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

Matteo Crosignani
New York Fed

Marco Macchiavelli
Federal Reserve Board

André F. Silva
Federal Reserve Board

October 2020

Abstract

We document the propagation through supply chains of the most damaging cyberattack in history and the important role of banks in mitigating its impact. Customers of directly hit firms saw reductions in revenues, profitability, and trade credit relative to similar firms. The losses were larger for customers with fewer alternative suppliers and suppliers producing high-specificity inputs. Internal liquidity buffers and increased borrowing, mainly through bank credit lines, helped affected customers maintain investment and employment. However, the shock led to persisting adjustments to the supply chain network.

JEL Codes: L14, E23, G21, G32
Keywords: cyberattacks, supply chains, bank credit, trade credit

*We thank Miguel Faria-e-Castro, Nicola Limodio, Brian Peretti, Julien Sauvagnat, Stacey Schreft, and conference and seminar participants at the New York Fed, Bank of Italy, EBRD, and Federal Reserve System Conference on Financial Institutions, Regulation, and Markets for their comments. We also thank William Arnesen and Frank Ye for the excellent research assistance. The views expressed in this paper are those of the authors and do not necessarily represent those of the Federal Reserve Bank of New York, the Board of Governors of the Federal Reserve System, or other members of its staff. First draft: July 2020. Emails: matteo.crosignani@ny.frb.org, marco.macchiavelli@frb.gov, andre.f.silva@frb.gov.

1 Introduction

Cybercrime is now one of the most pressing concerns for firms.[1] Hackers perpetrate frequent but isolated ransomware attacks mostly for financial gains while state-actors use more sophisticated techniques to steal intellectual property and, in some cases, disrupt the operations of critical organizations. These more severe cyberattacks can damage firms' productive capacity, thereby potentially affecting their customers and suppliers as well. They also spread instantaneously without warning signs, and are often not geographically clustered. However, despite these unique features and their growing importance, there is little to no empirical evidence on the effects of cyberattacks on directly hit firms and, through their supply chains, on the broader productive sector.

In this paper, we study a particularly severe cyberattack that inadvertently spread beyond its original target and disrupted the operations of several firms around the world. Through supply chain relations, the effects of the cyberattack were propagated downstream to the customers of directly hit firms.[2] To cope with the shock without undermining investment and employment, affected customers used their liquidity buffers and increased their reliance on external finance, drawing down their credit lines at banks. Nonetheless, there were persisting adjustments to the supply chain network in response to the shock.

More specifically, we examine the impact of the most damaging cyberattack in history so far (Greenberg, 2018, 2019).[3] Named NotPetya, it was released on

[1] For instance, the latest World Economic Forum Executive Opinion Survey ranks cyberattacks as the number one risk for CEOs in North America and Europe (WEF, 2019).

[2] We refer to customers (suppliers) of directly hit firms as affected customers (suppliers) throughout the paper.

[3] See also the White House press release (https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/) and an assessment by Kaspersky

June 27, 2017 and targeted Ukrainian organizations in an effort by the Russian military intelligence to cripple Ukrainian critical infrastructure. The initial vector of infection was a software that the Ukrainian government required all vendors in the country to use for tax reporting purposes. When this software was hacked and the malware released, it spread across different companies, including large global firms through their Ukrainian subsidiaries. For instance, the shipping company Maersk had its entire operations coming to a halt, creating chaos at ports around the globe. A FedEx subsidiary was also affected, becoming unable to take and process orders. Manufacturing, research, and sales were halted at the pharmaceutical giant Merck, making it unable to supply vaccines to the to the Center for Disease Control and Prevention (CDC), the health protection agency of the US. Several other large companies (e.g., Mondelez, Reckitt Benckiser, Nuance, Beiersdorf) had their servers down and could not carry out essential activities, generating billions of dollars in damages for the firms directly hit by the cyberattack.

First, we show that the halting of operations among the directly hit firms had a significant negative effect on the productive capacities of their customers around the world, which reported significantly lower revenues and profits. A conservative estimate implies a $10 billion loss by the affected customers, an amount more than four times larger than the losses reported by the firms directly hit by the cyberattack. Importantly, affected customers also faced a significant decrease in trade credit from suppliers—one of the main sources of firms' short-term financing (Barrot, 2016) and a vital part of global trade (Antras and Foley, 2015). Faced with this temporary shock, affected customers

(https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/).

depleted some of their pre-existing liquidity buffers and increased the amount of borrowing, allowing them to maintain investment and employment. While the downstream disruptions to customers were severe, we do not find significant upstream effects to the suppliers of the directly hit firms.

Second, we investigate the role of supply chain vulnerabilities in driving these effects. We find that the downstream disruption caused by the cyberattack is concentrated among customers that have fewer alternatives for the directly hit supplier. This holds both when considering how many other suppliers a customer has in the same industry of the directly hit supplier, and when focusing on suppliers of less substitutable goods and services—that is, suppliers providing high-specificity inputs.

Third, we analyze in detail the role of banks in mitigating the negative liquidity effects of the cyberattack on affected customers. To this end, we use confidential credit register data for the US (i.e., the Y-14Q corporate schedule), with loan-level information at a quarterly frequency for banks with total assets of more than $50 billion. While there was no change in credit line commitments granted by banks, affected customers drew down relatively more on their credit lines to compensate for the liquidity shortages coming from lower revenues and less trade credit. Interest rate spreads also increased relatively more for affected customers, a result explained by an increase in risk, as measured by the expected probability of default that each bank assigns to a given firm.

Finally, we examine the dynamic supply chain response to the disruption caused by the cyberattack. We find that after the shock, affected customers form new relations with firms in the same industry as the directly hit supplier. This result suggests that the disruption caused by the cyberattack served as a "wake up call" for the affected customers which responded by forming new trading relations with alternative suppliers. We also find supporting evidence

that the affected customers are more likely to end their trading relations with the suppliers directly hit by the cyberattack. These findings suggest that the temporary disruptions caused by the cyberattack had long-lasting effects on trading relations by eroding the reputation of the directly hit firms as reliable suppliers. In fact, reliability and timeliness are essential for the smooth functioning of widely used "just-in-time" production systems (Crémer, 1995).

The contribution of this paper is twofold. First, we contribute to the nascent literature on the economic and financial effects of cybercrime, an area getting increasing attention by both practitioners (Accenture, 2019; Verizon, 2019; Siemens, 2019; NERC, 2020; Moody's, 2020) and academics (Kashyap and Wetherilt, 2019; Duffie and Younger, 2019; Kopp, Kaffenberger and Wilson, 2017; Aldasoro et al., 2020; Eisenbach, Kovner and Lee, 2020). A recent literature studies abnormal equity returns following data breaches (Kamiya et al., 2020; Garg, 2020; Akey, Lewellen and Liskovich, 2018; Amir, Levi and Livne, 2018). However, data breaches are a subset of the broader set of cyberattacks and usually do not disrupt the ability of firms to carry out their operations.[4] In fact, while most cyberattacks lead to either a monetary or a data loss, the cyberattack we study constitutes a tail event, generating consequences that are far more damaging and widespread than the more common, though isolated, data breaches.[5]

[4]See Accenture (2019) for a review of the damages caused by different types of cyberattacks.

[5]Our paper also contributes to the small literature on intelligence and espionage. Berger et al. (2013) and Dube, Kaplan and Naidu (2011) study the effects of CIA influence on trade and stock returns for firms with a particular interest in regime change, respectively. Martinez-Bravo and Stegmann (2018) use the CIA vaccine campaign to verify a target's DNA to show the effects of vaccine distrust on immunization, Ahn and Ludema (2019) document the effects of sanctions related to the Russian annexation of Crimea, Lichter, Löffler and Siegloch (2020) examine the effect of state surveillance on civic capital and economic performance, while Glitz and Meyersson (2020) estimate the economic returns

Second, we contribute to the literature on the supply chain effects following economic and financial shocks. Boehm, Flaaen and Pandalai-Nayar (2019) exploit an earthquake in Japan and estimate a near zero elasticity of substitution of intermediate goods in the short-run, while Carvalho et al. (2020) use the same shock to map its propagation patterns through supply chains. Barrot and Sauvagnat (2016) document that suppliers hit by natural disasters propagate the shock downstream to their customers as well as horizontally to the other suppliers of their customers. Cingano, Manaresi and Sette (2016) and Costello (2020) find that firms facing financing constraints transmit shocks downstream via declines in trade credit. Cortes, Silva and Van Doornik (2019) show that firms borrowing from more stable funding sources benefit both their suppliers and customers, being able to pay the former and providing trade credit to the latter. Finally, Alfaro, García-Santana and Moral-Benito (2020) show how bank credit supply shocks that affect borrowing firms are propagated downstream to their customers. However, they find mixed evidence on upstream propagation.

The cyberattack we study has several advantages relative to these more commonly analyzed shocks. On the one hand, credit supply disruptions are often slower-moving and systemic, hitting many companies at the same time and therefore making it hard to disentangle demand from supply. On the other hand, natural disasters tend to follow seasonal and geographical patterns, making the identification of transmission channels particularly challenging. Instead, the type of cyberattack we study is arguably more unpredictable and faster to materialize, occurs amid normal economic conditions, and affects different geographical regions. In addition, while we show that cyberattacks

resulting from state-sponsored industrial espionage.

can create supply chain disruptions akin to those that originate from financial crises and natural disasters, we also document a new dimension of supply chain vulnerabilities and estimate how supply chains dynamically evolve in response to this unique type of disruptive shock. These results are especially relevant for the theoretical literature on endogenous production networks that stress the importance of having trading relations with alternative suppliers, and how a network adjusts to a shock (Elliott, Golub and Leduc, 2020; Taschereau-Dumouchel, 2019; Acemoglu and Tabhaz-Salehi, 2020).

2 Background on NotPetya

In the intelligence world, few things are what they seem. Petya is the name of a ransomware that circulated in 2016. The victim was infected after opening a PDF file purporting to be the resume of a job applicant. From there, the ransomware encrypted the master file table which serves as a roadmap for the hard drive, making the data on the computer unreachable. The victim was then asked to make a Bitcoin payment to get the hard drive decrypted. What seemed to be a new version of Petya spread quickly in June 2017. It hit Ukraine the hardest but it also appeared worldwide. However, this new version was able to spread across networks, without requiring to obtain administrative access. Even though it appeared to be a ransomware, as shown in Figure OA.1 in the Online Appendix, it was quickly found out that the true intent was not the financial gain from the ransom payment. Indeed, the attack was not even designed to keep track of the decryption codes. The true intent was to encrypt and paralyze the computer networks of Ukrainian banks, firms, and government. This was *not* a new version of Petya.

