WHITE PAPER

Cyber Risk and Security Implications in Smart Agriculture and Food Systems

Jahn Research Group
University of Wisconsin–Madison
College of Agriculture and Life Sciences
January, 2019

Authors[1]

Dr. Molly M. Jahn[a], William L. Oemichen[a], Dr. Gregory F. Treverton[b], Scott L. David[c], Matthew A. Rose[d], Max A. Brosig[e], Dr. Buddhika "Jay" Jayamaha[a], William K. Hutchison[a], Braeden B. Rimestad[a]

[1] Detailed author bios are included in the appendix. [a] Jahn Research Group, University of Wisconsin-Madison, Department of Agronomy. [b] University of Southern California, School of International Relations. [c] University of Washington, Applied Physics Laboratory. [d] U.S. Department of Defense. [e] WI National Guard and U.S. Army War College.

We thank the following colleagues for their insights and review: Major Jahara "Franky" Matisek (USAF); Dr. Will Reno, Northwestern University; Lt. Col. Jennifer J. Snow (USAF); Sara-Jayne Terp, SOFWERX Affiliate; and Dr. Jen Ziemke, John Carroll University. The authors remain responsible for any and all errors.

Table of Contents

Introduction

Rapid changes in American agriculture and the ways in which food is produced and distributed are opening new and often unappreciated cyber attack vectors with unappreciated economic and security implications. 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 same vulnerabilities also make food systems highly vulnerable to hybrid warfare tactics of both state and non-state actors.[1] 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.[2] 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,[3] (2) vertical integration through the food supply chains in which agricultural producers may also directly process agricultural commodities, e.g., milk, into dairy products, e.g., cheese and yogurt, directly supplying supermarkets and grocery stores,[4] (3) widespread lack of compliance with food safety, traceability and insurance requirements, (4) rapidly advancing use of "smart technology" throughout supply chains,[5] (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 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),

---

[1] Hybrid warfare tactics deploy an array of both military and non-military subversive tactics to alter the strategic and tactical space while staying below the threshold of active warfare.
[2] "The Global Risks Report 2018: 13th Edition." World Economic Forum. April, 2018. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.
[3] "Three Decades of Farm Consolidation." USDA Economic Research Service. March 2018. https://www.ers.usda.gov/webdocs/publications/88057/eib189_summary.pdf?v=43172.
[4] "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.
[5] "Logistics 4.0: How IoT is Transforming the Supply Chain." Forbes. June 14, 2018. https://www.forbes.com/sites/insights-inteliot/2018/06/14/logistics-4-0-how-iot-is-transforming-the-supply-chain/ - 34dd4dd4880f.

it is not inconceivable given the potential vulnerabilities we highlight below that the attack could be "lucky" and cause real damage with cascading effects throughout the system. We conclude 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 interacting over time have generated the trend toward smart technologies in agriculture. In the last 60 years, interconnections between new technologies, commodity markets, diet preferences, and population dynamics have dramatically changed the face of American agriculture. In 1960 there were roughly 4 million farms in the United States, in 2015 there were a little over 2 million.[6] The total area of farmed land decreased only slightly in that time, meaning that the average farmer in 2015 farmed 444 acres, compared to less than 300 acres per farmer in 1960. Despite farming less land, productivity gains in American agriculture have allowed for 2.5 times greater overall output in 2015 than in 1960.[7] Data from 2012's agricultural census showed that, of the roughly 325 million acres of harvested cropland,[8] 96 million acres were devoted to corn, 76 million acres were devoted to soy, and 56 million acres were devoted to wheat.[9] Productivity growth in these staple commodities has been particularly strong in the last 50 years—bushels of corn per acre have increased 2.5 times since 1961, and soy and wheat yield have also more than doubled during that time.[10]

