Cybersecurity and its cascading effect on societal systems

Constantine Toregas[1] and Joost Santos[1]

with Appendix by

Molly Jahn[2], William L. Oemichen[2], Gregory F. Treverton[3], Scott L David[2,4],

Matthew A. Rose[2,5], COL Max Brosig[2,5,6], William K. Hutchison[2], Braeden

Rimestad[2] and Taryn Otto[2]

[1] Cybersecurity and Privacy Research Institute, George Washington University

[2] Department of Agronomy and Nelson Institute for Environmental Studies, University of Wisconsin-Madison

[3]School of International Relations, University of Southern California

[4] Information Risk Research Initiative, Applied Physics Laboratory, University of Washington

[5]US Army War College

[6]Wisconsin National Guard

1. Introduction

The high risk emanating from the increasing number of cyber attacks on critical infrastructure systems at national or local level is only now beginning to be understood. The cascading effect of that risk beyond the system under attack into allied and interconnected fields can be even more devastating, creating chaos to major economic, food and health systems and lasting for long periods of time. Modern society has benefited from the additional efficiency achieved by improving the coordination across interdependent systems using information technology (IT) solutions. IT systems have significantly contributed to enhancing the speed of communication and reducing the geographic barriers across consumers and producers, leading to a more efficient and cost-effective exchange of products and services across an economy. Nonetheless, IT dependence has also exposed critical infrastructure and industry systems to a myriad of cyber security risks, ranging from accidental causes, technological glitches, to malevolent willful attacks.

In order for risk management decision makers to understand and properly prepare for such risks, models that can describe single system vulnerabilities for cyber attack are not helpful. What would be more useful are models that can describe the degree of risk expansion as the interrelated technological systems propagate the attack deep into the ecosystem of society. Such models can begin to provide risk indices helpful to governments, the insurance industry and the corporate world so that proper preparations for cyber attack commensurate with the risks can be organized and supported.

Currently, the majority of modeling efforts for cyber risk are scenario-based (Swiss Re 2017). Given the dearth of information regarding cyber attacks and the long time it will take to develop collaborative strategies for sharing data that may lead to better data-driven analytic models of risk, new ways of risk assessment must be found.

Work has been done in two allied fields by the authors: developing conceptual models exploring the impact of cyber attack on rate setting and other risk measurement mechanisms (Toregas 2015), and detailed mathematical models that explore the impact of cyber attacks on interconnected economic and infrastructure sectors (Santos 2006).

The current paper unites these two streams of exploration on the multi-dimensional level, highlighting additional hazards, risks and dynamic interactions that need to be considered for understanding the full impact of cyber attacks, following the adoption of the Sendai framework and the shift away from hazard to risk–based strategies for UN member states.

2. Need to address the topic

From OECD (2017), two dominant themes emerge: that private and public sectors must collaborate if an effective solution to cyber risk is to be found, and that the lack of data on cyber incidents is a significant impediment to the management of cyber risk, including the transfer of cyber exposure risks to insurance markets. Based on surveys of major re/insurance companies and governments, the report suggests harmonization strategies for data collection and increased awareness for the importance of cyber insurance, but offers little tangible advice to the insurance underwriters regarding actual rate setting mechanisms that would accurately assess the risk inherent in different corporate and personal settings.

In the Nippon Telegraph and Telephone Corporation (NTT) resiliency framework for executives (NTT 2018), the same theme of public private partnership is addressed, but from the viewpoint that safety in cyber space should be considered as a public good, but cognizant that more than 90% of IT assets are in non-public hands (either corporate or individual). Aligning the recommendations with the intent of the current paper, they cite (NTT 2018, p. 112) that “managers should not seek perfection in cybersecurity, but should approach it with risk-based initiatives.” From a process perspective, a systematic approach for prioritizing self-help measures, cooperating with others and collaborating with government initiatives are the foundation of the recommended strategy in this management-oriented book. While risk is recognized, it is handled by management strategy, allowing internal processes to develop data-driven tactics.

From the two recent reports, it can be seen that there is a gap that exists in the intersect of cybersecurity modeling and insurance rate setting. This paper attempts to fill this void by suggesting a first step towards

establishing risk ratios within economic activity sectors that may suggest rate-setting relativities that could be used and tested in the field. It is an important first step to begin differentiating risk categories based on factual evidence rather than current hypothetical models based on scenarios and individual analyst assessments based on assumptions lacking evidence.

3.0 Methods and Data

3.1 Positioning Our Work

The claim has been made (Toregas 2014, 2015, 2018) that the market for cyber insurance, currently in the single digit billions of US dollars is significantly undervalued and could reach trillions if proper techniques for quantifying risk and reflecting it on a rate setting methodology could be devised.

Insurance rates can be seen as a direct surrogate for risks presented by cyber security attacks. The traditional mechanism for rate setting is using historical data from losses, and developing empirical analytic techniques that reflect the historical data in an actuarial table for future estimates of re-occurrence. The problem with this approach is that historical loss data from cyber attacks is scarce, as those incurring losses are loath to share the information lest it reflect badly on their business or individual standing. In addition, actuarial techniques may not be able to capture the cascading nature of the cyber attack and its impact.

A new path to rate setting for cyber risk is suggested: an econometric analysis at high level (economic sectors) for which data are likely to be collected and ratified by states; from such analysis, the way that the IT sector (taken as a surrogate for cyber connectivity and impact among sectors) interrelates to other economic sectors provides rations of coupling that can themselves suggest relative risk to cyber attack. The lack of detail and precision of the approach is more than compensated by the readily available data in most countries; once calibrated with emerging actual loss data, this approach could be a practical way for the insurance industry to appreciate the

magnitude of the cascading risk, and organize appropriate insurance products to encompass the totality of the proposed risk.

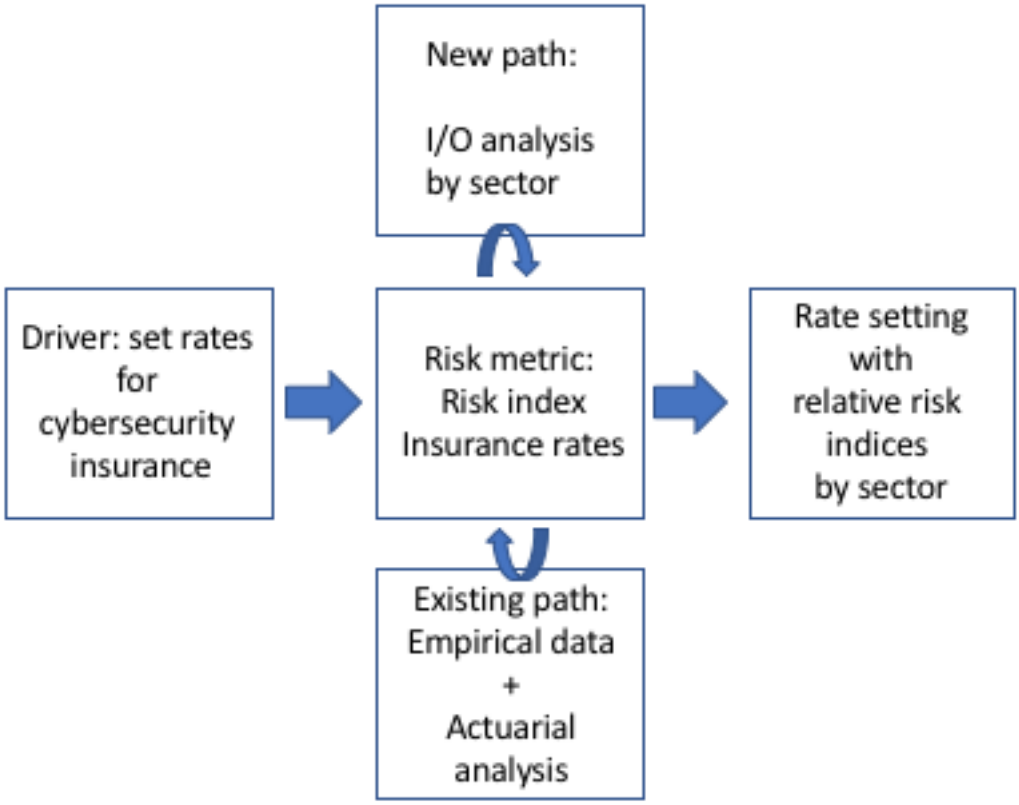

Figure 1. The context of our work

In assessing the strength of interconnectedness of economic and infrastructure sectors with information technology, we leverage the available input-output (IO) data, which are published by statistical agencies of many countries across the globe.

In this study, the proposed conceptual modeling framework is demonstrated using the IO datasets published by the US Bureau of Economic Analysis, and applied to estimate the magnitude of losses of IT disruptions on the US economy.

The approach will be to evaluate the degree of dependence of each sector on IT. When the IT resources are disrupted (such as in the case of Denial-of-Service attacks), there will be cascading impacts on the production of goods and provision of critical services. Recent publications by the authors have estimated the significant societal and financial losses triggered by IT disruptions on the economy.

3.2 The Economic Input-Output (IO) Model of Interdependent Systems

The economic input-output (IO) model represents an economy as a system of interdependent economic sectors, which provides a systematic accounting of the flow of consumed and produced goods throughout the system. Due to the vast applications of the IO model across the globe and its practicality for evaluating the impacts of supply and demand shifts on an economy, Wassily Leontief (1951, 1966) has been awarded the Nobel Prize in Economics in 1973. Miller and Blair (2009) provide the theoretical foundations of the IO model, and they also give examples on how the model has been deployed successfully in a myriad of country-specific applications. The model itemizes the output of an economic sector as a combination of intermediate consumptions and final demands. The model has been applied to a myriad of economic problems in both intraregional and multiregional perspectives (Isard 1960). The model is a useful tool in formulating economic policies in many countries because it is capable of describing the degree of interdependencies among various economic sectors and providing estimates of ripple effects associated with changes in the levels of consumption, production, as well as prices. Notably, contemporary extensions and frontiers of the IO model can be found in Dietzenbacher and Lahr (2004). The availability of high-resolution economic data and social accounting matrices has further enhanced the applicability and relevance of the model.

In the subsequent discussions, we introduce the basic mathematical formulation of IO model and give simple examples in order to explain concepts such as the Leontief technical coefficients and economic multipliers. Such concepts will eventually be central to describing the role of the IO model for evaluating the dependence of the sectors on information technology (IT) resources, as well as to better understand how cyber-security risks could cascade amongst interdependent economic sectors.

3.3 IO Model and its Parameters

In order to derive the basic IO model, suppose that an economy consists of n interacting sectors. The following notation will be used to represent the following variables and parameters for the IO model.

