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

Matteo Crosignani[1] Marco Macchiavelli[2] André F. Silva[2]

[1]New York Fed [2]Federal Reserve Board

2020 EBA Policy Research Workshop

November 12, 2020

The views expressed are solely my own and do not necessarily reflect those of the Board of Governors of the Federal Reserve System or of the Federal Reserve Bank of New York

Motivation

1. **Cyberattacks** are a pressing concern for firms and banks ▸ WEF
   - Ever-changing threat → different actors, objectives, techniques
     - *Hackers:* ransomware and denial-of-service attacks for financial gains
     - *State-actors:* more sophisticated techniques to obtain strategic information or, in more extreme cases, disrupt critical infrastructure of a target country

2. Production of goods and services structured around complex and global **supply chain** networks
   - Customer-supplier relationships are *key for the transmission of shocks* e.g., natural disasters (Barrot and Sauvagnat, 2016); credit supply shocks (Costello, 2020); pandemics (Bonadio et al., 2020)
   - *Unique features of cyberattacks* → can spread instantaneously without warning signs and are often not geographically clustered

- Increased attention to the impact of cybercrime on directly hit firms
  → but *no empirical evidence* on whether the effects of cyberattacks can be *propagated through customer-supplier relationships* ...

Motivation

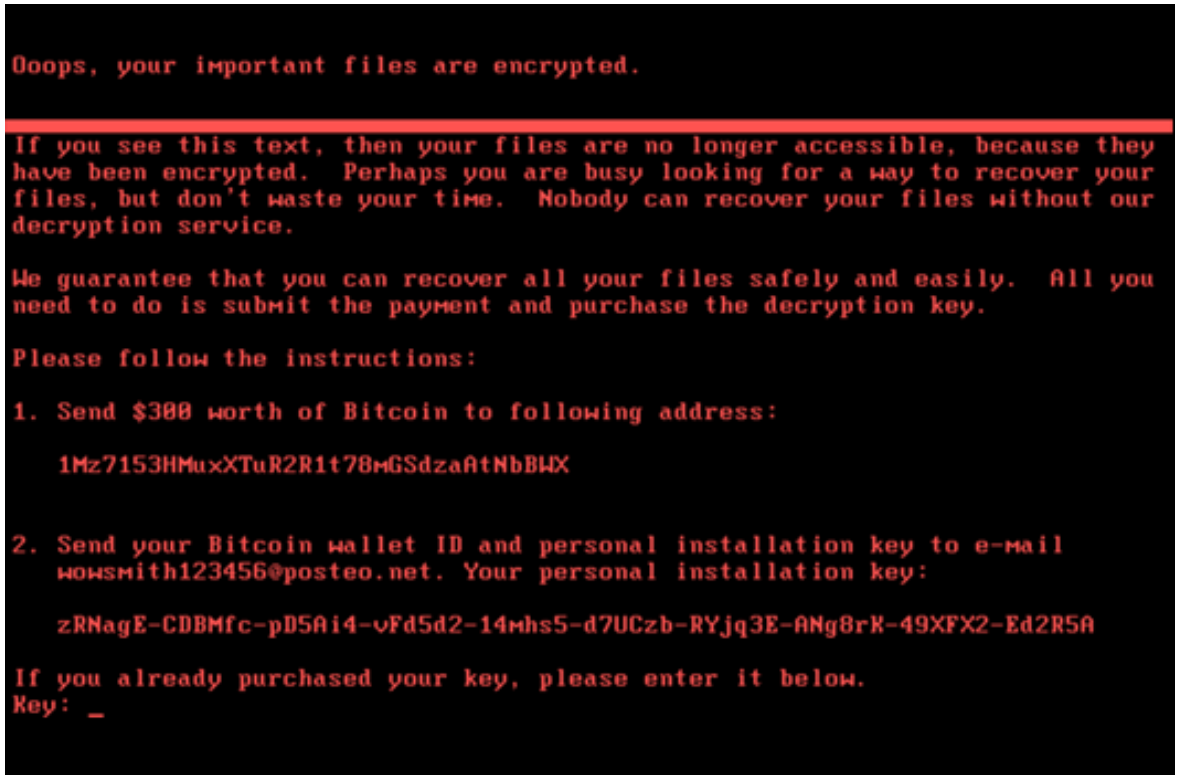
- This Paper: examines the **economic impact** and **supply chain effects** of the **most damaging cyberattack in history** so far