The development of "smart" agricultural systems can be seen as the continuation of a trend toward larger scale and technology-driven productivity gains in farming. The relationship between between price and productivity dictates a large portion of this trend: technological advancements enable more efficient production of staple crops, which leads to greater total output and, as a result, lower commodity prices. To stay competitive in the low-price markets, farms continually invest in new technologies. As the data suggest, smaller farms face greater difficulties staying viable in low-price markets, and are often consolidated into larger ventures. In this analysis, low prices are self-perpetuating: as each farmer strives to produce more per acre, overall output increases, maintaining saturated markets with low commodity prices.[11] Because agricultural producers typically operate as price-takers, the individual farm is ill-equipped to intervene in this cycle, and average per-acre productivity continues to rise despite commodity

[6] USDA. "The number of farms has leveled off at about 2.05 million." *United States Department of Agriculture – Economic Research Service*. 2018. https://www.ers.usda.gov/data-products/chart-gallery/gallery/chart-detail/?chartId=58268.
[7] USDA. "Productivity growth is still the major driver of U.S. agricultural growth." *United States Department of Agriculture – Economic Research Service*. 2017. https://www.ers.usda.gov/data-products/chart-gallery/gallery/chart-detail/?chartId=58284.
[8] Bigelow, Daniel. "A Primer on Land Use in the United States." *United States Department of Agriculture – Economic Research Service.* 2017. https://www.ers.usda.gov/amber-waves/2017/december/a-primer-on-land-use-in-the-united-states/.
[9] USDA. "Acreage." *United States Department of Agriculture – National Agricultural Statistics Service.* 2012. http://usda.mannlib.cornell.edu/usda/nass/Acre/2010s/2012/Acre-06-29-2012.pdf.
[10] FAO. "FAOSTAT: Crops." *Food and Agriculture Organization of the United Nations.* 2016. http://www.fao.org/faostat/en/ - data/QC.
[11] MacDonald, James M., Robert A. Hoppe, Doris Newton. "Three Decades of Consolidation in U.S. Agriculture." *United States Department of Agriculture – Economic Research Service*. 2018. https://www.ers.usda.gov/webdocs/publications/88057/eib-189.pdf?v=43172.

prices that have trended steadily downward over the last 60 years.[12] Large scale interventions like Farm Bill programs and the Renewable Fuel Standard (also known as the ethanol mandate) have attempted to offer financial relief for farmers, but have not been sufficient in mitigating the overall decline of prices. The USDA predicts only a modest uptick in staple commodity prices by 2026.[13]

As a function of this economic backdrop, farmers are virtually required to pursue higher per-acre productivity and lower operating costs.[14] The pursuit of those goals in the face of challenging environmental and market conditions has generated the recent demand for highly-connected "smart" devices in agriculture and throughout the food supply chain, including "smart markets" and smart production and distribution systems. As these technologies continue to proliferate, 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.

The Trend Towards Smart Farming

The adoption of these technologies has precipitated what might be called 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[15] with the overall goal of increasing production per acre through more efficient use of inputs including seed, water, crop nutrients, herbicides and pesticides.[16] Taken together, smart technology, smart markets, and precision agriculture deliver game-changing advances in agriculture favored by those financing and insuring the industry, as well as those processing harvested crops into a wide variety of food products for retail sale. Such financiers and insurers still apply traditional measures of economic risk, such as those based on efficiency and productivity.[17] However, these technology shifts, and the un-measured, uncharacterized dependencies that they engender, 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

---

[12] USDA. "Inflation-adjusted price indices for corn, wheat, and soybeans show long-term declines." *United States Department of Agriculture – Economic Research Service*. 2016. https://www.ers.usda.gov/data-products/chart-gallery/gallery/chart-detail/?chartId=76964.

[13] USDA. "USDA Agricultural Projections to 2026." *United States Department of Agriculture – Interagency Agricultural Projections Committee.* 2017. https://www.usda.gov/oce/commodity/projections/USDA_Agricultural_Projections_to_2026.pdf.