- z_{ij} : input of industry i to industry j (intermediate consumption)
- a_{ij} : input of industry i to j, normalized with respect to the total output of industry j
- f_i : final demand for industry i
- x_i : total output of industry i
- x_j : total output of industry j

where $i, j = 1, 2, \ldots, n$

The proportionality assumption leads to the following equation.

$$z_{ij} = a_{ij} x_j \qquad \text{(Eq. 1)}$$

Furthermore, the balance equation shown in (Eq. 2) in suggests that the total output of industry i is consumed either as intermediate demands (i.e., z_{ij}), or as final demand (f_i). For example, suppose that industry i produces cameras. The output of industry i (i.e., camera industry) can either be directly purchased for final use by photographers, or can be used as an intermediate input for an overarching system such as a closed circuit television (CCTV) device. Such

allocation of an industry's output to various consumers (intermediate and final) translates to the following mathematical formulation.

$$x_i = \sum_{j=1}^{n} z_{ij} + f_i \quad \text{(Eq. 2)}$$

Substituting (Eq. 1) to (Eq. 2) will reveal the basic Leontief IO model.

$$x_i = \sum_{j=1}^{n} a_{ij} x_j + f_i \quad \text{(Eq. 3)}$$

In matrix form, (Eq. 3) can be written as follows.

$$\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{f} \quad \text{(Eq. 4)}$$

In the matrix notation of (Eq. 4), the variables are interpreted similarly as their scalar counterparts: **x** is the total output vector (a column vector representing the total output of each industry), **f** is the final demand vector (a column vector representing the final demand for each industry), and **A** is a square matrix whose elements represent the proportion of the input of industry *i* to *j* with respect to the total output of industry *j*. In IO literature, **A** is typically called the Leontief technical coefficient matrix. The elements of the A matrix will be revisited later to assess the extent to which various sectors of the economy are dependent on IT resources.

In the following equations, we will show how to derive and describe the interpretations for the Leontief inverse, typically denoted in the literature by **L**. Using (Eq. 4) as the starting point, the aim is to explicitly isolate **x** on the left side of the equation. We do this through the following steps.

$$\mathbf{x} - \mathbf{A}\mathbf{x} = \mathbf{f} \quad \text{(Eq. 5)}$$

$$(\mathbf{I} - \mathbf{A})\mathbf{x} = \mathbf{f} \quad \text{(Eq. 6)}$$

$$\mathbf{x} = (\mathbf{I} - \mathbf{A})^{-1}\mathbf{f} \quad \text{(Eq. 7)}$$

Note that **I** is an identity matrix with the same size as **A**. In (Eq. 7), we can define **L** as the inverse term:

$$\mathbf{L} = (\mathbf{I} - \mathbf{A})^{-1} \quad \text{(Eq. 8)}$$

Substituting (Eq. 8) to (Eq. 7) will reveal an even more simplified version of the IO model:

$$\mathbf{x} = \mathbf{L}\mathbf{f} \quad \text{(Eq. 9)}$$

Note that the inverse term (**I** - **A**)$^{-1}$, which is denoted by **L**, is often referred to in the literature as the Leontief inverse. It is also called the total requirements matrix, which will be revisited further in this paper for measuring the impact of sector interconnectedness on the propagation of cyber security risks.

3.4 Inoperability Extension to the IO Model

Within the domain of IO modeling, the concept of inoperability has been used in recent studies to determine the direct and indirect economic losses in the aftermath of disasters. Haimes and Jiang (2001) revisited the Leontief model and expanded it to account for inoperability, or the inability for sectors to meet demand for their output. The *inoperability* measure is a dimensionless number between 0 (ideal state) and 1 (total failure); and as such, it is interpreted as the proportional extent in which a system is not functioning relative to its ideal state. Examples of studies that implemented Inoperability IO Model (IIM) to estimate economic losses include terrorism (Santos and Haimes 2004), electric power blackouts (Anderson et al. 2007), disease pandemics (Orsi and Santos 2010), and hurricane scenarios (Resurreccion and Santos 2013), among others.

The IIM is structurally similar to the classical IO model. The mathematical formulation is as follows:

$$\mathbf{q} = \mathbf{A}^*\mathbf{q} + \mathbf{c}^* \quad \text{(Eq. 10)}$$

where:

- **q** is the inoperability vector (i.e., the element, q_i, denotes the inoperability of sector *i*)
- $\mathbf{A}^*$ is the interdependency matrix matrix (i.e., the element a^*_{ij} denotes the input requirement of sector *j* that comes sector *i*, normalized with respect to the total input requirements of sector *j*)
- $\mathbf{c}^*$ is the demand perturbation vector (i.e., the element, c^*_i, denotes the demand perturbation to sector *i*)

3.4.1 Sector inoperability

Inoperability is conceptually related to the term unreliability, which expresses the ratio with which a sector's production is degraded relative to some ideal or 'as-planned' production level. Sector inoperability (**q**) is an array comprised of multiple interdependent economic sectors. The inoperability of each sector represents the ratio of unrealized production (i.e., ideal production minus degraded production) relative to the ideal production level of the industry sectors. To understand the concept of inoperability, suppose that a given sector's ideal production output is worth $100. Suppose also that a natural disaster causes this sector's output to reduce to $90. The production loss is $10, which is 10% of the ideal production output. Hence, the inoperability of the sector is 0.10. Since a region is comprised of interacting sectors, the value of inoperability will further increase due to the subsequent ripple effects caused by sector interdependencies.

3.4.2 Interdependency Matrix

The interdependency matrix ($\mathbf{A}^*$) is a transformation of the Leontief technical coefficient matrix (**A**), which is published by the Bureau of Economic Analysis and is publicly available. It is a square matrix with equal rows and columns, which correspond to the number of industry sectors. The elements in a particular row of the interdependency matrix can tell how much additional inoperability is contributed by a column industry sector to the row industry sector. Each element of the interdependency matrix can be estimated using the following formula:

$$a_{ij}^{*} = a_{ij}\left(\frac{x_j}{x_i}\right) \quad \text{(Eq. 11)}$$

When the interdependency matrix (**A***) is multiplied with the sector inoperability (**q**), this will generate the intermediate inoperability due to endogenous sector transactions. Endogenous transactions in the context of this report pertain to the flow of intermediate commodities and services within the intermediate sectors. These endogenous commodities and services are further processed by the intermediate sectors (i.e., commodities and services that are not further transformed or those used immediately for final consumption are excluded from endogenous transactions). The Bureau of Economic Analysis's detailed IO matrices can be customized for desired geographic resolutions using regional multipliers, or location quotients based on sector-specific economic data. This process of regionalization is performed to generate region-specific interdependency matrices.

3.4.3 Demand Perturbation

The demand perturbation (**c***) is a vector comprising of final demand disruptions to each sector in the region. The demand perturbation, just like the inoperability variable in the IIM formulation, is normalized between 0 and 1. In this basic IIM formulation, supply disruptions are modeled as "forced" demand reductions. Consider a hypothetical disruption where the supply for a commodity or service decreases but demand remains virtually unaffected. In this case, the consumers will have to temporarily sacrifice their need for that commodity or service until it bounces back to its as planned supply level. The assumption in the basic IIM formulation is that it uses "forced" demand reduction as a surrogate to supply reduction. More sophisticated formulations of the IIM include the dynamic extension to enable a more flexible definition of disruption parameters, as well as the inclusion of sector-specific economic resilience attributes.

3.4.4 Economic Loss

Similar to sector inoperability, economic loss is an array comprised of multiple interdependent economic sectors. Each element in this array indicates the magnitude of economic loss of each sector, in monetary units (or particularly in US dollars for the scenarios to be explored in the case study presented in Section 4). The economic loss of each sector is simply the product of the sector inoperability and the ideal production output. For example, an inoperability of 0.1 for a sector whose production output is $100 will result in an economic (or production) loss of $10. Economic loss, in terms of decreased production or output, is treated as a separate disaster consequence metric since it complements and supplements the inoperability metric. Both the inoperability and economic loss metrics are desired to be kept at minimum. It is also worth noting that when the sectors are ranked according to the magnitude of their inoperability and economic loss metrics, two distinct rankings will be generated. Suppose that a second sector has an inoperability of 0.2 and a production output of $40. The resulting economic loss will be $0.2 \cdot \$40 = \$8$. Although the inoperability of the second sector (0.2) has a higher rank compared to the first sector (0.1), the direction of priority will reverse when economic loss is considered as the sole basis for ranking. To wit, the second sector has an economic loss of $8, which has a lower rank in contrast to the first sector's $10 economic loss.

3.5 Input-Output Data

Economic data exist to describe the relationships among the interdependent sectors of the economy, and many statistical agencies across the globe are making significant efforts to publish IO data sets for public use. In the United States, extensive IO data are published by the Bureau of Economic Analysis (BEA) to generate the technical coefficient matrix (BEA 2016). Interdependencies across regions are becoming more prevalent due to the increasing trend in interregional transportation and trading activities. Significant segments of the working population commute across regions, as evidenced from the Journey to Work and Place of Work data (US Census Bureau 2017). This section provides a discussion of the data sources that will support the case study in Section 4. After a disruptive event (such as in the case of a cyber-security attack), the affected region will expect degraded access to IT service and resources. Such

disruptions in turn can lead to decreased production levels. In order to quantify the impact of reduced sector production levels on the economy, economic data for each sector of the region are collected and assembled from different sources.

The Bureau of Economic Analysis also publishes the annual IO data for 70 sectors[1] as depicted in Table 1. This methodology could be coupled with the Regional Input-Output Multiplier System (RIMS II) to provide a useful framework for evaluating economic interdependencies (US Department of Commerce 1997). These data sets are available from BEA for the nation as a whole, each state, metropolitan regions (using the US Census definitions), and counties. In this paper, we format the data using the North American Industry Classification System (NAICS). The RIMS II data also adheres to the NAICS classification. The standardized sector classification method allows users to yield comparable results when applying the same model to another region. Given the IO technical coefficient matrix (**A**) and sector output (**x**) for a region, the regional interdependency matrix ($\mathbf{A}^*$) can be established using RIMS II data.

[1] The 70-sector NAICS aggregation is adapted from the annual I-O accounts available in the BEA website. For the purposes of this study, we combined the two sectors: (i) Broadcasting and telecommunications, and (ii) data processing, internet publishing, and other information services. The combined sector will represent the “IT sector,” which is now designated with a code of S42.