Research Questions

1. *Can the effects of cyberattacks on directly hit firms propagate downstream to their customers and upstream to their suppliers?*
2. *If so, how do the firms in the supply chain cope with the shock? Are there any real effects? Do banks play a role in mitigating its impact?*
3. *Do customer-supplier networks change in response to cyberattacks?*

Background

- Unexpected, large-scale **cyberattack in June 2017** ("**NotPetya**")



- Effort by the Russian military intelligence targeted at Ukraine (CIA, 2018)
- Initial vector of infection was a software widely used for tax reporting
  - Appeared to be a ransomware, but true intent was to encrypt and paralyze the computer networks of Ukrainian organizations

Background

- Cyberattack inadvertently spread beyond its original target and **infected global firms** through their Ukrainian subsidiaries ▸ News

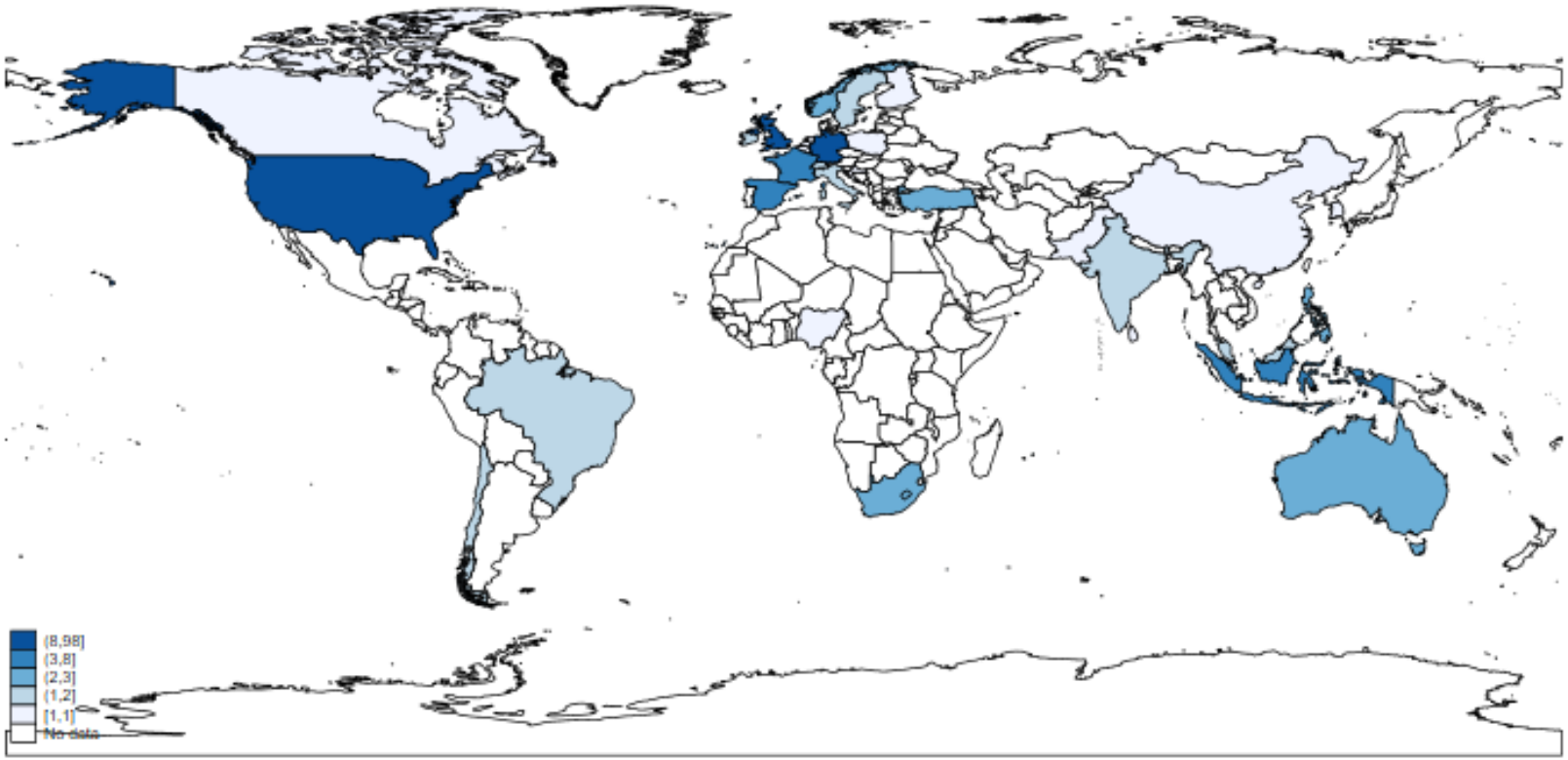
- 10 DIRECTLY HIT FIRMS – large, global, and public (costs: $2.2bn)
  - Merck (US): $670mn
  - FedEx (US): $400mn
  - Saint-Gobain (France): $387mn
  - Maersk (Denmark): $300mn
  - Mondelez (US): $180mn
  - Reckitt Benckiser (UK): $117mn
  - Nuance Communications (US): $92mn
  - Beiersdorf (Germany): $43mn
  - WPP (UK): $15mn
  - DLA Piper (UK): >$2mn

