Risk Analysis, Vol. 42, No. 8, 2022 DOI: 10.1111/risa.13715

Systemic Cyber Risk and Aggregate Impacts

Jonathan W. Welburn* and Aaron M. Strong

With some of the largest cyber attacks occurring in recent years—from 2010 to 2019—we are only beginning to understand the full extent of cyber risk. As businesses grapple with the risks of cyber-incidents and their imperfect ability to prevent them, attention has shifted toward risk management and insurance. While there have been efforts to understand the costs of cyber attacks, the systemic risk—a result of risks spreading across interdependent systems—associated with cyber attacks remains a critical and problem in need of further study. We contribute a theoretical framework that describes systemic cyber risk as the result of cascading, common cause, or independent failures following a cyber incident. We construct a quantitative model of cascading failures to estimate the potential economic damage associated with a given cyber incident. We present an interdisciplinary approach for extending standard sector-level input–output analyses to the cyber domain, which has not been done. We estimate the aggregate losses associated with firm-level incidents, a contribution to risk analysis and computational economic modeling. We use this model to estimate the impact of potential cyber incidents and compare model results to a case with known damages. Finally, we use the model of systemic cyber failure to consider the implications on the growing cyber insurance market and the need for broader cyber policy. While we discuss the topic of systemic cyber risk, our contribution of using I/O analysis to estimate the aggregate losses from firm-level incidents is applicable across a variety of risk analysis applications from environment to health.

KEY WORDS: Cyber insurance; cyber policy; cyber risk; systemic risk

1. INTRODUCTION

The benefits of a heavily interconnected world through cyberspace have increasingly come with a cost.[1] Cyber incidents have risen both in prevalence and significance in their disruptions to individuals, businesses, and governments. In 2015, a cyber attack on Saudi Aramco allowed state actors to destroy 35,000 of the state-run oil company's workstations (Pagliery, 2015). In 2016, state actors sought to interfere in U.S. elections by hacking the Democratic National Committee (Office of the Director of National Intelligence, 2017). In 2017, a hack against Equifax allowed cyber actors to steal 145.5 million sensitive records that included social security numbers, credit cards, and addresses (SEC, 2018). These examples are three of many that provide evidence of the potentially far-reaching impact of cyber attacks, calling attention to escalating risks in cyberspace, where sophisticated, and often state affiliated actors, are capable of evading even the best defenses, a problem extending beyond these three examples (e.g., the compromise of the U.S. Department of Defense classified computing network discussed by Lynn III (2010)), causing significant disruption and financial damage. However, the potential perils of cyber risk may be even worse than these examples.

RAND Corporation, 1776 Main St., Santa Monica, CA, 90401, USA.
*Address correspondence to Jonathan W. Welburn, RAND Corporation, 1776 Main St., Santa Monica, CA 90401; jwelburn@rand.org

[1]Romanosky (2016) and Aldasoro, Gambacorta, Giudici, and Leach (2020) provide empirical evidence on the rising costs of cyber incidents.

The problem of malicious activity in cyberspace is not just about self-contained incidents. Others cyber incidents have spread, if not grown, across dependent systems. In a 2016 cyber attack, hackers, widely considered to be hacktivists, employed a botnet to launch a distributed denial-of-service (DDoS) attack on Dyn, a domain name system (DNS) provider. Dependent on the services of Dyn, many significant customers, in turn, suffered outages as a result; Amazon, Netflix, PayPal, and the BBC were all disrupted over a period of hours (Meyer & Lafrance, 2016). Additionally, in 2017, two cyber attacks—WannaCry and NotPetya—led to the rapid spread of perceived ransomware that disrupted diverse industries ranging from healthcare to transportation, to telecommunication and infrastructure across the world (Collins, 2017). The costs were significant. Maersk, a single large global shipping company, reported $300M in lost revenue resulting from the NotPetya attack (Thomson, 2017). Perhaps the most worrying of all cyber incidents has been the emerging use of cyber tools to disrupt civilian power grids. In March of 2018, the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a joint report outlining an intended cyber intrusion into the U.S. power grid, which could allow state actors to disrupt power to a large number of civilians. Had the attack been fully realized, it would not have been the first time: a cyber attack on the Ukrainian power grid in 2015 disrupted power to over 225,000 residents (ICS-CERT, 2016). In contrast to cyber incidents isolated effects, these incidents, resulting in outsized effects and often ill-understood cascading failure[2], exemplify the potential for systemic risk in cyberspace.

This article addresses the emerging form of cyber risk called *systemic cyber risk*. We seek to elucidate the scale of systemic cyber risks and, specifically the potential economic consequences of systemic cyber failures. That is, we distinguish between the broader term of systemic cyber risk, encompassing probability, uncertainty and consequence, and the more specific systemic cyber failure. This article focuses on the later portion of risk, we seek to understand systemic cyber failure and potential impacts. In doing so, we give specific attention to the question of whether cyber insurance is a sufficient tool for managing cyber risks, or whether systemic cyber risk warrants new conversations on cyber policy are needed. In Section 2, we build on current definitions and discussions of systemic cyber risk to advance the discussion through a theoretical framework of systemic cyber risk, which we use to develop a quantitative model of systemic cyber failure in Section 3. In Section 4, we use the model to analyze specific cyber incident scenarios and their potential damage. We then use insights from Sections 3 and 4 on the economic consequences of systemic cyber failures, to discuss the implications of systemic cyber risk for cyber insurance and cyber policy in Section 5. Finally, in Section 6, we provide a set of conclusions on systemic cyber risk.

[2]See, for example, the results of the workshop held by Brenner et al. (2017) that highlight both concern over the impact of cascading network failure and the inadequacy of current models in capturing them.

2. EFFORTS TO UNDERSTAND SYSTEMIC CYBER RISK

Within the context of financial networks, De Bandt and Hartmann (2000) have defined systemic risk as follows:

> "an event, where the release of 'bad news' about a financial institution, or even its failure, or the crash of a financial market leads in a sequential fashion to considerable adverse effects on one or several other financial institutions or markets, e.g. their failure or crash."

In the De Bandt and Hartmann (2000) definition, a systemic event is a "domino effect" following a limited idiosyncratic shock or the result of "simultaneous adverse effects" due to widespread systemic shocks. Following the 2008 global financial crisis, numerous studies were conducted on systemic risk in finance, with many focusing on network structures (e.g., Acemoglu, Ozdaglar, and Tahbaz-Salehi (2015)) and the broader policy challenges of financial institutions that are either too big or too interconnected to fail.

The interconnections of financial networks that drove the studies of systemic risk following the 2008 financial crisis are highly similar to those of cyberspace. Like financial networks, cyberspace presents a system of heavily interdependent organizations connected through network ties (both in terms of supply chain networks and computer networks in cyberspace). This has given rise to the term, *systemic cyber risk*, as the deliberate combination of fields—systemic risk and cyber risk. As a result, the study of systemic risks in cyberspace is inherently interdisciplinary; it builds on the fields of cyber security, finance, economics, and risk analysis. In this

section, we leverage these fields to contribute to a unified understanding of systemic cyber risk.

However, before defining systemic cyber risk, it is useful to establish a cyber lexicon for this article. We define the term *cyber incidents* under the widely used C-I-A framework[3] as a *loss of confidentiality, integrity, and availability of digital information and information systems*. In this context, the term *hacking* is the act of causing a cyber incident. As a specific type of incident, we define the term *data breach* as the *loss and exposure of confidential data following a cyber incident* coming from either the access to data or transfer of data by an unauthorized user or insider threat. Furthermore, we define the term *cyber attack* as the *degradation, disruption, or corruption of digital information and information systems* that in many cases (such as the distributed denial of service attack) result in the *loss of availability*. We make the assumption that all cyber incidents can be categorized as either data breaches or cyber attacks (with some potential for overlap between the two). Thus, the 2017 cyber incident at Equifax[4] qualifies as a data breach as hackers gained unauthorized access to sensitive data transferring it to unauthorized systems, while the 2016 cyber incident disrupting the Ukrainian power grid[5] represents a cyber attack as hackers were able to disrupt the critical functions of information systems providing electrical power.

2.1. Approaches for Characterizing Systemic Cyber Risk

Several efforts have been made to reach a common definition of the term systemic cyber risk. The World Economic Forum (2016) defines it as follows:

> "Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security. The adverse real economic, safety and security effects from realized systemic risk are generally seen as arising from significant disruptions to the trust in or certainty about services and/or critical data (i.e. the integrity of data), the disruption of operations and, potentially, the incapacitation or destruction of physical assets."

