Conceptual Modeling to Advance Agrifood Cybersecurity Ontologies

Richard Hull[1], Matt Bishop[1], Karl Levitt[1], Mohammad Sadoghi[1], Matthew Lange[2*]

[1] *University of California, Davis, California, USA*

[2] *International Center for Food Ontology Operability Data and Semantics (IC-FOODS), Davis, California, USA*

Abstract

Agriculture is central to the survival and comfort of the human race. In recent decades tremendous advances in the application of digital technologies increasingly enable significant efficiency, productivity, environmental sustainability and climate change resilience gains across the continuum of agrifood systems, including processing, distribution-product, purveyance, knowledge and practice. Digital technologies now underpin new methods, practices, and equipment, altering the way we define and manage issues and indicators, meaningful metrics ranging across topics stretching from soil quality and agricultural practices, to food processing, to wholesaling/retailing, and transportation and warehousing logistics. The increasing ubiquity of digital agrifood technologies has brought a substantial expansion in the range of cybersecurity vulnerabilities and the magnitude of their potential consequences, which will continue to grow in the foreseeable future.

As a step towards reducing the cyber risks to modern agrifood systems, this paper describes work to develop a conceptual model that will underpin a comprehensive agrifood cybersecurity ontology. This will include systems actors/agents, the types of technologies they use and their prevalence across food systems, the cyber and social vulnerabilities associated with these actors and technologies, known attacks on the technologies, and best practices for preventing, detecting, and mitigating cyber attacks. The approach for building this ontology includes bringing together cybersecurity and agriculture experts, applying Large Language Models, and integrating relevant existing ontologies and other structured vocabularies in the cybersecurity and agricultural spaces. At this point the team has constructed a conceptual model that can act as a guide for developing a formal ontology across digital local-to-global food systems.

Keywords

agrifood systems, cybersecurity, ontologies

1. Introduction and Motivation

Across the world, cyber attacks on the agrifood sector have been increasing rapidly, including ransomware attacks and, more recently, attacks on farm and food processing operations (Kulkarni et al. 2024; Sontowski et al. 2020). All aspects of the agrifood supply chain, including farms, food processors, plant/animal breeding, transportation, and storage are experiencing a tremendous growth in the use of digital technology, including AI/ML. This is resulting in a substantial increase in the cyber attack surface across agrifood. Successful cyber attacks can have dramatic operational impacts (e.g., complete stoppage of farm or food processing activity), agricultural impacts (e.g., crop or animal loss, tainted products getting to the marketplace), and economic and food security impacts (days- or weeks-long disruptions to markets with associate

[1*] Corresponding author

$M price tags)(Window 2019; Kulkarni et al. 2024; Sontowski et al. 2020). A particularly pernicious kind of cyber attack can arise because of the increasing reliance of precision agriculture on AI/ML. Specifically, an attack on the corruption of data used, or the AI/ML algorithms themselves, could lead to subtle alterations of recommendations made. For example, this might lead to the application of suboptimal amounts of fertilizer, and suboptimal yields. But, the alterations might go undetected for months or years, all the while reducing crop yields by 10% or more.

The cybersecurity challenges arising in agrifood stem from the many technologies being used, including sensors and other embedded devices; Cyber Physical Systems (CPS); Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA); HW in general; SW in general; and IoT, local and wide-area networking. Agrifood systems also bring differentiating challenges. This includes the broad heterogeneity of technologies being used on farms around the globe, and the tendency of farmers to use less expensive components which may have insecure HW or SW supply chains. It includes the presence of legacy ICS/SCADA equipment, especially in food processors, which was designed and implemented before cybersecurity was a concern. Unlike many CPS contexts, the technology in agriculture is working on biological objects, which introduces many more variables in the interaction of the technology and the focus of technology usage. This can make it harder to determine whether the technology is working correctly or has become corrupted. Another difference is that much of the technology used in agriculture is located on farms in rural areas, making physical security especially challenging. For example, a malicious actor might be able to disrupt some firewall software by direct tampering, thereby enabling an cyber infiltration of numerous internet-connected devices on a farm. Finally, in many agrifood systems there is a wide diversity of technological sophistication in the workforce, ranging from migrant farm workers (who will be technology users) to highly skilled IT workers at large corporate farms.

The cost of cyber defenses (including detection, mitigation, prevention) can be prohibitive for farmers, especially because most farmers have limited technological sophistication. It is thus essential that tools be developed to (a) help reduce cybersecurity risk to agrifood, and (b) enable effective and inexpensive cyber defenses.