▸ Stock Price Reaction

Background

- Cyberattack inadvertently spread beyond its original target and **infected global firms** through their Ukrainian subsidiaries ▸ News

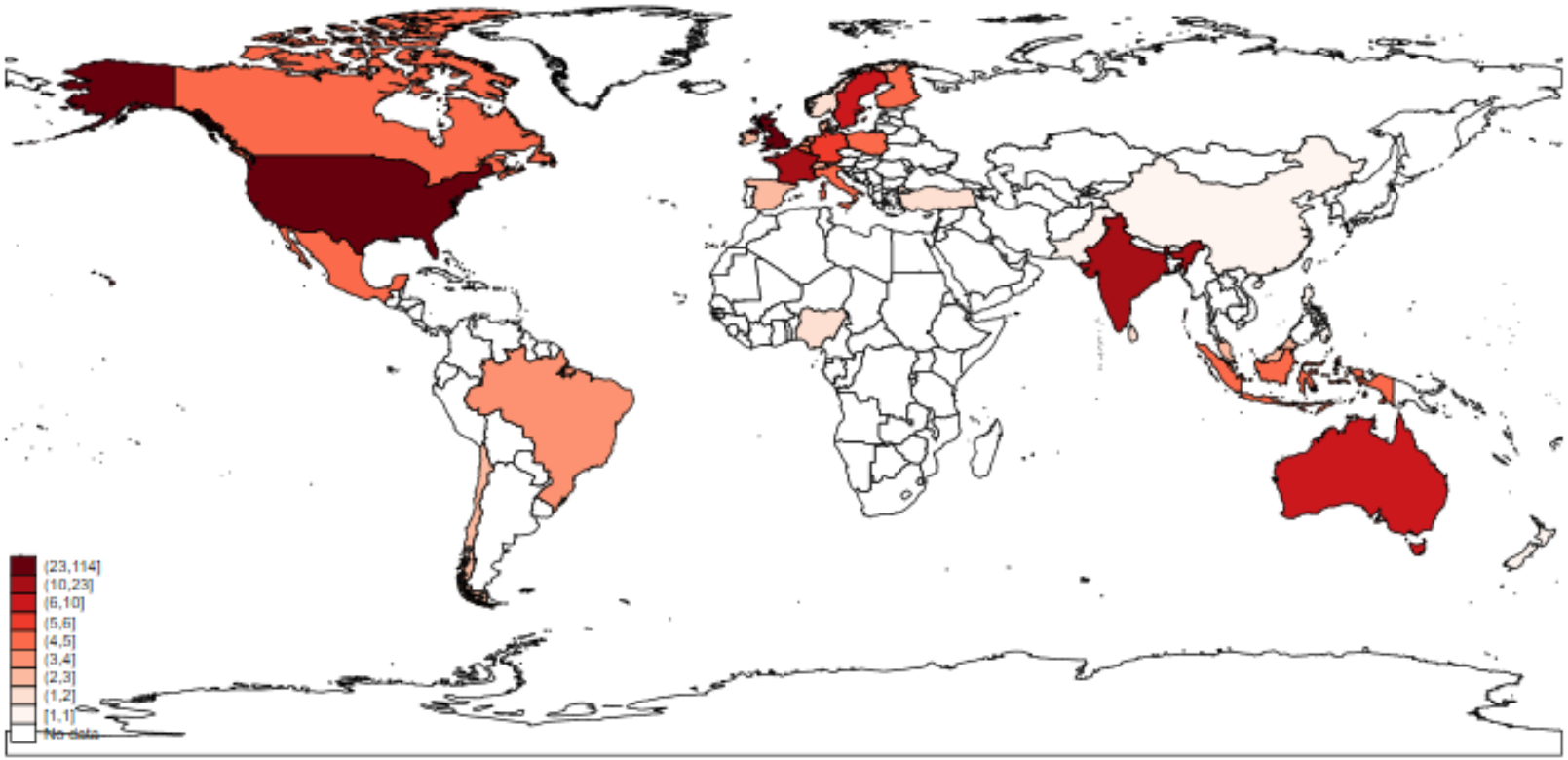
- 209 INDIRECTLY AFFECTED CUSTOMERS



Background

- Cyberattack inadvertently spread beyond its original target and **infected global firms** through their Ukrainian subsidiaries ▸ News

