Cyber Risk as Systemic Risk

Jon Danielsson
Systemic Risk Centre
London School of Economics

www.systemicrisk.ac.uk

June 10th 2016

Based on

- "Cyber Risk as Systemic Risk"
- by Jon Danielsson, Morgane Fouché and Robert Macrae
- out on VoxEU.org today

Lots of cyber events, like

- $81 million theft from the Bangladeshi Central Bank via SWIFT
- Ecuador's Banco el Austro got $12 million stolen via SWIFT
- DRIDEX virus causes $100m in losses
- JP Morgan had data on 76 million US household account details stolen in 2014
- Stuxnet worm sabotaging Irans nuclear programme
- US government had 18 million personnel records stolen

Cyber risk — Risk emanating from computer systems and computer networks

The question is

- Is cyber risk a significant channel for systemic risk?
- A lot of authorities say so
  - Bank of Canada, BIS (2014), Bank of England, SEC, etc.
  - and plenty of consultants
- Is it true, and then how?

Where does cyber risk come from?

- Technical computer system failures
- Thiefs
- Hacktivists, terrorists and smaller states
- Largest state actors

1914 is perhaps the closest we ever got to a systemic crisis

- Globalism was at its peak in 1914
- The world's financial system was highly integrated
- The assassination of Archduke Franz Ferdinand on June 28 changed all of that
- The important observation is that the financial crisis did not happen *because* of World War I But *in anticipation* of it
- In other words, *confidence*, and hence *liquidity*, disappeared
- It is the *mechanism* that matters, not the trigger

What is systemic risk?

IMF, BIS and FSB (2009)

"The disruption to the flow of financial services that is (i) caused by an impairment of all or parts of the financial system; and (ii) has the potential to have serious negative consequences for the real economy."

The conditions for systemic risk tend to be created when all outward signs point to stability and low risk.

Macro and micro

Macro deals with systemic risk

- *Micro–prudential* focuses on individual banks and consumer protection
  - individual/idiosyncratic risk, correlations are ignored; bottom-up
  - risk is exogenous; partial equilibrium
- *Macro–prudential* focuses on the financial system
  - systemic risk, herd behaviour and shift in risk perception; top down
  - risk is endogenous; general equilibrium

How often do systemic crises happen?

- Ask the IMF–WB systemic crises database
- Every 42 years for OECD members (17 for UK)
- If anything, that is an overestimate
- Database includes relatively non–extreme events, like 1987 and 1998
- Best indication of the target probability for policymakers

The root cause of systemic crises is risk-taking behavior of economic agents

- Excessive risk–taking by financial institutions
  - best indicator of a future crisis is large credit growth
- The hidden mechanisms matter
  - interlinkages, excessive risk-taking with under appreciation of risk, pro–cyclicality, liquidity
  - hidden trigger
- Same chain of events can blow up into a crisis or wimper into nothing
- Risk that is undetected or ignored by the powers that be
- Creating the potential for an abrupt fall in confidence

Confidence and liquidity

- Behaviour motivated by confidence
- We only participate in markets if we believe the financial system functions as always
- Especially the plumbing
- Disappearance of confidence is a strong and often early indication of crisis
  - We have to believe that the financial edifice is at real risk of collapse for a crisis to really turn systemic (think 1914)

Cyber as cause of systemic risk

- *Cyber risk can not be the root cause of a systemic crisis*
- Systemic risk is caused by excessive risk taking
- And cyber risk has nothing to say about that
- No direct connection between the failure of computer systems and risk taking behaviour of economic agents

- OK, we can envision a large enough cyber event
- And an asteroid hitting city of London
- And a nuclear attack
- But timing of the event matters

Timing matters

- Suppose a country's ATM system fails for a few days. Would that be systemic?
- It depends
  - If it happened today, no
  - If 1 October 2008 yes
- Any attacker must
  1. be very lucky
  2. maintain her attack vectors in place for years or decades
  3. or be able to create a heightened state of financial market vulnerability

A cyber event could act as a trigger

- Provided the timing is just right
- Any event causing fall in confidence and liquidity is not systemic unless
- The levels of excessive risk-taking are at a tipping point
- Else recover quickly
  - October 1987, LTCM in 1998 and the 2011 flash crash.
- In general, triggers are irrelevant
- A very large number of potential triggers exist
- Unless the timing is fortuitous

Systems failures and theft

- Systems failures and theft can have a very large micro-prudential impact
- But since the timing and victims are likely to be idiosyncratic
- It is practically impossible for them to act as a trigger for a systemic crisis

Hacktivists, terrorists and smaller state actors

- Subvert IT systems to promote a political agenda
- Possibly with multiple targets and as part of a broader strategy of disruption
- Very unlikely to have systemic consequences
  - have to combine the attack with other forms of aggression
  - and would need absolutely right timing

- Financial institutions have become well equipped
  - Multiple backup systems
  - Robust recovery mechanisms
  - State-of-the-art countermeasures and liquidity backstops
- All these make a cyber attack very unlikely to trigger a systemic event

Largest state actors

- Can spend years developing and deploying attacks
- Keeping them hidden
- Until coordinated attacks on multiple IT systems
- Can be assumed to be on a colossal scale
  - involving multiple computer systems and their backup mechanisms
- Even then...

Cyber as one element of economic war

- Manufacture the necessary uncertainty through financial means, e.g.
  - making credible threats to world trade
  - the sequestration of foreign assets
  - repudiation of international liabilities.
- On a a sufficiently large scale could easily lead to a repeat of the experiences of 1914
- All these attacks require is enough international connectedness to allow trust in domestic institutions to be destroyed by a foreign actor

But

- While financial warfare of this type would presumably be accompanied by a cyber attack
- It is not clear that the cyber element would really be necessary
- And even then would only play a secondary role

Cyber risk is micro–prudential

- Cyber events can cause very serious damage to the financial system
- Significant micro–prudential risk

Cyber and financial systemic risk

- Many argue that cyber risk can be systemic
- Cyber risk cannot be the cause of systemic risk
- It can be the trigger provided timing is fortuitous
- But even then, the main issue for policymakers is *why* timing is is fortuitous

Policy conclusion

- The cyber risk debate has focused solely on IT considerations
- Many assertions are inconsistent with existing macro understanding
- Particular economic circumstances are required to make a cyber attack systemic

If cyber risk has systemic consequences, the chain of causality will be found in the macro-prudential domain