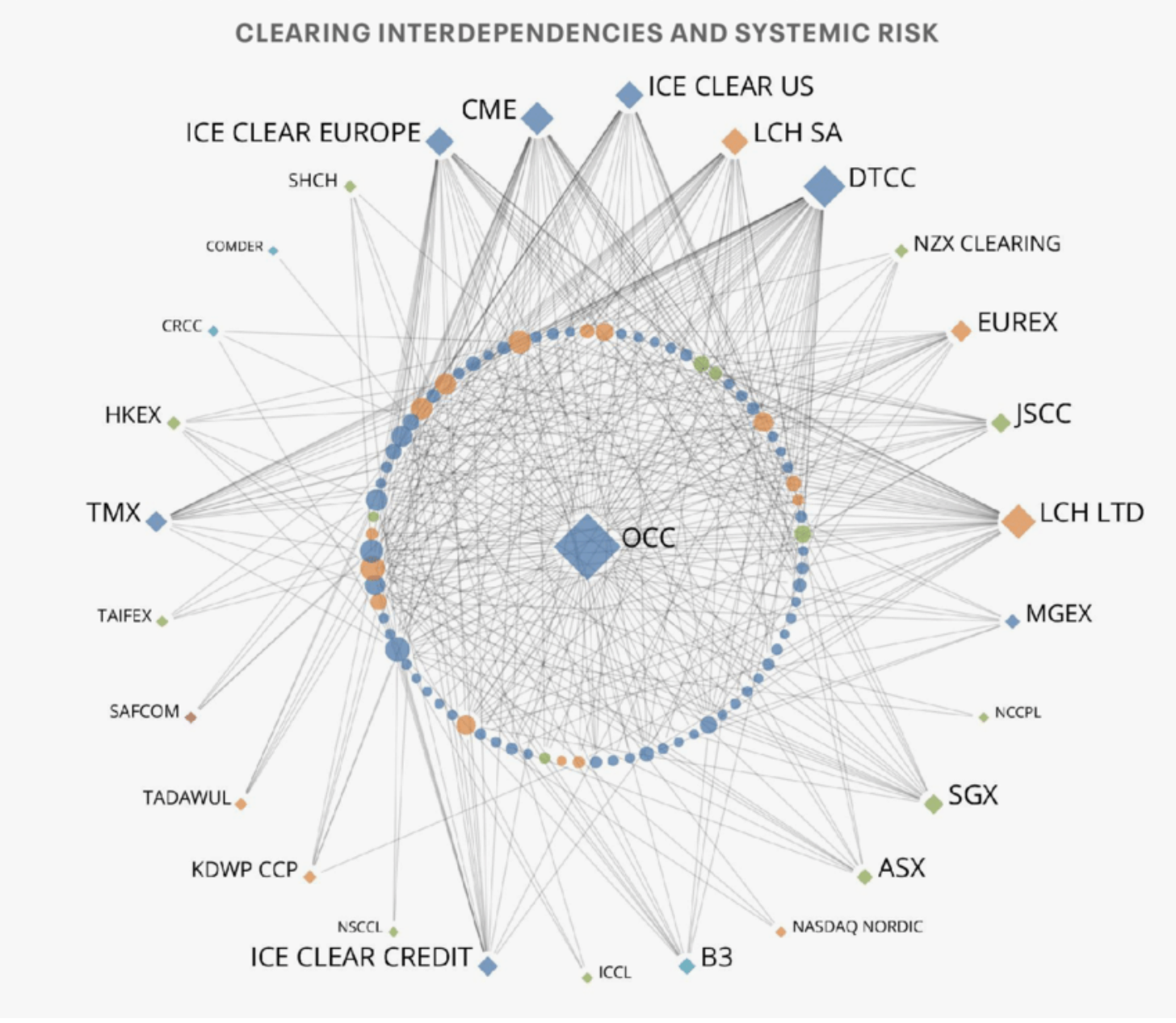
General cyber threats

- For financial institutions, it is a matter of when not if

- Intent may be purely to do maximum damage. Mediant reports (their case load)
  - 7% originate or used compromised third party access
  - 22% had data theft likely in support of intellectual property or espionage end goals
  - 29% were likely for direct financial gain, including extortion, ransom, card theft and illicit transfers
  - 3% were for the purpose of reselling access gained in the intrusion
  - 4% were apparently purely to create compromised architecture for future attacks

- Tradeoff: Maximum damage vs what can I get away with?

Clearing Risks



My nightmare scenario

- Data integrity attack because

1. Runs counter to the policy of restore things as quickly as possible

2. Firms regularly overwrite backups

3. If executed on third-party software, could infect many firms at once and overwhelm private sector resources