An effort by the Homeland Security Systems Engineering and Development Institute (HSSEDI) and the Department of Homeland Security (DHS) has also sought to define systemic cyber risk. While their characterization of systemic cyber risk fits within the broad definition from the World Economic Forum, it is more specific on potential systemic cyber incidents. They apply existing concepts from risk analysis to the field of cyber risk to produce a cyber threat model and identify 11 systemic cyber attack patterns: common mode/repeated attacks, common mode/scattershot attacks, common mode/pervasive attacks, rolling attacks, transitive attacks, cascading attacks, shared resource consumption attacks, critical function attacks, regional attacks, service dependency attacks, and coordinated supply chain attacks (Bodeau & McCollum, 2018). These 11 systemic cyber risk patterns provide a step forward toward beginning to model the likelihood of systemic cyber incidents.

Furthermore, others have contributed to the understanding of the potential impacts of systemic cyber incidents. For example, the U.S. Department of Treasury's Office of Financial Research (OFR) notes that systemic cyber risk can be a source of systemic financial risk where a cyber event on systemically important firms could lead to substantial spillover effects, or outward propagations (OFR, 2017). A report from the Organisation for Economic Cooperation and Development (OECD) shares this view and identifies specific types of systemic cyber incidents that could serve as a potential drivers of country-level and global-level shocks (Sommer & Brown, 2011). OFR (2017), notably, identifies three key channels for cyber risks to affect financial stability: a lack of substitutability for services from key firms, a potential loss of confidence, and the potential loss of data integrity. Furthermore, OFR (2017) suggests the use of "cyber stress tests" as a regulatory tool.

2.2. Approaches for Modeling the Economic Impact of Cyber Risk

The modeling of economic consequences cyber risk for is an evolving field and has leveraged methods from risk analysis in different ways. For example, a growing branch of this work has taken a game-theoretic approach to modeling cyber risk and

[3]For example, see discussion of the C-I-A framework by Andress (2014).
[4]See detailed incident description by SEC (2018).
[5]See detailed incident description by US-CERT (2018).

defensive investment (e.g., Acemoglu, Malekian, and Ozdaglar (2016); Hausken (2009); Kovenock and Roberson (2018); Nagurney and Shukla (2017); Simon and Omar (2020)) as well as general network security (see, for example, the surveys from Roy et al. (2010) and Do et al. (2017)). Others have addressed the need for enhanced modeling to adjust to the new risks of the digital era; "because of the complexities involved in quantifying the full range of cyber risks, companies and insurers have tended to take a relatively rudimentary approach to modeling" (SwissRe, 2017). As a result, the literature on estimating the range of costs associated with cyber incidents is expanding. Using an empirical approach, Romanosky (2016) examined data from over 12,000 cyber incidents through descriptive statistics finding that the median incident results in a cost just under $200,000. Exploring the impact of a specific type of incident, Lloyd's and AIR estimated the potential financial impact of a cyber attack on a major cloud provider causing an outage that disrupts service to its users. Using data on industry exposures and "what-if" scenario evaluation, they used a simulation approach to estimate the potential financial losses. They estimated total losses between $5 and15 billion for an outage lasting between —three and six days (AIR & Lloyd's, 2018). Others have estimated aggregate costs of incidents. To do so, cyber value-at-risk models, which borrow from the Value at Risk (Var) techniques popular within financial risk management to estimate likely cyber incident-driven losses a specific period of time, have gained in use (World Economic Forum & Deloitte, 2015). Using the cyber value at-risk approach, a study by Deloitte estimated an annual expected loss of €10 billion annually to the Dutch economy, or 1.5% of GDP (van Wieren, van Luit, Estourgie, Jacobs, & Bulters, 2016). Lloyd's estimated that cyber attacks cost companies $400 billion in aggregate annually (Gandel, 2015). While each of these approaches offer varying approaches with varying estimations of cyber incident costs, from moderate to high, they are also challenged by the observation bias inherent to data-driven analyses of cyber risk.

Others have turned to incident data. The sample of cyber incidents from the Advisen data set has been studied by Romanosky (2016), and more recently Aldasoro et al. (2020), to demonstrate variation and trends in cyber incidents and their costs. Aldasoro et al. (2020), for example, notes the high prevalence on of cyber incident occurrence in the financial sector which, in conjunction with the Eisenbach, Kovner, and Lee (2020) analysis of contagion within financial systems following cyber incidents, is reason for concern. However, Aldasoro et al. (2020) also note the low costs in this sector suggesting the success of regulation and increased investment in cyber security practices. Yet, while such studies may represent a large number of cyber incidents, there is the uncomfortable reality that such data may miss the full distribution, and the upper tail in particular. With all likelihood, some incidents have either gone unobserved, unreported, or have yet to occur. As a result, descriptive statistics over partially observed incidents risks underestimating tail risk. In contrast, structural models have the potential for understanding the mechanisms that could result in unobserved risks.

The use of structural models, models that estimate economic impact through the use of structural relationships rather than statistical, has been largely under explored for estimating the economic impact of cyber incidents. Dreyer et al. (2018) created a tool to estimate potential aggregate costs of cyber incidents across economic sectors for over 60 countries. In this setting, Dreyer et al. (2018) estimated both the direct costs and the systemic costs resulting from an incident. Importantly, to estimate systemic costs, they used sector level input–output analysis to estimate the propagation across backward linkages or *upstream* supply chain linkages of costs following a cyber incident. While the Dreyer et al. (2018) analysis found a high level of sensitivity to input parameters, where costs could range from the hundreds of billions of dollars annually to the trillions, they also found that direct costs associated with cyber incidents could pale in comparison to systemic costs, which include both upstream and *downstream*, the result of propagations across forward linkages in the supply chain, costs. However, acknowledging that downstream costs could exceed upstream costs, the authors leave this as an area for future work.

2.3. A Framework for Characterizing Systemic Cyber Risk

We build on the existing definitions of systemic cyber risk and introduce a framework for understanding and modeling systemic cyber risk, which leverages common concepts from risk analysis and economics and is more parsimonious than the DHS framework discussed by Bodeau and McCollum (2018). An individual cyber incident can occur by many different means, exploiting one or many

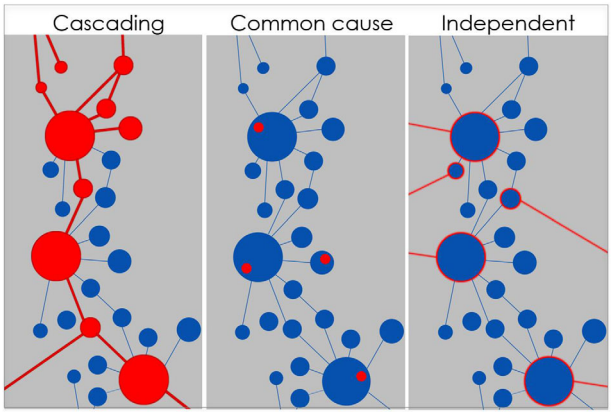

Fig 1. Types of systemic cyber risk
Figure 1 visualizes the three categories of systemic cyber failures. Cascading failures result from the propagation of disruptions across network connections following a cyber incident on a given firm, common cause failures result from the exploitation of common vulnerabilities shared by many firms, and independent failures result from the simultaneous individual and isolated cyber incidents occurring at many firms.

vulnerabilities. We define three categories of systemic failures: *cascading*, *common cause*, and *independent*, each depicted below in Fig. 1.

Cascading cyber failures are the result of one cyber incident propagating outward and causing many disruptions. They lead to a domino effect across firms and organizations interconnected through supply chains. The DDoS cyber attack on Dyn, where firms dependent on Dyn's services suffered outages and business disruptions due to the single attack on Dyn's network (Meyer & Lafrance, 2016), exemplifies a cyber incident leading to cascading cyber failures. In this definition of cascading failure, we refer specifically to the propagation of firm level disruptions, not necessarily the propagation of cyber vulnerabilities. That is, in the Dyn example, the initial attack leads to cascading failures due to disrupted business services and operations.

Furthermore, *common cause cyber failures* are the result of one cyber exploit triggered at many firms causing many cyber incidents. Unlike cascading failures, common cause failures exploit a common vulnerability held by multiple firms and organizations causing numerous cyber incidents either simultaneously or in quick succession. The WannaCry cyber attack provides a well-known example where a software vulnerability was exploited by a single hack to compromise thousands of machines for ransom across the world within days (Collins, 2017).

It is worth noting that, in cyberspace, cascading and common cause failures are not mutually exclusive. A quick spreading worm, for example, may exploit a widely held vulnerability on a single machine to spread from the source outward to many directly and indirectly connected systems. While this kind of incident has features of cascading failures, we classify this type of failure as a common cause cyber failure with cascading consequences. For cascading failures, we focus on the cascade resulting from the direct and indirect effects of business outages where customers lose access and supplier lose revenue.

Finally, *independent cyber failures* are the result of cyber incidents exploiting independent vulnerabilities at individual firms and organizations. In theory, numerous individual cyber incidents could happen simultaneously to create a systemic event, however in practice this type of event is currently unlikely. However, absent advances in postquantum cryptography, the advent of quantum computing could enable encryption breaking en masse, leading to concern over large scale independent failures (Vermeer & Peet, 2020).