Table 1. Economic Sector Classification

Code	Description
S1	Farms
S2	Forestry, fishing, and related activities
S3	Oil and gas extraction
S4	Mining, except oil and gas
S5	Support activities for mining
S6	Utilities
S7	Construction
S8	Wood products
S9	Nonmetallic mineral products
S10	Primary metals
S11	Fabricated metal products
S12	Machinery
S13	Computer and electronic products

Code	Description
S36	Transit and ground passenger transportation
S37	Pipeline transportation
S38	Other transportation and support activities
S39	Warehousing and storage
S40	Publishing industries, except internet (includes software)
S41	Motion picture and sound recording industries
S42	Information technology
S43	Federal Reserve banks, credit intermediation & related activities
S44	Securities, commodity contracts, and investments
S45	Insurance carriers and related activities
S46	Funds, trusts, and other financial vehicles
S47	Housing
S48	Other real estate

S14	Electrical equipment, appliances, and components
S15	Motor vehicles, bodies and trailers, and parts
S16	Other transportation equipment
S17	Furniture and related products
S18	Miscellaneous manufacturing
S19	Food and beverage and tobacco products
S20	Textile mills and textile product mills
S21	Apparel and leather and allied products
S22	Paper products
S23	Printing and related support activities
S24	Petroleum and coal products
S25	Chemical products
S26	Plastics and rubber products
S27	Wholesale trade
S28	Motor vehicle and parts dealers
S29	Food and beverage stores
S30	General merchandise stores

S49	Rental and leasing services and lessors of intangible assets
S50	Legal services
S51	Computer systems design and related services
S52	Miscellaneous professional, scientific, and technical services
S53	Management of companies and enterprises
S54	Administrative and support services
S55	Waste management and remediation services
S56	Educational services
S57	Ambulatory health care services
S58	Hospitals
S59	Nursing and residential care facilities
S60	Social assistance
S61	Performing arts, spectator sports, museums, and related activities
S62	Amusements, gambling, and recreation industries
S63	Accommodation
S64	Food services and drinking places
S65	Other services, except government

S31	Other retail
S32	Air transportation
S33	Rail transportation
S34	Water transportation
S35	Truck transportation

S66	Federal general government (defense)
S67	Federal general government (nondefense)
S68	Federal government enterprises
S69	State and local general government
S70	State and local government enterprises

Furthermore, the gross domestic product (GDP) data is needed in order to assess the economic value or significance of each sector. GDP can be interpreted as the value of final uses (or consumptions) of the sectors in an economy, which includes personal consumption expenditure, gross private domestic investment, government purchases, and net foreign exports (i.e., difference in exports and imports) (Miller and Blair, 2009). GDP data is available for all states and metropolitan areas within the United States[2].

4.0 Case Study and Analysis

In assessing the strength of interconnectedness of economic sectors with IT resources, we leverage the available IO data, which are published by statistical agencies of many countries across the globe. In this study, the proposed conceptual modeling framework will be demonstrated using the IO datasets published by the US Bureau of Economic Analysis, which will be applied to estimate the magnitude of losses of IT disruptions on the US economy. The approach will be to evaluate the degree of dependence of each sector on IT.

When the IT resources are disrupted (such as in the case of Denial-of-Service attacks), there will be cascading impacts on the production of goods and provision of critical services. Recent publications by the authors have estimated the significant societal and financial losses triggered by IT disruptions on the economy.

4.1 Sector Prioritization Based on IT Dependence

In Section 3, the concept of Leontief IO technical coefficients was explained. It was designated with the matrix notation **A**. In the subsequent discussions, the analysis will be based on the 70 US sectors as defined in Table 1. Hence, the **A** matrix will have a dimension of 70 rows and 70 columns. Each element is denoted by a_{ij}, which represents the input of sector *i* to sector *j*, normalized with respect to the total output of sector *j*. Hence the elements of a particular

[2] Gross state product and gross regional product are commonly referred to as GDP in the BEA website.

column *j* of the **A** matrix, when multiplied with 100, can be interpreted as the percentage dependence of sector *j* on each of the row sectors.

A particularly interesting analysis to be made here is the assessment of the dependence of each of the 70 sectors on the IT sector (which is designated with the code of S42, see Table 1). Because of the relatively large dimension of the **A** matrix, we shall only present the elements associated with the row of the IT sector. Notably, the IO technical coefficients associated with the S42 row can be arranged from highest to lowest to show a rank-ordered list of sectors based on the strength of their dependence on the IT sector. The underlying data used here as well as in subsequent sections were based on the 2016 IO data of the US, which is the most up to date for the current analysis.

Table 2. Rank-Ordered List of Sectors Based on their % Information Technology Dependence (ITD)

Rank	Code	Description	ITD
1	S42	Information technology	12.28
2	S44	Securities, commodity contracts, and investments	6.15
3	S67	Federal general government (nondefense)	5.04
4	S53	Management of companies and enterprises	4.06
5	S54	Administrative and support services	3.31
6	S68	Federal government enterprises	2.90
7	S50	Legal services	2.57
8	S28	Motor vehicle and parts dealers	2.57
9	S69	State and local general government	2.56
10	S52	Miscellaneous professional, scientific, and technical services	2.28
11	S31	Other retail	2.27
12	S34	Water transportation	1.92
36	S66	Federal general government (defense)	1.11
37	S70	State and local government enterprises	1.10
38	S41	Motion picture and sound recording industries	1.06
39	S64	Food services and drinking places	1.05
40	S11	Fabricated metal products	1.05
41	S59	Nursing and residential care facilities	1.02
42	S9	Nonmetallic mineral products	0.98
43	S39	Warehousing and storage	0.98
44	S12	Machinery	0.88
45	S26	Plastics and rubber products	0.85
46	S30	General merchandise stores	0.84
47	S22	Paper products	0.83

13	S48	Other real estate	1.83
14	S58	Hospitals	1.70
15	S56	Educational services	1.69
16	S17	Furniture and related products	1.61
17	S21	Apparel and leather and allied products	1.57
18	S49	Rental and leasing services and lessors of intangible assets	1.55
19	S40	Publishing industries, except internet (includes software)	1.54
20	S61	Performing arts, spectator sports, museums, and related activities	1.40
21	S27	Wholesale trade	1.40
22	S62	Amusements, gambling, and recreation industries	1.38
48	S16	Other transportation equipment	0.74
49	S7	Construction	0.66
50	S46	Funds, trusts, and other financial vehicles	0.63
51	S32	Air transportation	0.59
52	S33	Rail transportation	0.53
53	S10	Primary metals	0.51
54	S38	Other transportation and support activities	0.51
55	S35	Truck transportation	0.49
56	S45	Insurance carriers and related activities	0.48
57	S19	Food and beverage and tobacco products	0.46

23	S36	Transit and ground passenger transportation	1.34
24	S63	Accommodation	1.34
25	S51	Computer systems design and related services	1.31
26	S65	Other services, except government	1.28
27	S43	Federal Reserve banks, credit intermediation & related activities	1.25
28	S60	Social assistance	1.23
29	S57	Ambulatory health care services	1.23
30	S8	Wood products	1.22
31	S29	Food and beverage stores	1.22
32	S55	Waste management and remediation services	1.20
58	S6	Utilities	0.46
59	S37	Pipeline transportation	0.38
60	S14	Electrical equipment, appliances, and components	0.38
61	S15	Motor vehicles, bodies and trailers, and parts	0.37
62	S25	Chemical products	0.34
63	S13	Computer and electronic products	0.32
64	S4	Mining, except oil and gas	0.31
65	S5	Support activities for mining	0.26
66	S1	Farms	0.21
67	S3	Oil and gas extraction	0.17

33	S23	Printing and related support activities	1.15
34	S18	Miscellaneous manufacturing	1.15
35	S20	Textile mills and textile product mills	1.12
68	S24	Petroleum and coal products	0.14
69	S2	Forestry, fishing, and related activities	0.09
70	S47	Housing	0.01

Based on the results from Table 2, it can be seen that S42 Information technology has the highest IT dependence, which is quite intuitive. It is followed by S44 Securities, commodity contracts, and investments, with 12.28% dependence on IT. The remainder of the sectors in the top 10 ranking of highest dependence on IT are: S67 Federal general government nondefense, S53 Management of companies and enterprises, S54 Administrative and support services, S68 Federal government enterprises, S50 Legal services, S28 Motor vehicle and parts dealers, S69 State and local general government, and S52 Miscellaneous professional, scientific, and technical services.

4.2 Sector Prioritization Based on Disruptions to the IT Sector

Another approach for prioritizing sectors is by simulating a scenario wherein a proportion of the IT resources is rendered unavailable by a disruptive event. Examples of disruptive events include natural disasters, which could impair the infrastructure that supports the delivery of IT resources, or a willful attack that causes denial of service. In this section, the process of prioritizing the sectors are based on the magnitude of the IT disruption, as well as the overall ripple effects across the interdependent sectors. This approach is fundamentally different from the sector prioritization as discussed in Section 4.1, which only measures the direct dependence of each sector on IT, without explicitly considering how the sectors would behave and react in an interdependent manner.

Using the concept of inoperability as discussed in Section 3.4, suppose that a denial of service attack would only allow the IT sector to deliver only 90% of its intended output (or 90% reliability). By taking the complement of reliability, the scenario could be interpreted as a 10% inoperability to the IT sector. Note that this value of 10% is only the direct inoperability to the IT sector; as such, the impact on the IT sector is expected to be higher than 10% because of the indirect effects caused by other sectors (i.e., the IT sector also relies on other sectors to generate its output). All the other sectors will consequently be affected based on their reliance on the IT sector, as well as how interdependent they are with the rest of the sectors.

A 10% direct inoperability to the IT sector will lead to a cascade of inoperability across all the sectors of the economy. The ranking of the sectors based on the magnitude of total inoperability (i.e., direct plus indirect inoperability due to the IT disruption scenario), is shown in Table 3. Note that total inoperability is denoted by **q**, which was the basis for the sector

prioritization. Based on the simulation results, the top-10 sectors based on total inoperability (in %) are as follows: S42 Information technology (12.87%), S53 Management of companies and enterprises (6.64%), S44 Securities, commodity contracts, and investments (6.60%), S55 Waste management and remediation services (6.36%), S68 Federal government enterprises (5.76%), S54 Administrative and support services (5.35%), S41 Motion picture and sound recording industries (5.32%), S67 Federal general government nondefense (5.05%), S50 Legal services (4.72%) and, S49 Rental and leasing services and lessors of intangible assets (4.05%).

Note that some of the sectors are prioritized relatively consistently in both ITD (Section 2.1) and inoperability measures (this section). Examples include Information technology, Securities, commodity contracts, and investments, Management of companies and enterprises, and Legal services, among others. Nonetheless, the inoperability approach for prioritization has brought new sectors into the top 10 ranking, including Waste management and remediation services, and Motion picture and sound recording industries.