One critical tool for addressing both of these issues is the development of a comprehensive ontology focused on the interacting domains of agrifood systems and cybersecurity. An ontology is needed to provide a universally shared structure for the huge volume and heterogeneity of data about digital technologies used in agrifoods, the myriad of cybervulnerabilities of those technologies, along with the associated cyber risks, potential consequences of successful attacks, and best practices for defense against them. In particular, this ontology will enable easier communication between humans and enable organizations and tools to seamlessly share and automatically process ag cybersecurity information.

This paper describes preliminary work towards the development of a comprehensive Agrifood Cybersecurity Ontology (ACO). The first step of the process, currently underway, is the development of a concept map that includes a small family of high-level classes (Agrifood Technologies, Cyber Vulnerabilities, Impacts, …) and then focuses on more specific ag

technology classes (sensors, IOT networks, AI/ML, …) and associated cyber vulnerabilities (counterfeit HW, unauthorized data access, code injection attack,…). Section 2 provides some specific ways that the ACO could be used. Section 3 describes the methodology being followed. There is not a separate related work section because that is covered in Sections 2 and 3. Section 4 provides an overview of the portions of the (preliminary) concept map already developed. And Section 5 provides brief conclusions and next steps.

2. Target Applications for a Comprehensive ACO

We envision at least four main applications for the ACO.

Agrifood Cybersecurity Technical Landscapes: As farmers, food processing companies and others expand or replace technology, it is essential that they understand the cybersecurity implications of that technology. A key application of the ACO will be to provide a comprehensive, machine-readable framework for understanding and capturing the "cybersecurity technical landscapes" of the myriad of agrifood activities and processes. Such landscapes will include a variety of information about the technologies used in the various aspects of agrifood, including the prevalence of the technology in the field; the manufacturers and vendors; cybervulnerabilities of the technologies along with risk levels; history of known and potential attacks, including root causes if available; potential operational, agricultural and economic consequences of successful attacks; and cybersecurity defenses.

As an example, the cybersecurity technical landscape for dairy would include information about milking machines, including the various manufacturers and vendors (including nationality). It would include information about the number of installations of the different brands, and information on possible and known attacks. For example, there were attacks against automated milking machines on two dairy farms in California in December, 2023[2]. The tech landscape would also include information on cybersecurity defenses and best practices, including for detection, mitigation and prevention. These tech landscapes would be "living documents", because the technologies will continue to evolve, the attacks and vulnerabilities will continue to evolve, and the best practices will continue to evolve.

AI-powered Integrated Query Capability: We envision a system that will enable farmers and other stakeholders in agrifood to be able to ask wide-ranging queries that involve cybersecurity aspects of different agrifood subsystems. Answering these queries might require pulling data both from sources related to the ACO, and also from sources related to a variety of other areas, such as crop yields, soil conditions, weather projections, bio hazards, market conditions, etc. For example, a farmer might want to understand the investment/reward trade-offs of using various technologies, incorporating cybersecurity risks, crop yield projections, economic projections that incorporate anticipated markets, and climate change.

[2] Communication with Joseph Gendreau, UC Davis.

This kind of querying capability can be accomplished along the lines described in the Integrated Knowledge and Learning Environment (Tu et al. 2023). That framework uses three languages/paradigms to enable an effective, easy-to-use workflow for answering queries that integrate knowledge from families of interrelated knowledge sources. In particular, it uses LinkML to specify linkages between multiple ontologies for the different knowledge sources, SPARQL for exploring and navigating the linked ontologies, and Vega-Lite to provide visualization recommendations. The ACO would be critical for incorporating agrifood cybersecurity information into the query answers.

Incorporation of Cybersecurity into Operationalization of Agrifood Technology Systems: The ACO can also support a capability that is more foundational than the tech landscapes and integrated query capabilities described above. In particular, the ACO (and associated data structured according to it) can enable cybersecurity considerations to be incorporated into the very fabric of the full lifecycle of agrifood technology usage. In connection with a new technology being considered for a farm, cybersecurity implications and best practice recommendations would be included into product exploration, product acquisition, deployment of the product, on-going usage, and upgrades. For example, if a farmer is considering the use of drones for crop health surveillance, they could be informed about cyber risks of various manufacturers, such as counterfeit HW, security flaws in the SW development supply chain, and the potential for malware propagation through the drone. During initial acquisition and deployment of the drones the farmer could be informed of best practices for preventing those threats, including checking with authorities about the cyber reliability of the manufacturer, incorporating a policy of strong passwards, routine software patches, and secure firewalls.