This cyberattack was the hand of a hacking group from the Russian military

intelligence, the GRU. The Russian government had been actively involved in meddling in Ukrainian matters since Ukraine, previously part of the Soviet Union, took steps to build closer ties to NATO. Initially, Russia directed a series of cyberattacks to Ukraine, including its power grid, and then resorted to military action by invading and annexing Crimea. It should also be noted that the timing of the NotPetya attack was in a way serendipitous. The ease with which NotPetya spread from network to network without human intervention depended on a never-seen-before piece of code that was leaked in April 2017 by the Shadow Brokers, a hacking group. The leaked code, called Eternalblue, is a very sophisticated tool developed by the NSA to harvest passwords and move from network to network. Eternalblue was used together with another tool, Mimikatz, that was already circulating among hackers and can find network administrator credentials stored in the infected machine's memory.[6]

Notpetya was itself a supply chain attack, in the sense that the initial point of entry was a backdoor planted in an accounting software, called M.E. Doc, widely used by Ukrainian firms for tax reporting. As a result, most companies operating in Ukraine got infected, including global companies through their Ukrainian subsidiaries.[7] More generally, Moody's (2020) argues that small companies with less sophisticated cybersecurity are at risk of attacks stemming from suppliers and vendors with access to their IT systems. For instance, a compromised software company can become a vector through which thousands

[6]Microsoft released a patch for Eternalblue prior to the NotPetya incident. However, NotPetya could infect unpatched computers, grab the passwords via Mimikatz and spread to patched computers. Many firms reportedly do not update regularly for fear that the updates could interfere with their software.

[7]More details about Notpetya can be found in Greenberg (2019), a book about NotPetya and other cyberattacks conducted by Russian military intelligence on Ukraine in 2014-2017.

of customers' computers are infected, as in the case of NotPetya.

3 Data

We use several data sources to conduct our analysis at both the firm- and loan-level, including global supply chain relationships data from FactSet Revere, balance sheet data on firms worldwide from Orbis, and credit register data for the US from the Federal Reserve's Y-14Q.

First, to identify the firms directly affected by NotPetya, we start by web scraping SEC filings in 2017 and 2018. We experiment with different keywords, including "Petya", "NotPetya", and "Cyber". Among the filings that contain a match, we exclude matches that are unrelated, such as cybersecurity firms citing NotPetya as the main cyberattack of the year. We also look for instances in which NotPetya is cited in newspaper articles worldwide. Using the Dow Jones Factiva database that contains a repository of international newspaper articles, we obtain over 4,500 relevant articles which we manually check for stories of firms directly hit by NotPetya. Finally, we cross-check the list of directly hit firms with Greenberg (2019). We exclude firms in Ukraine, Russia, as well as non-public firms that we would not be able to find in other data sets, e.g., government agencies and hospitals. Overall, as described in detail in Table 1, we identify 10 public firms that were directly hit by NotPetya—including FedEx, Maersk, Merck, Mondelez, as well as other very large companies in the US, UK, Germany, Denmark, and France.[8] In Figure 1, we show that the stock

[8]We show the geographical distribution of these directly hit firms in Figure OA.2 in the Online Appendix. We do not consider the customers and suppliers of the French multinational corporation Saint-Gobain in our specifications since there is no available supply chain information for this particular firm before the shock. Other companies reportedly hit

Firm Name	Costs	Additional Details
Beiersdorf	$43 mln	Various locations of the Beiersdorf pharmaceutical group were cut off from mail traffic for days. Beiersdorf, said 35 million euros worth of second-quarter sales were delayed to the third quarter and it was totting up the costs of the attack for items such as calling in outside experts,promotions and using other production sites to make up for shortfalls.
DLA Piper	>$2 mln	Lawyers at the global law firm DLA Piper had limited access to their computer systems or email, a major disruption of their business. The first three weeks of the cyberattack, they recorded about 15,000 hours of overtime which the organisation paid. After two weeks, they decided to wipe everything and start afresh. They had planned for the loss of an entire data center or a critical online services. What they had not planned for was the complete loss of everything. DLA Piper is bringing a case against Hiscox for refusing to pay out on a multimillion-pound insurance claim for damages caused by NotPetya.
FedEx	$400 mln	Delivery service FedEx lost $400 million after NotPetya crippled its European TNT Express business. The reported costs came from loss of revenue at TNT Express and costs to restore technology systems. Six weeks after the attack, customers were still experiencing service and invoicing delays, and TNT was still using manual processes in operations and customer service.
Maersk	$300 mln	Maersk reinstalled 4,000 servers, 45,000 PCs, and 2,500 applications over ten days. The company only experienced a 20% drop in volume, while the remaining 80% of operations were handled manually. Losses were about $300 million, including loss of revenue, IT restoration costs and extraordinary costs. The company was hiring 26 new employees a week, planning to have 4,500-5,000 IT employees within 18 months. At Maersk terminals in the Port of New York and New Jersey, computers, phones, and gate system shut down, forcing workers to use paper documents.
Merck	$670 mln	At Merck, NotPetya temporarily disrupted manufacturing, research and sales operations, leaving the company unable to fulfill orders for certain products, including vaccines. The attack cost Merck about $670 million in 2017, including sales losses and manufacturing and remediation-related expenses.
Mondelez	$180 mln	The global logistics chain of the food company Mondelez was disrupted by Notpetya. The forensic analysis and restoration of all IT networks cost $84 million. Added to this was the loss of sales. Altogether Mondelez had to record $180 million of damage by the attack.
Nuance	$92 mln	NotPetya affected Nuance's cloud-based dictation and transcription services for hospitals. Nuance estimated a negative impact of $68 million in lost revenues and $24 million in restoration costs.
Reckitt Benckiser	$117 mln	Reckitt Benckiser was hit by NotPetya, halting production, shipping and invoicing at a number of sites. The British consumer goods company suffered $117 million in losses, 1% of annual sales.
Saint-Gobain	$387 mln	For French construction company Saint-Gobain, the attack led to downtime of IT systems and supply chain disruptions. The attack had a negative impact of $258 million on sales and $76 million on operating income in the first half of 2017. Total losses are expected to rise to $387 million.
WPP	$15 mln	UK multinational advertising firm WPP was hit by Notpetya, costing about $15 million before insurance. The damage was limited by the fact that WPP's systems are not fully integrated.

Table 1: Firms Directly Affected by NotPetya. Firms directly affected by NotPetya, total reported costs and additional details. Sources: SEC Filings and Dow Jones Factiva.

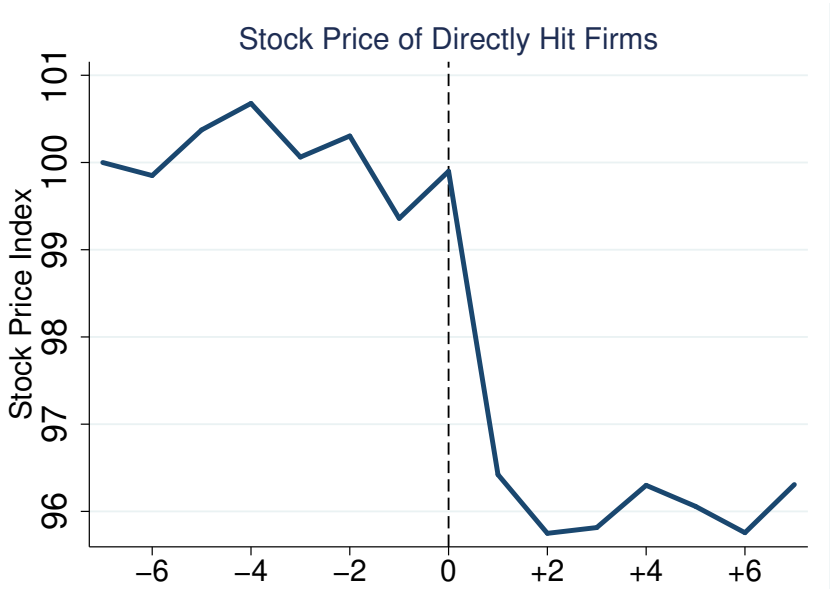

Figure 1: Stock Price of Directly Hit Firms Around News of the Damages of NotPetya. This figure shows the stock price evolution around the news of the damages of NotPetya (from seven trading days prior to the news to seven days after the news). Stock prices are averaged across the nine publicly traded directly hit firms (DLA Piper is a private company) and normalized to 100 seven trading days before the disclosure of the news. The dates when the news of the damages were publicly released are as follows: August 16, 2017 for Moller-Maersk (link); August 2, 2017 for Beiersdorf (link); July 26, 2017 for Compagnie de St-Gobain (link); July 16, 2017 for FedEx (link); June 28, 2017 for Mondelez (link); October 26, 2017 for Merck (link); June 28, 2017 for Nuance (link); July 5, 2017 for Reckitt Benckiser (link); August 22, 2017 for WPP (link). Source: Datastream.

price of these directly hit firms collapsed by about 4% after they disclosed the damages of NotPetya.

Second, we obtain global supply chain relationships data from FactSet Revere, arguably the most comprehensive source of firm-level customer-supplier relationships currently available.[9] Specifically, the data set includes almost a

by the cyberattack, though to a much small extent, include the Italian Buzzi Unicem and the German Deutsche Bahn and Deutsche Post. These firms are also excluded from our analysis due to the lack of supply chain information both before and after the shock.

[9]Alternative sources of supply-chain data either do not have information with sufficiently high-frequency on the start and end dates of a relationship between two firms (e.g., Bloomberg,

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. FactSet collects this information through the firms' public filings, investor presentations, websites, corporate actions, press releases, and news reports. Following Gofman, Segal and Wu (2020), we drop redundant relationships whose start and end dates fall within the period of a longer relationship between the same firm pair and combine multiple relationships between two firms into a continuous relationship if the time gap between two relationships is shorter than six months. Using each firm's International Securities Identification Number (ISIN), we are able to identify a total of 209 customers and 331 suppliers indirectly affected by the cyberattack i.e., exposed through their supply chain connections to directly hit firms.[10]

Third, we collect balance sheet and income statements information on firms worldwide from Orbis—a database by Bureau Van Dijk (part of Moody's Analytics) that contains data for more than 350 million companies globally. In addition to its extensive coverage, Orbis is particularly attractive due to its cross-country comparability since the data provider organizes the information in a standard global format (Kalemli-Ozcan et al., 2019). We merge Orbis with FactSet using the ISIN of each firm and disregard companies that are not present in both data sets to avoid selection bias due to the inclusion of smaller listed firms that appear in Orbis but that do not report supply chain relations. We obtain an intersection of 47,651 firm-year observations, corresponding to 10,640 firms from 2014 to 2018, the most recent date available in Orbis.

Capital IQ) or are not as granular as FactSet (e.g., Compustat Segment data which only reports, with an annual frequency, the largest customers of a supplier).

[10]We show the geographical distribution of affected customers and affected suppliers in Figure OA.3 and Figure OA.4 in the Online Appendix.

