# Pirates without Borders: the Propagation of Cyberattacks through Firms' Supply Chains

**by Matteo Crosignani, Marco Macchiavelli, and André Silva**

Discussion by

Michael Gofman

University of Rochester

2020 Financial Stability Conference: Stress, Contagion, and Transmission

Cleveland Fed and OFR

# Key Question: Is Cyber Risk = Systemic Risk?

- **Cyber event that affects some firms spreads in the production network**
  - **Sales Channel**: Affected firms purchase less inputs and reduces output affecting both suppliers and customers
  - **Liquidity Channel**: Affected firm provide less trade credit to customer firms and requests more trade credit from suppliers
  - **IT Channel**: Computer Systems of suppliers and customers of the affected company also become affected by the virus/ransomware (February 11, 2020)

- **Cyber event that affects many/most firms at the same time**
  - Security flaw in Intel (November 10, 2020; March 6, 2020; August 12, 2019; January 4, 2018) and AMD CPUs (March 9, 2020)
  - Potential vulnerability at Google Cloud, Azure, or AWS (January 20, 2020; October 25, 2019)

- **Cyber event that affects a small number of systemically important targets**
  - SIFI Banks, such as Chase (December 22, 2014), Bank of America (May 27, 2020)
  - Large value payment systems, such as ECB's TARGET2 (October 28, 2020).
  - COVID-19 vaccine developers, such as Moderna (July 30, 2020) and Pfizer (October 22, 2020)

# First impression: Cyber Risk ≠ Systemic Risk

- **NotPetya** is the most devastating cyber-attack in history (Greenberg 2018).
- **The paper uses this "shock" to study the supply chain propagation of cyber risk**
  - 10 Western firms directly affected
    - 4% stock drop on announcement for the 7 publicly traded firms that were directly affected
    - Estimated losses of $2.2B (Table 1)
  - 209 customer firms of the 10 directly affected firms experience:
    - $10B reduction in profits over 2 years period
    - No effect on labor and investment
    - Draw credit lines
    - Receive less trade credit
  - No effect on 331 suppliers of the 10 directly affected firms
  - No effect on customers of the customers of the affected firms
  - Supply chains "rebuild" themself to absorb the shock
- **Potential reasons for overestimation of the effect:**
  - Treated vs. Control group
    - Ex-ante differences in some characteristics (Table 3)
    - Control group of 10K firms from the same sector and size quartile, would like to see better matching
  - Time frame
    - The event lasted several weeks, but the effect is measured over 2 years period, could include other shocks
  - Clustering
    - Customers of the same firm that are in different industries are not clustered

# The Untold Story of NotPetya

- **Cyber War**
  - **Not ransom and not pirates**. NotPetya looked like ransomware, but it was not (pg. 7). NotPetya was launched by Russian military intelligence (pg. 7-8)
  - **Not just 10 firms**. It affected "at least four hospitals in Kiev alone, six power companies, two airports, more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport, and practically every federal agency". "… one senior Ukrainian government official estimated that 10 percent of all computers in the country were wiped" (Greenberg 2018).
  - **Speed**. "It took 45 seconds to bring down the network of a large Ukrainian bank." (Greenberg 2018)

- **Sending a signal**: "Cisco's Craig Williams argues that "This was a piece of malware designed to send a political message: If you do business in Ukraine, bad things are going to happen to you."(Greenberg 2018)
  - If a signal causes $10B of damage, the potential for real damage is probably 100 times larger
  - NotPetya could be designed to spread only to places/companies it was intended to spread, putting a lower bound on the contagion estimates. "Stuxnet did not do any damage outside of its target of Iranian industrial control systems engaged in enriching uranium." (pg. 37)

- **Direct and indirect damages are underestimated**
  - Maerks reported 300 million (Table 1). "Most of the staffers WIRED spoke with privately suspected the company's accountants had low-balled the figure." (Greenberg 2018)
  - "Maersk also reimbursed many of its customers for the expense… One Maersk customer described receiving a seven-figure check." (Greenberg 2018) It suggests the damage on customers is underestimated.
  - A blackout in Ghana saved one server with a map of Maerks's computer network. (Greenberg 2018)

- **Incentives**: "The security revamp was green-lit and budgeted. But its success was never made a so-called key performance indicator for Maersk's most senior IT overseers, so implementing it wouldn't contribute to their bonuses. They never carried the security makeover forward." (Greenberg 2018)

# Conclusion

- Very timely paper on a super important topic
- First evidence for downstream propagation of a cyber attack
- Will be well cited
- The main concern that the paper might provide a wrong perception to regulators that cyber risk is not important for financial stability
- NotPetya is a wake-up call to financial regulators that cyber risk can be global, devastating, and systemically important
    - Regulators need to do stress tests for a cyber event that is 100 times larger than NotPetya
    - Incentives to firms/banks for mitigation of cyber-risk are important
    - SIFI's living wills will not help if all computers are paralyzed.
- The next crisis is not likely to be as 2008 or 2020, Cyber risk triggered crisis should not be take off the table.