To summarize, consideration of cybersecurity risks, costs, and best practices would no longer be an afterthought, but would instead become a dimension that is seamlessly incorporated into all phases of the technology lifecycle.

Security Operations Centers (SOCs): In the US, government agencies, NGOs and industry are now working towards the creation of a family of cooperating Security Operations Centers that will serve as national clearinghouses for sharing information about cyber threats, technology vulnerabilities, actual attacks and their aftermath, and best practices for safeguarding against cyber attacks. These SOCs will maintain a comprehensive and growing knowledge base with user-friendly querying capabilities. The UCO can be an invaluable tool to help these SOCs by providing a comprehensive structure for holding the information they gather, and facilitating easy query access to it. Further, the UCO will enable effective information sharing between the SOCs and other interested stakeholders, because the UCO will provide an authoritative vocabulary and structure for the breadth of agrifood cybersecurity information, useful both for human communication and automated processing.

3. Approach for Building the Ontology

Development of the ACO will be a multi-phase effort, involving the collaboration of experts from the Agrifood domain and from the Cybersecurity domain, and using recently emerging techniques based on Large Language Models (Toro et al. 2023; Kommineni, König-Ries, and Samuel 2024; Sanju Saravanan and Bhagavathiappan 2024). This paper reports on the first step of the effort, which is focused on the development of a concept map that includes a small family of high-level classes, and then focuses on more specific ag technology classes and associated cyber vulnerabilities. We expect the concept map to evolve into the comprehensive ACO through a number of iterative expansions.

A key part of our work has been to survey the numerous ontologies already in existence in the areas of (a) Agrifood, and (b) Cybersecurity. On the Agrifood side the most relevant are the Food Ontology (D. M. Dooley et al. 2018), as well as the Crop, Agronomy and other Agrifood-related Open Biological Foundry Ontologies (Arnaud et al. 2016; Laporte, Aubert, and Arnaud 2021; D. Dooley et al., n.d.), the work reported in Ontology Engineering and Knowledge Services for Agriculture Domain (Kawtrakul 2012), the Ontology-based Knowledge Map Model for Digital Agriculture (OAK Framework) (Ngo, Kechadi, and Le-Khac 2020), and the FAO AGROVOC vocabulary(Lauser et al. 2006). On the Cybersecurity side, the most relevant ontologies are the Unified Cybersecurity Ontology (UCO)(Syed et al. 2016), the work on ontology for Cyber Physical Systems (CPS)(Kumar et al. 2022; Abbaszadeh and Zemouche 2022; Venkata, Maheshwari, and Kavi, n.d.) and IoTSec ontology for industrial IoT systems(Mozzaquatro et al. 2018). While each of these includes classes that are related to the interaction of modern Agrifood and Cybersecurity, none of them address the interaction of Agrifood technologies and processes with cyber vulnerabilities, cyber defenses, and the potential impacts of cyber attacks. The goal of our work is to fill this void with an ontology that addresses these topics, relies on relevant classes and relationships from the existing ontologies, and enables linkages with those ontologies.

To allow for a very direct focus on the essential features of the interaction between Agrifood and Cybersecurity, we begin by drawing on expert knowledge about the two domains and their interaction. From here we will pursue two directions in parallel. One will be to validate and refine our concept map by using it as the framework for developing Cybersecurity Technical Landscapes in three agrifood areas (Precision Ag, Dairy farming, and Poultry farming). The second will be to adapt the classes in our concept map, where appropriate, to fit more closely to the style and specifics of the existing ontologies.

To give a brief illustration of the second direction, we consider the relationship of our current concept map and the aforementioned UCO. Similar to our goals for the ACO, the UCO includes a variety of classes related to cybersecurity incidents, indicators, mitigations, severity levels, courses of action, etc. However, it does not provide classes at a more granular level, focusing on specific kinds of cyber vulnerabilities and attacks, such as code injection attack, unauthorized

data access, (AI/ML) training data corruption, insecure firewall, etc. Also, it does not address potential operational, agricultural or economic impacts of successful cyber attacks. Incorporation of the more granular level is essential for helping farmers and stakeholders to understand specific cyber vulnerabilities and cyber defenses for specific kinds of digital ag technology. Incorporation of the potential impacts of successful attacks is essential for understanding the cost/benefit of following best practice cyber defenses.