Cascading and common cause cyber failures are, therefore, the drivers of systemic cyber risk. This article puts a specific focus on cascading cyber failures, and the next sections offer a methodology for quantifying them.

3. QUANTITATIVE MODEL

Brenner et al. (2017) notes that, while the potential for cascading failure is a significant concern for experts in industry, academia, and government, sector-specific models have been inadequate in bringing the costs and consequences of cascading failure to light. This inadequacy stems, in large part, from the challenges in applying traditional structural modeling approaches to firm-level risks. That is, while data on the input and output flows between economic sectors exist enabling analysis at the level of sectors, firm-level data on production networks, which identify a complete network of connections between firms, do not.[6] This reality is underscored by the recent review of the literature on production networks by Carvalho and Tahbaz-Salehi (2019), which find the lack of firm-level data a likely cause for scant research of firm-level production networks.

[6]There are current efforts by vendors such as Cyence, CyberCube, BitSight, and Security Scorecard to collect information on cyber network connections.

This challenge has been addressed in different ways. Some authors (e.g., Carrera, Standardi, Bosello, & Mysiak, 2015; Rose, Oladosu, & Liao, 2007) have relied on sector-level computable general equilibrium (CGE) models to estimate the economic impacts arising from natural or human induced business interruptions. This approach explicitly assumes that following a significant disruption and firms adjusting production to accommodate changes in prices, an economy instantaneously moves to a new equilibrium, with prices adjusting. However, in the real world, prices tend to be sticky and contracting is costly from a supply chain perspective. As a result, it may not be appropriate to assume that an economy is in an equilibrium following a disruption. By definition, a disruption should invoke a disequilibrium that needs to be taken into account and prices may not adjust due to contracts. Our approach only considers shocks that are small enough so that firms cannot recontract. We, therefore, require a different approach than the traditional CGE models which would allow for the instantaneous adjustment of prices and lack of consideration of contracts within a supply chain.

As a result, input–output (I/O) modeling offers advantages over CGE models in the context of estimating the immediate economic impact of an idiosyncratic shock (cyber attack). I/O models, pioneered by Leontief (1966), describe the movement of goods between sectors are models of economic interdependence frequently used to estimate the economy wide impact of sectoral fluctuations. The use of I/O modeling in the cyber context has, consequently, grown; Andrijcic and Horowitz (2006); Santos and Haimes (2004); Santos, Haimes, and Lian (2007); and Dreyer et al. (2018) each provide examples of I/O modeling applications to cybersecurity. Importantly though, a traditional I/O modeling approach does not capture downstream impacts. Computable general equilibrium analysis does capture these downstream supply chain impacts through changes in prices. Due to the nature of the I/O model with Leontief production functions, the loss of a proportion of an input corresponds to the same loss in production (Leontief, 1966). In the short run, for outages lasting on the order of days to weeks, this may be the appropriate assumption, since recontracting (i.e., creating new contracts for new supplier) is not necessarily feasible on this time scale. The current work considers outages that are economically significant but short enough so that firms may not be able to recontract with an alternative supplier or customer.

Furthermore, firms have varying abilities to maintain operations during and recover from cyber attacks, an ability henceforth referred to as resilience. The benefit of using I/O analysis over the short run versus CGE modeling over the long run has been generally accepted resilience of firms, their ability to withstand and recover from cyber attacks, may depend on numerous factors ranging from their cyber maturity to the nature of their business. Given that many of these factors are unknown, and the differing natures of static and dynamic resilience, estimating the resilience of individual firms is nontrivial. We can, however, look to efforts to estimate average resilience at the level of economic sectors. Rose et al. (2007) investigates the impact of a terrorist attack driven power outage calibrating the resilience of different industry sectors to a power outage. With some differences in impact, a power outage and a cyber network outage result in a similar temporary loss in availability of production or services for the impacted firm, enabling the Rose et al. (2007) results to be used in the cyber context.

Therefore, we use this section to define a structural model which builds on traditional I/O modeling to estimate the potential impacts of cyber incidents at individual firms. Specifically, the quantitative model presented in this section estimates the potential economic consequences of cyber incidents (in terms of terms of the aggregate loss in sales across the economy), which result from a cyber attack on a given firm with effects that propagate upstream and downstream through its supply chain. We incorporate a firm level resilience that control for temporal substitution and other business operations that minimize the impacts of business interruptions on firm output and revenue using results from Rose et al. (2007) at the sector level.

3.1. Cyber attack Foundations of Idiosyncratic Firm Risk

To understand the aggregate impacts resulting from a cyber attack-driven outage at individual firms, we model the economy using a method similar to that of Acemoglu, Carvalho, Ozdaglar, and Tahbaz-Salehi (2012). The economy is, thus, defined by the tuple $\mathcal{E} = \{S, \boldsymbol{W}, \epsilon\}$ where S is a set of sectors, $\boldsymbol{W}$ is a weighted adjacency matrix, and ϵ is a vector of sector-level shocks. In this economy, each sector is made up of firms where each firm f produces output y_f such that the total sector output Y_i is determined

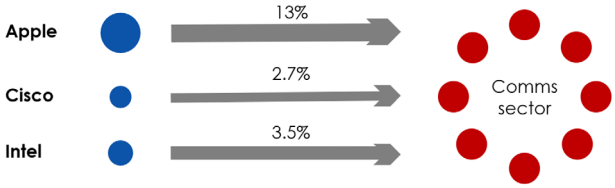

Fig 2. Representative firm linkages from technology to communications.

Figure 2 provides three example connections between technology and communications sectors where Apple, Cisco, and Intel's input–output linkage to the communications sector are proportional to their output share 2017 such that each linkage, ω_{fi}, is 13%, 2.7%, and 3.5% of total sector-level input–output linkages, respectively.

by the sum of its firms ($Y_i = \sum_{f \in i} y_f$) and aggregate output Y is determined by the sum of all firms ($Y = \sum_f^m y_f$).

To model the economy of $\mathcal{E}$, we first focus on the microorigins of aggregate shocks. We present an approach for estimating the microfoundations of aggregate shocks stemming from firm-level outages using a model of firms with representative sectoral ties. This approach begins with the following assumption.

Assumption 1. Representative firm linkages

> We assume that the flows in and out of each sector are representative of the firms in that sector. That is, each firm is a representative firm in that sector that only differ in output but not the underlying production process.

Assumption 1 implies that for any given firm f in sector i, its flows to and from all other sectors j are proportional to its share of sector level output as follows:

$$u_{fj} = \omega_{fi} w_{ij} \; \forall f \in i, \quad j \in S, \tag{1}$$

where w_{ij} are the flows from sector i to sector j, ω_{fi} is firm f's output (as determined by revenue) share of sector i and u_{fj} are the output flows from firm f used as inputs to production in sector j, a relationship depicted below in Fig. 2. Note that, u_{jf} can be determined similarly as the output flows from sector j used as inputs to production by firm f. Importantly, given the heterogeneity of firms across and within firms, we do not argue that Assumption 1 is ideal for estimating trade flows but rather that it leads to an important contribution to the estimation of *aggregate* losses from firm-level shocks.

Next, by introducing idiosyncratic firm-level shocks, ϕ_f, sector-level shocks ϵ_i can therefore be explained by microfoundations as follows:

$$\epsilon_i = \phi' \; \boldsymbol{\omega_i}, \tag{2}$$

where $\boldsymbol{\omega_i} = [\omega_{1i} \ldots \omega_{mi}] \in \mathbb{R}^m$ is the vector of firm output shares and $\phi = [\phi_1 \ldots \phi_m] \in \mathbb{R}^m$ is the vector of idiosyncratic firm-level shocks. Note that the vector ϕ is conceptually similar to the inoperability vector used by Santos and Haimes (2004) and Santos et al. (2007). Furthermore, we define the idiosyncratic firm-level shocks as the result of a cyber attack lasting for a duration of Λ days as follows where $\boldsymbol{\omega_i} = [\omega_{1i} \ldots \omega_{mi}] \in \mathbb{R}^m$ is the vector of firm output shares and $\phi = [\phi_1 \ldots \phi_m] \in \mathbb{R}^m$ is the vector of idiosyncratic firm-level shocks. Furthermore, we define the idiosyncratic firm-level shocks as the result of a cyber attack lasting for a duration of Λ days as follows:

$$\phi_f = \left(\frac{y_f}{365}\right) M_f \Lambda, \tag{3}$$

where M_f is a sector resilience multiplier attached to each firm f. Furthermore, we make the simplifying assumption that output is evenly disbursed across each day of the calendar year, thereby dividing annual revenue by 365 (in reality, output may exhibit varying levels of aseasonality). Thus, in this setting we define idiosyncratic shocks ϕ as the result of independent cyber attacks on individual firms f with heterogenous levels of resilience, M_f, lasting for a duration of Λ. As a result, the resilience multiplier plays a central role in determining the impact of a shock. When $M_f = 0$ firm f is perfectly resilient and is unaffected by the shock. As M_f increases resilience decreases and more of the shock is absorbed. Thus, when $M_f = 1$ firm f receives the entirety of the shock. Notably, Rose et al. (2007) estimates the sector resilience multiplier M_f in a model calibrated to the effects of a power outage. The application of power outages bares considerable similarities to the resilience of a cyber attack and therefore provides a good initial estimate for quantifying the impact of potential cyber incidents.