Finally, we obtain loan-level information on bank credit to firms from the corporate loan schedule (H.1) of the Federal Reserve's Y-14Q. These data have been collected since 2012 to support the Dodd-Frank Act's stress tests and assess bank capital adequacy for large banks in the US. The credit register provides confidential information at the quarterly frequency on all credit exposures exceeding $1 million for banks with more than $50 billion in assets. These loans account for around 75% of all commercial and industrial (C&I) lending volume during the period we analyze. In addition to the amount of committed credit for each firm-bank pair, the data set also contains information on the committed and drawn amounts on credit lines, the amount that is past due, as well as information on other loan characteristics, such as the interest rate spread, maturity, and collateral. Finally, we also have information on each bank's internal assessment of the default probability of a given firm—a model-based metric that captures the bank's hard information about a given borrower and that predicts loan delinquency (Adelino, Ivanov and Smolyansky, 2020).

In order to identify firms indirectly affected by the cyberattack, we merge these firm-bank data for the US with Orbis and FactSet using the firms' tax identification numbers and CUSIPs available in the Y-14Q. This results in a sample of 137,630 bank-firm-quarter observations from 2014:Q1 to 2018:Q4, covering 37 banks and 1,997 firms. Of these, 85 are customers of firms directly hit by the cyberattack, corresponding to 42% of global customers and 87% of US customers in the Orbis-FactSet firm-level sample.[11]

[11]The reduction in the number of affected customers when compared to the Orbis-FactSet global sample is to be expected as the Y-14Q data only covers US banks domestic credit.

4 Identification Strategy

4.1 Firm-level Analysis

Our goal is to document the effects of the NotPetya cyberattack through the supply chain. Given that the attack caused the directly hit firms to halt operations for several weeks, we are interested in estimating the effects on these firms' customers and suppliers, which we refer to as affected customers and affected suppliers. We use a difference-in-differences approach, comparing the change in behavior of firms indirectly affected by the shock through their supply chain with that of unaffected firms operating in the same industry, country, and size quartile in the same year. Specifically, we estimate the following specification:

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

where i corresponds to a firm, t to a year, and j to the peer group of firm i—an industry-country-size quartile combination in the baseline case, with industries defined at the SIC2-level. The sample period runs from 2014 to 2018. Y_{ijt} is one of several outcome variables we consider, including the ratio of operating revenues, EBITDA, trade credit, and long-term debt to total assets, and the liquidity ratio (current assets minus inventories over current liabilities). $Affected_i$ is a firm-level indicator variable equal to one if a firm is connected (as a supplier or as a customer) to a directly hit firm. In some specifications, for robustness, we use a continuous version of $Affected_i$ defined for affected customers (affected suppliers) as the share of the firm i's suppliers (customers) that are directly hit by the cyberattack. $Post$ equals one for 2017 and 2018, the two time periods after the June 2017 cyberattack. We estimate the β coefficient

within a peer group, captured by the fixed effects η_{jt}. We also include firm fixed effects ξ_i. Standard errors are clustered at the industry-country-year level.

The NotPetya cyberattack hit many firms in Ukraine, including the Ukrainian subsidiaries of international firms, and then spread to the entire network infrastructure of most of these companies, affecting their global operations. Importantly for our identification strategy, the attack came from a third party vendor, whose software is widely used in Ukraine for tax filing purposes. Hence, within the set of international firms, it is plausible to assume that the attack was unrelated to firm characteristics. Nevertheless, one may still argue that the severity with which each firm was hit depends on the adoption of best practices to improve cybersecurity, or "cyber-hygiene." However, we go one step further and study the effect on customers and suppliers of the directly hit firms. As a result, even if the severity of the attack on the directly hit firms may depend on their cybersecurity practices, it is unlikely that the attack was correlated with characteristics of the indirectly affected firms—either customers or suppliers. In addition, as we show later, affected customers and similar but unaffected firms share similar trends across different outcomes prior to the cyberattack.

The summary statistics of Table 2 show that firm characteristics are similar across affected customers (treatment group) and non-affected firms (control group) within size quartiles—which are constructed relative to the sample of affected firms so as to select firms in the control group that are similar in size to the treated firms.[12] Across size quartiles, firms in the treatment and control groups have similar profitability (EBITDA to assets ratio and return on assets), liquidity ratio (current assets net of inventories divided by current liabilities,

[12]Given that we do not find economically and statistically significant effects for affected suppliers, we show the summary statistics on suppliers in Table OA.1 in the Online Appendix.

		Full	Size Q1		Size Q2		Size Q3		Size Q4	
	Stat	Sample	Treated	Control	Treated	Control	Treated	Control	Treated	Control
No. Obs.	Tot	47651	233	31126	234	12159	229	2921	238	511
Age	μ	29.40	26.91	27.51	28.43	31.02	48.57	37.71	51.55	41.34
	p(50)	21.00	19.00	21.00	22.00	22.00	31.00	26.00	31.00	28.00
	σ	27.31	23.21	24.72	23.37	29.77	45.82	32.80	46.25	38.14
Assets (M)	μ	4512	504	376	4583	3864	26750	20823	140292	107246
	p(50)	578	349	242	3745	3013	24140	17634	117676	78264
	σ	19950	451	370	2995	2465	12325	10410	90605	102669
Capital/A	μ	0.24	0.15	0.31	0.05	0.10	0.04	0.07	0.03	0.08
	p(50)	0.03	0.02	0.05	0.01	0.01	0.01	0.01	0.01	0.02
	σ	1.07	0.49	1.31	0.10	0.20	0.09	0.14	0.09	0.12
EBITDA/A	μ	0.08	0.02	0.06	0.12	0.11	0.12	0.10	0.11	0.10
	p(50)	0.09	0.09	0.09	0.10	0.10	0.12	0.09	0.11	0.09
	σ	0.19	0.25	0.23	0.13	0.07	0.08	0.06	0.05	0.06
Liquidity Ratio	μ	1.99	2.58	2.30	1.58	1.47	1.10	1.12	1.22	1.23
	p(50)	1.20	1.53	1.32	1.12	1.09	0.83	0.95	0.90	0.94
	σ	3.38	2.95	3.84	1.87	2.37	0.98	0.84	1.48	1.97
LT Debt/A	μ	0.17	0.13	0.12	0.21	0.25	0.24	0.28	0.22	0.24
	p(50)	0.13	0.04	0.06	0.18	0.24	0.23	0.27	0.21	0.24
	σ	0.17	0.16	0.15	0.16	0.17	0.13	0.15	0.11	0.13
Op.Revenues/A	μ	0.86	1.27	0.93	1.03	0.73	0.96	0.60	0.68	0.49
	p(50)	0.70	0.99	0.79	0.87	0.58	0.70	0.45	0.57	0.40
	σ	0.78	1.12	0.83	0.66	0.68	0.82	0.54	0.48	0.40
Trade Credit/A	μ	0.08	0.13	0.09	0.11	0.07	0.11	0.07	0.08	0.06
	p(50)	0.06	0.08	0.06	0.09	0.05	0.08	0.04	0.07	0.04
	σ	0.09	0.13	0.09	0.10	0.08	0.13	0.08	0.08	0.05
ROA	μ	1.13	-4.39	-0.24	4.64	3.81	5.27	3.64	4.56	3.68
	p(50)	3.34	3.70	3.11	4.49	3.68	5.23	3.23	4.00	3.11
	σ	14.70	23.65	17.20	8.53	7.32	6.80	5.98	5.43	4.93
Sales/A	μ	0.85	1.26	0.92	1.02	0.73	0.96	0.59	0.68	0.48
	p(50)	0.69	0.98	0.78	0.85	0.58	0.70	0.45	0.57	0.39
	σ	0.78	1.12	0.82	0.66	0.68	0.82	0.54	0.48	0.40
No. Employees	μ	10349	2676	2256	21038	12574	63695	43225	134333	86187
	p(50)	1804	1500	831	8000	6289	39135	20700	98089	47457
	σ	33072	3070	5041	39941	27866	65496	68854	112498	91580
Cost of Empl./A	μ	0.15	0.11	0.17	0.09	0.10	0.12	0.09	0.08	0.04
	p(50)	0.08	0.08	0.09	0.07	0.05	0.12	0.03	0.06	0.03
	σ	0.21	0.11	0.23	0.09	0.14	0.08	0.27	0.07	0.05
Tang. Assets/A	μ	0.28	0.20	0.25	0.21	0.32	0.23	0.36	0.27	0.32
	p(50)	0.20	0.14	0.18	0.16	0.24	0.15	0.31	0.22	0.26
	σ	0.25	0.18	0.24	0.18	0.28	0.20	0.28	0.19	0.26
Intang. Assets/A	μ	0.15	0.17	0.14	0.29	0.18	0.29	0.18	0.28	0.21
	p(50)	0.05	0.07	0.04	0.27	0.09	0.24	0.10	0.25	0.12
	σ	0.20	0.20	0.19	0.22	0.21	0.21	0.21	0.23	0.22

Table 2: Summary Statistics. This table shows summary statistics for our sample firms. The table reports mean, median, and standard deviation. The sample period runs yearly from 2014 to 2018. The table shows the summary statistics for the full sample as well as the summary statistics for treated and control firms in each of the four size bucket groups. Treated firms are customers of a directly affected firm. Age is in years. Assets is in million USD. The liquidity ratio is 100*(current assets - inventories)/current liabilities. Current means that it converts into cash (matures) within one year. Long-term debt (LT Debt) is financial debt with a maturity greater than one year. Trade Credit is trade credit debt with suppliers. All the variables divided by total assets (A) are expressed as ratios. However, for ease of interpretation of the estimates, Trade Credit/A and LT Debt/A are multiplied by 100 in Table 5. Sources: BvD Orbis, FactSet Revere.

where current means that it converts to cash within one year), and reliance on long-term debt (long-term debt to total assets ratio). Treated firms have slightly more trade credit than control firms, with trade credit defined as debits to suppliers divided by total assets. Slight differences between treated and control firms might be due to having relatively more firms in the control group of a certain industry which makes greater use of trade credit. These differences are accounted for in the empirical analysis by using industry-country-size-year fixed effects, which allow us to compare a treated firm to a set of control firms within the same industry, country, and size. In addition, we show that treated and control customers share similar trends in the outcome variables prior to the cyberattack, addressing residual concerns that pre-existing differences across groups prior to the shock may drive our results.

4.2 Loan-level Analysis

While the firm-level analysis allows us to examine the effect of the cyberattack on the affected customers and suppliers' balance sheets, we also go a step further and use firm-bank matched loan-level data for the US to be able to test the effect of the shock on the amount and terms of the bank credit. The specification we use is as follows:

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

where i corresponds to a firm, b to a bank, t to a quarter between 2014Q1 and 2018Q4, and j to the peer group of firm i—an industry-state-size quartile combination in the baseline case, with industries defined at the SIC2 level. As before, $Affected_i$ is a firm-level indicator variable equal to one if a firm is connected (as a supplier or as a customer) to a directly hit firm, and $Post$ is a

dummy variable equal to one after the June 2017 cyberattack. All specifications control for time-varying bank characteristics using bank-quarter fixed effects γ_{bt}, which absorb bank-specific shocks to credit supply.