4. Preliminary Concept Map

After consulting existing ontologies that describe various aspects of Agrifood systems, as well as extant cybersecurity ontologies, we created a conceptual model in the form of a concept map, that enumerates the high level classes of an emerging Agrifood Cybersecurity Ontology. These concept maps underpin the development of more formal agrifood system cybersecurity ontologies by providing easy to reference visual resources

Figure 1 shows the top-level classes of the current concept map. Starting with Ag Sector (e.g., row crops, specialty crops (fruits, nuts, vegetables), dairy cattle, range cattle, …) it highlights both Cybersecurity Best Practices and Ag Technologies. The Ag Technology class has several subclasses (Animal Breeding, Rangeland Livestock Mgmt., …). The figure also shows how Cyber Vulnerabilities can lead to Operational Consequences, which in turn can lead to several society-impacting consequences.

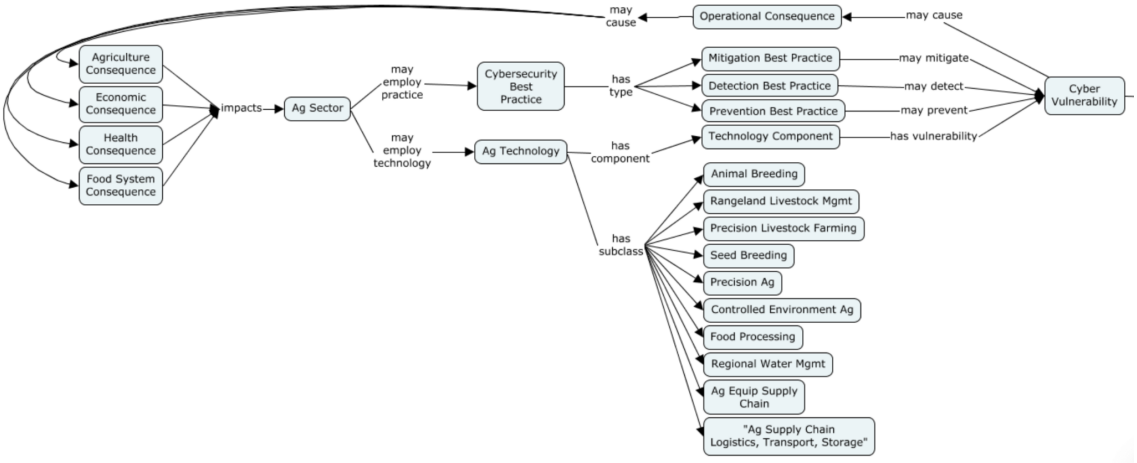

Figure 1: A high-level view of AgriFoods technologies, practices, their vulnerabilities, and consequences.