- 331 INDIRECTLY AFFECTED SUPPLIERS



Data

1. *Directly hit firms:* **SEC filings** and **Dow Jones Factiva**
   - Scraping SEC filings in 2017 and 2018 (keywords: "Petya", "NotPetya", and "Cyber")
   - Manually check over 4,500 newspaper articles worldwide citing NotPetya – available in the Dow Jones Factiva database
   - Cross-check the list of directly hit firms with Greenberg (2019), a book about NotPetya and other cyberattacks

2. *Global supply chain relationships:* **FactSet Revere**
   - Almost 1 million relationships between large (mostly publicly-listed) firms around the world
   - Each customer-supplier relationship has information on the start date, end date, and relationship type

Data

3. *Global firm-level data:* **BvD Orbis** (part of Moody's Analytics)
   - B/S information for more than 350 million firms worldwide
   - Orbis and FactSet merged using ISINs → disregard firms not present in both data sets to avoid selection bias
     - 47,651 firm-year observations
     - 10,640 firms; 2014 to 2018
     - 209 customers, 331 suppliers

4. *Loan-level data for the US:* **Federal Reserve Y-14Q**
   - Information at the quarterly frequency on all credit exposures exceeding $1 million for banks with more than $50 billion in assets
   - Merged with Orbis-FactSet sample using TINs and CUSIPs
     - 137,630 bank-firm-quarter observations
     - 37 banks and 1,997 firms; 2014:Q1 to 2018:Q4
     - 85 customers → 41% of global customers and 87% of US customers in Orbis-FactSet sample

Identification strategy

- **Difference-in-differences** comparing, before and after the shock:
  1. Firms indirectly affected by cyberattack through their supply chain
  2. Unaffected firms operating in the same industry, country, and size quartile in the same year

Firm-level Analysis

$$Y_{ijt} = \alpha + \beta \text{Post}_t \times \text{Affected}_i + \xi_i + \eta_{jt} + \epsilon_{ijt} \quad (1)$$

- Y_{ijt}: ratio of operating revenues, EBITDA, trade credit, and long-term debt to total assets, and the liquidity ratio (current assets-inventories/current liabilities)
- $Post_t$: equals 1 for 2017 and 2018, and 0 otherwise
- $Affected_i$: equals 1 if a firm is connected (as a supplier or as a customer) to a directly hit firm, and 0 otherwise
- ξ_i: firm FE to control for unobserved time-invariant firm characteristics
- η_{jt}: peer group of firm i – industry (SIC2)-country-size quartile-year combination

Identification strategy

Loan-level Analysis

$$Y_{ibjt} = \alpha + \beta \text{Post}_t \times \text{Affected}_i + \xi_i + \eta_{jt} + \gamma_{bt} + \epsilon_{ibjt} \quad (2)$$

- Y_{ijt}: total committed credit, total committed credit lines, share of the committed line of credit that is drawn down, interest rate spread, bank's subjective default probability of the borrower, dummy equal to one if the loan is non-performing, maturity of the committed exposure, amount of collateral
- $Post_t$: equals 1 after 2017:Q2, and 0 otherwise
- *Affected*$_i$: equals 1 if a firm is a customer of a directly hit firm, and 0 otherwise
- ξ_i: firm FE to control for unobserved time-invariant firm characteristics
- η_{jt}: peer group of firm i – industry (SIC2)-state-size quartile-quarter combination
- γ_{bt} bank-quarter FE to control for time-varying bank characteristics and absorb bank-specific shocks to credit supply