Table 3. Rank-Ordered List of Sectors Based on Inoperability (q), Due to a 10% Disruption to the IT Sector

Rank	Code	Description	q
1	S42	Information technology	12.87
2	S53	Management of companies and enterprises	6.64
3	S44	Securities, commodity contracts, and investments	6.60
4	S55	Waste management and remediation services	6.36
5	S68	Federal government enterprises	5.76
6	S54	Administrative and support services	5.35
7	S41	Motion picture and sound recording industries	5.32
8	S67	Federal general government (nondefense)	5.05
9	S50	Legal services	4.72
10	S49	Rental and leasing services and lessors of intangible assets	4.05
11	S52	Miscellaneous professional, scientific, and technical services	3.99
12	S23	Printing and related support activities	3.65
36	S4	Mining, except oil and gas	2.04
37	S3	Oil and gas extraction	2.04
38	S61	Performing arts, spectator sports, museums, and related activities	2.04
39	S17	Furniture and related products	1.99
40	S65	Other services, except government	1.97
41	S32	Air transportation	1.97
42	S2	Forestry, fishing, and related activities	1.97
43	S70	State and local government enterprises	1.88
44	S37	Pipeline transportation	1.84
45	S33	Rail transportation	1.82
46	S6	Utilities	1.80
47	S18	Miscellaneous manufacturing	1.75

13	S13	Computer and electronic products	3.62
14	S48	Other real estate	3.57
15	S62	Amusements, gambling, and recreation industries	3.45
16	S51	Computer systems design and related services	3.28
17	S10	Primary metals	3.24
18	S8	Wood products	3.17
19	S11	Fabricated metal products	3.00
20	S39	Warehousing and storage	2.92
21	S43	Federal Reserve banks, credit intermediation & related activities	2.60
22	S9	Nonmetallic mineral products	2.56

48	S63	Accommodation	1.74
49	S45	Insurance carriers and related activities	1.72
50	S64	Food services and drinking places	1.63
51	S12	Machinery	1.63
52	S56	Educational services	1.58
53	S25	Chemical products	1.49
54	S35	Truck transportation	1.45
55	S58	Hospitals	1.39
56	S24	Petroleum and coal products	1.26
57	S16	Other transportation equipment	1.24

23	S22	Paper products	2.56
24	S36	Transit and ground passenger transportation	2.55
25	S38	Other transportation and support activities	2.53
26	S14	Electrical equipment, appliances, and components	2.35
27	S26	Plastics and rubber products	2.33
28	S20	Textile mills and textile product mills	2.33
29	S34	Water transportation	2.31
30	S28	Motor vehicle and parts dealers	2.30
31	S40	Publishing industries, except internet (includes software)	2.28
32	S21	Apparel and leather and allied products	2.18
58	S66	Federal general government (defense)	1.16
59	S57	Ambulatory health care services	1.08
60	S60	Social assistance	1.03
61	S29	Food and beverage stores	1.01
62	S59	Nursing and residential care facilities	0.97
63	S19	Food and beverage and tobacco products	0.96
64	S1	Farms	0.93
65	S7	Construction	0.91
66	S15	Motor vehicles, bodies and trailers, and parts	0.90
67	S46	Funds, trusts, and other financial vehicles	0.85

33	S27	Wholesale trade	2.17
34	S69	State and local general government	2.15
35	S31	Other retail	2.06
68	S30	General merchandise stores	0.75
69	S5	Support activities for mining	0.43
70	S47	Housing	0.01

4.3 Sector Prioritization Based on Economic Loss

A final approach for prioritizing sectors is by taking the monetary value (i.e., economic loss) associated with the disruption to the IT sector. The same scenario described in Section 4.2 is used here; nonetheless, the focus of the ranking is on the economic loss and not on the inoperability *per se*. Rankings based on economic loss provides an alternative perspective that could complement the inoperability measure. For example, two sectors may have the same inoperability values, but their contribution to the GDP could significantly differentiate the magnitude of financial impacts.

Suppose that the same 10% direct inoperability scenario is applied to the IT sector. Or aim here is to compute for the economic losses (in annualized values) associated with the inoperability values as simulated in the previous section. The economic loss values are computed by multiplying the inoperability of each sector with its corresponding production output (in million USD, estimated based on year 2016 GDP data). The ranking of sectors based on economic losses are shown in Table 4. Included in the top 10 are: S42 Information technology ($139,963M), S52 Miscellaneous professional, scientific, and technical services ($53,033M), S69 State and local general government ($47,395M), S54 Administrative and support services ($44,954M), S53 Management of companies and enterprises ($42,116M), S48 Other real estate ($38,877), S44 Securities, commodity contracts, and investments ($32,509), S27 Wholesale trade ($30,021), S43 Federal Reserve banks, credit intermediation & related activities ($20,785), S67 Federal general government nondefense ($20,318).

Because the above rankings are GDP-based, new sectors have been included in the top 10 in contrast to the previous prioritization approaches. Examples include Other real estate, and also Wholesale trade. Despite their relatively lower placements in the ranking for inoperability, these sectors have been included in the rankings for economic loss because they tend to be hit with higher financial impact (due to the high GDP contribution), albeit their relatively lower inoperability values.

Table 4. Rank-Ordered List of Sectors Based on Economic Loss (in Million USD), Due to a 10% Disruption to the IT Sector

Rank	Code	Description	Loss
1	S42	Information technology	139,963
2	S52	Miscellaneous professional, scientific, and technical services	53,033
3	S69	State and local general government	47,395
4	S54	Administrative and support services	44,954
5	S53	Management of companies and enterprises	42,116
6	S48	Other real estate	38,877
7	S44	Securities, commodity contracts, and investments	32,509
8	S27	Wholesale trade	30,021
36	S68	Federal government enterprises	5,642
37	S26	Plastics and rubber products	5,484
38	S56	Educational services	5,348
39	S24	Petroleum and coal products	5,231
40	S62	Amusements, gambling, and recreation industries	5,115
41	S35	Truck transportation	4,783
42	S22	Paper products	4,725
43	S3	Oil and gas extraction	4,177

9	S43	Federal Reserve banks, credit intermediation & related activities	20,785
10	S67	Federal general government (nondefense)	20,318
11	S31	Other retail	17,857
12	S45	Insurance carriers and related activities	15,802
13	S50	Legal services	14,828
14	S13	Computer and electronic products	14,488
15	S49	Rental and leasing services and lessors of intangible assets	13,824
16	S65	Other services, except government	13,382
17	S7	Construction	13,168
18	S51	Computer systems design and related services	12,297
44	S63	Accommodation	4,139
45	S16	Other transportation equipment	3,926
46	S1	Farms	3,600
47	S61	Performing arts, spectator sports, museums, and related activities	3,447
48	S32	Air transportation	3,357
49	S8	Wood products	3,301
50	S9	Nonmetallic mineral products	3,168
51	S23	Printing and related support activities	3,038
52	S14	Electrical equipment, appliances, and components	2,802
53	S39	Warehousing and storage	2,745

19	S25	Chemical products	11,999
20	S64	Food services and drinking places	11,946
21	S58	Hospitals	11,782
22	S11	Fabricated metal products	11,198
23	S57	Ambulatory health care services	11,098
24	S19	Food and beverage and tobacco products	9,050
25	S41	Motion picture and sound recording industries	8,285
26	S40	Publishing industries, except internet (includes software)	7,844
27	S66	Federal general government (defense)	7,099
28	S10	Primary metals	6,808
54	S18	Miscellaneous manufacturing	2,692
55	S59	Nursing and residential care facilities	2,309
56	S29	Food and beverage stores	2,208
57	S4	Mining, except oil and gas	1,970
58	S60	Social assistance	1,942
59	S17	Furniture and related products	1,580
60	S36	Transit and ground passenger transportation	1,530
61	S30	General merchandise stores	1,437
62	S46	Funds, trusts, and other financial vehicles	1,415
63	S33	Rail transportation	1,381

29	S6	Utilities	6,679
30	S15	Motor vehicles, bodies and trailers, and parts	6,074
31	S55	Waste management and remediation services	6,012
32	S70	State and local government enterprises	5,958
33	S12	Machinery	5,936
34	S38	Other transportation and support activities	5,801
35	S28	Motor vehicle and parts dealers	5,720
64	S20	Textile mills and textile product mills	1,338
65	S34	Water transportation	1,323
66	S2	Forestry, fishing, and related activities	1,026
67	S21	Apparel and leather and allied products	852
68	S37	Pipeline transportation	613
69	S5	Support activities for mining	204
70	S47	Housing	122

5. Summary of results and areas for future study

Three approaches to tracking and prioritizing the ripple effect of cyber attacks across economic sectors have been suggested and test results drawn in section 4:

1. By assessing the dependence of each of the 70 sectors on the IT sector

2. By simulating a scenario wherein a proportion of the IT resources is rendered unavailable by a disruptive event

3. By taking the monetary value (i.e., economic loss) associated with the disruption to the IT sector

in each, the ten highest rankings were identified and are summarized in the table below:

	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th
Dependency	IT	Securities	Fed non-defense	Mgt of Cos	Admin svcs	Fed enterprs	Legal	Motor veh	St+Loc Govts	Misc prof svcs
Inoperability	IT	Mgt of Cos	Securities	Waste Mgt	Fed enterprs	Admin svcs	Motion pictires	Fed non-defense	Legal	Rental cos
Econ Loss	IT	Misc prof svcs	St+Loc Govts	Admin svcs	Mgt of Cos	Other real estate	Securities	Wholesale trade	Fed Res banks	Fed non-defense

It is interesting to observe changes in priorities depending on the parameters used; more interesting are the sectors that seem to be impacted in a priority fashion irrespective of the approach used- perhaps they are prime for exploring cyber security linkages and developing cascading interruption strategies quickly and on a priority basis. Four sectors are in all top ten lists:

S44 Securities, commodity contracts, and investments

S67 Federal general government nondefense

S53 Management of companies and enterprises

S54 Administrative and support services

These four sectors could perhaps be the first ones where risk management strategies should be focused, and investments deepened in cyber security defenses. The models developed suggest that the down stream impact of cyber attacks could be reduced most effectively if successful risk reduction strategies could be introduced first in these sectors.

Of course these results are based on an initial pilot test in a single country (i.e., US); further research using additional national data from other countries could suggest additional priority sectors most susceptible to the cascading effects of cyber attacks. In addition, UN ISDR could establish a rapid global assessment of these risks using readily available economic data, thus sidestepping issues of lack of data in cyber security operations of many countries.

In a different, yet equally important direction, each model and the corresponding priority rankings could be used by insurance and reinsurance carriers to begin a filtering and discrimination process towards establishing more refined and stable cyber security insurance rates. The ratios and relative positions of major economic sectors can suggest a starting risk ratio by sector. In turn, if the total risk of an economy can be estimated, these ratios could indeed to establish insurance exposures for each economic sector.

These suggested applications cannot be clarified and made market ready without the exploration of shared strategies between the cyber security, insurance industry risk management and government sectors. Each has different optimization goals and stance towards sharing data, open collaboration and semantic barriers. Bringing them together, establishing a shared agenda and developing an overall work plan across sectors is a worthwhile goal to consider, and will be the topic of future research.

Furthermore, although not directly apparent from the "top-10" sector rankings that were generated by the IO model, it is also important to look holistically at all the sectors included in the study and to evaluate their criticality in supporting human existence. A case in point, food is arguably one of the most essential requirement for sustaining human life, according to Maslow's Hierarchy of Needs. In the IO sector classification used in this paper (see Table 1), at least five sectors contribute directly to ensuring food availability and security. These are:

- S1: Farms
- S2: Forestry, fishing, and related activities
- S19: Food and beverage and tobacco products
- S29: Food and beverage stores
- S64: Food services and drinking places

Taken individually, the above food-related sectors may have relatively lower magnitudes of IT-dependence, inoperability, and GDP loss compared to larger sectors such as Securities, commodity contracts, and investments (S44), Federal general government nondefense (S67), Management of companies and enterprises (S53), and Administrative and support services (S54). Nonetheless, when aggregated, the vulnerability of these food-related sectors to IT disruptions, as well as the significance of financial losses, would be much more amplified. Hence, a use case study is presented in the Appendix of this paper to emphasize the potential threats and consequences of cyber-attacks to food-related sectors and how such scenarios could impact the reliability and integrity of food supply chains.

