Food Supply Chain Cyber Threats: A Scoping Review

Janne Alatalo(✉), Tuomo Sipola, and Tero Kokkonen

Institute of Information Technology,
Jamk University of Applied Sciences,
Jyväskylä, Finland
{janne.alatalo, tuomo.sipola, tero.kokkonen}@jamk.fi

Abstract. Cyber attacks against the food supply chain could have serious effects on our society. As more networked systems control all aspects of the food supply chain, understanding these threats has become more critical. This research aims to gain a better understanding of the threat landscape by reviewing the existing literature about the topic. Previous research concerning food supply chain cyber threat was surveyed using the scoping review method. In total, 43 research articles focusing on different parts of the food supply chain were reviewed and summarized in this study. The most prominent identified cybersecurity topics include smart farming, cyber-physical systems, threats against industrial control systems and old unmaintained software.

Keywords: Food Supply Chain, Critical Infrastructure, Cybersecurity

Introduction

As an industry that affects the everyday life of everyone worldwide, the food supply chain is one of the most critical functions of a society. A.H. Lewis wrote already in 1896: *"the only barrier between us and anarchy is the last nine meals we've had"* [32]. Actors in the food supply vary from individual farms to logistic companies, food production companies and retail chains. Farm to Fork Strategy for a fair, healthy and environmentally-friendly food system, released by European Commission, states that *"The COVID-19 pandemic has underlined the importance of a robust and resilient food system that functions in all circumstances, and is capable of ensuring access to a sufficient supply of affordable food for citizens"* [19]. Systems and actors of the food supply can be valuable targets for a cyber attack because literally every human is dependent on food. Indeed, EU's Cybersecurity Strategy for the Digital Decade [20] and EU's directive on the resilience of critical entities [21] acknowledge the importance of farming, food production, processing and distribution. Similarly, a private industry notification from the FBI states that since 2021 ransomware attacks have impacted agricultural cooperatives and warns about probable ransomware attacks against agricultural cooperatives during the upcoming plant and harvest season [23].

The original article appeared as: Janne Alatalo, Tuomo Sipola and Tero Kokkonen. "Food Supply Chain Cyber Threats: A Scoping Review." In: Information Systems and Technologies. WorldCIST 2023. Ed. by Álvaro Rocha, Hojjat Adeli, Gintautas Dzemyda, Fernando Moreira and Valentina Colla. Vol. 801. Lecture Notes in Networks and Systems. Cham, Switzerland: Springer, 2024, pp. 94–104. DOI: 10.1007/978-3-031-45648-0_10

There are several networked software and hardware components included in this system of systems [33], for example, automated robotic logistic systems, food production systems, refrigeration machines and milking robots. A cyber attack against one point of this crucial chain may cause cascade effects and deny the usage of the whole food supply chain [52]. Factors such as industrial espionage, criminal intent and hostile state activities could present motivations for various attacks. News outlets have already described attacks against advanced smart farming machinery [36], and, e.g., a ransomware attack against AGCO corporation [2]. Futhermore, Bowcut lists some notable cyber attacks against food and agriculture actors in 2020 and 2021 and introduces a case study of ransomware against the food company JBS in 2021 [11].

Related work in this research topic includes Latino and Menegoli, who have conducted a systematic literature review in the topic of "cybersecurity in the food and beverage industry" [31]. They used thematic analysis to analyze the results and built a reference framework for future research and for identifying the future research directions. They used Scopus knowledge database for finding the relevant articles with a final sample of 17 studies that were included in the final analysis. The small number of analyzed articles is probably the result of strict exclusion criteria that are dictated by the restrictions in the research methodology chosen by the authors. Although the topic of our paper is very similar to this paper, our scoping study research methodology is more flexible giving us the freedom to include many more studies into the final analysis. That way we bring more complete overview of the existing research about the topic and contribute new knowledge to the research area.

Methods

Our research question in this study is: "What literature exists about the food supply chain cybersecurity?" We wanted to get a high level overview of existing research about cybersecurity in food supply chain. For this purpose, the scoping review methodology was chosen [40]. We used the methodological framework defined by Arksey and O'Malley in [6] as the basis for our research. The framework is flexible enough to cast a wide enough net over the wide topic of food supply chain cybersecurity, and it allows us to use an iterative method to converge on the right keywords to identify the relevant studies.