Results

– Part 1 –

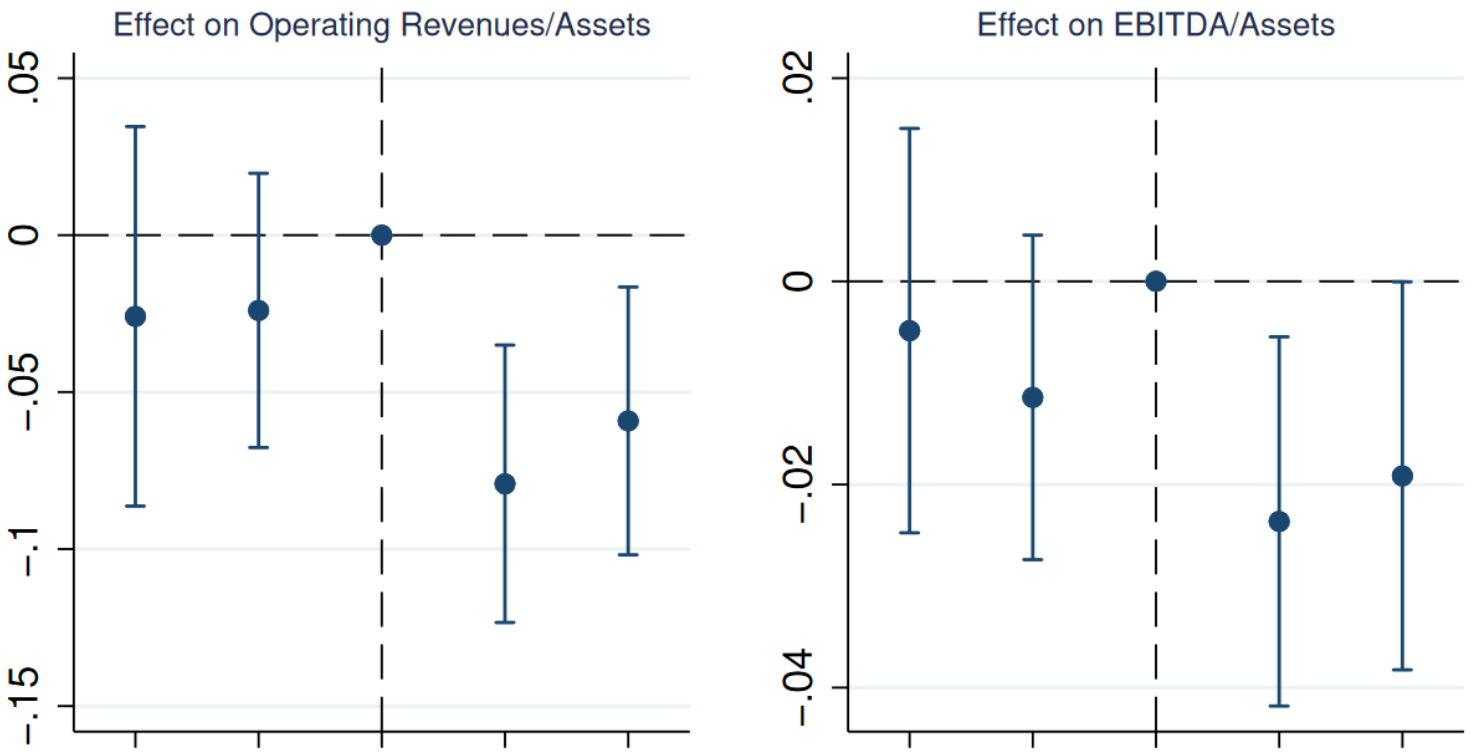
Can the effects of cyberattacks on directly hit firms propagate downstream to their customers and upstream to their suppliers?

1.1. Downstream Propagation to Customers

	Operating Revenues/Assets			EBITDA/Assets		
	(1)	(2)	(3)	(4)	(5)	(6)
$\text{Post}_t \times$ Affected Customer$_i$	-0.036***	-0.047***	-0.054***	-0.009**	-0.012**	-0.016**
	(0.014)	(0.014)	(0.020)	(0.005)	(0.005)	(0.007)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		
Industry-Year	✓			✓		
Size Bucket-Year	✓	✓		✓	✓	
Ind-Cou-Year		✓			✓	
Ind-Cou-Size-Year			✓			✓
Observations	47,651	44,207	40,704	47,651	44,207	40,704
R-squared	0.931	0.942	0.944	0.809	0.820	0.823

- Disruption caused by the cyberattack strongly propagated downstream
- Economically significant impact: a 5% drop in operating revenues and 2% drop in EBITDA – a conservative estimate suggests drop in profits of at least $10bn (vs. $2.2bn for directly hit firms)

1.1. Downstream Propagation to Customers



- Effects relatively stronger in the first year after the cyberattack
- Parallel trends assumption holds → firm characteristics are also similar across treatment and control group within size quartiles