Appendix: Use case on food security by Molly Jahn et al "Cyber Risks in North American Agriculture and Food Systems"

The *use case* is made up of a set of possible sequences of interactions in a vital economic system- that of food security- under conditions of cyber attack. It is intended to give the reader a deeper look into a known system so that the value of the application of the risk methodology suggested can be properly assessed and appreciated.

GAR19 is intended to reach not only the scientific community but also key decision makers who can take action and align their organizations to a more risk-driven stance. The use case is written so that policy implications of a risk analysis can be visualized strongly, and suggested actions made more evident under a particular economic system of vital importance. Thus, the agriculture and food systems economy where the role of IT and cyber security is not always understood and may be totally overlooked is brought to sharp focus. Similar use cases can be undertaken in all important economic sectors as a precursor to a strong cyber security strategy development and deployment, useful as a qualitative RoI example of rationalizing new investments that must be made.

The authors are grateful to Moly Jahn and her team for undertaking this use case effort and highlighting with precision why it is vital to begin the dialog between the computer science and cyber security community with the individual sector managers across the economy expeditiously.

Appendix: Cyber Risks in North American Agriculture and Food Systems[3]

Rapid changes in American agriculture and the ways in which food is produced and distributed are opening new and often unappreciated cyber attack vectors. The structure and operation of modern highly "networked" food systems (and the obvious requirement for functional energy, transportation and other systems) fundamentally depends on networked information systems, some of which may not be secured from cyber attacks. The combined complexities of these networked systems interacting together stands to amplify threats and vulnerabilities that exist in any of the major systems, as well as risk to other dependent systems. The result is uncharacterized risks that are highly relevant for food safety and supply, manufacturing, banking, financial, commodities, insurance, and other sectors.

Among the salient large scale features in contemporary food systems that have potential to increase cyber risk are: (1) increasing farm consolidation with heavy reliance on technology,[4] (2) vertical integration through the food supply chains in which agricultural producers may also directly proces agricultural commodities, e.g., milk, into dairy products, e.g., cheese and yogurt, directly supplying supermarkets and grocery stores,[5] (3) widespread lack of compliance with food safety, traceability and insurance requirements, (4) rapidly advancing use of "smart technology" throughout supply chains, (5) increasing inter-dependency among food system components in "smart markets" resulting from new and often uncharacterized outsourcing relationships, service and highly-coordinated supply arrangements, creating greater exposure to inter-organizational cascading defaults and failures, and (6) lack of systematic surveillance of social media, markets and other dynamic real time or near real time reflections of food

---

[3] Dr. Molly Jahn, Professor, Department of Agronomy, College of Agricultural and Life Sciences, University of Wisconsin-Madison; William L. Oemichen, University of Wisconsin-Madison Food Systems Security Research Fellow, former Deputy Minnesota Agriculture Commissioner and State of Wisconsin Consumer Protection Division Administrator; Dr. Gregory F. Treverton, Professor of the Practice of International Relations, School of International Relations, University of Southern California; Scott David, University of Washington Applied Physics Laboratory; Matthew A. Rose, Department of Defense; Max A. Brosig, U.S. Army War College; Research Assistant William K. Hutchison, University of Wisconsin-Madison; and Research Intern Braeden B. Rimestad, University of Wisconsin-Madison. We thank Peter S. Brooks for comments on the manuscript.

[4] "Three Decades of Farm Consolidation." USDA Economic Research Service. March 2018. https://www.ers.usda.gov/webdocs/publications/88057/eib189_summary.pdf?v=43172.

[5] "Trends in U.S. Agriculture." USDA National Agricultural Statistics Service. May 4, 2018. https://www.nass.usda.gov/Publications/Trends_in_U.S._Agriculture/Broiler_Industry/index.php.

systems in a defensive mode to quickly detect both material and digital issues of substantial concern. Just-in-time distribution further exacerbates potential fragility in food supply between farm and table. All of these changes cause or are caused by advances in information flows and interactive systems that support the food system. Wherever information flows are crucial to the regular function of food systems, the potential for interruption or disruption via cyber attack exists.

Even a short-duration interruption in the refrigeration chain or other essential infrastructure for food distribution, or a targeted disruption of a highly time-sensitive process such as harvest, could cause major, long-lasting effects globally and significant economic losses. In fact, past cyber events that were neither well timed nor coordinated have caused mass disruption, e.g., disruption of markets in the Sony attack, while well-coordinated attacks, usually attributed to state actors (Stuxnet/Saudi Aramko/Russia Ukraine power), could also be devastating. If the actor was trying to build a profile (usually lone actor) or simply vandalize (i.e. college hackers), it is not inconceivable given the potential vulnerabilities we highlight below that the attack could be "lucky" and cause real damage. It is our conclusion that competitor-on-competitor attacks also cannot be ruled out in this sector, especially given the global nature of supply chains. In addition to this and other similar direct effects of cyber-insecurity on food systems, there are a host of other indirect and secondary impacts that could negatively affect global and national security.

A variety of economic and sociological factors affect these changes, but the main driver is the need to produce ever increasing quantities of food in a quickly changing climate to feed a rapidly growing and increasingly affluent and urban-dwelling world population, one that is expected to increase from 7.6 billion now to 8.6 billion in 2030 and 11.2 billion in 2050.[6] The combination of increased demand alongside globalized ingredient markets, decreased cost, increased dependence on energy, increased ubiquity and reliance on information-network-dependent "smart markets," smart production and distribution systems, and more extremes in weather means that the North American agricultural system and the billions of people it serves around the world are increasingly at risk from cyber threats and other information-related risks.

---

[6] "World Population Prospects: The 2017 Revision." United Nations Department of Economic and Social Affairs. June 21, 2017. https://www.un.org/development/desa/publications/world-population-prospects-the-2017-revision.html.

The Trend Towards Smart Farming

To meet the world population challenge and better manage resources and extreme weather, North American agricultural producers have rapidly embraced new technologies at a large scale and at an ever increasing pace. The adoption of these technologies has led to the "precision agriculture" revolution, where smart devices integrated with "smart markets" enable more precise and timely allocation of on-farm resources during the growing season and through harvest and transport of the crop off-farm. This practice raises production efficiency[7] with the overall goal of increasing production per acre through more efficient use of inputs including seed, water, crop nutrients, herbicides and pesticides.[8] Taken together, smart technology, smart markets, and precision agriculture deliver historic game-changing advances in agriculture favored by those financing and insuring American agriculture—and which apply traditional measures of economic risk, such as those based on efficiency and productivity.[9] These technology shifts, and the un-measured, uncharacterized dependencies that they engender, however, may themselves create major new risks. Any smart technology in the system left unsecured, and any smart market in the system that is unmonitored may be hacked or manipulated by hostile actors with major direct or collateral damage to North American agriculture and food distribution systems.

Examples of smart technologies abound. Already, sensors integrated into agricultural implements determine the rate of application of water, pesticides and herbicides. Autonomous robots such as robotic milkers are deployed in large part to relieve a shortage of labor on farms. At the same time, autonomous agricultural planters, cultivators and harvesters are becoming so advanced that they are rapidly eliminating the need for agricultural producers to actually drive their equipment. Driverless tractors, for example, are being tested on

---

[7] "The Future of Food and Agriculture: Trends and Challenges." Food and Agricultural Organization of the United Nations. 2017. http://www.fao.org/3/a-i6583e.pdf.
[8] Cleary, David. "Guest Commentary - Precision Agriculture Potential and Limits." The Chicago Council on Global Affairs. March 23, 2017. https://www.thechicagocouncil.org/blog/global-food-thought/guest-commentary-precision-agriculture-potential-and-limits.
[9] "Agricultural Finance & Agricultural Insurance." The World Bank. February 2, 2018. http://www.worldbank.org/en/topic/financialsector/brief/agriculture-finance.

American farms and will greatly reduce the hours spent by agricultural producers in the cab. This means the agricultural producer will focus less on applying their physical labor to their farming operation and focus more on planning and managing the planting, cultivating, and the harvesting (and even on-farm processing) of the agricultural crop.[10] Physical labor is not the only area at risk of being replaced or augmented by machines. Artificial intelligence and data analytics are also being widely implemented in agricultural and food production plants, removing or profoundly changing the role of humans in the system.

The challenges of AI integration do not end with replacing labor. The machine augmentations of AI and machine learning are also applied directly and indirectly in myriad agricultural growing and marketing decisions. "Smart market" data (which increasingly applies AI and machine learning and big data analytic techniques) are becoming increasingly applied by all actors in the agricultural process creating vulnerabilities where interventions may not even be detected until well after the damage is done. Today, AI nudges decision makers on when to plant and spray crops, when to release stored crops to market and other decisions that affect farming production. Intentional attacks and accidental and unintended damage that could result from faulty "decisions" by these systems will introduce a host of new non-linear threats into food systems.

Smart implements are already being used in all major North American commodities, especially corn, soybean, cotton, wheat and sugar beet, to determine what rate and distance to plant the seed, what level of fertilizers, pesticides and herbicides need to be applied for maximum production, and when to harvest the crops. These "smart" enhancements are achieved through the dynamic calibration of the technology and its control systems using analyses of historical crop production, soil tests, weather satellite information, and the like, all integrated into suggested technology settings in an effort to ensure crop supplements are applied at the most ideal time. This information is dynamically downloaded into and utilized by the software of the tractor, cultivator or harvester to determine the timing and machine settings for maximum planting and cultivation efficiency. Informal surveys of trade shows during the winter of 2017-8 suggest that little or no attention has been devoted to securing these systems from outside intrusion. Attacks on these systems could involve both short term disruption of

[10] Brown, Meghan. "Smart Farming—Automated and Connected Agriculture." Engineering.com. March 15, 2018. https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/16653/Smart-FarmingAutomated-and-Connected-Agriculture.aspx.

availability of calibration information or long term manipulation of one or more of the data inputs that are integrated into the calibration settings. In the latter case, the negative effect of the system "hacks" (such as the over-application of fertilizer, etc.) might not be detected until it is too late in the growing season, causing irreversible damage.

In relatively dry portions of the United States, agricultural producers are applying unsecured smart technologies to control irrigation equipment that, in the past, delivered water to crops in only broad and imprecise ways. Now, smart irrigation systems, such as sensors tied to subsurface drip irrigation, allow precise field conditions to be monitored, and, by doing so, ensure water is applied at the right time to ensure continued crop health.[11] Interference with the functioning of smart technology applied to irrigation could disrupt water availability during heat waves, which are occurring with increasing frequency due to climate change, and quickly destroy an entire season's crop. Again, this type of interference or large scale malfunction may not be detected until well after lasting damage is done.