[14] USDA. "Agricultural Productivity in the US: Table 1. Indices of farm output, input, and total factor productivity for the United States, 1948-2015." *United States Department of Agriculture – Economic Research Service.* 2017. https://www.ers.usda.gov/webdocs/DataFiles/47679/table01.xlsx?v=2945.1.

[15] "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.

[16] 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.

[17] "Agricultural Finance & Agricultural Insurance." The World Bank. February 2, 2018. http://www.worldbank.org/en/topic/financialsector/brief/agriculture-finance.

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 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.[18] 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.[19]

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 agricultural 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 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.[20]

---

[18] 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.

[19] "Russian hacking could affect U.S. ag." Feedstuffs.com. July 3, 2018. https://www.feedstuffs.com/news/russian-hacking-could-affect-us-ag.

[20] "Threats to Precision Agriculture." Department of Homeland Security, Public-Private Analytic Exchange Program. October 3, 2018. https://www.dhs.gov/sites/default/files/publications/2018 AEP_Threats_to_Precision_Agriculture.pdf.

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.[21] 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.

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.[22] Blue chip technology firms, such as Microsoft, are investing heavily in this area due to apparent market drivers.[23] 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

[21] "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.
[22] Ravindra, Savaram. "IOT Applications in Agriculture." IOT for All. January 3, 2018. https://www.iotforall.com/iot-applications-in-agriculture/.
[23] 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/.

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.[24]

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 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 generally 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).[25] Across industries, these networks are prime targets for

[24] 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.

[25] Russell, Nicholas. "Cybersecurity and Our Food Systems." Tufts University. December 13, 2017. http://www.cs.tufts.edu/comp/116/archive/fall2017/nrussell.pdf.

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.[26] 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—potentially overwhelming health care systems in the most heavily affected regions.

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 facilities where levels of essential chemicals like chlorine could be manipulated to contaminate the water supply.[27] 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.[28] Such an attack (or 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 large-scale attack, could pose a cyber-threat to food systems by negatively impacting the electric grid, e.g., a well-timed manipulation of high energy-use appliances could overload the grid and cause widespread blackouts.[29]

Some tech experts 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.[30] 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.[31] This

---

[26] 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/.

[27] 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/.

[28] Russell, Nicholas. "Cybersecurity and Our Food Systems." Tufts University. December 13, 2017. http://www.cs.tufts.edu/comp/116/archive/fall2017/nrussell.pdf.

[29] 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/.

[30] 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.

[31] Banafa, Ahmed. "A Secure Model of IoT with Blockchain." BBVA OpenMind. December 21, 2016.

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.* Therefore, until smart sensors and RFID technologies decrease in cost and spread more widely across the supply-chain, blockchain's distributed means of data management does not provide a cost-effective advantage over traditional techniques.[32] 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.[33]

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.[34] Finally, grocery retailers require the timely delivery of processed agricultural products, along with fresh fruits and vegetables, 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.[35] 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 behind Sysco's network of more than 300 distribution facilities was disrupted, thousands of businesses relying on their products would feel the effects.[36]

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.[37] Compared to other sectors such as transportation or manufacturing, the

https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain.

[32] Hannum, Derek. "Blockchain in The Food Supply Chain – Tomorrow's Hope versus Today's Reality." Unpublished. ReposiTrak. 2018.

[33] 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.

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

[35] "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.

[36] Sysco Corporation. "2017 Annual Report." 2017. http://investors.sysco.com/~/media/Files/S/Sysco-IR/documents/annual-reports/sysco-2017-annual-report-web.pdf.

[37] 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.

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 suggests 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.[38] 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 it inaccessible for the operation of the equipment or system. This could simultaneously shut down vast swaths of infrastructure, including infrastructure necessary to support the food system.[39]

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 like this could occur, for example, if hackers exploited a common vulnerability to shut down smart combines across the country at peak harvest time. Smart nutrient systems could be similarly vulnerable, with hackers, perhaps going undetected, able to manipulate fertilizer delivery systems to destroy rather than nourish crops 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,[40] 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.