The outcome variable Y_{ibjt} is either the logarithm of total committed credit, the logarithm of total committed credit lines, the share of the committed line of credit that is drawn down, the interest rate spread, the bank's subjective default probability of the borrower, a dummy equal to one if the loan is non-performing, the maturity of the committed exposure, or the logarithm of one plus the amount of collateral. Standard errors are double-clustered at the industry-state-quarter and bank level.

5 Results

This section presents our results. In Section 5.1, we show that the cyberattack had a significant negative effect on the revenues and profits of customers of the directly hit firms, while their suppliers were not affected. In Section 5.2, we show that the downstream effects are driven by customers that have fewer alternatives for the directly hit supplier. In Section 5.3, we show that the cyberattack caused a reduction in trade credit among affected customers that, in response, depleted their pre-existing liquidity buffers and increased borrowing. In Section 5.4, we use our loan-level data to show that affected customers drew down their credit lines at higher interest rates after the shock due to increased risk. In Section 5.5, we show that bank credit helped affected customers maintain their investment and employment. In Section 5.6, we show that affected customers formed new relationships with alternative suppliers after the shock, consistent with a wake up call effect of the cyberattack.

5.1 Downstream Propagation to Customers

Table 3 reports the coefficient estimates of Equation (1), separately for affected customers (Panel A) and affected suppliers (Panel B). In Panel A (B), the control group consists of similar firms to the affected customers (suppliers) but that were not connected to the firms directly hit by the cyberattack. The dependent variable is the ratio of operating revenues to total assets in columns (1) to (3) and the ratio of EBITDA to total assets in columns (4) to (6).

We first consider the effect on affected customers in Panel A. The disruption caused by the cyberattack was strongly propagated downstream, leading to a significant drop in customers' profitability relative to similar but unaffected firms—a 5% drop in operating revenues and 1.8% drop in EBITDA, corresponding to 7.5% and 20% of the respective sample medians. These magnitudes are in line with the fact that the cyberattack caused operations to halt at the directly affected firms for about three weeks in many cases. For both dependent variables, the coefficients become slightly larger in terms of magnitude as we increase the degree of fixed effects saturation. In columns (3) and (6), we employ firm and industry-country-size-year fixed effects, which amounts to comparing affected with unaffected firms in the same industry, country, size bucket, and year. In Table OA.3 of the Online Appendix, we show that the documented downstream effect is robust to an alternative definition of the treatment variable, where *Share Affected* is a continuous variable equal to the number of directly affected suppliers divided by the total number of suppliers in the same industries of the directly hit firms. The results are also unchanged if we use sales instead of operating revenues as the dependent variable, as shown in Table OA.3 in the Online Appendix.

Turning to the estimation of the upstream effect of the attack (Panel B of

Panel A: Customers	(1)	(2)	(3)	(4)	(5)	(6)
	Operating Revenues/Assets			EBITDA/Assets		
$Post_t \times Affected_i$	-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	✓	✓		✓	✓	
Industry-Country-Year		✓			✓	
Industry-Country-Size Bucket-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

Panel B: Suppliers	Operating Revenues/Assets			EBITDA/Assets		
$Post_t \times Affected_i$	-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	✓	✓		✓	✓	
Industry-Country-Year		✓			✓	
Industry-Country-Size Bucket-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

Table 3: Effect on Revenues and Profitability, Customers and Suppliers. This table presents results from Equation (1). The sample period runs yearly from 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. In Panel A, $Affected_i$ is a dummy equal to one if firm i is a customer of a directly hit firm. In Panel B, $Affected_i$ is a dummy equal to one if firm i is a supplier of a directly hit firm. The dependent variable in columns (1)-(3) is operating revenues divided by assets. The dependent variable in columns (4)-(6) is EBITDA divided by assets. Standard errors are clustered at the industry-country-year level. *** p<0.01, ** p<0.05, * p<0.1. Sources: BvD Orbis, FactSet Revere.

Table 3), we find a negative effect on the profitability of affected suppliers, albeit small in magnitude and statistically insignificant. These strong downstream but weak upstream effects are consistent with the findings of Alfaro, García-Santana and Moral-Benito (2020) in a different context and with the fact that the bottleneck occurred on the directly hit firms' ability to deliver their products to their customers. Instead, suppliers could have still been able to deliver their products to the directly hit firms. Given that the propagation effects of the cyberattack are concentrated on customers, we focus on them for

the remainder of the paper.

It is important to note that the downstream supply chain effects of the cyberattack are sizable. The damages to the directly hit firms in our sample add up to $2.2 billion (see Table 1) while a conservative estimate of the supply chain effects on customers suggests a drop in profits by $10 billion.[13] In Table OA.4 in the Online Appendix, we show that there are no effects on revenues and profitability at the second downstream level of the supply chain, namely among the customers of the affected customers.

5.2 Disruptions and Supply Chain Vulnerabilities

We now ask whether some features of the supply chain make customers more vulnerable to the disruption caused by the cyberattack. Specifically, we look at two dimensions of vulnerability: reliance on few suppliers and input specificity. As firms need several intermediate inputs and services in their production function, they become more vulnerable to sudden interruptions if they cannot easily substitute the supplier that is hit by a shock (Elliott, Golub and Leduc, 2020). Therefore, we hypothesize that affected customers that have fewer suppliers in the same industry of the directly hit supplier may face more production difficulties and therefore display a larger decline in revenues and profitability. Similarly, we test whether the customers of directly hit suppliers that produce highly specific inputs were hit relatively more in terms of revenues

[13] This estimate is obtained by combining the coefficient of column (5) in Table 3 with summary statistics on the number of firms, EBITDA over assets and average assets for each size quartile from Table 2. The number of firms in each size quartile is obtained by dividing the total number of observations in the treated group by 5, the number of years.

and profitability. Specifically, we estimate the following specification:

$$Y_{ijt} = \alpha + \sum_{k} \beta_k \text{Post}_t \times \text{Affected}_i \times \mathbb{1}(k)_i + \xi_i + \eta_{jt} + \epsilon_{ijt} \tag{3}$$

where, in addition to the variables defined in Equation (1), $\mathbb{1}(k)_i$ is a set of indicator variables.

In Panel A of Table 4, these indicator variables identify customer firms with one, two to four, or more than four suppliers in the same industry as the directly hit supplier they are connected to. Alternatively, in Panel B the indicator variables identify customer firms whose directly hit suppliers produce highly specific inputs. Following Barrot and Sauvagnat (2016), we define a supplier as producing a highly specific input if it has a high ratio of R&D expenditure to sales. In our case, among the directly affected firms, only Nuance and Merck have a non-negligible R&D ratio.

The results reported in Panel A of Table 4 show that the magnitude of the supply chain disruption is larger for customers with fewer suppliers in the same industry of the directly hit supplier. For instance, affected customers with five or more alternative suppliers see a negative but insignificant effect on revenues; those with two to four alternative suppliers see a 5.3% reduction; and those with only one supplier a 7.4% drop (column 3). The results are qualitatively similar for EBITDA in columns (4) to (6). Consistent with the endogenous network model of Elliott, Golub and Leduc (2020), these findings suggest that firms with more vulnerable supply chains, namely those with fewer alternative suppliers, are hit harder when one of their suppliers is temporarily shut down.[14]

[14]Given that we do not observe the size of the linkages, we cannot rule out that the affected supplier might represent a lower share of costs for customers with several suppliers.

	(1)	(2)	(3)	(4)	(5)	(6)
PANEL A: No. of Suppliers	Operating Revenues/Assets			EBITDA/Assets		
$Post_t \times Affected_i \times$ 1 $Supplier_i$	-0.073**	-0.083***	-0.092**	-0.016**	-0.018**	-0.026**
	(0.028)	(0.030)	(0.038)	(0.008)	(0.009)	(0.011)
$Post_t \times Affected_i \times$ 2-3-4 $Suppliers_i$	-0.030	-0.047**	-0.051*	-0.020*	-0.020	-0.028
	(0.023)	(0.020)	(0.027)	(0.011)	(0.013)	(0.018)
$Post_t \times Affected_i \times$ 5+ $Suppliers_i$	-0.016	-0.023	-0.020	0.002	-0.002	0.001
	(0.018)	(0.018)	(0.029)	(0.006)	(0.006)	(0.009)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		
Industry-Year	✓			✓		
Size Bucket-Year	✓	✓		✓	✓	
Industry-Country-Year		✓			✓	
Industry-Country-Size Bucket-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

PANEL B: Input Specificity	Operating Revenues/Assets			EBITDA/Assets		
$Post_t \times Affected_i \times SpecificInput_i$	-0.042	-0.054*	-0.089*	-0.022	-0.027*	-0.045**
	(0.030)	(0.029)	(0.048)	(0.014)	(0.015)	(0.022)
$Post_t \times Affected_i \times NotSpecificInput_i$	-0.035**	-0.045***	-0.043**	-0.006	-0.007	-0.008
	(0.015)	(0.015)	(0.020)	(0.004)	(0.005)	(0.007)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		
Industry-Year	✓			✓		
Size Bucket-Year	✓	✓		✓	✓	
Industry-Country-Year		✓			✓	
Industry-Country-Size Bucket-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

Table 4: Effect on Customers' Revenues and Profitability, Heterogeneity Across Number of Suppliers and Input Specificity. This table presents results from Equation (3). The sample period runs yearly from 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable in columns (1)-(3) is operating revenues divided by assets. The dependent variable in columns (4)-(6) is EBITDA divided by assets. In Panel A, n Suppliers equals one for customers that have n suppliers in the same industry of the directly affected supplier. In Panel B, SpecificInput equals one for the customers of the two directly affected firms that stand out for the non-negligible ratio of R&D to sales (Nuance and Merck). Standard errors are clustered at the industry-country-year level. *** p<0.01, ** p<0.05, * p<0.1. Sources: BvD Orbis, FactSet Revere.

Finally, in line with Barrot and Sauvagnat (2016) and Boehm, Flaaen and Pandalai-Nayar (2019), the results of Panel B show that disruptions are more severe when the directly affected supplier produces a more specific and therefore less substitutable product. Indeed, across columns the magnitude of the coefficient of interest is higher for SpecificInput$_i$ relative to NotSpecificInput$_i$.

5.3 Disruptions and Liquidity Risk Management

Next, we ask how the affected customers dealt with the decline in revenues and profits coming from the supply chain disruption. To pay their fixed and variable costs in the face of lower revenues, affected customers may utilize their internal liquidity or increase their external borrowings. In addition to the decline in revenues, affected customers may also suffer from a reduction in trade credit if the directly hit firms decide to extend less credit to their customers to deal with their own more pressing liquidity shortages. In Table 5, we estimate Equation (1) for the affected customers, using the ratio of trade credit from suppliers, long-term debt to total assets, and the liquidity ratio (current assets minus inventories divided by current liabilities) as the dependent variables. All these ratios are multiplied by 100.