The review started by searching all types of literature using general search terms encompassing the whole wide topic. The literature found this way was used to identify more keywords that are often used in specific parts of the food supply chain literature. The new keywords were added to the list of the searched keywords, and the process was iterated until the topic was sufficiently covered. In the end, the search phrases were constructed from the keywords by combining terms referring to the food supply chain: "food industry", "food production", "food production chain", "food logistics", "smart farming", "agribusiness", "food retail" and "catering industry", with a term that specifies the cybersecurity focus: "cybersecurity" and "cyber attacks".

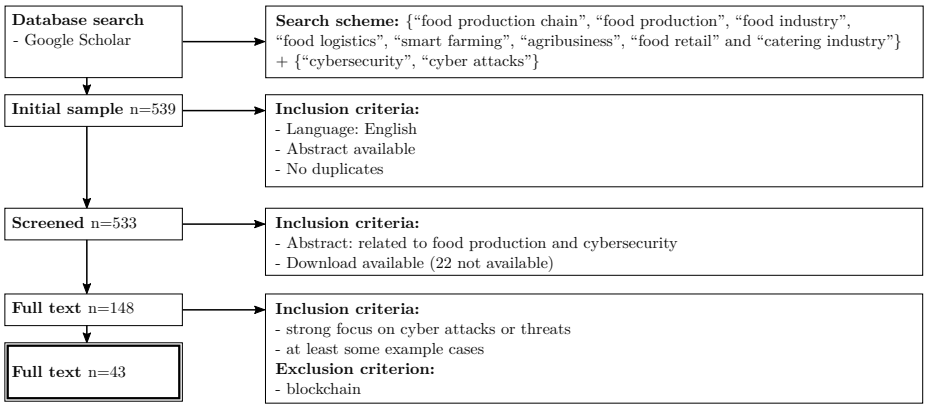

Fig. 1. Review protocol.

The Google Scholar service was used as the primary search engine. The search queries were constructed by joining the cybersecurity keyword to the food keyword using a space e.g. "smart farming cyber attacks". Special query characters such as quotes or logical operators like OR and AND were not used when constructing the search queries. The searches were carried out using the normal Google Scholar search user interface. From each query, the first 50 search results were taken under review. A program was developed for automating the search result extraction using the Playwright[1] browser automation framework. This was done to prevent human errors in the repetitive task of copying the search results from the browser to the Excel worksheet where the review of the search results was coordinated. All the search results were in English. No restriction was placed on the literature type: grey literature was also considered during the review process. Because of space restrictions, all papers about blockchains were deemed out of scope for this study. Figure 1 illustrates the different stages of the review protocol used during the scoping review.

Results

Smart farming cybersecurity is one of the main topics that was studied in multiple papers. Smart farming uses modern technologies such as the Internet of Things (IoT), artificial intelligence and robotics to increase crop yields, maximize production and streamline farming processes [51].

Chi et al. have defined a security framework for innovations that support smart farming in [12]. They identify that the data generated by smart farming sensors is a very valuable resource for all kinds of other purposes such as research of plants biology and genetics, forecasting the market and economics, and new farm equipment design. This makes the data a high value target for corporates,

[1] https://playwright.dev/

activists or even nation level adversaries to steal, sabotage or inject misinformation. To mitigate these threats the paper defines the cybersecurity framework for smart farming to include three components: abnormal measurement detection, access control, and encryption.

Bogaardt et al. focused on dairy industry in their research report [9]. The study claims that 90% of new installations in dairy farms are robotic milking equipment, and by 2025 half of the cows in north-western Europe are milked by robots. The milking robots collect a large amount of data from the cows and the milk, and the normal everyday processes are starting to be dependent on this data. For that reason, it is important to protect the data against cyber threats. Additionally, the business management systems that some farmers use for food safety tracking reasons can be a tempting target for data theft. The report identifies unmaintained software and human errors as the main threats to these systems.