---

[38] "What You Need to Know about WannaCry Ransomware." Symantec. October 23, 2017. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.

[39] Verizon Enterprise Solutions. "2018 Data Breach Investigations Report." 2018. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf.

[40] 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.

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, disrupting other operations and resource flows that are critical to national security and normal functioning of society.[41]

Lack of Cyber Insurance Coverage

With the abundant cyber risks involved in smart systems agriculture, one might 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 and narrow in scope. 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.[42] 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, and the farmer bears the full cost of the risk and any measures taken against it. 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 University 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.).[43]

[41] "World Trade Statistical Review." World Trade Organization. 2017. https://www.wto.org/english/res_e/statis_e/wts2017_e/wts2017_e.pdf.
[42] McGoran, Jonathan. "Hacking the Food Supply." Risk and Insurance. March 27, 2018. http://riskandinsurance.com/hacking-the-food-supply/.
[43] 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 the 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.[44]

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 requiring the adoption of 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.

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-insecurity, 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. "AAAA threats" (cyber-attacks, cyber-accidents, acts of nature, and

[44] 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.

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,[45] the weaponization of unprotected cyber infrastructures could become a key tactic for adversarial nation-states looking to boost their economic or political 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.[46]

Potential Risk Scenarios

Disruption of Livestock Health Monitoring Data

The international market for wearable smart technology for animals has increased significantly in recent years, with a continuing increase from $900 million to $2.5 billion dollars estimated in the next 10 years.[47] This trend can be attributed to increased focus in food system traceability along with recent laws like the Traceability for Livestock Moving Interstate rule, which was finalized in 2013.[48] Varying types of connected sensors are now used, including bolus tags, ear tags, leg bands, and collars. These monitoring systems track animal identification, location, and health. Varying smart monitoring systems have the ability to detect or analyze many indicators for disease like sweat constituents, body temperature, movement and behavior, stress, sound, and pH, with some systems having the ability to detect viruses or pathogens themselves.[49] Smart monitoring can provide a great benefit in the prevention of disease spread, but there are also risks associated with increased reliance on these smart monitoring systems: a cyber attack designed to destroy or garble data on disease detection and treatment. Such an attack would, at least, deliver economic consequences of undocumented, potentially unsaleable animals. At worst, a mishandled data disruption could lead to the undetected spread of a transboundary animal disease like foot-and-mouth disease (FMD). For example, because an animal with a disease will often have a high temperature long before other signs of disease appear, temperature signals are often used as disease indicators.[50] A cyber attack strategically altering an animal's reported temperatures could allow a

---

[45] 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.

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

[47] Neethirajan, Suresh. "Recent advances in wearable sensors for animal health management." *Sensing and Bio-Sensing Research*. 2017. https://reader.elsevier.com/reader/sd/pii/S2214180416301350?token=E91FDCB6EAC385F612DF54BE544084221E57E688403AB0483D7018F16D5B580DEF91F5B177F5F34C541F89645C41925C - pfe.

[48] USDA. "Animal Disease Traceability." *United States Department of Agriculture: Animal and Plant Health Inspection Service*. 2018. https://www.aphis.usda.gov/aphis/ourfocus/animalhealth/SA_Traceability.

[49] Ibid.