Given that firm-level data on production networks, the actual flows of goods and services between firms, do not exist, the assumption that each firm is representative of the given sector it occupies allows us to use standard I/O analysis and exploit the I/O network available from the Bureau of Economic Analysis.[7] Implicitly, we are assuming that the

[7]https://www.bea.gov/industry/input-output-accounts-data

firm is large relative to other firms in the sector since the supply chain for a small firm may only include a few sectors. I/O models assume that production takes place with a recipe and does not allow substitution across inputs when inputs are not available, or prices change. We therefore impose the following assumption:

Assumption 2. The duration of each attack is sufficiently short

> We assume that the duration Λ of each cyber attack driven is sufficiently short as to not allow for recontracting of business relationships keeping network ties static.

In the case of a short-term disruption, the perfect complements assumption embedded within an I/O model may be appropriate to consider short term disruptions rather than allowing prices to adjust to clear markets, as in a general equilibrium model.

3.2. Upstream Impacts

We first exploit the I/O model through the use traditional I/O modeling to estimate the backward linkages or upstream supply chain linkages in the economy of $\mathcal{E}$ through the implied multipliers. That is, we define $\boldsymbol{W} = w_{ij_{i,j}} \in \mathbb{R}^{n\times n}$ as the sector-level weighted adjacency matrix where w_{ij} are the flows from sector i–j. Note $i, j \in S$ where n is the number of sectors and m is the number of firms. Furthermore, we define $\boldsymbol{x} = [x_1 \dots x_n] \in \mathbb{R}^n$ as the sector-level output vector and $\boldsymbol{d} = [d_1 \dots d_n] \in \mathbb{R}^n$ as the sector-level demand vector. Recall that sector-level output x_i is the sum of firm-level output, y_f for all firms f within each sector s. Sector-level output can thus be determined as the sum of flows and demand as follows:

$$\boldsymbol{x} = \boldsymbol{W}\boldsymbol{x} + \boldsymbol{d} \tag{4}$$

Manipulation via matrix operations yield the following canonical relationship from I/O models:

$$\boldsymbol{x} = (\boldsymbol{I} - \mathbf{W})^{-1}\boldsymbol{d} = \boldsymbol{L}^{-1}\boldsymbol{d} \tag{5}$$

where $\boldsymbol{I}$ is the identity matrix and $\boldsymbol{L} = (\boldsymbol{I} - \mathbf{W})^{-1}$ is defined as the inverse Leontief matrix. The inverse Leontief matrix defines the indirect effects associated with an exogenous output change in one sector and how it affects other sectors through upstream interactions. That is, if we reduce output in sector j by $\bar{x}_j$, then indirect effects are given by $L^{-1}[0, \dots 0, \bar{x}_j, 0, .., 0]'$.

This standard approach allows for the estimation of shocks originating at the sector level and the aggregate costs of their propagation across sectors of the economy. In this context, $\epsilon = [\epsilon_1 \dots \epsilon_n] \in \mathbb{R}^n$ is the vector of sector-level shocks as determined by idiosyncratic firm-level shocks ϕ in (2). The aggregate upstream impact of sector shocks is thereby determined as follows:

$$\Delta\boldsymbol{x} = \boldsymbol{L}^{-1}\epsilon \tag{6}$$

Fig. 3 provides a visual representation of the multiplier process.

3.3. Downstream Impacts

Not only do firms purchase goods and services from other firms for production through the upstream supply chain, but they are also providers of goods and services to other firms. Thus, not only does a shock affect the upstream firms but also the downstream or forward linkages within the supply chain. Our approach is similar to that of Ghosh (1958).[8]

To estimate the downstream impacts of an outage, we first identify the sector in the economy that is affected by identifying the North American Industry Classification System (NAICS) code associated with the firm that is attacked and has a business interruption. We estimate the direct revenue loss of the firm by calculating the proportion of annual output lost due to the disruption. At present, we assume that the outage duration is directly correlated to the revenue loss as in Equation (3). The firm may engage in mitigating activities to reduce this loss, but ultimately the losses are a function of the duration of the outage. This outage has network effects determined by the supply chain. As discussed earlier, we would ideally like to identify the firms that are customers of the firm that experiences an outage due to a cyber attack, but such a network has not been developed. As such, we use the NAICS code to identify the sector that has a reduction of output and the corresponding sectors that use that output as an input.

In the nomenclature of I/O modeling, we identify the row (inputs) outputs corresponding to the sector that experienced the shock ϵ_i. The Leontief production function assumptions holds that all inputs are perfect complements. Consequently, the shock of ϵ_i leads to proportional reduction in sector i's outputs

[8]There have been others that implement a similar approach to study downstream impacts such as Santos and Haimes (2004) and Richardson (1985).

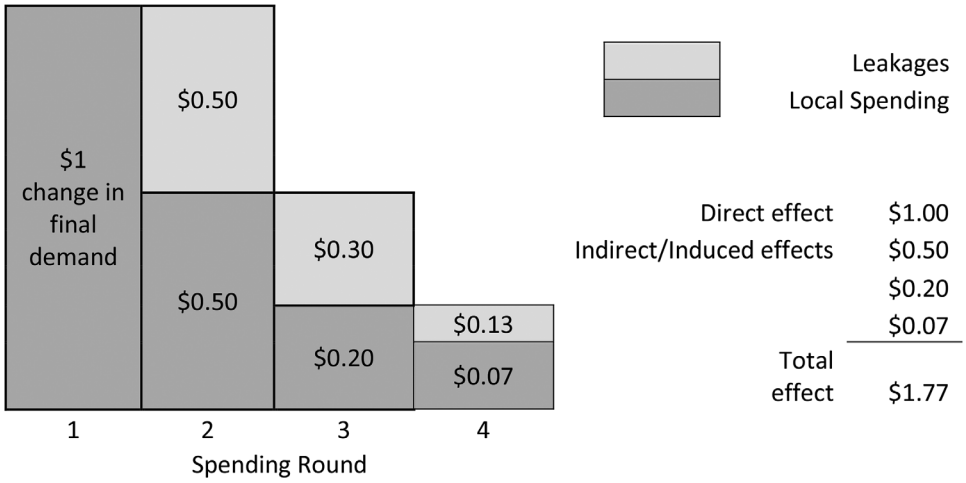

Fig 3. Illustration of Backwards Linkages in an Economy
Source: Schnaubelt, Christopher, Craig A. Bond, Frank Camm, Joshua Klimas, Beth E. Lachman, Laurie L. McDonald, Judith D. Mele, Paul Ng, Meagan Smith, Cole Sutera and Christopher Skeels. The Army's Local Economic Effects. Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/pubs/research_reports/RR1119.html.

to production going to all other sectors j, X_{ji}, who use that output as an input That is, we allocate the lost output to each of the sectors based on the ratio of the sector input to the total economy input of that sector. Thus, the change in production, ΔX_{ji}, is equal to the product of the shock, ϵ_i, and the percentage of sector i's inputs to production from sector j as follows:

$$\Delta X_{ji} = \epsilon_i \frac{X_{ij} X_{ji}}{\sum_s X_{is} X_{si}}, \tag{7}$$

where ϵ_i is the result of an idiosyncratic shock to firm f in sector i leads of ϕ_i results in a shock of $\epsilon_i = \phi' \ \boldsymbol{\omega}_i$ where $\phi_g = 0$ for all other firms g in sector i. Equation (7) implies that the shock ϵ_i equally propagates to all upstream suppliers. Furthermore, this change in flows ΔX_{ijji} drives a reduction in the output of sector j, Y_j. Given the percentage reduction in total inputs, $\Delta X_{ji}/X_{ijji}$, following shock ϵ_i and the assumption of perfect complements, the resulting change in output ΔY_j is:

$$\Delta Y_i = Y_i \left(\frac{\Delta X_{ij} X_{ji}}{X_{ji}} \right) = Y_j \frac{\epsilon_i}{\sum_s X_{si}} \, . \tag{8}$$

Consequently, each sector experiences a cascading shock equal to the relative importance of firm f to the overall economy in terms of inputs from a particular sector. Given the cost to sector j from an attack on a firm f and Equations (2) and (3), the total upstream economic cost of the shock ϵ_i resulting from a cyber attack on firm f is then expressed as:

$$\begin{aligned} \sum_{j'} \left(Y_j \frac{\epsilon_i}{\sum_s X_{si}} \right) &= \sum_{j'} \left(Y_j \frac{y_f M_f \Lambda \omega_{fi}}{365 \left(\sum_s X_{si} \right)} \right) \sum_{j'} \left(Y_j \frac{\epsilon_i}{\sum_s X_{issi}} \right) \\ &= \sum_{j'} \left(Y_j \frac{y_f M_f \Lambda \omega_{fi}}{365 \left(\sum_s X_{issi} \right)} \right). \end{aligned} \tag{9}$$

Thus, a firm may have a large impact on the overall economy if it is large within its sector or the sector plays an important role in the overall economy. In the next section, we use the quantitative model of this section to estimate the potential impact of cyber attacks causing temporary outages at several large firms.