1.2. Upstream Propagation to Suppliers

	Operating Revenues/Assets			EBITDA/Assets		
	(1)	(2)	(3)	(4)	(5)	(6)
$\text{Post}_t \times$ Affected Supplier$_i$	-0.004	-0.011	-0.013	-0.003	-0.003	-0.004
	(0.010)	(0.011)	(0.013)	(0.004)	(0.004)	(0.005)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		
Industry-Year	✓			✓		
Size Bucket-Year	✓	✓		✓	✓	
Ind-Cou-Year		✓			✓	
Ind-Cou-Size-Year			✓			✓
Observations	47,651	44,207	38,467	47,651	44,207	38,467
R-squared	0.931	0.943	0.950	0.809	0.820	0.834

- No statistically significant upstream effects to suppliers of directly hit firms
  - Shock impaired the directly hit firms' ability to deliver products to their customers, but not the suppliers' ability to deliver products to directly hit firms
- Consistent with Alfaro et al. (2020) in the context of credit supply shocks

Results

– Part 2 –

How do the firms in the supply chain cope with the shock? Are there any real effects? Do banks play a role in mitigating its impact?

2.1. Cyberattack and Trade Credit

	Trade Credit/ Assets			Trade Credit/ COGS		COGS/ Assets	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
$Post_t \times$ Affected Customer$_i$	-0.467**	-0.539**	-0.792***	-0.008		-0.061***	
	(0.207)	(0.227)	(0.303)	(0.006)		(0.017)	
$Post_t \times$ Affected $\times$ 1 Supplier$_i$ Customer$_i$					-0.017**		-0.090***
					(0.009)		(0.030)
$Post_t \times$ Affected $\times$ 2-3-4 Suppliers$_i$ Customer$_i$					-0.007		-0.047*
					(0.011)		(0.026)
$Post_t \times$ Affected $\times$ 5+ Suppliers$_i$ Customer$_i$					0.001		-0.041
Fixed Effects							
Firm	✓	✓	✓	✓	✓	✓	✓
Country-Year	✓						
Industry-Year	✓						
Size Bucket - Year	✓	✓					
Ind-Cou-Year		✓					
Ind-Cou-Size-Year			✓	✓	✓	✓	✓
Observations	47,651	44,207	40,704	34,113	34,113	34,113	34,113
R-squared	0.913	0.923	0.925	0.849	0.849	0.948	0.948

- Affected customers received less trade credit, further straining their liquidity conditions → trade credit is a key source of short-term financing (Barrot, 2016)
- Trade credit contraction (as a share of purchases) only affects customers fully dependent on the directly hit suppliers → reduction driven by directly hit firms

2.2. Cyberattack and Liquidity Risk Management

	Long-Term Debt/Assets			Liquidity Ratio		
	(1)	(2)	(3)	(4)	(5)	(6)
$\text{Post}_t \times \text{Affected}_i$	1.410***	1.168**	1.082*	-0.144**	-0.155**	-0.177*
	(0.431)	(0.474)	(0.612)	(0.068)	(0.077)	(0.104)
Fixed Effects						
Firm FE	✓	✓	✓	✓	✓	✓
Country-Year	✓		✓			
Industry-Year	✓		✓			
Size Bucket-Year	✓	✓		✓	✓	
Ind-Cou-Year	✓			✓		
Ind-Cou-Size-Year			✓			✓
Observations	47,651	44,207	40,704	47,651	44,207	40,704
R-squared	0.876	0.889	0.895	0.741	0.752	0.758

- To deal with this decline in both revenues and trade credit from suppliers, affected customers (i) increased external borrowing and (ii) relied on their pre-existing internal liquidity

2.3. Real Effects

	Tang. Assets/Assets			Intang. Assets/Assets		
	(1)	(2)	(3)	(4)	(5)	(6)
$\text{Post}_t \times$ Affected Customer$_i$	0.000	0.002	0.005	0.001	0.001	-0.004
	(0.003)	(0.003)	(0.003)	(0.004)	(0.005)	(0.006)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		
Industry-Year	✓			✓		
Size Bucket-Year	✓	✓		✓	✓	
Ind-Cou-Year		✓			✓	
Ind-Cou-Size-Year			✓			✓
Observations	47,644	44,200	40,697	47,644	44,200	40,697
R-squared	0.964	0.968	0.97	0.937	0.942	0.944

- Affected customers also did not have to reduce investment following the shock
- Extra: affected customers also have similar employment growth and wages after the shock relative to firms in the control group

2.4. Role of banks – loan-level evidence from the US

	Log(Tot Committed)		Log(Committed Line)		Share Drawn	
	(1)	(2)	(3)	(4)	(5)	(6)
$\text{Post}_t \times$ Affected Customer$_i$	-0.037	-0.199	-0.018	0.097	0.045**	0.084**
	(0.078)	(0.128)	(0.055)	(0.067)	(0.021)	(0.040)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Bank-Quarter	✓	✓	✓	✓	✓	✓
Ind-State-Quarter	✓		✓		✓	
Ind-State-Size-Quarter		✓		✓		✓
Observations	137,630	131,428	129,756	123,936	129,756	123,936
R-squared	0.581	0.583	0.624	0.623	0.586	0.620