The attack types against the smart farming systems are well studied. Studies by Gupta et al. [27], Zanella et al. [42], Demestichas et al. [15], Koduru and Koduru [30], Yazdinejad et al. [54], Farooq et al. [22], Boghossian et al. [10], Okupa [39], Barreto and Amaral [7], Rosline et al. [43], Angyalos et al. [5], Akshatha and Poornima [53] and Racovita [41] try to identify the major cybersecurity threats in smart farming. Data security is one major security issue that is raised in some form by all the studies. Data theft is always possible in systems where data is collected and stored. Another threat is data forgery. Smart farms use the data collected by the sensors to make decisions. By injecting forged data to the system, a hacker can easily disrupt farm operations. The hacker can physically take control of a sensor and modify the hardware or software to transmit malicious data to the system, or in some cases the hacker can exploit the problems in authentication and authorization to inject the data remotely. In addition of these threats, the threat of autonomous vehicles and robots was identified in some of the studies. A hijacked autonomous tractor could cause real physical damage to the infrastructure and be even a life-threatening danger. More common attack types such as denial of service, phishing, RF jamming and malware attacks were also identified as threats to smart farms.

Some papers have a narrower scope. Cho et al. limited their study to the cyber threats in smart greenhouses [13]. Rouzbahani et al. studied the potential cyber attacks of smart farming communication technologies [44]. Linsner et al. tested the cybersecurity of wireless sensor networks using simulated attacks [35]. Alsinglawi et al. studied the cybersecurity threats and attack types of microservice based meat production smart farm. Alahmadi et al. researched side channel attacks in smart farming systems [3]. Nikander et al. summarized a case study that studied the cybersecurity of 6 dairy farms in Finland [38]. Dorairaju conducted a case study on the cybersecurity of an IoT enabled pest trap system that was targeted for agricultural use [16].

Studies of the existing publications about the topic have also been carried out. Nakhodchi et al. conducted a bibliometric analysis on the publications about the privacy and security in smart farming [37]. Rudrakar and Rughani have com-

pleted a systematic literature review about IoT based agriculture cybersecurity and forensics challenges [45].

Cyber-physical system cybersecurity in food production is another topic that is quite well researched. This topic includes studies about the cybersecurity of industrial control systems (ICS) that are used, for example, in food packaging plants.

Beluli has studied the possibility of cyber attack in the beer production industry [8]. The industry uses computer automation in the beer production process with high temperature and pressure tanks. Cyber attack against the process control systems could cause an explosion that damages the equipment, or even cause danger to human life.

Alim et al. studied the cybersecurity threats of a modeled canal SCADA system [4]. Water management systems are critical infrastructure for agriculture industry. They are used in crop irrigation and water processing. Attacks against these kinds of systems can cause major financial losses to the farmers. The authors tested multiple attack types against the model with successful results. One of the attack types was a message injection attack that caused flooding in the modeled farmland.

Freyhof studied the cybersecurity of agricultural machinery [24]. The focus of the study was to estimate the financial losses of a cyber attack against an electrically controlled variable rate nitrogen side-dressing equipment. The suggested attacks keep the cumulative quantity of the applied nitrogen the same but use different strategies to distribute the total nitrogen quantity so that actual application rates are different from the prescribed rates. This way the cyber attack can reduce the crop yields and thus cause financial losses.

Streng studied the cybersecurity of the ICSs used in food processing and manufacturing [50]. The study identifies common cybersecurity problems in these systems, such as old operating system versions, insecure protocols and old unmaintained software. The study concludes that cyber attacks targeting these cyber-physical systems are possible in food industry, and they can be even life threatening if they target equipment such as co-robots that work alongside people in production lines. Additionally, a cyber attack against the food production system can make the produced food somehow unsafe for consumption, which can cause danger to the consumers. This study can be seen as a continuum to a report written by the same author about an industry summit meeting in Washington USA [49]. In the meeting, the cyber-physical systems, such as the ICSs used in food packing plants, were identified a major security threat to the food industry.

Chundhoo et al. conducted a case study about the cybersecurity of a meat processing plant [14]. They identified serious threats in the meat processing system where the meat temperature must be closely monitored. IoT sensors monitor the meat temperature, and the thawing, chilling, freezing, cooking, and smoking rooms are controlled by the readings coming from these sensors. Spoofed sensor readings can change the actual temperature of the meat to a range that can make the product unsafe for consumption or even cause equipment damage

further in the processing line, and that way contaminate the food with, for example, broken blades.