Producers are also embracing the use of smart cultivators that can identify and eliminate weeds in a field, thereby reducing or perhaps eliminating the common agricultural practice of broadly applying herbicides across the entire field regardless of need. Smart agricultural technologies also include increasingly sophisticated equipment to harvest fruits and vegetables at the right time. Multiple scenarios can be readily imagined through which interruption with either of these processes at a critical time in a growing season affects harvest quality or quantity. As with the other cyber risks, the attack might be launched against software in a way that would disable the physical equipment such that timely repair was impossible. If such an attack were deployed against equipment that is broadly used, the effects could devastate a particular crop harvest or area, affecting markets and the availability of that input for food manufacturing or other uses where agricultural commodities are crucial inputs, e.g., fiber, biomass, agri-pharmaceuticals, etc.

---

[11] "Reducing the Drip of Irrigation Energy Costs." USAID Global Waters. July 18, 2017. https://medium.com/usaid-global-waters/reducing-the-drip-of-irrigation-energy-costs-ea2e1756bcd2.

Agricultural drones, already in common use by agricultural cooperatives and other agricultural suppliers, ensure the agricultural producer has real time crop monitoring data to ensure the efficient use of crop inputs. [12] Blue chip technology firms, such as Microsoft, are investing heavily in this area due to apparent market drivers.[13] Drones also make it more efficient for farm lenders, like the $330 billion American Farm Credit System, to determine the value of the crop and other agricultural collateral that is the basis for the production loan. The data generated by these technologies help to enhance insight into production capacity and operating efficiencies, and thereby have the potential to reduce lender risk and increase capital availability.

All of these smart agricultural implements are in the process of being tied together through the Internet of Things (IoT) in an effort to enhance integration and optimization within the agricultural production system. This strength is ultimately also a source of weakness, since massively interconnected systems of devices, combined with increasingly automatic and autonomous/AI driven controls have the potential to be subject to attack and cascading failures through accident. A "weak link" in the massively networked information systems that increasingly serve all aspects of farming practices can lead to massive disruptions through connected systems. A unique but telling example of "weak link" entry point occurred in 2017, when hackers successfully breached a casino's network through the PC-connected monitors used to regulate the conditions of a fish tank. Through this single point of entry, hackers were able to gain access to the larger system and acquire protected financial data, illustrating how single cyber-security weak points can easily lead to broader instability across interconnected systems.[14]

Because of this interconnectedness and the increasing application of smart technology and devices, the risk of the American agricultural industry being negatively impacted by a service interruption caused by a cyber attack or accidents, acts of nature or AI/autonomous systems (collectively "AAAA Threats") is rapidly growing. The

---

[12] Ravindra, Savaram. "IOT Applications in Agriculture." IOT for All. January 3, 2018. https://www.iotforall.com/iot-applications-in-agriculture/.
[13] Choney, Suzanne. "Farming's most important crop may be the knowledge harvested by drones and the intelligent edge." Microsoft News. May 7, 2018. https://news.microsoft.com/transform/farmings-most-important-crop-may-be-the-knowledge-harvested-by-drones-and-the-intelligent-edge/.
[14] Schiffer, Alex. "How a fish tank helped hack a casino." Washington Post. July 21, 2017. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?noredirect=on&utm_term=.fc6178c844a3.

exposure is a result of a failure of education and market information, since the issue is not yet well known or understood by equipment manufacturers or producers, and equipment consumers are not yet demanding that the equipment they purchase be cyber secure. This leaves not just North Americans but all consumers across the globe vulnerable to price shocks or shortages resulting from a cyber attack in North America.

This situation also exposes financial lenders and their investors to potential additional risk, although at present, such exposures are not taken into account in lending criteria. This lender exposure exists whether the loans are secured by the equipment itself (through lease financing, purchase money security interests, etc.) and for loans that are secured by receivables generated by farming operations.

At the farm level and throughout the supply chain, and in broader food, commodity and financial markets generally, gains from integration and remote control come with risks. Appropriate decisions about vulnerability prevention and threat mitigation will depend on both better information and better training of stakeholders throughout the supply chain. The imperative to include cybersecurity in the design and development of food systems is clear. Systematic approaches to place key elements, both virtual and material in "fail safe default states" are badly needed. A fail safe default state is specifically designed to anticipate and minimize harm in the event that intended performance is interrupted or compromised.

Technological and policy solutions at all levels will also need to be designed and deployed in a way that can match the massively distributed "interaction surface" of food systems. This will advantage solutions that can be deployed with minimal cost and other resources, and which take advantage of other installed networks and communication systems (such as social systems and training through agricultural extension and private sector outreach systems, or technology systems such as mobile "apps" alerting farmers to threats to their equipment and information systems used to run their farms).

The Role of Smart Systems in Agricultural Processing

Similar to farming and food production, the food processing system is increasingly reliant on automated equipment, much of which is linked together via the IoT or through networks of programmable logic controllers

(PLCs).[15] Across industries, these networks are prime targets for cyber attacks. The security of these systems in food processing is particularly important due to the potentially large-scale public health ramifications of an attack. One example is the increasing use of smart sensors to monitor food product temperature during processing and transportation.[16] Smart temperature monitors ensure products being processed or shipped remain at optimal temperatures and make determinations about freshness and shelf-life for goods. The sensors are also intended to be connected through the IoT so the processor or shipper may receive real time data on the quality of the food product and can share the data with partners such as retail grocery stores. A potential risk is that the sensors could be manipulated by a bad actor, allowing food products to be stored at less than optimal temperatures, thereby leading to an enhanced risk of bacterial contamination. If done covertly and with intention to harm, this disruption could go unnoticed and lead to a wave of illness among consumers.

The potential for contamination from intentional or accidental causes is a problem in a variety of food processing contexts. As these processing elements all migrate toward IoT and AI/autonomous controls, the control systems for such elements become increasingly complex. The potential for attack and accident both lurk in the shadows of that complexity. Complex interactions are like "chaff" released from an aircraft to obscure radars– they make it hard to discern "signal" of a given interaction among all the "noise" of the many interactions. Where stakeholders cannot detect the signals of attack or accident in complex systems, risk increases. Other examples of contamination settings include water-treatment facility where levels of essential chemicals like chlorine could be manipulated to contaminate the water supply.[17] On the consumer end, connected appliances create more opportunities for remote manipulation—if hackers were able to control the temperature settings on smart refrigerators, consumers could unwittingly be exposed to food spoilage or food poisoning.[18] Such an attack (or

---

[15] Russell, Nicholas. "Cybersecurity and Our Food Systems." Tufts University. December 13, 2017. http://www.cs.tufts.edu/comp/116/archive/fall2017/nrussell.pdf.
[16] Brown, Heather. "The Internet of Things and the Future of Food." Food Industry Executive. April 29, 2016. http://foodindustryexecutive.com/2016/04/the-internet-of-things-and-the-future-of-food/.
[17] James, Nicole C.K. "Cyberterrorism: How Food Companies Are Planning for Threat of Cybersecurity Risks." Food Quality and Safety. May 18, 2018. https://www.foodqualityandsafety.com/article/cyberterrorism-food-industry-cybersecurity-risks/.
[18] Russell, Nicholas. "Cybersecurity and Our Food Systems." Tufts University. December 13, 2017. http://www.cs.tufts.edu/comp/116/archive/fall2017/nrussell.pdf.

accident due to a software or AI/data bug) could be launched with a software patch, simultaneously affecting thousands of installed appliances of a given brand or using a particular IoT dependent component. In this example the issue emanated from a legitimate software provider, thus further complicating security. Even apparently unrelated elements, such as smart appliances in widespread use in homes that could be vulnerable to a largescale attack, could pose a cyber-threat to food systems through impacts the electric grid, e.g., a well-timed manipulation of high energy-use appliances could overload the grid and cause widespread blackouts.[19]

Some experts in tech are optimistic that integration of the IoT with blockchain's ability to create a verified, distributed ledger will improve security and allow for more reliable data tracking across smart systems.[20] Because data stored and shared via the blockchain are encrypted and distributed across many verifying nodes, the possibility of a single point of failure is eliminated.[21] This decentralized format better matches IoT designs than the traditional server/client model of centralized data management. However, business leaders in food-system supply-chain management have noted that, while blockchain does offer innovations in *data management,* the prohibitive costs to improved supply-chain management in the food system actually occur in *data capture,* meaning that, until smart sensors and RFID technologies decrease in cost and spread across the industry, blockchain's distributed means of data management does not offer a cost-effective advantage over traditional techniques.[22] As new data capturing techniques become common, blockchain may provide improved security, but the variety of potential costs and benefits across industries and the food system are not fully understood. As more businesses attempt to integrate on the platform, a clearer picture of risks and rewards should emerge.[23]

---

[19] Greenberg, Andy. "How Hacked Water Heaters Could Trigger Mass Blackouts." Wired. August 13, 2018. https://www.wired.com/story/water-heaters-power-grid-hack-blackout/.
[20] Petracek, Nelson. "Is Blockchain The Way To Save IoT?" Forbes. July 18, 2018. https://www.forbes.com/sites/forbestechcouncil/2018/07/18/is-blockchain-the-way-to-save-iot/ - 24dae5865a74.
[21] Banafa, Ahmed. "A Secure Model of IoT with Blockchain." BBVA OpenMind. December 21, 2016. https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain.
[22] Hannum, Derek. "Blockchain in The Food Supply Chain – Tomorrow's Hope versus Today's Reality." Unpublished. ReposiTrak. 2018.
[23] Santhana, Prakash and Abhishek Biswas. "Blockchain risk management: Risk functions need to play an active role in shaping blockchain strategy." Deloitte. 2017. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-blockchain-risk-management.pdf.

The Dependency on Timely Agricultural Transportation and Processing

Few industries are so reliant on just-in-time transportation as American agriculture. At the front end, agricultural producers depend on timely transportation of seed, fuel, fertilizer, pesticides and herbicides to help ensure a productive crop can be planted and grown. On the back end, agricultural producers also depend on the timely transportation of harvested crops to processors to ensure crop quality is maintained prior to processing.[24] Finally, processors require the timely delivery of processed agricultural products, including fresh fruits and vegetables, to grocery stores for ultimate delivery to the consumer. Many of these food products are grown domestically, but many producers grow crops in other countries to provide a supply of fresh fruits and vegetables year round.[25]

In these systems, inventories are kept light, and much of the "inventory" is in transit at any one time. As a result, the presence in the system of large food distributors pose particular risks to the food system, as a cyber-infrastructure breach in just-in-time distribution settings could have seriously disruptive ripple effects across the supply chain. Sysco, for example, provides products to approximately 16% of the foodservice market. If the IT infrastructure running Sysco's network of more than 300 distribution facilities was disrupted, thousands of businesses relying on their products would feel the effects.[26]

---

[24] Blanton, Bruce. "The Importance of Transportation to Agriculture." USDA Agricultural Marketing Service. February 27, 2017. https://www.ams.usda.gov/reports/importance-transportation-agriculture.
[25] "Ocean Spray Cranberries, Inc. Acquires Cranberry Operations in Chile." Business Wire. January 10, 2013. https://www.businesswire.com/news/home/20130110005903/en/Ocean-Spray-Cranberries-Acquires-Cranberry-Operations-Chile.
[26] Sysco Corporation. "2017 Annual Report." 2017. http://investors.sysco.com/~/media/Files/S/Sysco-IR/documents/annual-reports/sysco-2017-annual-report-web.pdf.