- Affected customers significantly increase credit line draw downs to cope with the pressing liquidity needs $\rightarrow$ highlights the liquidity insurance function of banks

2.4. Role of banks – loan-level evidence from the US

	Rate Spread	Pr(Default)	NPL	Maturity	Collateral
	(1)	(2)	(3)	(4)	(5)
$\text{Post}_t \times$ Affected Customer$_i$	0.146**	1.559***	0.002	-0.279	0.028
	(0.066)	(0.458)	(0.011)	(2.142)	(0.022)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Bank-Quarter	✓	✓	✓	✓	✓
Ind-State-Size-Quarter	✓	✓	✓	✓	✓
Observations	131,428	104,591	131,428	130,890	114,641
R-squared	0.608	0.547	0.055	0.595	0.498

- Increase in the interest rate affected customers are charged
  - No bias arising from affected customers matching with banks offering less competitive pricing $\rightarrow$ results are within bank-quarter, comparing the rate charged by the same bank to affected and unaffected firms
- Consistent with the fact that banks perceive affected customers as being riskier

Results

– Part 3 –

Do customer-supplier networks change in response to cyberattacks?

3. Dynamic Supply Chain Responses

	New Relations		Ended Relations		Ended Relations excl. Hit Supplier	
	(1)	(2)	(3)	(4)	(5)	(6)
$Post_{2017} \times$ Affected Customer$_i$	0.203***	0.220***	0.097**	0.102**	0.095**	0.102**
	(0.056)	(0.073)	(0.041)	(0.051)	(0.041)	(0.050)
$Post_{2018} \times$ Affected Customer$_i$	-0.066	-0.081	0.197***	0.213***	0.084*	0.102*
	(0.044)	(0.059)	(0.049)	(0.061)	(0.046)	(0.057)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Size Bucket-Year	✓		✓		✓	
Ind-Cou-Year	✓		✓		✓	
Ind-Cou-Size-Year		✓		✓		✓
Observations	14,209	12,727	14,209	12,727	14,209	12,727
R-squared	0.670	0.677	0.663	0.675	0.661	0.674

- Affected customers more likely to form new relations with alternative suppliers (wake-up call) and to end relations with directly hit suppliers

Summary

- We examine the **economic impact** and **supply chain effects** of the **most damaging cyberattack in history** so far

1. Downstream propagation effects $\rightarrow$ reduction in revenues, profits, and trade credit among customers of directly hit firms
2. Affected customers depleted pre-existing liquidity buffers and increased borrowing through bank credit lines, which allowed them to maintain investment and employment
3. There are persisting adjustments to the supply chain network following the shock

- POLICY IMPLICATIONS: given how interconnected firms are at a global scale, results highlight the need to have better cybersecurity and contingency planning, as well as a more diversified supply chain

WORLD ECONOMIC FORUM

Top ten risks in North America

1. Cyberattacks
2. Data fraud or theft
3. Terrorist attacks
4. Critical information infrastructure breakdown
5. Failure of critical infrastructure
6. Fiscal crises
7. Failure of national governance
8. Failure of climate-change adaptation
9. Extreme weather events
10. Natural catastrophes

Top ten risks in Europe

1. Cyberattacks
2. Asset bubble
3. Interstate conflict
4. Energy price shock
5. Fiscal crises
6. Data fraud or theft
7. Failure of national governance
8. Unemployment or underemployment
9. Large-scale involuntary migration
10. Profound social instability

Source: World Economic Forum (WEF) Executive Opinion Survey. January-April 2019.

Back

FINANCIAL TIMES

Maersk, WPP and FedEx still struggling with cyber attack fallout

Global companies ranging from shipping lines to advertising firms are still struggling with the havoc wreaked by the huge cyber attack that last week swept from Ukraine to organisations in more than 60 countries.

AP Moller-Maersk, WPP, Reckitt Benckiser and FedEx all said their businesses were still not back to normal after the ransomware attack last week compromised hundreds of thousands of computers, industrial equipment and other technology.

Some ports remain hobbled, packages are going missing and customers are struggling to place and track orders, the companies said.

The New York Times

Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.

Mondelez was deemed collateral damage in a cyberwar.