4. CYBER INCIDENT ANALYSIS

4.1. Analysis of Potential Incidents

To understand the potential costs of cyber incidents, we analyze the potential impact of a cyber attack on large and likely targets. For this, we chose a large telecommunications firm, a hardware firm, a retail banking firm, and a point-of-sale firm for their diversity, size, and potential exposure to cyber risks. They include AT&T, Cisco Systems, JP Morgan Chase,[9] and Visa. Additionally, we include Ford,

[9]JP Morgan Chase is a complex firm with several separate business activities. Here, we consider its business as retail banking rather than its investment services. Disruptions to any of its

Table I. Input Data for Analysis

	Visa	Cisco Systems	JP Morgan Chase	AT&T	Ford Motors
2017 Revenue (millions), y_f	$ 18,358	$ 48,005	$ 93,689	$ 160,546	$ 156,800
NAICS Sector, i	44–45 Retail trade	51 Information	52 Finance & insurance	51 Information	31–33 Manufacturing
Duration (days), Λ	1	1	1	1	1
Resilience multiplier, M_f	0.661	0.700	0.217	0.700	0.712

Table I displays all input values – revenue, sector, duration, and resilience – used to analyze the potential impact of a one-day cyber attack on Visa, Cisco, JP Morgan Chase, AT&T, and Ford. We use the North American Industry Classification System (NAICS) for sectors. For the sector specific resilience multiplier, we use the calibration results of Rose et al. (2007). That is, while Rose et al. (2007) estimates resilience multipliers at the sector level, not the firm level, firms are assumed to have the same resilience multipliers as their sectors. As a result, while the analysis considers an attack which disrupts the entire business operations of each firm for one day, each firm has some level of resilience preventing complete outages. Data on firm revenue is taken from S&P Capital IQ NetAdvantage. The authors chose firm sectors to most closely alight to the immediate impact of their respective shocks.

the global automotive manufacturer, as a comparison to AT&T, due to their similar sizes but different sectors. This list of firms is, therefore, intended to provide a range of examples, but not an exhaustive sample of all firms and all sectors. To analyze the impact of atypically large yet still fathomable incidents, we assume a stoppage of all operations and services (subject to resilience) of each company lasting one day. Furthermore, using the firm specific data on revenue, sector, attack duration, and resilience shown in Table I, our analysis estimates the *potential* losses associated with each incident rather than the statistical expectation of losses where actual losses could be smaller (in fact, due to cyber risk management strategies of individual firms and the resilience across supply chains, actual losses are *likely* to be smaller than the potential losses estimated here).

Each of the five companies is large and interconnected by selection. Visa, a large payments services company, had a 2017 annual revenue of $18 billion; Cisco, a producer of information technology goods and services, had $48 billion in revenue; JP Morgan Chase, a financial services company, had $94 billion in revenue; AT&T, a telecommunications company had $160 billion in revenue, and Ford, an automotive manufacturer with $157 billion in revenue. The direct impact of the cyber attack of 1 day, ϕ_f as determined by Equation (3), is largely proportional to revenue. The results, shown in Fig. 4 in solid orange, estimate potential direct impact could reach nearly $33 million for Visa, $92 million for Cisco, $56 million for JP Morgan, and more than $300 million for AT&T and Ford. While these losses would likely be manageable by themselves through risk management and insurance, systemic cyber failure may change the picture.

Each cyber attack scenario could have impacts that propagate across the economy. Consequently, the upstream impact of each incident, as shown in Fig. 4 in dashed blue, could exceed the direct costs incurred by each firm. For Visa, the direct cost of $33 million incurred by the one-day outage could lead to a further $77 million in upstream losses. The results of attacks on the other firms are similar: Upstream losses to Cisco, JP Morgan Chase, AT&T, and Ford could reach $209, $145, $700, and $706 million respectively. While this result is indeed large, it is largely in line with the estimates produced by previous work on cyber incidents and systemic losses.

However, the potential downstream impacts completely alter the picture, stretching far above direct and upstream costs, as shown in Fig. 4. Downstream losses reflect the fact that the effects of a cyber attack propagate down from each firm to their customers, with important implications. AT&T, the largest firm in our scenarios, has the largest downstream impacts, potentially $20 billion in damages in addition to the direct and upstream impacts. Notably, while Visa is the smallest firm in our scenario, it has the potential for the second largest total impact from cascading failures downstream, reaching $13 billion. Furthermore, in stark contrast to AT&T, a firm of similar size, Ford's potential downstream costs are much lower at $6.4 billion. Cisco and JP Morgan Chase have the potential for downstream impacts of nearly $6 billion and $4 billion, respectively. It is worth noting that, in some cases, our analysis could even underestimate total impacts. In the case of JP Morgan Chase, an outage impacting banking services could drive contagion effects which, while not

activities could lead to many systemic impacts, notably bank runs. Given the large literature on those impacts (e.g., Diamond & Dybvig, 1983) we do not consider those effects here.

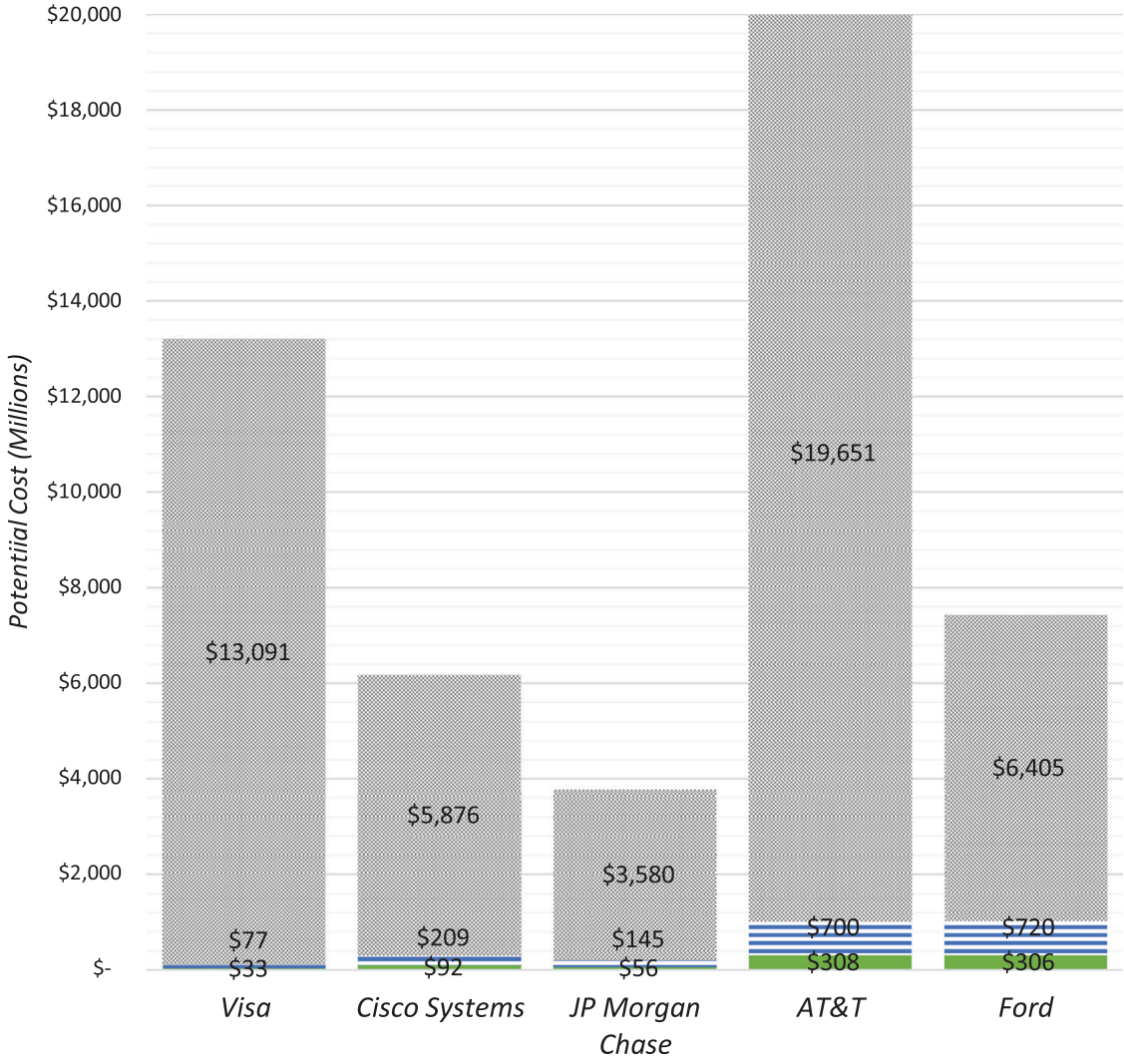

Fig 4. Potential impact of 1-day cyber attack.
Figure 4 displays the potential impact of a one-day cyber attack on Visa, Cisco, JP Morgan Chase, AT&T, and Ford. The direct, upstream, and downstream costs are shown for each scenario as a stacked chart. On bottom, the direct cost to the firm is shaded as a solid orange region. In the middle, the total upstream costs to suppliers is shaded in horizontal blue lines. On top, the total downstream costs are shaded with gray dots.