[50] Activeherd. "Livestock Tracking System." *NFC Group*. 2018. https://www.tracks360.com/asset-tracking-solutions/asset-tracking-applications/livestock-tracking-system/.

high-risk disease to go undetected in a herd. Data on disease prevention could also be altered through a cyber attack, as a hacker could alter vaccine or treatment data, confusing which animals have been treated and which have not. The manipulation of data for a high-risk animal could have consequences across an entire herd. The implications of undetected FMD are particularly extreme because of the highly contagious nature of the disease. FMD can be transmitted directly and indirectly, with airborne transmission being especially problematic when climate conditions are favorable or when large numbers of animals are grouped in close proximity. By air, the FMD virus can travel up to 10 kilometers over land and has travelled up to 250 kilometers over water.[51] Animals can hold and transmit the disease for four days before open signs are shown, and animals have high morbidity rates in disease free regions.[52] If a data breach were to cause mistreatement of infected animals, the rapid and undetectable transmission of FMD could result in widespread contamination, with particularly high morbidity rates in naive regions. The economic effects of such a contagion could be substantial. Estimates of the cost of an FMD outbreak in a region with no built-up immunity are over $1.5 billion a year—with direct impacts to farmers by way of lost production, lower weight gains, dead animals, fertility problems, delays in sales, and changes in herd structure.[53] The risk of such an outbreak may remain low, but without appropriate cyber security measures, malicious actors targeting livestock health data could seriously disrupt management and transportation protocol and spur a cascading animal health event.

Disinformation Campaigns Targeting Perceptions of Food Safety

In a dynamic social media environment, information cannot always be easily parsed as valid or invalid. Despite algorithmic and human monitoring, there remains a significant volume of disinformation in online media systems. Such disinformation, often dubbed "fake news," is largely designed to fan political divisions, but consequences spill across the information ecosystem—particularly, the rise of fake news has decreased trust in traditional media outlets.[54] These two trends—the capacity for disinformation on social media, and the degradation of traditional media outlets—creates an environment where carefully-crafted rumours could become viral and influence the behaviors of civilians unable to distinguish between real and false information. In a food systems context, this might look like strategically crafted and disseminated rumours about food safety. If a large enough effort were conducted by malicious actors (and "bot" accounts of their creation) a critical mass of disinformation could arise, prompting a widespread scare about the safety of certain food products. In some cases, this is already occurring—in 2018, social media "bots" linked to Russian disinformation campaigns attempted to stoke health concerns about GMO crops and herbicide use in U.S. agriculture.[55] Potent manufactured crises outside of the food system demonstrate the possibility of such attacks affecting agriculture in the United States. Take, for example, a 2014 hoax about the Columbian Chemicals plant in St. Mary Parish, Louisiana. This

[51] Aftosa, Fiebre. "Foot and Mouth Disease." *Iowa State University – Center for Food Security and Public Health*. 2015. http://www.cfsph.iastate.edu/Factsheets/pdfs/foot_and_mouth_disease.pdf.
[52] Ibid.
[53] Knight-Jones, T.J.D and J. Rushton. "The economic impacts of foot-and-mouth disease—What are they, how big are they and where do they occur?" *National Institues of Health*. 2013. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3989032/.
[54] West, Darrell M. "How to combat fake news and disinformation." *The Brookings Institute.* 2017. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.
[55] "How the Agriculture Industry is Impacted by Disinformaiton." *New Knowledge*. 2018. https://www.newknowledge.com/articles/how-the-agriculture-industry-is-impacted-by-disinformation/.

disinformation campaign, also linked to Russian efforts, was executed across a number of social media platforms and published hundreds of fabricated accounts of a toxic explosion at the chemical plant. Photos and videos were edited to make accounts appear credible, and posts were strategically directed at reporters, politicians and local leaders to achieve maximum impact. Statements were later released by local authorities and management at the plant to confirm that no such explosion had occurred.[56] Similar disinformation campaigns attacking food systems in the U.S. could be generated on ideological grounds by non-state actors, or could potentially be waged as a hybrid tactic by an unfriendly state attempting to incite instability or distrust within a vital infrastructure. In response to criticism following widespread disinformation campaigns during and after the 2016 elections, Facebook and other social media platforms have escalated efforts to control such behavior.[57] State and federal governments have also engaged in the monitoring of public social media data for homeland security purposes, though this activity has come under both internal[58] and external[59] scrutiny over concerns of effectiveness and personal freedom. Values of privacy and open dialogue will continue to evolve in tension with the challenges of disinformation and coordinated propaganda as companies and governments learn to manage risks in the changing media environment. Campaigns to destabilize perceptions of food safety are one of many channels that malicious actors may utilize as they attempt to generate physical consequences from online media systems.