When the United States government assigned responsibility for NotPetya to Russia in 2018, insurers were provided with a justification for refusing to cover the damage. Just as they wouldn't be liable if a bomb blew up a corporate building during an armed conflict, they claim not to be responsible when a state-backed hack strikes a computer network.

DW Made for minds.

US charges 6 Russian military intelligence officers over cyberattacks

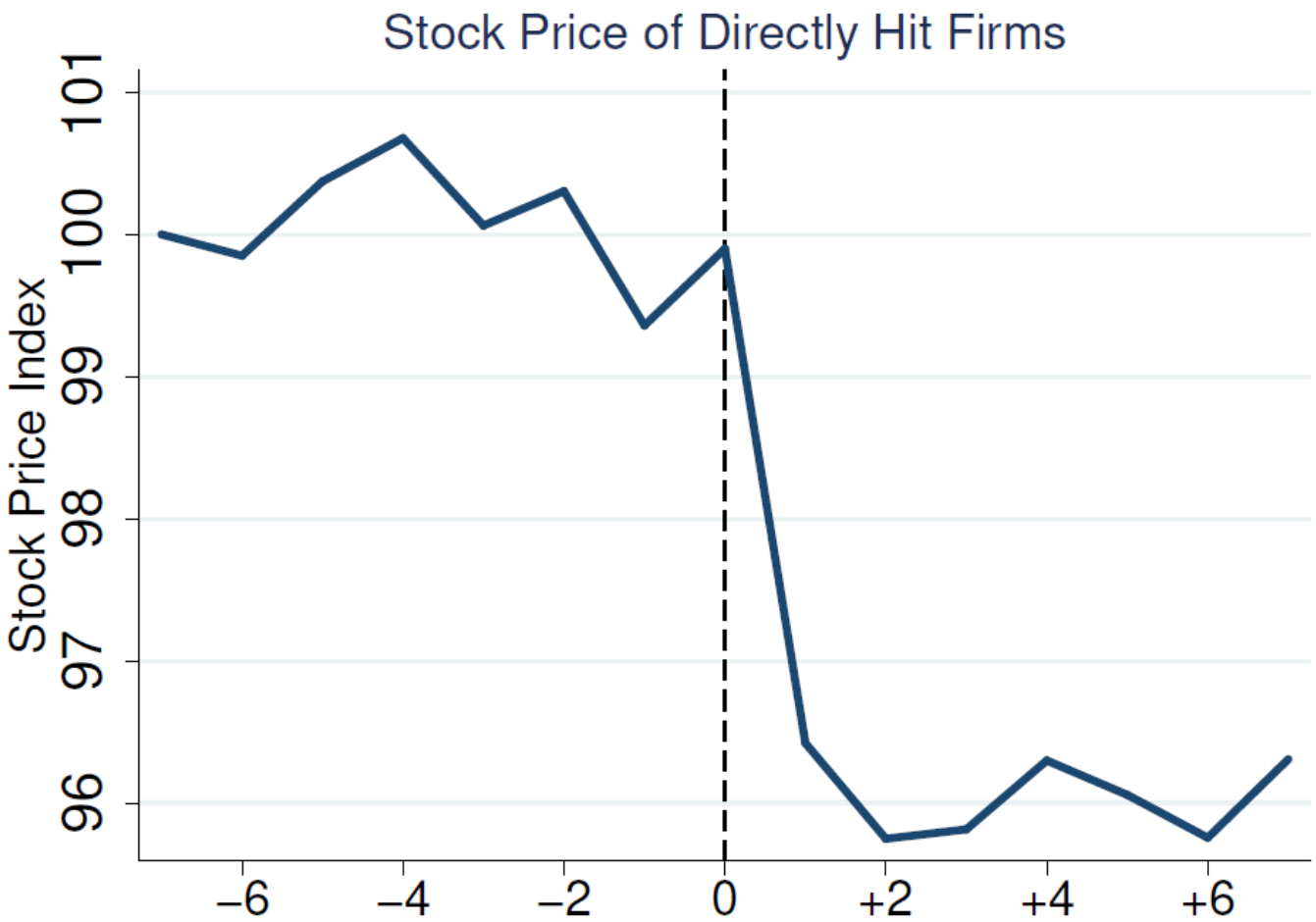
The hackers attacked the 2017 French elections, the 2018 Winter Olympics, the Ukraine's power grid and investigations into a Novichok poisoning, claims the US. They may also have used the destructive NotPetya malware.

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

WIRED

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

Back


Stock Price of Directly Hit Firms
Stock Price Index
96
97
98
99
100
101
−6
−4
−2
0
+2
+4
+6

Back