In addition to a decline in revenues, affected customers also received less trade credit, further straining their liquidity conditions since trade credit is among the largest sources of short-term financing for firms.[15] The coefficients of columns (1) to (3) indicate a reduction in trade credit equal to 8 to 12% of its median value.[16] To deal with this double-whammy decline in both revenues and

[15] When a supplier sells goods to its customers, it typically demands payment for a fraction of the sales, with the remainder logged as account receivables (trade credit).

[16] Table OA.5 in the Appendix shows that the credit contraction affects customers fully

trade credit, affected customers relied on both internal liquidity and external borrowings. In columns (4) to (6), we find that affected customers increase their borrowings of long-term debt by about 1.5% of total assets relative to similar but unaffected firms. This effect is both statistically and economically significant, representing 13% of the median share of long-term debt to total assets. Finally, in columns (7) to (9) we estimate that affected customers reduce their liquidity ratio by 0.2 percentage points, which corresponds to 15% of the sample median.

Note that while directly hit firms may have wanted to continue to provide credit to their customers, they may not have been able to. In addition to the substantial liquidity stress coming from the disruption in operations, their insurance claims for the cyberattack damages were denied. Even if most firms had insurance policies that covered damages from cyberattacks, insurance companies refused to pay the claims citing a contractual clause exempting them from paying out if the damages were the result of an act of war (which NotPetya was equated to). The controversy is still being debated in court.

dependent on the directly hit suppliers for their trade credit, consistent with the decrease in trade credit being exclusively driven the directly hit firms.

Panel A: Customers	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
	Trade Credit/Assets			Long-Term Debt/Assets			Liquidity Ratio		
$Post_t \times Affected_i$	-0.467**	-0.539**	-0.792***	1.410***	1.168**	1.082*	-0.144**	-0.155**	-0.177*
	(0.207)	(0.227)	(0.303)	(0.431)	(0.474)	(0.612)	(0.068)	(0.077)	(0.104)
Fixed Effects									
Firm FE	✓	✓	✓	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		✓			
Industry-Year	✓			✓		✓			
Size Bucket-Year	✓	✓		✓	✓		✓	✓	
Industry-Country-Year		✓			✓			✓	
Industry-Country-Size Bucket-Year			✓			✓			✓
Observations	47,651	44,207	40,704	47,651	44,207	40,704	47,651	44,207	40,704
R-squared	0.913	0.923	0.925	0.876	0.889	0.895	0.741	0.752	0.758

Table 5: Effect on Customers' Financing. This table presents results from Equation (1). The sample period runs yearly from 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable in columns (1)-(3) is trade credit from suppliers divided by assets–the ratio is multiplied by 100 for ease of interpretation of the point estimate. The dependent variable in columns (4)-(6) is long-term debt divided by assets–the ratio is multiplied by 100 for ease of interpretation of the point estimate. The dependent variable in columns (7)-(9) is the liquidity ratio, defined as 100 times current assets minus inventories, divided by current liabilities. Standard errors are clustered at the industry-country-year level. *** p<0.01, ** p<0.05, * p<0.1. Sources: BvD Orbis, FactSet Revere.

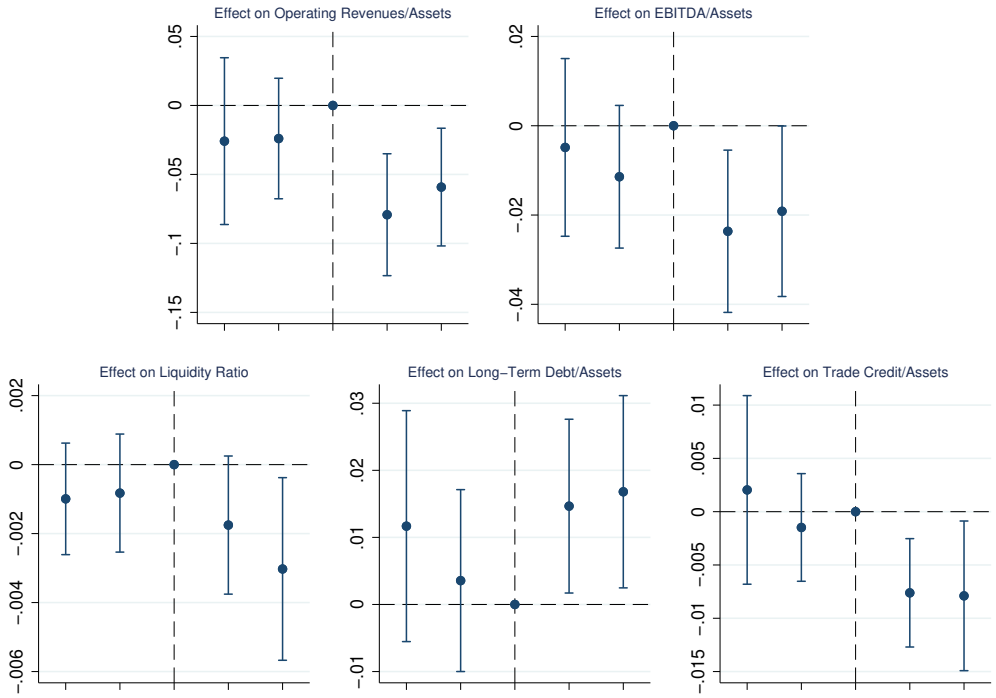

Figure 2: Parallel Trend Assumption, Coefficient Plots. This figure shows the estimated coefficients from the following specification: $Y_{ijt} = \alpha + \sum_{\tau=2014}^{2018} \beta_\tau \mathbb{I}_\tau \times \text{Affected}_i + \xi_i + \eta_{jt} + \epsilon_{it}$, where i is a firm and j is a country-year-industry-size bucket. Affected_i is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variables are operating revenues, EBITDA, holdings of liquid assets, long-term debt, trade credit. All dependent variables are normalized by assets. Standard errors are clustered at the industry-country-year level. Sources: BvD Orbis, FactSet.

Overall, we have found so far that the 2017 NotPetya cyberattack caused severe downstream supply chain disruptions. Affected customers saw significant declines in revenues, profitability, and trade credit. To cope with the shock, affected customers relied on both internal liquidity and external borrowing. While we exploit a shock exogenous to any given firm we analyze, to help validating our identification strategy we also show the coefficients plots of the difference-in-differences models in Figure 2. The parallel trends assumption seems to be validated by the lack of pre-trends for any of the outcome variables.

5.4 Disruptions and Bank Credit

We previously documented that affected customers increase their reliance on external financing to cope with the supply chain losses. Next, we focus on one of the most flexible ways in which firms can access external financing, namely bank credit. We use confidential quarterly bank-borrower data from the Federal Reserve's Y-14 collection.[17] First, we test whether affected customers increase their borrowings from banks, in the form of either drawing down their credit lines or taking out new term loans. The results are reported in Table 6. Total committed credit (columns 1 and 2) and committed lines of credit (columns 3 and 4) remain unchanged. However, affected customers significantly increase credit line draw downs. These findings highlight the importance of having access to credit lines that can be drawn down whenever a firm faces immediate liquidity needs.[18]

We also test whether banks charge affected customers with less favorable terms, such as higher interest rates, shorter maturities, or requiring more collateral. These requests could be indeed motivated by a perceived increase in the riskiness of these borrowers. The results are presented in Table 7. Relative to similar firms, affected customers see an increase in the interest rate they are charged. This is not due to possible selection bias originating from the matching of affected customers with banks offering less competitive pricing—in fact, the results are within bank-quarter, thus comparing the rate charged by the same bank to affected and unaffected firms.

[17] In unreported results, we confirm that our main effects are also present in the subsample of US firms.

[18] These results are consistent with Brown, Gustafson and Ivanov (2020) who, using the same data, show that firms respond to exogenous cash flow shocks (i.e., unexpectedly severe winter weather) by drawing down their credit lines at banks.

	(1)	(2)	(3)	(4)	(5)	(6)
	Log(Tot Committed)		Log(Committed Line)		Share Drawn	
$Post_t \times Affected_i$	-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	✓	✓	✓	✓	✓	✓
Industry-State-Quarter	✓		✓		✓	
Industry-State-Size Bucket-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

Table 6: Effect on Bank Credit. This table presents results from Equation (1). The quarterly sample runs from 2014Q1 to 2018Q4. *Post* is a time dummy equal to one from 2017Q3 onward. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable in columns (1)-(2) is the logarithm of the total committed credit (committed line of credit and term loan). The dependent variable in columns (3)-(4) is the logarithm of the committed line of credit. The dependent variable in columns (5)-(6) is the share of the committed line of credit that is drawn down. Standard errors are double-clustered at the industry-state-quarter and bank level. *** p<0.01, ** p<0.05, * p<0.1. Sources: Federal Reserve Y-14, FactSet Revere.

The higher interest rate charged to affected customers is consistent with the fact that banks perceive these affected customers are being riskier, as shown in column (2) by the higher probability of default perceived by the bank. However, this higher risk perception does not translate into a higher ex-post risk, since affected customers are as likely as other firms to make payments on time (column 3). Finally, columns (4) and (5) show that loan maturity and collateral are also unchanged.

Overall, our results suggest that affected customers significantly draw down their credit lines to cope with the pressing liquidity needs arising from the supply chain disruption. This comes at a cost because banks revise the riskiness of these borrowers and accordingly charge higher interest rates.

5.5 Real Effects of Cyberattack Disruptions?

So far we have documented the downstream effects of supply chain disruptions on customers and how they adjusted their liquidity and financing positions to

	(1) Rate Spread	(2) Pr(Default)	(3) NPL	(4) Maturity	(5) Collateral
$\text{Post}_t \times \text{Affected}_i$	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	✓	✓	✓	✓	✓
Industry-State-Size Bucket-Quarter	✓	✓	✓	✓	✓
Observations	131,428	104,591	131,428	130,890	114,641
R-squared	0.608	0.547	0.055	0.595	0.498

Table 7: Effect on Credit Terms. This table presents results from Equation (1). The quarterly sample runs from 2014Q1 to 2018Q4. *Post* is a time dummy equal to one from 2017Q3 onward. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable in column (1) is the interest rate spread, in column (2) the bank's subjective default probability of the borrower, in column (3) a dummy equal to one if the loan is non-performing, in column (4) the maturity of the committed exposure, and in column (5) the logarithm of one plus the amount of collateral. Standard errors are double-clustered at the industry-state-quarter and bank level. *** p<0.01, ** p<0.05, * p<0.1. Sources: Federal Reserve Y-14, FactSet Revere.

cope with the profit losses. Next, we test whether the supply chain disruptions felt by the affected customers also produced real effects i.e., lower employment and investment. Most papers on supply chain disruptions focus on the downstream effects on profitability and trade credit and not on employment and investment. One exception is Costello (2020) that, in the context of the 2007-09 financial crisis, shows that suppliers' financing constraints are propagated downstream to customers.[19] Among them, the smaller and more likely to be themselves financially constrained reduce employment. Our setup is different in three ways. First, our shock is more transitory than the financial shocks that occurred in 2007-09. Second, we have a set of relatively larger firms with access to external finance. Third, our shock occurs during normal times when

[19] Cingano, Manaresi and Sette (2016) show that banks more exposed to interbank borrowing during the 2007-09 crisis reduce lending by more. As a result of the credit contraction, firms borrowing from the more exposed banks cut investment, employment, and trade credit to customers. However, they do not study the real effects on the customers of these firms exposed to the credit contraction, which is instead our and Costello (2020)'s focus.

banks have no difficulties providing credit. Therefore, even if our shock was severe, affected customers could rely on bank credit to absorb the losses (as shown in Table 7), making it unlikely that they had to reduce employment and investment.