Frontiers in Connectivity: Fifth Generation (5G) Wireless Networks

The key threats described above have been primarily considered in the context of the current connectivity environment—that is traditional networks of internet cables and wi-fi routers, and more recent 4G networks of data-equipped cellular towers. The connective capacities of these technologies, particularly the development and proliferation of 4G networks over the last decade, allow for much of the mobile and IoT capabilities that present the rapidly growing risks and benefits across the food system. The next rendition of broadband cellular network technologies, collectively known as 5G networks, have been developed and experimentally deployed across the United States and other countries around the globe. The capabilities of 5G technologies are promoted as superior to 4G networks in both speed and bandwidth diversity, enabling download speeds 10 to 20 times faster, with decreased latency time between devices, enabling advancements in connected systems like self-driving cars and robotic networks.[60] With the improved speed and capacity for interconnectivity, economic returns on IoT systems and other capabilities will increase, encouraging further expansion of smart systems. In the development of 5G systems, the security flaws of prior generations were taken into account. Paricularly, 5G networks will not require the central hubs necessary in previous networks. This distributed or "virtualized" structure,

[56] Chen, Adrian. "The Agency." *New York Times Magazine*. https://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.
[57] Mak, Tim. "As Midterms Approach, Facebook Ramps Up Disinformation Fight." *National Public Radio.* 2018. https://www.npr.org/2018/10/18/658376619/as-midterms-approach-facebook-ramps-up-disinformation-fight.
[58] OIG. "DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted)." *Office of Inspector General.* 2017. https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.
[59] McCullough, Kimberly. "Why Government Use of Social Media Monitoring Software is a Direct Threat to Our Liberty and Privacy." *American Civil Liberties Union.* 2016. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/why-government-use-social-media-monitoring.
[60] Al-Falahy, Naser and Omar Y. Alani. "Technologies for 5G Networks: Challenges and Opportunities." IT Professional. 2017. https://ieeexplore.ieee.org/abstract/document/7839836.

with integrated software and hardware systems, will enable increased authentification across networks, with potential for improved data and threat monitoring capabilities at each node.[61,62] However, the increased traffic and complexity of 5G systems will also bring seen and unforeseen challenges, including increasingly diverse security demands and heightened privacy concerns.[63] As both technologies and regulations continue to evolve, a continuous and dynamic cycle of threats, failures and responses will unfold as users, providers and malicious actors across sectors pursue their goals in the new IT environment.

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

In 2017, Americans exported $140 billion in agricultural goods while importing $119 billion[64] through a variety of transportation modes, including trucking, rail, barge and ocean shipping. Fully 75% of American agricultural exports are shipped by ocean.[65] 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.[66]

The consequences of such vulnerabilities were realized in June of 2017 when the 'NotPetya' malware attack infected the IT networks of Danish shipping giant Maersk. The company, which is responsible for 15% of all global freight[67], reported $300 million in losses,[68] 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 systems by reinstalling more than 4,000 servers, 45,000 PCs, and 2500 applications.[69] The attack, which was