Survey and interview studies have also been conducted about the topic. All these studies targeted the farmers. One of the studies was written by Geil, who surveyed the cybersecurity awareness of the people working in the agriculture business ($N = 138$) [25]. The survey responders were farmers, producers and other workers from the industry in three different counties in Illinois USA. The study concludes that there are gaps in cybersecurity knowledge among the people working in the agriculture industry, and for that reason there is a need for more cybersecurity training for the industry workers. Also, see Geil et al. [26].

A similar survey was conducted by Spaulding and Wolf [48] ($N = 222$). They surveyed the farmers in Illinois USA, but targeted the survey towards beginning farmers. They conclude that even though the beginning farmers use computers more than experienced farmers, they still lack the skills to identify the cyber threats against their farming business accompanied with the computer usage.

Russell studied the cybersecurity risks at smart farms by interviewing farmers in Ontario Canada with supplemental interviews with five cybersecurity experts [46]. The paper includes a very detailed analysis of the interviews with some examples of phishing cyber attacks that the farmers have already experienced, and examples of attacks that the farmers see realistic and that could take place against their farm.

Linden et al. conducted a case study in the cybersecurity of dairy farming in Israel [34]. The authors interviewed a farmer about the usage of smart farming and threats that it poses. The authors discovered that in Israel it is common to share data between the farming community and the researchers, and for that reason the farmer did not identify data theft as a major threat. Additionally, losing the data was not seen as a high threat as the relevant data could be obtained from colleagues. The highest threat that the interviewed farmer identified was the injection of fraudulent data, or cases where data was otherwise inaccurate, because that directly impacts the productivity and welfare of the animals. The authors claim that the openness of sharing the data is not as common elsewhere, like in the UK, where leaking of the farm data is identified as a major threat. For that reason, the authors claim that the socio-cultural context matters when the cybersecurity of smart farming is considered.

The general state of the cybersecurity in food industry was also studied in many papers. Ajith et al. studied cyberespionage and cyberterrorism in the food industry [1]. They discuss the motives and review some of the existing research about the topic.

Hoffmann et al. studied cyber attacks against agribusiness industry [28]. They searched English news articles from the internet and found 31 reports of attacks against different parts of the food production infrastructure.

Jahn et al. conducted a high-level overview of cyber risks in north American food industry [29]. They identified some of the same cyber threats discussed in the previous sections caused by increased automation in farming and food

processing processes. They also discuss how the food industry works by using the just-in-time principle. Farmers rely on the delivery of the fertilizer, fuel, seeds etc. in time when needed, and the stores cannot keep large stocks of perishable food products, hence they also rely on the timely deliveries of the products. This can make the whole food delivery chain especially vulnerable to cyber attacks.

Russell and Chow discussed food cybersecurity in general in their paper [47]. They present examples of possible attacks against home smart refrigerators and processing plant irradiation machines used to sterilize food products. Both cases are potential health hazards, as they can lead to food poisoning.

Duncan et al. also presented a high-level view of cybersecurity in food and agriculture industry [17]. The paper includes some concrete examples of possible attacks, such as attacks against genetic databanks that the breeders use to develop more productive dairy cows and other food animals. Some of the same authors contributed to the second paper where they considered these attacks more closely and suggested possible mitigations, such as cryptographic signatures for the data [18].

Conclusion

There is a large number of studies about the food supply chain cybersecurity. The threat of cyber attacks against food industry has been well identified by researchers. Especially the new cyber threats that come with the increasing popularity of smart farming are well studied. Many of the reviewed papers identified industrial control systems as a major security threat. Furthermore, old unmaintained software is vulnerable to attacks and is expensive to update. This is not unique to the food industry; in every industry where automation is used, there are also legacy systems that are vulnerable to attacks. Food industry is unique in the sense that these vulnerabilities can easily threaten human health and life. This was a well identified threat, but not many concrete examples exist in the literature. This could be an area where more research is needed. In addition, future research could study the topics excluded from this work, such as the use of blockchain technologies in food industry and the cybersecurity threats that they cause.

Acknowledgements

This research is funded by the Regional Council of Central Finland/Council of Tampere Region with fund of Leverage from the EU, European Regional Development Fund (ERDF), Recovery Assistance for Cohesion and the Territories of Europe (REACT-EU). Research is implemented as part of the Food Chain Cyber Resilience project project of Jamk University of Applied Sciences Institute of Information Technology.