addressed in this article, have been recently studied by Eisenbach et al. (2020).

The exercise of estimating losses following a one-day cyber attack on each of the four firms reveals the staggering potential impacts of systemic cyber risk. The potential losses incurred by each firm directly are large but manageable. However, for heavily interconnected firms such as Visa, Cisco, JP Morgan Chase, and AT&T, cascading failures could result in sizeable damages incurred by other firms, organizations, and individuals. In the case of AT&T, our approach estimates that the impact of the one-day attack could reach nearly $20 billion, a value that itself represents 0.1% of 2017 U.S. gross domestic product. Yet the differences between direct and systemic losses vary significant based on the type of firm, its sector, and how interconnected it is. Ford, a firm that produces final goods rather than intermediate goods, is less interconnected, leading to fewer downstream impacts in proportion to its cost. As a result, the total potential cost of the attack on Ford of $7.4 billion is roughly a third that of the potential cost of an attack on AT&T, a firm of similar size. Furthermore, while we note that resilience in business

Table II. Input Data for Maersk Case

	Maersk
2017 Revenue (millions), y_i	$ 30,945
NAICS Sector, s	48-49 Transportation & Warehousing
Duration (days), Λ	10-60
Resilience measure, M_i	0.052

This table displays all input values—revenue, sector, duration, and resilience—used to analyze the potential impact of a cyber attack ranging from 10–60 days on Maersk where the North American Industry Classification System (NAICS) is used for sectors, and the sector specific resilience multiplier comes from the calibration results of Rose et al. (2007).

operations is likely to lessen the potential impacts of cyber attack driven outages (see, for example, Barker, Ramirez-Marquez, & Sansavini, 2019), the analysis in this section reveals the significance of systemic risk resulting from cyber attacks' cascading failures.

4.2. Maersk Case

We now look to the 2017 NotPetya cyber attack that disrupted Maersk's operations as a case for comparing our model with a real incident. It took Maersk 10 days from the beginning of the attack to fully rebuild their information systems and an estimated two months to fully recover (Greenberg, 2018). In total, Maersk estimated that it incurred between $250 and $300 million in lost revenue due to the incident (Maersk, 2018). In this section, we consider the characteristics of this case and its known and unknown features, in the context of the quantitative model Section 3.

As we did in Section 4.1, we use the quantitative model derived in Section 3 to analyze the case of the Maersk outage and estimate the potential impacts. While several key input parameters are known, the true resilience of Maersk to a cyber attack driven outage is not. Therefore, we estimate the range of potential impacts using the parameters in Table II which we vary the level of resilience between the value of transportation sector resilience calibrated by Rose et al. (2007), $M_i = 0.052$, for power outages and the value of no resilience, $M_i = 1$. The resulting potential range of damage inflicted on Maersk and its network from the NotPetya attack is significant.

The left panel in Fig. 5 displays the range of direct (solid red) and upstream (dashed red) impacts. Our estimation of the direct impact varies from $44 million with the resilience value from Rose et al. (2007) to $848 million with no resilience. The upstream values stretch over a wider range; the minimum and maximum upstream impact $115 million and $2.2 billion. The range of potential impacts conveys the central importance of resilience on varying impacts.

The solid-red box in the left of Fig. 5 displays a relatively narrow range of estimation of potential direct impacts. The actual lost revenue (direct cost) from the Maersk case of $250–$300 million (values disclosed in the annual financial reports of Maersk, 2018) falls on the lower end of this window suggesting that value of sector level resilience from Rose et al. (2007) is overly optimistic for this specific case, Maersk did benefit from some level of resilience. Indeed, the values of resilience that would correspond to actual losses reported by Maersk (2018) between $250 and $300 million would be between $M_i = [0.3, 0.35]$ instead of $M_i = 0.052$, a meaningful difference. While the resilience from Rose et al. (2007) are calibrated to a sector, firm heterogeneity within sector can plausibly result in significant variation. Without efforts to estimate individual firm resilience, this is likely to result in further uncertainty.

The right panel Fig. 5 displays the range of downstream (solid blue) and total (dashed blue) impacts. Both potential impacts of the NotPetya incident vary significantly. At the extremes, downstream costs vary from $2.8 billion minimum to $54 billion while total costs vary from $3 billion minimum to $57 billion. While the high-end of estimates is notably high due to improbable values of resilience (or lack of resilience), the values on the low end convey that the potential impact of the Maersk case was nonetheless significant in its total costs.

Furthermore, provided that the corresponding value of resilience for actual losses ranges from $M_i = [0.3, 0.35]$, we can estimate total losses for the actual Maersk case. The results in Table III show the range of potential impacts within the range of resilience values corresponding to the actual losses estimated between $250 and $300 million (Maersk, 2018). As shown in the table, upstream losses vary from $663 to $773 million while downstream losses vary from $16 to $19 billion. Given the centrality of Maersk and the large downstream impacts, the results estimate that the total potential losses from the incident, which

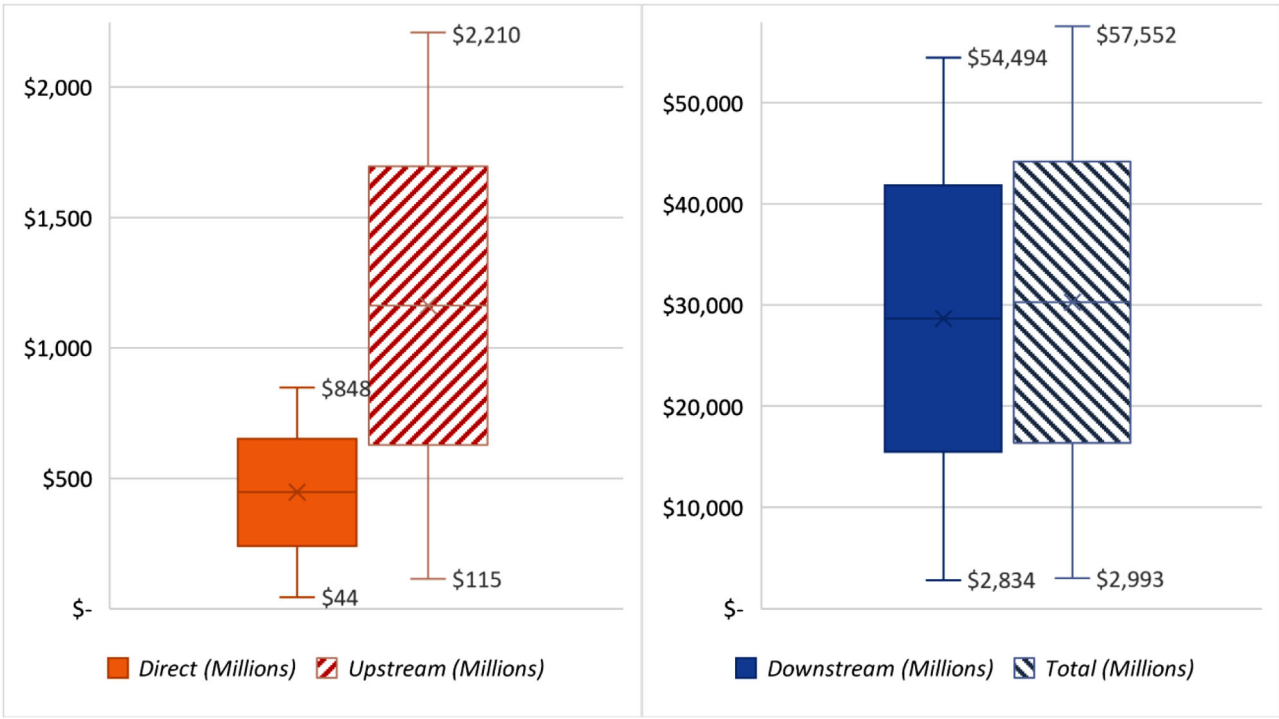

Fig 5. Range of potential NotPetya impacts on Maersk and its supply chain
This figure displays an estimated range of potential impacts in millions of dollars of the NotPetya cyber attack on Maersk and dependent upstream and downstream firms varying by the value of firm resilience.