This is indeed what we find in Table 8. Using the same difference-in-differences setup of Equation (1), Panel A reveals that affected customers have similar employment growth after the shock relative to firms in the control group (columns 1–3). The same holds when considering wages (columns 4–6). Able to rely on external financing, affected customers similarly did not have to reduce investment. Specifically, Panel B shows that the effect of supply chain disruptions on customers' investment in tangible and intangible assets is insignificant. Our findings suggest that reliable access to external finance allowed affected customers to absorb the loss in profitability (coming from the supply chain disruption) without having to cut either employment or investment, which could have produced negative spillovers to the broader economy.

5.6 Disruptions and Dynamic Supply Chain Responses

As the NotPetya cyberattack exposed firms to the possibility that a supplier could stop operations for several weeks, in this final section we test whether affected customers build new trading relations with alternative suppliers after the shock. We call alternative supplier a firm operating in the same industry as the directly hit supplier. Consider affected customer i, which is exposed to the shock due to its connection with directly hit supplier s that operates in industry k. We then count the number of *new* trading relations that affected customer i forms after the cyberattack with suppliers in industry k.

	(1)	(2)	(3)	(4)	(5)	(6)
PANEL A: Employment	Δ Employees			Cost of Employees/Assets		
$Post_t \times Affected_i$	-1.458	-1.476	-2.252	0.001	0.003	-0.004
	(1.481)	(1.192)	(1.880)	(0.004)	(0.006)	(0.006)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		
Industry-Year	✓			✓		
Size Bucket-Year	✓	✓		✓	✓	
Industry-Country-Year		✓			✓	
Industry-Country-Size Bucket-Year			✓			✓
Observations	24,627	22,414	20,285	35,976	32,714	29,619
R-squared	0.271	0.415	0.612	0.897	0.905	0.951

PANEL B: Investment	Tang. Assets/Assets			Intang. Assets/Assets		
$Post_t \times Affected_i$	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	✓	✓		✓	✓	
Industry-Country-Year		✓			✓	
Industry-Country-Size Bucket-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

Table 8: Effects on Employment and Investment. This table presents results from Equation (3). The sample period runs yearly from 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. In Panel A, the dependent variable is the yearly percentage change in the number of employees in columns (1)-(3) and the cost of employees normalized by total assets in columns (4)-(6). In Panel B,the dependent variable is tangible fixed assets normalized by total assets in columns (1)-(3) and intangible fixed assets normalized by total assets in columns (4)-(6). Standard errors are clustered at the industry-country-year level. *** p<0.01, ** p<0.05, * p<0.1. Sources: BvD Orbis, FactSet Revere.

To test whether affected customers form a significantly larger number of new relations with alternative suppliers, we need to compute the number of new trading relations formed by firms in the control group as well. For the control group to provide a useful benchmark, we use the following procedure. First, each firm c in the control group is in the sample because it belongs to the same country, industry, and size bucket of affected customer firm i. As we

mentioned before, firm i is affected because its supplier s operating in industry k was directly hit by the cyberattack. Therefore, for the control group to offer a useful benchmark, we compute the number of new relations that control firm c has with suppliers in industry k. We repeat this process for each firm c in the control group.

Similarly, we are interested in studying whether affected customers are more likely to terminate trading relations with the directly hit suppliers. However, we cannot estimate the probability that affected customers stop trading with the directly hit supplier using the same empirical framework. This is because, by construction, firms in the control group do not have any trading relations with the directly hit firms—and thus cannot terminate them. Therefore, we use a different approach. We first utilize a dependent variable (Ended Relations) that counts the number of relations ended by affected customers with any supplier in the same industry as the directly hit supplier. Then we use a second dependent variable (Ended Relations excl. Hit Supplier) that counts the number of relations that affected customers terminate with suppliers, other than the directly hit one, in the same industry. As a result, the difference between the two estimates can be attributed to affected customers ending trading relations with the directly hit supplier. In both cases, the count of relations ended by firms in the control group is limited to the suppliers in the relevant industry k, as previously defined.

To highlight the dynamic supply chain adjustments, we estimate the immediate response that happened within six months from the attack (Post_{2017}) separately from the medium-term response that occurred more than one year after the attack (Post_{2018}). Notice that we are interested in the number of *new* and *ended* trading relations as opposed to just the total number of relations. Consider for instance an affected customer that terminates its relation with

	(1)	(2)	(3)	(4)	(5)	(6)
	New Relations		Ended Relations		Ended Relations excl. Hit Supplier	
$\text{Post}_{2017} \times \text{Affected}_i$	0.203***	0.220***	0.097**	0.102**	0.095**	0.102**
	(0.056)	(0.073)	(0.041)	(0.051)	(0.041)	(0.050)
$\text{Post}_{2018} \times \text{Affected}_i$	-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	✓		✓		✓	
Industry-Country-Year	✓		✓		✓	
Industry-Country-Size Bucket-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

Table 9: Effect on Supply Chain Relationships. This table presents results from Equation (3). The sample period runs yearly from 2014 to 2018. $Post_{2017}$ is a time dummy equal to one in 2017. $Post_{2018}$ is a time dummy equal to one in 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable in columns (1)-(2) is the logarithm of (one plus) relations started in year t with firms in the same industry (SIC2) of the directly hit firm. The dependent variable in columns (3)-(4) is the logarithm of (one plus) relations ended in year t with firms in the same industry (SIC2) of the directly hit firm. The dependent variable in columns (5)-(6) is the logarithm of (one plus) relations ended in year t with firms in the same industry (SIC2) of the directly hit firm, excluding those ended with the directly hit firm. Standard errors are clustered at the industry-country-year level. *** p<0.01, ** p<0.05, * p<0.1. Sources: BvD Orbis, FactSet Revere.

the directly hit supplier while starting a new one with an alternative supplier. This economically meaningful adjustment would not be captured by the total number of relations, which remains constant. Only by looking at new and ended relations would we capture this supply chain adjustment to the shock.

The results are reported in Table 9. In columns (1) and (2), the dependent variable is the logarithm of one plus the number of new relations (in the same industry as the directly hit supplier). Estimates indicate that affected customers significantly increased the number of new alternative suppliers soon after the cyberattack. The point estimate suggests that affected customers have 20% more new alternative suppliers than firms in the control group within six months after the cyberattack. No significant change in the number of new

relations occurs in 2018. In columns (3) and (4), we consider the number of ended relations with any supplier in the same industry as the directly hit supplier. Specifically, the dependent variable is the logarithm of one plus the number of ended relations. Estimates indicate that affected customers are more likely than similar firms in the control group to terminate suppliers in the same industry as the directly hit one. The intensity with which affected customers end relations is stronger in 2018 than in 2017. We contrast these results to those in columns (5) and (6), where the dependent variable is the logarithm of one plus the number of relations ended with all suppliers except the directly hit one (in the relevant industry). The coefficient of $\text{Post}_{2017} \times$ Affected$_i$ is the same in columns (4) and (6), indicating that affected customers do not immediately end relations with the directly hit suppliers. However, affected customers are likely to terminate relations with the directly hit suppliers in the medium-term. Indeed, the coefficient of $\text{Post}_{2018} \times$ Affected$_i$ is 0.21 in column (4) when considering all suppliers and 0.10 in column (6) when considering all suppliers except for the directly hit one.

Overall, the evidence presented in Table 9 suggests that customers are likely to take immediate steps to form new trading relations with alternative suppliers and later on terminate those with the suppliers that caused the disruption. This dynamic adjustment can be explained by customers preferring to trade with a new supplier before they stop trading with the old one in order not to interrupt production.

6 Conclusion

We study the supply chain effects of the most damaging cyberattack in history. Originated by Russian military intelligence to hit the Ukrainian economy, the

virus also infected Ukrainian subsidiaries of international companies and spread to their global network infrastructure, thus forcing them to halt operations for several weeks. As a result, the customers of these directly hit firms suffered significantly lower revenues and profits relative to similar but unaffected firms. In addition, these affected customers saw a reduction in trade credit provided to them by suppliers, putting further strains to their liquidity position. To cope with the shock, affected customers used their internal liquidity and increased borrowing, mainly by drawing down their credit lines with banks. Access to external finance allowed affected customers to absorb the loss in profitability without having to reduce either employment or investment.

We also document how the severity of the downstream disruption depended on the vulnerability of the supply chain. Specifically, we show that affected customers with fewer suppliers that can potentially substitute for the directly hit one experienced larger reductions in profitability. This result highlights the importance of building more resilient supply chains to mitigate the effects of disruptive cyberattacks as well as other shocks, including the Covid-19 pandemic. Finally, we uncover evidence consistent with the fact that affected customers build new trading relations with alternative suppliers immediately after the cyberattack and subsequently terminate relations with the suppliers responsible for the disruption.

Our paper has several policy implications. First, our results show the crucial need for better cybersecurity. This includes more compartmentalization of the network infrastructure, more scrutiny on the cybersecurity of third-party suppliers, and at least one backup facility that is offline at any time. For instance, Maersk's Ghana office happened to be offline due to a blackout and, only thanks to that, Maersk was able to restore its networks (Greenberg, 2019). Second, firms need to improve their risk management and contingency

planning with the goal of continuing activities in the event that anyone of their suppliers is unable to provide goods and services. The resilience of a supply chain rests on having multiple options for each intermediate good or service, so that no single supplier is irreplaceable (Elliott, Golub and Leduc, 2020). Third, the intelligence community should establish credible deterrence for cyber-aggressions of the magnitude of NotPetya, so that state-sponsored hackers at least have an incentive to put in place controls to make sure that the attack does not spread beyond its intended reach. For instance, even though Stuxnet allegedly infected more than 100,000 computers worldwide, it did not do any damage outside of its target of Iranian industrial control systems engaged in enriching uranium.

References

Accenture. 2019. "The Cost of Cybercrime." *Accenture*.

Acemoglu, Daron, and Alireza Tabhaz-Salehi. 2020. "Firms, Failures, and Fluctuations: The Macroeconomics of Supply Chain Disruptions." *Working Paper*.

Adelino, Manuel, Ivan Ivanov, and Michael Smolyansky. 2020. "Humans vs Machines: Soft and Hard Information in Corporate Loan Pricing." *Working Paper*.

Ahn, Daniel P, and Rodney D Ludema. 2019. "The sword and the shield: the economics of targeted sanctions." *CESifo Working Paper*.