The authors would like to thank Ms. Elina Suni for identifying some relevant sources and Ms. Tuula Kotikoski for proofreading the manuscript.

References

1. Adetunji, C.O., Olugbemi, O.T., Anani, O.A., Hefft, D.I., Wilson, N., Olayinka, A.S., Ukhurebor, K.E.: Chapter 27 - cyberespionage: Socioeconomic implications on sustainable food security. In: A. Abraham, S. Dash, J.J. Rodrigues, B. Acharya, S.K. Pani (eds.) AI, Edge and IoT-based Smart Agriculture, Intelligent Data-Centric Systems, pp. 477–486. Academic Press (2022). DOI 10.1016/B978-0-12-823694-9.00011-6
2. AGCO Corporation: AGCO announces ransomware attack (2022). URL https://news.agcocorp.com/news/agco-announces-ransomware-attack
3. Alahmadi, A.N., Rehman, S.U., Alhazmi, H.S., Glynn, D.G., Shoaib, H., Solé, P.: Cyber-security threats and side-channel attacks for digital agriculture. Sensors **22**(9) (2022). DOI 10.3390/s22093520
4. Alim, M.E., Wright, S.R., Morris, T.H.: A laboratory-scale canal scada system testbed for cybersecurity research. In: 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 348–354 (2021). DOI 10.1109/TPSISA52974.2021.00038
5. Angyalos, Z., Botos, S., Szilagyi, R.: The importance of cybersecurity in modern agriculture. Journal of Agricultural Informatics **12**(2) (2022). DOI 10.17700/jai.2021.12.2.604
6. Arksey, H., O'Malley, L.: Scoping studies: towards a methodological framework. International Journal of Social Research Methodology **8**(1), 19–32 (2005). DOI 10.1080/1364557032000119616
7. Barreto, L., Amaral, A.: Smart farming: Cyber security challenges. In: 2018 International Conference on Intelligent Systems (IS), pp. 870–876 (2018). DOI 10.1109/IS.2018.8710531
8. Beluli, V.M.: Smart beer production as a possibility for cyber-attack within the industrial process in automatic control. Procedia Computer Science **158**, 206–213 (2019). DOI 10.1016/j.procs.2019.09.043
9. Bogaardt, M.J., Poppe, K.J., Viool, V., Zuidam, E.v.: Cybersecurity in the agrifood sector. Tech. rep. (2016). URL https://edepot.wur.nl/378724
10. Boghossian, A., Linsky, S., Brown, A., Mutschler, P., Ulicny, B., Barrett, L., Bethel, G., Matson, M., Strang, T., Wagner Ramsdell, K., Koehler, S.: Threats to precision agriculture (2018 public-private analytic exchange program report). Tech. rep., U.S. Department of Homeland Security (2018)
11. Bowcut, S.: Cybersecurity in the food and agriculture industry (2021). URL https://cybersecurityguide.org/industries/food-and-agriculture/
12. Chi, H., Welch, S., Vasserman, E., Kalaimannan, E.: A framework of cybersecurity approaches in precision agriculture (2017)
13. Cho, S.H., Kang, D.S., Kang, M.S., Kim, H.S., Bae, J.W., Lee, C.I., Ji, H.B., Won, Y.H., Hong, H.K., Kim, K.: A study on threat modeling in smart greenhouses. Journal of Information Security and Cybercrimes Research **3**(1), 1–12 (2020). DOI 10.26735/KKJN1042
14. Chundhoo, V., Chattopadhyay, G., Karmakar, G., Appuhamillage, G.K.: Cybersecurity risks in meat processing plant and impacts on total productive maintenance. In: 2021 International Conference on Maintenance and Intelligent Asset Management (ICMIAM), pp. 1–5 (2021). DOI 10.1109/ICMIAM54662.2021.9715193
15. Demestichas, K., Peppes, N., Alexakis, T.: Survey on security threats in agricultural iot and smart farming. Sensors **20**(22) (2020). DOI 10.3390/s20226458