Rapidly Developing Cyber Risks to America's Food System

In 2018, the US Council of Economic Advisers reported the agricultural sector experienced 11 cyber incidents in 2016.[27] Compared to other sectors such as transportation or manufacturing, the agricultural sector experienced a relatively low number of reported cyber incidents. While historical data show lower "likelihoods" of such attacks in the agricultural sector, the externalities of insufficient cyber protection, spillovers of attacks on linked sectors, and the growing implementation of cyber devices in general and in the agricultural sector in particular collectively suggest that the "severity" of any such incident or attack could be more profound in the near future. Cyber attacks such as the 2017 WannaCry ransomware and Petya malware illustrate the potential danger to American agriculture as smart technology is increasingly deployed. Operating systems in many countries were compromised as the ransomware and malware took control of internet-dependent operating systems that had not been properly updated with patches.[28] WannaCry victims, for example, found that files were encrypted and payment of a ransom of $300 in bitcoins was demanded, with the payment demand doubling after three days.

Fortunately for some users, decryption of the "frozen" data was possible without payment of the ransom in those attacks. However, this lucky result is not guaranteed for future ransomware attacks. A future attacker who is not motivated by immediate economic (extortion) goals, but rather by political or broader market manipulation goals, might not offer the ransom option, and simply "encrypt" the data to make in accessible for the operation of the equipment or system, period. This could simultaneously shut down vast swaths of infrastructure, including infrastructure necessary to run the food system.[29]

Indeed, if the hostile actor is more interested in disrupting smart systems at a time of conflict rather than collecting a financial benefit, decryption may not be possible. A case that is being widely considered at this time is hackers exploiting a common vulnerability to shut down combines across the country at peak harvest time. Smart

---

[27] The Council of Economic Advisers. "The Cost of Malicious Cyber Activity to the U.S. Economy." February 2018. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.
[28] "What You Need to Know about WannaCry Ransomware." Symantec. October 23, 2017. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.
[29] Verizon Enterprise Solutions. "2018 Data Breach Investigations Report." 2018. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf.

nutrient systems could be similarly vulnerable, with hackers, perhaps going undetected, able to manipulate fertilizer delivery systems to destroy crops, not nourish them, across a host of agricultural producers. Attacks may come from quarters not well anticipated, or given the interconnectedness of the system, have unexpected effects. One harbinger was the 2017 cyber-infrastructure meltdown in Maersk shipping – this case is spelled out in more detail below. A malware attack led the company to a complete IT shutdown, reverting to manual logistics as the full IT system was restored over a 10-day period. The attack caused a 20% drop in volumes and $300 million in losses to the company,[30] although insiders place this number closer to half a billion US dollars, and demonstrated how vulnerable distribution systems can be. What if a malware attack were simultaneously launched against an entire sector, rather than just a single company?

Interrelations across industries allow the consequences of a cyber-attack in one sector to ripple throughout the economy more broadly. Because of the food system's foundational role in all human activities and its "jaw-dropping vulnerabilities" (in the words of a U.S. intelligence analyst with extensive knowledge of this critical infrastructure), large shocks to production or distribution could result in particularly high spillovers to other key systems.

At the most extreme levels of food system disruption, "spillovers" would occur because human networks such as militaries, businesses and emergency response-teams require safe and plentiful food to function properly and a food shortage would challenge those capabilities. The disruptions need not be complete to disrupt national security interest. For example, an attack on the food system could limit supply, leading to higher prices for processors and consumers, and causing collateral drops in other forms of more typical business and consumer spending. Also, through commodity trading and derivative financial products, financial markets and food systems are closely tied at national and international levels. Serious disruptions to production and safety in heavily-traded primary commodities like cereal grains, seafood and coffee would ripple throughout the financial system,

---

[30] Saul, Jonathan. "Global shipping feels fallout from Maersk cyber attack." Reuters. June 29, 2017. https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE.

disrupting other operations and resource flows that are critical to national security and normal functioning of society.[31]

Lack of Cyber Insurance Coverage

With the abundant cyber risks involved in smart systems agriculture, one might reasonably assume that cyber insurance would be available and prevalent throughout the food system and its related industries. That is not the case. Cyber-insurance policies in agriculture have lagged in response to developing risks, and coverage remains relatively rare. There are various reasons for this lack of coverage. Constant developments in the applications of smart technologies, AI, and information-for-agriculture systems for decision-making, make it difficult for insurance carriers to predict and project future risks. Relatively few cyber-related claims have been filed to date from which such predictions and costs might be derived. For existing coverage, policy ambiguity remains an issue; it is not always simple to determine whether coverage for cyber events exists or not, and what policy it might be covered under.[32] This ambiguity is due, at least in part, from the continuing difficulties in characterizing threat, vulnerability, reliability and liability in cyber-physical systems that operate with many different inputs. These myriad inputs, and their potential for failure, confound the analysis of "causation" that is fundamental to the insurance underwriting business. Finally, part of the value of insurance coverage is that the insurer often provides risk analysis, training, and mitigation. When insurance isn't offered, that value doesn't enter the market. Protection against cyber threats in agricultural systems requires both insurers and producers to be fully apprised of risks—and this crucial development that has not yet occurred – or been possible, due in part to a lack of maturity of the measurements of risk factors associated with the "relationships" in which information "meaning" is derived. Metrics for system "edges" (as is proffered in the Univeristy of Washington IRRI "Atlas of Risk Maps") will help to fill this gap, supporting future insurance markets, and other risk-spreading market structures (like "derivatives" written on those risks, etc.).[33]

---

[31] "World Trade Statistical Review." World Trade Organization. 2017. https://www.wto.org/english/res_e/statis_e/wts2017_e/wts2017_e.pdf.

[32] McGoran, Jonathan. "Hacking the Food Supply." Risk and Insurance. March 27, 2018. http://riskandinsurance.com/hacking-the-food-supply/.

[33] David, Scott et al. "Atlas of Risk Maps." Unpublished. University of Washington, Applied Physics Laboratory Information Risk Research Initiative. July 7, 2018.

Slow Regulatory Response to the Use of Smart Devices

Unfortunately, there are few if any cybersecurity standards for the many smart devices being produced and placed into the stream of commerce. Also, these devices are produced internationally, straining application of one-nation's regulations to supply chains extended across borders. In response, U.S. Senators Mark Warner (D-Virginia) and Cory Gardner (R-Colorado) introduced S.1691, the Internet of Things (IoT) Cybersecurity Improvement Act of 2017, in August of 2017. This legislation is intended to "provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies" and has barely moved forward in the Congressional review process.[34]

The application of the "power of the purse" by federal government contracting (as is reflected in the legislation referenced above), can only do so much to drive "best practices" and standards in real-world supply chains. That government "purchasing push" is attenuated even further in the case of food systems, where the vast majority of the operating and administrative infrastructure is privately owned. As a result, a requirement for the government's own IoT purchases of such equipment to be secure will have minimal impact.

In that case, if the government cannot or will not regulate the interactions, it is up to the stakeholders involved to take care of themselves. It is, however, difficult for industry sectors within the food system (such as trade associations representing various types of equipment, crops, regions, etc.) to create "self-regulatory" structures to help mitigate the shared risks. Until there is market demand, competitive pressure or a critical event requires the adoption shared "best practices," or "standards" there will be little incentive for any one company, or group of companies in the vast food system apparatus, to internalize the costs of making changes that will negatively impact their bottom line, and potentially benefit and enrich their competitors.

---

[34] S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017. Senate Homeland Security and Governmental Affairs Committees. https://www.congress.gov/bill/115th-congress/senate-bill/1691/titles.

Fortunately, the nature of the cybersecurity challenges to the food system are sufficiently pervasive and "external" to the normal course of operations of all of the actors, that there is a strategic opportunity to join the parties together, by appeal to their self-interest, to self-bind to de-risking meta-structures that can help to mitigate shared threats and shared vulnerabilities in ways that none of them can achieve unilaterally. The urgencies and exigencies created by the perfect storm of cyber-in-security, food system complexity and interdependence, AI ascendance, and trade dynamics, offers ample opportunity for stakeholders to identify and mitigate risks at larger scales than previously attempted.

The Cyber Challenge for North American Agriculture

There is no evidence that North American agriculture is immune to cyber attacks or negative consequences of major cyber incidents. Due to the increasing use of smart devices in American agriculture and reliance on timely transportation and processing, the systemic risk to American agriculture is increasing. Cyber attacks (and cyber-accidents, acts of nature, and AI/autonomous systems) could disable and disrupt smart technology and smart decision-making systems to prevent the planting, cultivating, harvesting, transporting and processing of agricultural commodities that feed not only citizens of the United States, but also consumers across the globe. The secondary and tertiary effects of such "AAAA threats" would be felt in other critical systems upon which national security depends. Incentives for such an attack could vary. For example, as global tensions around agricultural trade rise[35], possibilities of economically or politically motivated cyber attacks once seen as unlikely could become tools of nation-states looking to boost their influence. Whatever rationale lies behind the attack (and whatever the other AAAA threat vector of the displacement), it is clear that these cybersecurity and "information risk" issues pose significant systems risks that are not well understood and require further evaluation, assessment, detection and mitigation.[36]

---

[35] Crampton, Liz. "Ag exports could be the losers in Trump tariffs." Politico. March 2, 2018. https://www.politico.com/newsletters/morning-agriculture/2018/03/02/ag-exports-could-be-the-losers-in-trump-tariffs-121586.

[36] Hawkins, Derek. "The Cybersecurity 202: Here's what security researchers want policymakers to know about the Internet of Things." The Washington Post. August 10, 2018. https://www.washingtonpost.com/news/powerpost/paloma/the-

Case Study: The A.P. Moller-Maersk Cyber Attack.

In 2017, Americans exported $140 billion in agricultural goods while importing $119 billion[37] through a variety of transportation modes, including trucking, rail, barge and ocean shipping. Fully 75% of American agricultural exports are shipped by ocean.[38] This expansive global trade system relies on complex logistical networks across sea, road, rail and air to fulfill demand. Widespread disruptions to the IT systems of logistics companies operating in agricultural markets would have severe economic and human consequences—delayed shipments would result in damaged or spoiled produce, leaving shelves empty and prices high.