Akey, Pat, Stefan Lewellen, and Inessa Liskovich. 2018. "Hacking corporate reputations." *Rotman School of Management Working Paper*.

Aldasoro, Iñaki, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach. 2020. "The drivers of cyber risk."

Alfaro, Laura, Manuel García-Santana, and Enrique Moral-Benito. 2020. "On the direct and indirect real effects of credit supply shocks." *Journal of Financial Economics, forthcoming.*

Amir, Eli, Shai Levi, and Tsafrir Livne. 2018. "Do firms underreport information on cyber-attacks? Evidence from capital markets." *Review of Accounting Studies*, 23(3): 1177–1206.

Antras, Pol, and C Fritz Foley. 2015. "Poultry in motion: a study of international trade finance practices." *Journal of Political Economy*, 123(4): 853–901.

Barrot, Jean-Noel. 2016. "Trade credit and industry dynamics: Evidence from trucking firms." *The Journal of Finance*, 71(5): 1975–2016.

Barrot, Jean-Noël, and Julien Sauvagnat. 2016. "Input specificity and the propagation of idiosyncratic shocks in production networks." *The Quarterly Journal of Economics*, 131(3): 1543–1592.

Berger, Daniel, William Easterly, Nathan Nunn, and Shanker Satyanath. 2013. "Commercial imperialism? Political influence and trade during the Cold War." *American Economic Review*, 103(2): 863–96.

Boehm, Christoph E, Aaron Flaaen, and Nitya Pandalai-Nayar. 2019. "Input linkages and the transmission of shocks: firm-level evidence from the 2011 Tōhoku earthquake." *Review of Economics and Statistics*, 101(1): 60–75.

Brown, James R, Matthew Gustafson, and Ivan Ivanov. 2020. "Weathering cash flow shocks." *The Journal of Finance, forthcoming.*

Carvalho, Vasco M, Makoto Nirei, Yukiko Saito, and Alireza Tahbaz-Salehi. 2020. "Supply chain disruptions: Evidence from the great East Japan earthquake." *The Quarterly Journal of Economics, forthcoming.*

Cingano, Federico, Francesco Manaresi, and Enrico Sette. 2016. "Does credit crunch investment down? New evidence on the real effects of the bank-lending channel." *The Review of Financial Studies*, 29(10): 2737–2773.

Cortes, Gustavo S, Thiago Christiano Silva, and Bernardus FN Van Doornik. 2019. "Credit Shock Propagation in Firm Networks: evidence from government bank credit expansions." *Working Paper.*

Costello, Anna Marie. 2020. "Credit market disruptions and liquidity spillover effects in the supply chain." *Journal of Political Economy, forthcoming.*

Crémer, Jacques. 1995. "Towards an economic theory of incentives in just-in-time manufacturing." *European Economic Review*, 39(3-4): 432–439.

Dube, Arindrajit, Ethan Kaplan, and Suresh Naidu. 2011. "Coups, corporations, and classified information." *The Quarterly Journal of Economics*, 126(3): 1375–1409.

Duffie, Darrell, and Joshua Younger. 2019. "Cyber runs." *Hutchins Center Working Paper.*

Eisenbach, Thomas M, Anna Kovner, and Michael Junho Lee. 2020. "Cyber risk and the us financial system: A pre-mortem analysis." *FRB of New York Staff Report.*

Elliott, Matthew, Benjamin Golub, and Matthew V Leduc. 2020. "Supply Network Formation and Fragility." *Working Paper.*

Garg, Priya. 2020. "Cybersecurity breaches and cash holdings: Spillover effect." *Financial Management*, 49(2): 503–519.

Glitz, Albrecht, and Erik Meyersson. 2020. "Industrial Espionage and Productivity." *American Economic Review*, 110(4): 1055–1103.

Gofman, Michael, Gill Segal, and Youchang Wu. 2020. "Production networks and stock returns: The role of vertical creative destruction." *The Review of Financial Studies, forthcoming.*

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired.*

Greenberg, Andy. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* Doubleday.

Kalemli-Ozcan, Sebnem, Bent E Sørensen, Carolina Villegas-Sanchez, Vadym Volosovych, and Sevcan Yesiltas. 2019. "How to Construct Nationally Representative Firm Level Data from the ORBIS Global Database." *Tinbergen Institute Discussion Paper 15-110/IV.*

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz. 2020. "Risk management, firm reputation, and the impact of successful cyberattacks on target firms." *Journal of Financial Economics, forthcoming.*

Kashyap, Anil K, and Anne Wetherilt. 2019. "Some principles for regulating cyber risk." *AEA Papers and Proceedings*, 109: 482–87.

Kopp, Emanuel, Lincoln Kaffenberger, and Christopher Wilson. 2017. "Cyber Risk, Market Failures, and Financial Stability." *Working Paper.*

Lichter, Andreas, Max Löffler, and Sebastian Siegloch. 2020. "The long-term costs of government surveillance: Insights from stasi spying in East Germany." *Journal of the European Economic Association, forthcoming.*

Martinez-Bravo, Monica, and Andreas Stegmann. 2018. "In vaccines we trust? The effects of the CIA's vaccine ruse on immunization in Pakistan." *CEMFI Working Papers.*

Moody's. 2020. "Suppliers and vendors are becoming the weakest link in corporate cybersecurity." *Moody's Corporates Global.*

NERC. 2020. "GridEx V Lessons Learned." *North American Electric Reliability Corporation.*

Siemens. 2019. "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?" *Siemens.*

Taschereau-Dumouchel, Mathieu. 2019. "Cascades and fluctuations in an economy with an endogenous production network." *Working Paper.*

Verizon. 2019. "Data Breach Investigations Report." *Verizon.*

WEF. 2019. "Regional Risks for Doing Business 2019."

For Online Publication[†]

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

OA.1 Additional Figures

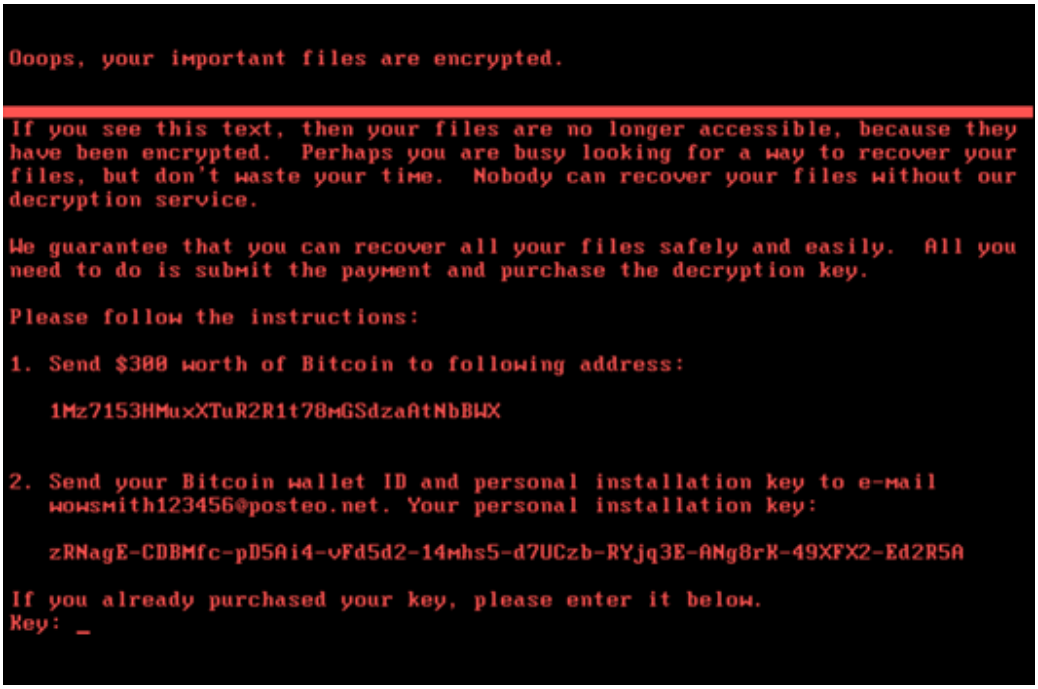

Figure OA.1: Computer Screen after NotPetya Infection. This figure shows the screen of a computer affected by NotPetya. It resembled a ransomware as it asks for a Bitcoin payment to obtain the decryption key. Source: www.crowdstrike.com/blog/.

[†]Date: October 2020. Not for publication. The views expressed in this paper are those of the authors and do not necessarily represent those of the Federal Reserve Bank of New York, the Board of Governors of the Federal Reserve System, or other members of its staff. First draft: July 2020. Authors: Matteo Crosignani (matteo.crosignani@ny.frb.org), Marco Macchiavelli (marco.macchiavelli@frb.gov), André Silva (andre.f.silva@frb.gov).

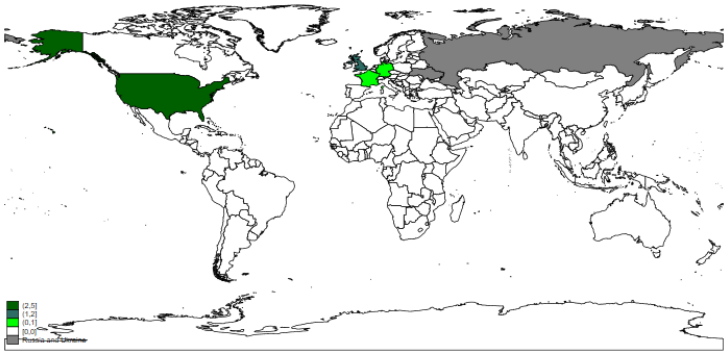

Figure OA.2: Geographical Location of Directly Hit Firms. This figure shows the geographical distribution of affected suppliers, i.e. suppliers of directly hit firms. Source: Orbis, FactSet.

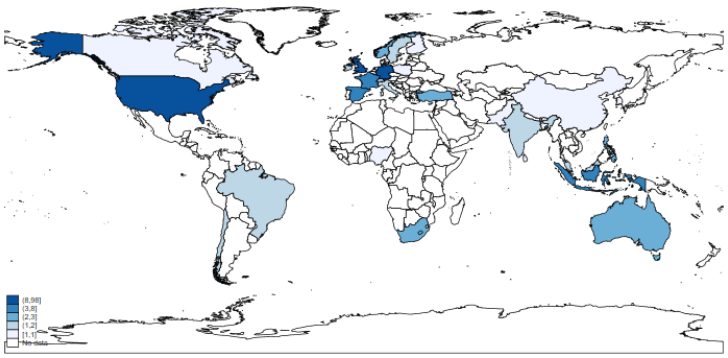

Figure OA.3: Geographical Location of Affected Customers. This figure shows the geographical distribution of directly hit firms. Sources: Bvd Orbis, FactSet Revere.