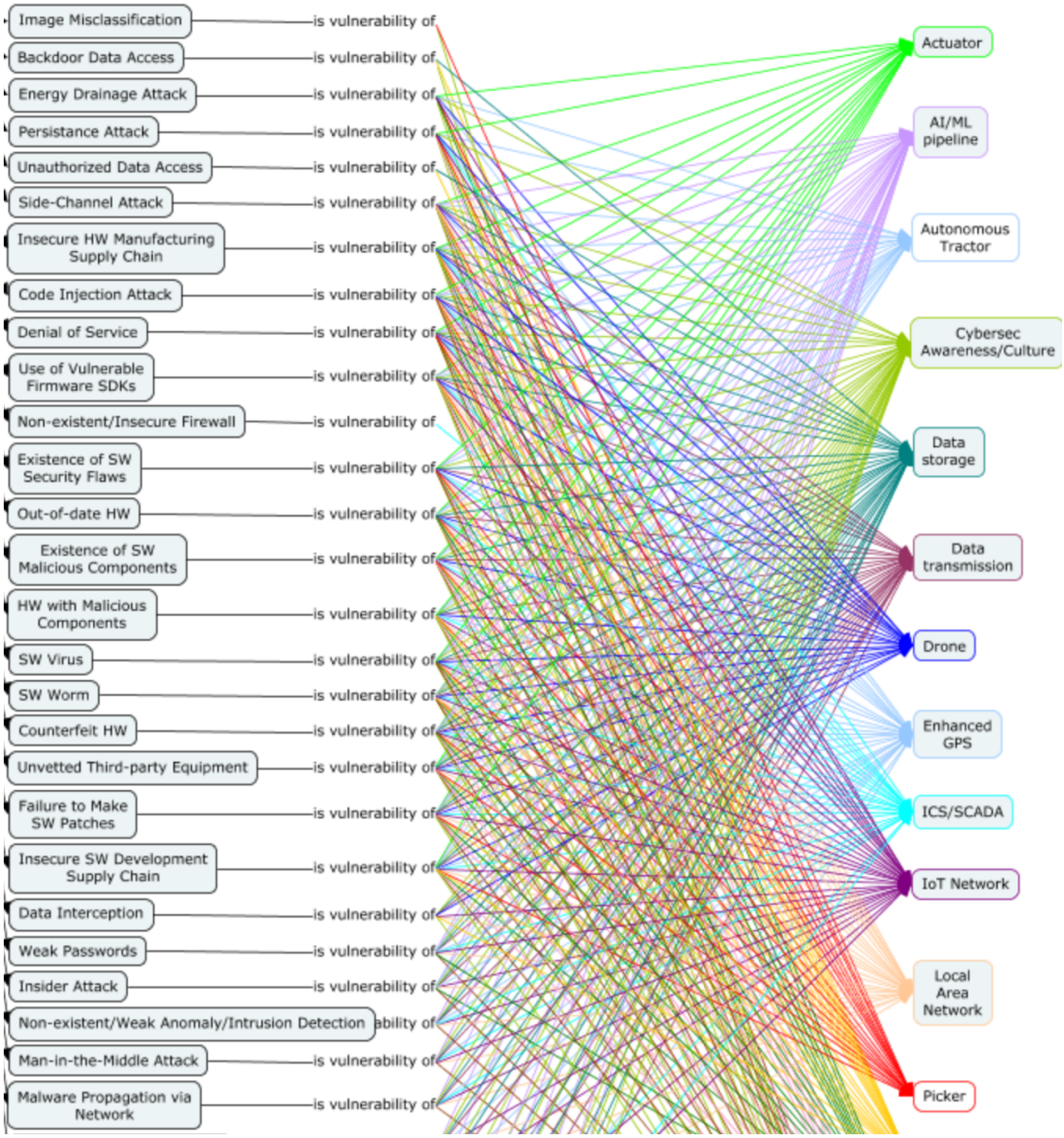

Figure 2: An example conceptual map of types of cybersecurity vulnerabilities and their associations with specific Agrifood cyberinfrastructure components.

Figure 2 shows a sample from a "drill-down" into a related part of our concept map. The right side shows key Technology Components (e.g., Actuator, AI/ML Pipeline, …); these stand in the "is component of" relationship to the Ag Technologies (Animal Breeding, …) shown in Figure 1. The left side are fine-grained classes of cyber vulnerabilities, and stand in the "is type of" relationship with the Cyber Vulnerability class of Figure 1.

5. Conclusions and Future Work

The paper establishes the urgent need for a comprehensive ontology focused on the interplay between Agrifood and Cybersecurity threats, defenses, and impacts. It further describes a first step towards the development of an Agrifood Cybersecurity ontology, namely, the creation of a concept map that focuses on the most important top-level classes and relationships between them, along with some detail around specific Agrifood technology components and related cyber vulnerabilities. We anticipate that the eventual ontology will be useful in a variety of ways, including (i) support for broad queries accessing integrated views of information relating to one or more of agrifood, cybersecurity risks, ag productivity, market conditions, etc.; and (ii) enabling the seamless incorporation of cybersecurity concerns into the full operational lifecycle of using ag technologies.

Immediate next steps include fleshing out the rest of the classes shown in the concept map of Figure 1, including the various kinds of Practices, Technologies, and their Potential Consequences. Likewise, further assessment and mapping of the linkages between the subclasses of Agrifood technologies, the cyberinfrastructure components they use, and their combined inherent vulnerabilities is needed. Further review of the literature and of analysis of extant source vocabularies, including ontology resources, to ensure correctness and completeness is critical.

Acknowledgements

The authors want to thank the many researchers from Iowa State University, Virginia Polytechnic Institute and State University, Washington State University, University of California, Davis, and North Carolina Agriculture and Technical State University who are involved in an initiative aimed at creating a national consortium (that would include academia, industry and government) focused on research, education and workforce development around cybersecurity for agriculture, for stimulating and informative conversations (see reference (M. Govindarasu et. al. 2024).