Table III. Estimated Total Impact of 2017 NotPetya Cyber Attack on Maersk and Dependent Firms

	Direct	Upstream	Downstream	Total
$M_i = 0.3$	$254.34	$663	$16,348	$17,265
$M_i = 0.35$	$296.73	$773	$19,073	$20,143

Table III displays the range of estimated direct, upstream, downstream, and total costs of the NotPetya attack on Maersk tailored to the resilience values corresponding to direct losses. All values are displayed in millions of 2017 dollars.

drove $300 million in direct revenue losses, could total $20 billion.

While it is hard to consider this case an exhaustive validation and verification of the quantitative model of Section 3 given the uncertainties surrounding duration and resilience, this case does demonstrate the capability of this approach to estimate potential cyber attack impacts. Beyond a first approximation, the analysis of the Maersk case is consistent with Maersk's reports while providing insight. However, the analysis also goes beyond the already quantified impacts of the NotPetya incident by estimating the potential total costs incurred from cascading failures.

5. IMPLICATIONS FOR CYBER INSURANCE AND CYBER POLICY

One of the motivations of our estimations of the potential costs associated with systemic cyber failures is to answer the question of whether cyber insurance is a sufficient tool for managing cyber risks, or whether systemic cyber risk warrants new conversations on cyber policy are needed. In this section, we turn to discussion the implication of the economic consequences discussed in Sections 3 and 4 for cyber insurance and policy.

In creating cyber insurance policies, many insurance carriers manage their portfolio risk through security questions and diversification across portfolios.

To understand the security questions, Romanosky, Ablon, Kuehn, and Jones (2019) examined a collection of cyber insurance questionnaires used by carriers to assess risk as well the actual rate schedules used to price premiums. They found a wide range of security information collected by different policies, as well as variation in how that information is incorporated into insurance pricing. For example, while some policies may include a few security control parameters in the pricing equation, others include a dozen or more (and some rate schedules include no security information at all). Even more problematic for these carriers is identifying the characteristics of firms that could result in systemic (closely related to the concepts of aggregated, accumulated, and correlated risk within the insurance practice) failure, undermining diversification's implicit assumption of independence, and possibly leading to catastrophic loss.

A small number of firms seek to develop better data modeling techniques in order to understand and predict aggregation (and specifically catastrophic) risk. For example, the Cambridge Centre for Risk Studies and Risk Management Solutions (RMS) developed the Cyber Accumulation Management System (CAMS) and the Cyber Insurance Exposure Data Schema, which attempted to standardize the information collected for cyber incidents (Cambridge Centre for Risk Studies). The hope is that only through a common language will insured companies, carriers, and reinsurers be able to properly record key metrics, and differentiate across incidents. Not to be outdone, AIR, another risk modeling firm, developed the VERISK cyber exposure data standard in 2016, which provides a competing framework. AIR also developed the analytics of risk from cyber (ARC) platform, which attempts to develop and flesh out aggregated losses stemming from a collection of cyber incidents. AIR claims to have modeled 18 unique (proprietary) scenarios, such as data theft (credit cards, personal health information, etc.), business interruption,[10] attacks on critical infrastructure (power, water), and vulnerabilities found in a commonly used software or hardware device.

While typical cyber attacks (e.g., those studied by Aldasoro et al., 2020; Romanosky, 2016) may fit within the realm of insurable losses, insurance companies may be more exposed to systemic losses than it appears. Take, for example, our analysis of the one-day cyber attack on Cisco. Assuming an insurance policy covers the incident, the initial hit to an insurance portfolio could reach $92 million from our estimation of potential impacts in Section 4.1. In all likelihood, the direct loses would be spread across numerous insurance companies rather than one single portfolio, reducing the exposure of each insurer. However, cascading failures up and downstream from Cisco may result in hidden portfolio risk for insurers where other contracts (most notably, contingent business interruption insurance) are triggered by the initial cyber event. The resulting portfolio risk of simultaneous policy losses following what initially appeared to be a single cyber incident affecting a single policy could be nontrivial.

However, when we look to the aggregate costs of cyber incidents including downstream losses, a need for broader policy discussion emerges. In the analysis of the 1-day outage AT&T, our estimation of the total potential impact to the economy in Section 4.1 reached nearly $20 billion. The 2015 Russian cyber attack on the Ukrainian power grid is a reminder that the potential impacts could exceed the scenarios considered in this article. The result, where systemic cyber risks have the potential to exceed private sector solutions, reveals a need for additional policy consideration. This is particularly concerning given the tendency toward underinsurance for correlated risks (Öğüt, Raghunathan, & Menon, 2011). Additionally, while we discuss the need for future research on the resilience of individual firms to cyber incidents our exploration into the role of resilience in Section 4.2 reveals the that enhancing resilience may be one of the largest factors for combating systemic cyber risk. As the policy discussion surrounding systemic risk in cyberspace grows, efforts to enhance cyber resilience should be considered.

6. CONCLUSIONS

This article presents a theoretical framework for characterizing systemic cyber risk based in risk analysis and computational economics. In this framework, systemic risk results from cascading and common cause failures in addition to a multitude of independent isolated cyber incidents. The article takes an initial step toward estimating systemic cyber risk. In doing so, we employ the use of I/O modeling for estimating the aggregate impact of firm-level shocks and estimating both upstream and downstream impacts. The results show that the potential direct

[10]Related is contingent business interruption (CBI), which is an industry term for loss of business to a firm caused by an outage of an upstream/supply chain vendor.

costs associated with cyber incidents are greatly outweighed by the multiplier effects of up- and downstream connections. While this concern could be true for any firm-level shock, it is particularly relevant given the heavy interconnections of cyberspace.

In fact, while we estimate cascading cyber failures in this article, it is only part of the growing problem of cyber risk. While this article does not quantify common-cause failures, it is clear that cyberspace contributes significant interdependencies from shared software, hardware, vendors, and digital networks. In the case of WannaCry and NotPetya, this interdependency allows incidents to quickly spread leading to high global costs. The added components of the obscurity of cyberspace with its hidden network connections and the changing nature of the threat, contribute to a challenge of both high risk and high uncertainty.

Consequently, we believe new policy approaches are needed for managing and mitigating cyber risk and its systemic impacts. Given our analysis and estimation of potential cyber incident costs, a reliance on private sector solutions including cyber risk management and insurance may be insufficient for the growing magnitude of risks. Notably, lessons on the policy of systemic risk could be borrowed from the rise of policy changes following the 2008 financial crisis. Borrowing from financial regulation, OFR (2017) suggests the use of cyber stress tests and Federal Financial Institutions Examination Council (2017) includes the use of stress tests in its cyber maturity model. The analogy has merit; just as firms were considered too big or too interconnected to fail in the financial sector following the start of the financial crisis, it is clear that cyber attacks on heavily interconnected firms could result in intolerable losses. Actually implementing stress tests, though, would require future advancements that build on this article with more insight on interfirm networks and the resilience of individual firms. However, the challenge of interconnections might leave a glimmer of promise; Sommer and Brown (2011) argue that the interdependencies that drive cascading cyber failures might also serve as mitigating solutions. Sommer and Brown (2011) argue the cyber infrastructure, which may propagate the effects of a cyber attack may also provide an alternative pathway for delivering information and services following an attack. The idea points to potential solutions for mitigating systemic risk that could arise from increasing reliance on digital systems.

The contribution of a theoretical framework for discussing and modeling systemic risk in cyberspace is a step forward in bridging the disciplines of cyber security, risk analysis, and economics to further model the complex nature of systemic cyber risks and the aggregate impacts. Furthermore, this framework highlights opportunities for future analysis. Namely, measuring common-cause cyber risk is an open challenge that may require innovative uses of data on information systems. Considerations of policy tools that may mitigate large scale incidents is a key area for future development. Additionally, while the focus of this article has been on cyber incidents, this article contributes a method for using I/O analysis to estimate the aggregate losses from firm-level incidents that could find valuable application across a variety of risk analysis applications.