16. Dorairaju, G.: Cyber security in modern agriculture. case study: Iot-based insect pest trap system. Master's thesis, JAMK University of Applied Sciences (2021). URL https://urn.fi/URN:NBN:fi:amk-202105128397
17. Duncan, S.E., Reinhard, R., Williams, R.C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., Murch, R.: Cyberbiosecurity: A new perspective on protecting u.s. food and agricultural system. Frontiers in Bioengineering and Biotechnology **7** (2019). DOI 10.3389/fbioe.2019.00063
18. Duncan, S.E., Zhang, B., Thomason, W., Ellis, M., Meng, N., Stamper, M., Carneiro, R., Drape, T.: Securing data in life sciences—a plant food (edamame) systems case study. Frontiers in Sustainability **1** (2020). DOI 10.3389/frsus.2020.600394
19. European Commission: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A Farm to Fork Strategy for a fair, healthy and environmentally-friendly food system (2020). URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0381
20. European Commission: Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade (2020). URL https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018
21. European Commission: Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities (2020). URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829
22. Farooq, M.S., Riaz, S., Abid, A., Abid, K., Naeem, M.A.: A survey on the role of iot in agriculture for the implementation of smart farming. IEEE Access **7**, 156,237–156,271 (2019). DOI 10.1109/ACCESS.2019.2949703
23. FBI: Ransomware attacks on agricultural cooperatives potentially timed to critical seasons (2022). URL https://www.ic3.gov/Media/News/2022/220420-2.pdf
24. Freyhof, M.T.: Cybersecurity of agricultural machinery: Exploring cybersecurity risks and solutions for secure agricultural machines. Master's thesis, Department of Biological Systems Engineering, University of Nebraska-Lincoln (2022)
25. Geil, A.: Cyber security on the farm: An assessment of cyber security practices in the agriculture industry. Master's thesis, Illinois State University, School of Information Technology (2014). DOI 10.30707/ETD2014.Geil.A
26. Geil, A., Sagers, G., Spaulding, A., Wolf, J.: Cyber security on the farm: An assessment of cyber security practices in the united states agriculture industry. International Food and Agribusiness Management Review **21**, 1–18 (2018). DOI 10.22434/IFAMR2017.0045
27. Gupta, M., Abdelsalam, M., Khorsandroo, S., Mittal, S.: Security and privacy in smart farming: Challenges and opportunities. IEEE Access **8**, 34,564–34,584 (2020). DOI 10.1109/ACCESS.2020.2975142
28. Hoffmann, C., Haas, R., Bhimrajka, N., Penjarla, N.S.: Cyberattacks in agribusiness. In: M. Gandorfer, C. Hoffmann, N. El Benni, M. Cockburn, T. Anken, H. Floto (eds.) 42. GIL-Jahrestagung, Künstliche Intelligenz in der Agrar- und Ernährungswirtschaft, pp. 117–122. Gesellschaft für Informatik e.V., Bonn (2022)
29. Jahn, M., Oemichen, W.L., Treverton, G.F., David, S., Rose, M.A., Brosig, M.A., Hutchison, W.K., Rimestad, B.B.: Appendix: Cyber risks in north american agriculture and food systems. Global Assessment Report on Disaster Risk Reduction (2019). Appendix of the article: Cybersecurity and its cascading effect on societal systems