[61] Abdelwahab, Sherif, Bechir Hamdaoui, Mohsen Guizani and Taieb Znati. "Network function virtualization in 5G." *IEEE Communications Magazine*. 2016. https://ieeexplore.ieee.org/abstract/document/7452271.
[62] Ahmad, Ijaz, Tanexh Kumar, Madhusanka Liyanage and Andrei Gurtov. "Overview of 5G Security Challenges and Solutions." *IEEE Communications Standards Magazine.* 2018. https://www.researchgate.net/publication/322753634_Overview_of_5G_Security_Challenges_and_Solutions.
[63] Nokia. "Bell Labs Consulting report finds human demand for a digital future anywhere can only partially be met by networks in 2020." *Nokia – Bell Labs.* 2016. https://www.nokia.com/en_int/news/releases/2016/04/13/bell-labs-consulting-report-finds-human-demand-for-a-digital-future-anywhere-can-only-partially-be-met-by-networks-in-2020.
[64] "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/.
[65] Blanton, Bruce. "The Importance of Transportation to Agriculture." USDA Agricultural Marketing Service. February 27, 2017. https://www.ams.usda.gov/reports/importance-transportation-agriculture.
[66] 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/.
[67] 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.
[68] 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.
[69] 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/.

reported to have been traced by the US Intelligence Community back to the Russian military,[70] 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.[71] 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. The examples included in this study demonstrate 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. Now, however, food systems are becoming 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 reach across the world, the vulnerabilities we describe in this paper that affect both the U.S. homeland and global shipping interests illustrate a key point: *Cyber vulnerabilities in national food systems may potentially have global scale impacts in a 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" apparatuses more reliable and predictable, offering improvements in leverage and enhancing risk mitigation for food systems information networks.

As interactions become increasingly 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.

---

[70] 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.

[71] 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/.

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. Advancements in genome editing present similar challenges—the development of viral bio-technologies capable of damaging crops outpaces our ability to detect and respond to these new threats.[72] These are just examples of the new sorts of risks that emerge as new technologies develop and food 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 deadlier and more disruptive if applied as a concerted tactic by an adversary.

Given the interconnected nature of food systems risk, effective anticipation and response 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.

By engaging with relational data and forward-looking risk assessment frameworks, food system actors will be better-equipped to manage and mitigate future risks before they occur. Such advancements are necessary to move beyond reactive risk management strategies to ensure a more stable food supply in the United States and globally.

[72] Reeves, R.G., S. Voeneky, D. Caetano-Anollés, F. Beck, C. Boëte. "Agricultural research, or a new bioweapon system?" *Science.* http://science.sciencemag.org/content/362/6410/35.

APPENDIX – Author Bios

Dr. Molly M. Jahn
Professor, University of Wisconsin-Madison; Adjunct Research Scientist, Columbia University, Guest Scientist, Los Alamos National Laboratory; NASA Earth Observations for Food Security and Agriculture Consortium

William L. Oemichen, J.D.
Senior Research Fellow in Food Systems Security, Jahn Research Group, University of Wisconsin-Madison; former Director of the Office of Preparedness & Emergency Health Care at the Wisconsin Department of Health Services; Administrator of the Trade & Consumer Protection Division at the Wisconsin Department of Agriculture; and Deputy Minnesota Agriculture Commissioner

Dr. Gregory F. Treverton
Professor of Practice of International Relations, University of Southern California; former Chair of the U.S. National Intelligence Council (NIC)

Scott L. David, J.D.
Director of Policy at the Center for Information Assurance and Cybersecurity at University of Washington Applied Physics Lab; former Executive Director of the Law, Technology and Arts Group at University of Washington School of Law

Matthew A. Rose
Defense Intelligence Officer, U.S. Department of Defense; Civilian in the Defense Intelligence Agency; U.S. Army War College resident class of 2018

Max A. Brosig
Wisconsin National Guard; U.S. Army War College resident class of 2018

Dr. Buddhika "Jay" Jayamaha
Assistant Research Scientist at the Jahn Research Group, University of Wisconsin-Madison, Department of Agronomy

William K. Hutchison
Research Specialist at the Jahn Research Group, University of Wisconsin-Madison, Department of Agronomy

Braeden B. Rimestad
Research Assistant at the Jahn Research Group, University of Wisconsin-Madison, Department of Agronomy