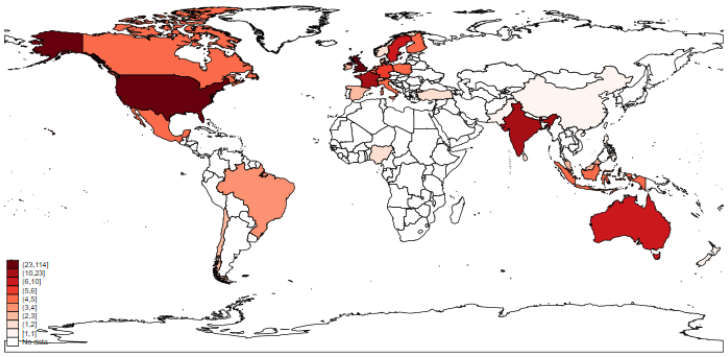

Figure OA.4: Geographical Location of Affected Suppliers. This figure shows the geographical distribution of affected suppliers, i.e. suppliers of directly hit firms. Source: Orbis, FactSet.

OA.2 Additional Tables

		Full	Size Q1		Size Q2		Size Q3		Size Q4	
	Stat	Sample	Treated	Control	Treated	Control	Treated	Control	Treated	Control
No. Obs.	Tot	47651	356	14138	361	11831	358	12259	366	7982
Age	μ	29.40	21.41	25.58	26.71	29.22	31.90	29.48	37.28	36.34
	p(50)	21.00	18.00	20.00	23.00	21.00	26.00	21.00	25.00	24.00
	σ	27.31	13.91	21.90	20.16	26.78	28.35	27.95	33.85	33.82
Assets (M)	μ	4512	105	89	460	449	1867	1888	33206	21582
	p(50)	578	101	79	443	408	1530	1672	10748	9434
	σ	19950	61	63	192	189	961	888	69632	41863
Capital/A	μ	0.24	0.36	0.51	0.10	0.16	0.08	0.11	0.07	0.08
	p(50)	0.03	0.03	0.08	0.02	0.03	0.01	0.02	0.01	0.01
	σ	1.07	0.85	1.89	0.23	0.35	0.16	0.23	0.18	0.15
EBITDA/A	μ	0.08	0.02	0.02	0.08	0.10	0.11	0.11	0.10	0.11
	p(50)	0.09	0.07	0.07	0.09	0.10	0.11	0.10	0.10	0.10
	σ	0.19	0.21	0.31	0.11	0.12	0.06	0.09	0.06	0.06
Liquidity Ratio	μ	1.99	2.94	2.75	1.83	2.00	1.60	1.62	1.33	1.23
	p(50)	1.20	1.61	1.50	1.29	1.24	1.07	1.14	1.01	0.99
	σ	3.38	4.04	4.55	1.81	3.22	2.11	2.69	1.37	1.40
LT Debt/A	μ	0.17	0.07	0.08	0.16	0.14	0.28	0.22	0.27	0.27
	p(50)	0.13	0.01	0.01	0.11	0.09	0.27	0.21	0.25	0.26
	σ	0.17	0.11	0.12	0.17	0.16	0.16	0.18	0.15	0.16
Op.Revenues/A	μ	0.86	0.89	0.97	0.91	0.93	0.78	0.80	0.63	0.64
	p(50)	0.70	0.83	0.84	0.83	0.78	0.70	0.65	0.54	0.49
	σ	0.78	0.52	0.89	0.61	0.80	0.53	0.73	0.47	0.59
Trade Credit/A	μ	0.12	0.18	0.15	0.17	0.12	0.12	0.10	0.11	0.07
	p(50)	0.09	0.15	0.12	0.15	0.10	0.11	0.08	0.08	0.05
	σ	0.11	0.12	0.13	0.14	0.11	0.09	0.10	0.10	0.07
ROA	μ	1.13	-5.41	-3.83	0.47	2.55	2.90	3.72	3.65	3.82
	p(50)	3.34	1.45	1.86	3.32	3.73	3.20	3.77	3.40	3.53
	σ	14.70	22.09	21.71	12.85	12.18	7.13	8.41	5.78	6.06
Sales/A	μ	0.85	0.87	0.96	0.90	0.92	0.77	0.79	0.62	0.63
	p(50)	0.69	0.82	0.82	0.83	0.77	0.69	0.65	0.54	0.49
	σ	0.78	0.52	0.89	0.60	0.80	0.53	0.73	0.47	0.59
No. Employees	μ	10349	713	759	2107	2697	7050	7543	54416	36756
	p(50)	1804	402	303	1417	1396	4200	4124	18011	14601
	σ	33072	1141	1790	2082	4947	10674	13179	95913	64048
Cost of Empl./A	μ	0.15	0.21	0.20	0.17	0.14	0.11	0.11	0.11	0.08
	p(50)	0.08	0.12	0.12	0.09	0.08	0.06	0.05	0.07	0.04
	σ	0.21	0.26	0.26	0.19	0.18	0.13	0.16	0.12	0.19
Tang. Assets/A	μ	0.28	0.17	0.21	0.24	0.28	0.36	0.30	0.27	0.34
	p(50)	0.20	0.08	0.14	0.17	0.21	0.31	0.23	0.16	0.27
	σ	0.25	0.19	0.22	0.23	0.25	0.28	0.27	0.26	0.28
Intang. Assets/A	μ	0.15	0.19	0.13	0.18	0.13	0.20	0.17	0.27	0.20
	p(50)	0.05	0.11	0.02	0.11	0.04	0.10	0.07	0.20	0.11
	σ	0.20	0.21	0.19	0.20	0.19	0.22	0.21	0.23	0.22

Table OA.1: Summary Statistics, Treated Vs. Control Suppliers. This table shows summary statistics for our sample firms. The table reports mean, median, and standard deviation. The sample period runs yearly from 2014 to 2018. The table shows the summary statistics for the full sample as well as the summary statistics for treated and control firms in each of the four size bucket groups. Treated firms are suppliers of a directly affected firm. Age is in years. Assets is in million USD. The liquidity ratio is 100*(current assets - inventories)/current liabilities. Current means that it converts into cash (matures) within one year. Long-term debt (LT Debt) is financial debt with a maturity greater than one year. Trade Credit is trade credit with customers. All the variables divided by total assets (A) are expressed as ratios. However, for ease of interpretation of the estimates, Trade Credit/A and LT Debt/A are multiplied by 100 in Table 5. Sources: BvD Orbis, FactSet Revere.

	(1)	(2)	(3)	(4)	(5)	(6)
	Sales/Assets					
$Post_t \times Affected_i$	-0.036***	-0.046***	-0.054***	-0.005	-0.010	-0.012
	(0.014)	(0.014)	(0.020)	(0.009)	(0.010)	(0.013)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		
Industry-Year	✓			✓		
Size Bucket-Year	✓	✓		✓	✓	
Industry-Country-Year		✓			✓	
Industry-Country-Size Bucket-Year			✓			✓
Affected Firms	Cust.	Cust.	Cust.	Suppl.	Suppl.	Suppl.
Observations	47,651	44,207	40,704	47,651	44,207	38,467
R-squared	0.932	0.943	0.945	0.932	0.944	0.950

Table OA.2: Effect on Sales for Customers and Suppliers. This table presents results from Equation (1). The sample period runs yearly from 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. The dependent variable is sales divided by assets. In columns (1)-(3), $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. In columns (4)-(6), $Affected_i$ is a dummy equal to one if firm i is a supplier of a directly affected firm. Standard errors are clustered at the industry-country-year level. *** p<0.01, ** p<0.05, * p<0.1. Sources: BvD Orbis, FactSet Revere.

	(1)	(2)	(3)	(4)	(5)	(6)
	Operating Revenues/Assets			EBITDA/Assets		
$Post_t \times Share\ Affected_i$	-0.064***	-0.077***	-0.090***	-0.017**	-0.019**	-0.027***
	(0.024)	(0.025)	(0.033)	(0.007)	(0.008)	(0.010)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		
Industry-Year	✓			✓		
Size Bucket-Year	✓	✓		✓	✓	
Industry-Country-Year		✓			✓	
Industry-Country-Size Bucket-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

Table OA.3: Effect on Revenues and Profitability, Customers, Continuous Treatment Variable. This table presents results from Equation (1). The yearly sample period runs from 2014 to 2018. *Share Affected*$_i$ is a continuous treatment variable equal to the number of directly affected suppliers divided by the total number of suppliers in the same industry of the directly affected firm. If a customer is linked to multiple directly affected firms, we use the industry with the weakest (less diversified) link. The dependent variable in columns (1)-(3) is operating revenues divided by assets. The dependent variable in columns (4)-(6) is EBITDA divided by assets. Standard errors are clustered at the industry-country-year level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis, FactSet Revere.

	(1)	(2)	(3)	(4)	(5)	(6)
	Operating Revenues/Assets			EBITDA/Assets		
$Post_t \times \widetilde{Affected_i}$	-0.002	-0.006	-0.007	0.004	0.004	0.006
	(0.007)	(0.008)	(0.010)	(0.003)	(0.003)	(0.004)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Year	✓			✓		
Industry-Year	✓			✓		
Size Bucket-Year	✓	✓		✓	✓	
Industry-Country-Year		✓			✓	
Industry-Country-Size Bucket-Year			✓			✓
Observations	47,651	44,207	38,713	47,651	44,207	38,713
R-squared	0.931	0.942	0.949	0.809	0.820	0.829

Table OA.4: Effect on Revenues and Profitability, Customers of Affected Customers. This table presents results from Equation (1). The yearly sample period runs from 2014 to 2018. $\widetilde{Affected_i}$ is a dummy equal to one if firm i is a customer of a customer of a directly hit firm. The dependent variable in columns (1)-(3) is operating revenues divided by assets. The dependent variable in columns (4)-(6) is EBITDA divided by assets. Standard errors are clustered at the industry-country-year level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis, FactSet Revere.

	(1)	(2)	(3)	(4)
	Trade Credit/Cost of Good Sold		Cost of Good Sold/Assets	
$Post_t \times Affected_i$	-0.008		-0.061***	
	(0.006)		(0.017)	
$Post_t \times Affected_i \times 1\ Supplier_i$		-0.017**		-0.090***
		(0.009)		(0.030)
$Post_t \times Affected_i \times 2\text{-}3\text{-}4\ Suppliers_i$		-0.007		-0.047*
		(0.011)		(0.026)
$Post_t \times Affected_i \times 5+\ Suppliers_i$		(0.011)		(0.026)
		(0.009)		(0.028)
Fixed Effects				
Firm	✓	✓	✓	✓
Industry-Country-Size Bucket-Year	✓	✓	✓	✓
Observations	34,113	34,113	34,113	34,113
R-squared	0.849	0.849	0.948	0.948

Table OA.5: Effect on Trade Credit and Cost of Good Sold, Customers. This table presents results from Equation (1). The yearly sample period runs from 2014 to 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly hit firm. The dependent variable in columns (1)-(3) is trade credit divided by cost of good sold. The dependent variable in columns (4)-(6) is cost of good sold divided by assets. Standard errors are clustered at the industry-country-year level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis, FactSet Revere.