30. Koduru, T., Koduru, N.P.: An overview of vulnerabilities in smart farming systems. Journal of Student Research **11**(1) (2022). DOI 10.47611/jsrhs.v11i1.2303
31. Latino, M.E., Menegoli, M.: Cybersecurity in the food and beverage industry: A reference framework. Computers in Industry **141**, 103,702 (2022). DOI 10.1016/j.compind.2022.103702
32. Lewis, A.H.: Further facts: In the case of the labor record of Mark Hanna, the republican party's manager. The Owensboro Messenger p. 2 (1896, October 16)
33. Lezoche, M., Hernandez, J.E., Díaz, M.d.M.E.A., Panetto, H., Kacprzyk, J.: Agri-food 4.0: A survey of the supply chains and technologies for the future agriculture. Computers in industry **117**, 103,187 (2020)
34. van der Linden, D., Michalec, O.A., Zamansky, A.: Cybersecurity for smart farming: Socio-cultural context matters. IEEE Technology and Society Magazine **39**(4), 28–35 (2020). DOI 10.1109/MTS.2020.3031844
35. Linsner, S., Varma, R., Reuter, C.: Vulnerability assessment in the smart farming infrastructure through cyberattacks. pp. 119–124. Wien (2019). URL http://tubiblio.ulb.tu-darmstadt.de/116032/
36. Marshall, C., Prior, M.: Cyber security: Global food supply chain at risk from malicious hackers. BBC (2022). URL https://www.bbc.com/news/science-environment-61336659
37. Nakhodchi, S., Dehghantanha, A., Karimipour, H.: Privacy and Security in Smart and Precision Farming: A Bibliometric Analysis, pp. 305–318. Springer International Publishing, Cham (2020). DOI 10.1007/978-3-030-38557-6_14
38. Nikander, J., Manninen, O., Laajalahti, M.: Requirements for cybersecurity in agricultural communication networks. Computers and Electronics in Agriculture **179**, 105,776 (2020). DOI 10.1016/j.compag.2020.105776
39. Okupa, H.: Cybersecurity and the future of agri-food industries. Master's thesis, Kansas State University, Department of Agricultural Economics (2020). URL https://hdl.handle.net/2097/40529
40. Peters, M.D., Godfrey, C.M., Khalil, H., McInerney, P., Parker, D., Soares, C.B.: Guidance for conducting systematic scoping reviews. JBI Evidence Implementation **13**(3) (2015). URL https://journals.lww.com/ijebh/Fulltext/2015/09000/Guidance_for_conducting_systematic_scoping_reviews.5.aspx
41. Racovita, M.: Cybersecurity for the internet of things and artificial intelligence in the agritech sector. Industry briefing, PETRAS National Centre of Excellence for IoT Systems Cybersecurity, London, UK (2021)
42. Rettore de Araujo Zanella, A., da Silva, E., Pessoa Albini, L.C.: Security challenges to smart agriculture: Current state, key issues, and future directions. Array **8**, 100,048 (2020). DOI 10.1016/j.array.2020.100048
43. Rosline, G.J., Rani, P., Gnana Rajesh, D.: Comprehensive analysis on security threats prevalent in iot-based smart farming systems. In: P. Karuppusamy, I. Perikos, F.P. García Márquez (eds.) Ubiquitous Intelligent Systems, pp. 185–194. Springer Singapore, Singapore (2022)
44. Rouzbahani, H.M., Karimipour, H., Fraser, E., Dehghantanha, A., Duncan, E., Green, A., Russell, C.: Communication layer security in smart farming: A survey on wireless technologies (2022). DOI 10.48550/ARXIV.2203.06013
45. Rudrakar, S., Rughani, P.: Iot based agriculture (iota): Architecture, cyber attack, cyber crime and digital forensics challenges (2022). DOI 10.21203/rs.3.rs-2042812/v1
46. Russell, C.: Cyber security in digital agriculture: Investigating farmer perceptions, preferences, & expert knowledge. Master's thesis, The University of Guelph,

Department of Geography, Environment and Geomatics (2022). URL https://hdl.handle.net/10214/27219
47. Russell, N., Chow, M.: Cybersecurity and our food systems. Tech. rep. (2017)
48. Spaulding, A.D., Wolf, J.R.: Cyber-security knowledge and training needs of beginning farmers in illinois. 2018 Annual Meeting, August 5-7, Washington, D.C. 273781, Agricultural and Applied Economics Association (2018). URL https://EconPapers.repec.org/RePEc:ags:aaea18:273781
49. Streng, S.: Food industry cybersecurity summit meeting report (2016). Retrieved from the University of Minnesota Digital Conservancy, https://hdl.handle.net/11299/217704
50. Streng, S.: Adulterating more than food: The cyber risk to food processing and manufacturing (2019). Retrieved from the University of Minnesota Digital Conservancy, https://hdl.handle.net/11299/217703
51. Sundmaeker, H., Verdouw, C., Wolfert, S., Pérez Freire, L.: Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds, chap. Internet of food and farm, pp. 129–152. River Publishers Series in Communications and Networking. River Publishers (2016). DOI 10.13052/rp-9788793379824
52. Urciuoli, L., Männistö, T., Hintsa, J., Khan, T.: Supply chain cyber security–potential threats. Information & Security: An International Journal **29**(1) (2013)
53. Y, A., Poornima, A.S.: Iot enabled smart farming: A review. In: 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 431–436 (2022). DOI 10.1109/ICICCS53718.2022.9788149
54. Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A.G., Russell, C., Duncan, E.: A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. Applied Sciences **11**(16) (2021). DOI 10.3390/app11167518