ACKNOWLEDGMENTS

The authors would like to thank the RAND Institute of Civil Justice, the members of its board, and Director James Anderson for their support of this work and for their useful comments. We also would like to thank Sasha Romanosky for his insight on cyber insurance, Nirabh Koirala for his research assistance, Sydney Newberry for her comments and edits, as well as John Davis, Geoffrey McGovern, and Zev Winkelman for their useful feedback during various stages of this work. We also thank the participants of the 2020 Financial Stability State of the Field Conference hosted by Columbia University and the Federal Reserve Bank of New York, the 2020 Volatility at Risk Conference hosted at New York University, and the 2019 Conference on Risk Analysis, Decision Analysis and Security hosted at the University of Buffalo where this work was presented. Finally, we thank Craig Bond and Joost Santos for their thorough reviews of an early version of this article in addition to the two anonymous reviewers of this journal for their useful insight and comments which elevated the quality of this publication.

REFERENCES

Acemoglu, D., Carvalho, V. M., Ozdaglar, A., & Tahbaz-Salehi, A. (2012). The network origins of aggregate fluctuations. *Econometrica*, *80*(5), 1977–2016.

Acemoglu, D., Malekian, A., & Ozdaglar, A. (2016). Network security and contagion. *Journal of Economic Theory*, *166*, 536–585. https://doi.org/10.1016/j.jet.2016.09.009

Acemoglu, D., Ozdaglar, A., & Tahbaz-Salehi, A. (2015). Systemic risk and stability in financial networks. *The American Economic Review*, *105*(2), 564–608.

AIR, & Lloyd's. (2018). Cloud down: Impacts on the US economy. *Technology*. Retrieved from https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2018/cloud-down/aircyberlloydspublic2018final.pdf

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). The drivers of cyber risk. BIS Working Papers, No 865.

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice*. Rockland, MA: Syngress.

Andrijcic, E., & Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk Analysis*, *26*(4), 907–923. https://doi.org/10.1111/j.1539-6924.2006.00787.x

Barker, K., Ramirez-Marquez, J. E., & Sansavini, G. (2019). Introduction to resilience analytics for cyber–physical–social networks. *Risk Analysis*, *39*(9), 1867–1869. https://doi.org/10.1111/risa.13392

Bodeau, D. J., & McCollum, C. D. (2018). *System-of-systems threat model*. McLean. VA: Homeland Security Systems Engineering and Development Institute (HSSEDI). https://www.mitre.org/sites/default/files/publications/pr_18-1631-ngci-system-of-systems-threat-model.pdf.

Brenner, J., Weitzner, D., Clark, D. C., Ableson, H., Hung, S., Reynolds, T., … Samuels, R. J. (2017). *Keeping America safe: Toward more secure networks for critical sectors*. Cambridge, MA: MIT Center for International Studies.

Cambridge Centre for Risk Studies. Cyber exposure data schema v0.9 *Cambridge Risk Framework*. Retrieved from https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-data-schema-v0.9.pdf

Carrera, L., Standardi, G., Bosello, F., & Mysiak, J. (2015). Assessing direct and indirect economic impacts of a flood event through the integration of spatial and computable general equilibrium modelling. *63*, 109–122. https://doi.org/10.1016/j.envsoft.2014.09.016

Carvalho, V. M., & Tahbaz-Salehi, A. (2019). Production networks: A primer. *Annual Review of Economics*, *11*(1), 635–663. https://doi.org/10.1146/annurev-economics-080218-030212

Collins, K. (2017, May 21). Inside the digital heist that terrorized the world—and only made $100 k. Quartz.

De Bandt, O., & Hartmann, P. (2000). Systemic risk: A survey. Working paper No. 35. European Central Bank.

Diamond, D. W., & Dybvig, P. H. (1983). Bank runs, deposit insurance, and liquidity. *Journal of Political Economy*, *91*(3), 401–419. https://doi.org/10.2307/1837095

Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., … Iyengar, S. S. (2017). Game theory for cyber security and privacy. *ACM Computing Surveys (CSUR)*, *50*(2), 30.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., & Winkelman, Z. (2018). Estimating the global cost of cyber risk: Methodology and examples. Santa Monica, CA: RAND Corporation.

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2020). Cyber risk and the us financial system: A pre-mortem analysis. FRB of New York Staff Report(909).

Federal Financial Institutions Examination Council. (2017). *Cybersecurity assessment tool*. Retrieved from https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

Gandel, S. (2015). Lloyd's CEO: Cyber attacks cost companies $400 billion every year. Retrieved from http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

Ghosh, A. (1958). Input-Output Approach in an Allocation System. *Economica*, *25*(97), 58. https://doi.org/10.2307/2550694

Greenberg, A. (2018). The untold story of Notpetya, The most devastating cyberattack in history. Wired. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hausken, K. (2009). Security investment and information sharing for defenders and attackers of information assets and networks. *Information Assurance, Security and Privacy Services*, *4*, 503–534.

ICS-CERT. (2016). Cyber-Attack Against Ukrainian Critical Infrastructure. *NCCIC DHS, Alert (IR-ALERT-H-16-056-01)*.

Kovenock, D., & Roberson, B. (2018). The optimal defense of networks of targets. *Economic Inquiry*, *56*(4), 2195–2211. https://doi.org/10.1111/ecin.12565

Leontief, W. (1966). *Input-output economics*. Oxford, UK: Oxford University Press.

Lynn, III, W. F. (2010). Defending a new domain-the Pentagon's cyberstrategy. *Foreign Affairs*, *89*, 97.

Maersk. (2018). 2017 Annual report. *A.P. Møller - Mærsk A/S*. Retrieved from http://investor.maersk.com/news-releases/news-release-details/annual-report-2017

Meyer, R., & Lafrance, A. (2016). When the Entire Internet Seems to Break at Once: The easiest way to take down the web is to attack people's access to it. Retrieved from https://www.theatlantic.com/technology/archive/2016/10/when-the-entire-internet-seems-to-break-at-once/504956/

Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588–600.

Office of the Director of National Intelligence. (2017). Assessing Russian activities and intentions in recent us Elections. Intelligence Community Assessment: U.S. Office of the Director of National Intelligence Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

OFR. (2017). Cybersecurity and financial stability: Risks and resilience. Office of Financial Research, Viewpoint, 17–01.

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis*, *31*(3), 497–512. https://doi.org/10.1111/j.1539-6924.2010.01478.x

Pagliery, J. (2015, August 5). The inside story of the biggest hack in history. *CNN*.

Richardson, H. W. (1985). Input-output and economic base multipliers: Looking backward and forward. *Journal of Regional science*, *25*(4), 607–661.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz002

Rose, A., Oladosu, G., & Liao, S.-Y. (2007). Business interruption impacts of a terrorist attack on the electric power system of Los Angeles: Customer resilience to a total blackout. *27*(3), 513–531. https://doi.org/10.1111/j.1539-6924.2007.00912.x

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Wu, Q. (2010). A survey of game theory as applied to network security. Paper presented at the 2010 43rd Hawaii International Conference on System Sciences, January 5—8, Koloa, Kauai, Hawaii.

Santos, J. R., & Haimes, Y. Y. (2004). Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures*. *Risk Analysis*, *24*(6), 1437–1451. https://doi.org/10.1111/j.0272-4332.2004.00540.x

Santos, J. R., Haimes, Y. Y., & Lian, C. (2007). A framework for linking cybersecurity metrics to the modeling of macroeconomic interdependencies. *Risk Analysis*, *27*(5), 1283–1297. https://doi.org/10.1111/j.1539-6924.2007.00957.x

SEC. (2018). Equifax's statement for the record regarding the extent of the cybersecurity incident announced on September 7, 2017. SEC. Exhibit 99.91.

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European*

Journal of Operational Research, *282*(1), 161–171. https://doi.org/10.1016/j.ejor.2019.09.017
Sommer, P., & Brown, I. (2011). Reducing systemic cybersecurity risk. Organisation for Economic Cooperation and Development, Working Paper No. IFP/WKP/FGS(2011).
SwissRe. (2017). Cyber: Getting to grips with a complex risk. *Sigma*. Retrieved from http://www.aiadc.org/File%20Library/Home/Swiss-Re-Sigma-Paper-030717.pdf
Thomson, I. (2017). NotPetya ransomware attack cost us $300 m–shipping giant Maersk. Forbes.
US-CERT. (2018). Russian government cyber activity targeting energy and other critical infrastructure sectors. *NCCIC DHS, Alert (TA18-074A)*.
van Wieren, M., van Luit, E., Estourgie, R., Jacobs, V., & Bulters, J. (2016). Cyber value at risk in the Netherlands. London, UK: Deloitte.
Vermeer, M. J. D., & Peet, E. D. (2020). *Securing communications in the quantum computing age: Managing the risks to encryption*. Santa Monica, CA: RAND Corporation.
World Economic Forum. (2016). Understanding systemic cyber risk. *Global Agenda Council on Risk & Resilience, White Paper*.
World Economic Forum, & Deloitte. (2015). Partnering for cyber resilience: Towards the quantification of cyber threats. *World Economic Forum, Industry Agenda*.