In many cases, the extensive IT systems of logistics and transport companies are outdated and were not designed to protect against cyber threats. Similarly, crew members operating these systems often lack cyber-security training and sufficient on-ship IT support.[39]

The consequences of such vulnerabilities were realized in June of 2017 when the 'Petya' malware attack infected the IT networks of Danish shipping giant Maersk. The company, which is responsible for 15% of all global freight[40], reported $300 million in losses,[41] although industry insiders place this loss closer to half a billion U.S. dollars, as a result of a temporary shutdown of all Maersk IT systems. Ships could not be located at sea, nor could they be unloaded at port. All Maersk operations came to a standstill. It took 10 days for the company to restore all

---

cybersecurity-202/2018/08/10/the-cybersecurity-202-here-s-what-security-researchers-want-policymakers-to-know-about-the-internet-of-things/5b6c6ec91b326b020795603d/?utm_term=.9b57661ec6f7.

[37] "Value of U.S. agricultural trade, by fiscal year." USDA Economic Research Service. December 15, 2017. https://www.ers.usda.gov/data-products/foreign-agricultural-trade-of-the-united-states-fatus/fiscal-year/.

[38] Blanton, Bruce. "The Importance of Transportation to Agriculture." USDA Agricultural Marketing Service. February 27, 2017. https://www.ams.usda.gov/reports/importance-transportation-agriculture.

[39] Baker, Joe. Did the Maersk cyber attack reveal an industry dangerously unprepared? Ship Technology. November 8, 2017. https://www.ship-technology.com/features/maersk-cyber-attack-reveal-industry-dangerously-unprepared/.

[40] Milne, Richard. Maersk CEO Soren Skou on surviving a cyber attack. Financial Times. August 13, 2017. https://www.ft.com/content/785711bc-7c1b-11e7-9108-edda0bcbc928.

[41] Wienberg, Christian. Maersk Says June Cyberattack Will Cost It up to $300 Million. Bloomberg. August 16, 2017. https://www.bloomberg.com/news/articles/2017-08-16/maersk-misses-estimates-as-cyberattack-set-to-hurt-third-quarter.

systems by reinstalling more than 4,000 servers, 45,000 PCs, and 2500 applications.[42] The attack, which was reported to have been traced by the US Intelligence Community back to the Russian military,[43] was spread through business networks via a Ukrainian website providing updates to tax and accounting software. According to Maersk Chairman Jim Snabe, 'human resilience' and support from customers made it possible for Maersk eventually to cover 80% of shipping volume through manual systems while IT was down.[44] Such factors are reminders of the unpredictable nature of resilience and of the fact that systemic tipping points exist, after which losses could become catastrophic. If the attack had spread more widely across the transport sector and related industries, damage costs could have grown exponentially with spillovers wreaking havoc across multiple sectors and economies.

Conclusions

We present a few examples of potential cyber vulnerabilities in a familiar, but largely unconsidered context—the North American agriculture and food system. This is a "use case" that demonstrates the alarming nature of modern information risk in causing "unknown unknown" risks to appear (seemingly out of nowhere) in systems that are perceived to be stable by virtue of their historically "analogue" structure, and relatively isolated from the vagaries of fast-evolving information/communication technologies. However, food systems are revealing themselves to be increasingly dependent on information networks—the same information networks that are broadly recognized as spawning new risks in nearly every aspect of modern life. This forces examination of the potential impact of cyber-insecurity on food systems, that are foundational for human survival and the bedrock of social cohesion and security. Because North American agricultural exports feed the world, the vulnerabilities we describe in this paper that affect the U.S. homeland and the potential vulnerabilities of global shipping interests illustrate a key point: *Cyber vulnerabilities in national food systems may potentially have global scale impacts in a*

[42] Cimpanu, Catalin. "Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack." Bleeping Computer. January 25, 2018. https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/.
[43] Moss, Michael. "Cyber Threats to Our Nation's Critical Infrastructure." Statement for the Record, Senate Committee on the Judiciary: Subcommittee on Crime and Terrorism. August 21, 2018. https://www.dni.gov/index.php/ctiic-newsroom/item/1899-statement-for-the-record-mr-michael-moss-for-confirmation-before-the-senate-select-committee-on-crime-and-terrorism-to-be-deputy-director-of-the-cyber-threat-intelligence-integration-center.
[44] Cimpanu, Catalin. "Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack." Bleeping Computer. January 25, 2018. https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/.

host of different dimensions. We have provided some specific examples of instances where attacks have or could result in massive disruptions, both directly and indirectly in systems dependent on food.

As attention shifts from traditional notions of cybersecurity at "Perimeter 1.0" (i.e., the edge of the technology system) towards emerging notions of "information security" at "Perimeter 2.0" (i.e., the "meaning making" apparatus of institutional policies, laws and human behaviors), a variety of other threats and vulnerabilities, as well as mitigation strategies present themselves. Approaches such as education/training, policy and legal standards, third party certification, etc. can help to render those "meaning making" apparatus more reliable and predictable, offering improvements in leverage and enhancing risk mitigation for food systems information networks.

As interactions become increasing complex, and frequent, additional challenges will present themselves. In the earlier discussion, we just touched on the human and institutional challenges in processing mis-information, but we have not discussed the false assertion of food system vulnerabilities that can cause disruptions even without actually affecting food systems themselves. Consider the consequences if "fake news" was launched with an intention to set into motion panic about a food-borne contaminant or pathogen. While "Rumor Intelligence" (RUMINT) is a growing field in intelligence, these vulnerabilities remain poorly characterized and difficult to recognize and address. This is just an example of the new sorts of risks that are emerging as food systems and information systems become increasingly connected.

We note that cyber risk comes from a variety of sources (AAAA Threats), and it is sometimes difficult to separate or identify the source. Even when an intentional "attack" is suspected, cyber attacks often, even typically apply key tactics in the grey zone between conflicts, crimes, open warfare, or other threats. It is sometimes difficult to ascertain the motivation for the threat from the tactics employed. This further hampers the efforts to mitigate or respond to ambiguous cyber threats.

Also with the pervasiveness of smart devices, IoT, and connected infrastructure, these cyber-physical systems create a potential for direct and indirect physical harms when information systems are hijacked to cause the physical systems to operate outside of optimal parameters, presenting a hybrid threat. These attacks are

already occurring on large scale on the grid, shipping and other infrastructure that has the potential to affect food distribution, and could be much more deadly and disruptive if applied as a concerted tactic by an adversary.

In response to the developments of cyber risks in food-systems, it is necessary to engage with forward-looking risk assessment frameworks to manage and mitigate future risk before it occurs. Reactive strategies toward food-system risks are inadequate for ensuring a stable food supply and jeopardize lives and livelihoods in the United States and globally. The interconnected nature of food system risk requires analysis of relational data. For example, data on economic transfers between sectors, or near-real time imagery may represent key metrics and tactics that better enable the quantification and mitigation of cyber risks to the food system.

6. References and bibliography

Ali J, Santos JR, 2014. Modeling the ripple effects of IT-based disasters on interdependent economic systems, Systems Engineering, 18(2): 146-161.

Anderson CW, Santos JR, Haimes YY, 2007. A Risk-Based Input-Output Methodology for Measuring the Effects of the August 2003 Northeast Blackout, Economics Systems Research 19(2): 183-204.

Bureau of Economic Analysis, 2016. Input-Output Accounts Data. Available at: https://www.bea.gov/industry/io_annual.htm. Accessed: March 4, 2018.

Dietzenbacher E. and M.L. Lahr, Wassily Leontief and Input-Output Economics, Cambridge University Press, Cambridge, UK, 2004.

Haimes Y.Y. and P. Jiang, Leontief-based model of risk in complex interconnected infrastructures, Journal of Infrastructure Systems 7 (2001), no. 1, 1-12.

Isard, W., 1960. Methods of Regional Analysis: an Introduction to Regional Science. Cambridge, MA: MIT Press.

Leontief, W.W., 1951. The Structure of the American Economy, 1919-1939, Second Edition. New York, NY: Oxford University Press.

Leontief, W.W., 1966. Input-Output Economics. New York, NY: Oxford University Press.

Miller RE, Blair PD. Input-output analysis: foundations and extensions. Cambridge University Press, 2009.

Nippon Telegraph and Telephone Corporation (NTT) “Business Management and Cybersecurity- digital resiliency for executives” Sinichi Yokohama, 2018

OECD “Enhancing the Role of Insurance in Cyber Risk Management”, December, 2017

Okuyama Y, Santos JR, 2014. Disaster impact and input-output analysis, Economic Systems Research, 26(1): 1-12.

Orsi MJ, Santos JR, 2010. Probabilistic modeling of workforce-based disruptions and input-output analysis of interdependent ripple effects, Economic Systems Research, 22(1): 3-18.

Resurreccion JZ, Santos JR, 2013. Uncertainty modeling of hurricane-based disruptions to interdependent economic and infrastructure systems, Natural Hazards, 69(3): 1497-1518.

Santos J. R. and Y. Y. Haimes, Modeling the demand reduction input-output (i-o) inoperability due to terrorism of interconnected infrastructures *, Risk Analysis 24 (2004), no. 6, 1437-1451.

Santos JR, 2006. Inoperability Input-Output Modeling of Disruptions to Interdependent Economic Systems, Systems Engineering, 9(1): 20-34.

Santos JR, Herrera, LC, Yu KDS, Pagsuyoin SA, Tan RG, 2014. State of the Art in Risk Analysis of Workforce Criticality Influencing Disaster Preparedness for Interdependent Systems, Risk Analysis, 34(6): 1056-1068.

Santos JR, Pagsuyoin SA, Herrera, LC, Tan RG, Yu KDS, 2014. Analysis of Drought Risk Management Strategies using Dynamic Inoperability Input-Output Modeling and Event Tree Analysis, Environment, Systems and Decisions, 34(4): 492-506.

Santos JR, Yu, KDS, Pagsuyoin, SA, Tan RR, 2014. Time-varying recovery model for interdependent economic systems using hybrid input-output and event tree analysis, Economic Systems Research, 26(1): 60-80.

Swiss Re (2017), "Cyber: getting to grips with a complex risk", sigma, No. 1/2017

Toregas “Framework for growth in Cybersecurity Insurance” forthcoming in National Association of Insurance Commissioners, 2018

Toregas, "Your Data Is Compromised. (Yes, Yours.) What Now?," National Journal, July 14, 2015.

Toregas, Nicolas Zahn, "Insurance for Cyber Attacks: The Issue of Setting Premiums in Context," Report GW-CSPRI-2014-1, January 7, 2014.

US Census Bureau, 2017. American Community Survey Content Test Evaluation Report: Journey to Work – Travel Mode of Commute and Time of Departure for Work. Available at https://www.census.gov/content/dam/Census/library/working-papers/2017/acs/2017_McKenzie_01.pdf

US Department of Commerce, Regional Multipliers: A User Handbook for the Regional Input-Output Modeling System, U.S. Government Printing Office, Washington, DC, 1997.