Funding for this research effort includes:
10.13039/501100008982-National Science Foundation (Grant Number: OAC-2112606)

References

Abbaszadeh, Masoud, and Ali Zemouche. 2022. *Security and Resilience in Cyber-Physical Systems: Detection, Estimation and Control*. Springer Nature.

Arnaud, E., Léo Valette, Julian Pietragalla, Marie-Angélique Laporte, C. Aubert, M. Devare, G. McLaren, and J. Ribaut. 2016. "The Crop Ontology: A Source of Standard Traits and Variables for Breeding and Agronomy," January. https://cgspace.cgiar.org/items/9d36fa5b-fd15-4ac9-9a90-dce4a0f937a8.

Dooley, Damion, Liliana Andrés-Hernández, Georgeta Bordea, Leigh Carmody, Duccio Cavalieri, Lauren Chan, Pol Castellano-Escuder, et al. n.d. "OBO Foundry Food Ontology Interconnectivity." Accessed April 29, 2023. https://www.semantic-web-journal.net/system/files/swj3305.pdf.

Dooley, Damion M., Emma J. Griffiths, Gurinder S. Gosal, Pier L. Buttigieg, Robert Hoehndorf, Matthew C. Lange, Lynn M. Schriml, Fiona S. L. Brinkman, and William W. L. Hsiao. 2018. "FoodOn: A Harmonized Food Ontology to Increase Global Food Traceability, Quality Control and Data Integration." *NPJ Science of Food* 2 (December): 23.

Govindarasu, Manimaran, Doug Jacobson, Surya Mallapragada, Jim Reecy, Feras Batarseah, Kang Xia, Monowar Hasan, Lav Khot, Matthew Bishop, Richard Hull, Karl Levitt, Mohammad Sadoghi, Greg Goins and Hossein Sarrafzadeh, Advancing Agriculture Cybersecurity: A Strategic Vision. 2024. (In preparation)

Kawtrakul, Asanee. 2012. "Ontology Engineering and Knowledge Services for Agriculture Domain." *Journal of Integrative Agriculture* 11 (5): 741–51.

Kommineni, Vamsi Krishna, B. König-Ries, and Sheeba Samuel. 2024. "From Human Experts to Machines: An LLM Supported Approach to Ontology and Knowledge Graph Construction." *ArXiv* abs/2403.08345 (March). https://doi.org/10.48550/arXiv.2403.08345.

Kulkarni, Ajay, Yingjie Wang, Munisamy Gopinath, Dan Sobien, Abdul Rahman, and Feras A. Batarseh. 2024. "A Review of Cybersecurity Incidents in the Food and Agriculture Sector." *arXiv [cs.CR]*. arXiv. http://arxiv.org/abs/2403.08036.

Kumar, Krishan, Sunny Behal, Abhinav Bhandari, and Sajal Bhatia. 2022. *Security and Resilience of Cyber Physical Systems*. CRC Press.

Laporte, Marie-Angélique, Céline Aubert, and Elizabeth Arnaud. 2021. "Requesting New Terms in Ontologies: The Example of Crop Ontology and the Agronomy Ontology." https://cgspace.cgiar.org/bitstream/handle/10568/113046/1.1%20Hands-On_03-2021.pdf?sequence=1.

Lauser, B., M. Sini, A. Liang, and J. Keizer. 2006. "From AGROVOC to the Agricultural Ontology Service/Concept Server. An OWL Model for Creating Ontologies in the Agricultural Domain." *Dublin Core Conference*. http://eprints.rclis.org/21109/.

Mozzaquatro, Bruno Augusti, Carlos Agostinho, Diogo Goncalves, João Martins, and Ricardo Jardim-Goncalves. 2018. "An Ontology-Based Cybersecurity Framework for the Internet of Things." *Sensors* 18 (9). https://doi.org/10.3390/s18093053.

Ngo, Quoc Hung, Tahar Kechadi, and Nhien-An Le-Khac. 2020. "OAK: Ontology-Based Knowledge Map Model for Digital Agriculture." In *Future Data and Security Engineering*, 245–59. Springer International Publishing.

Sanju Saravanan, Krithikha, and Velammal Bhagavathiappan. 2024. "Innovative Agricultural Ontology Construction Using NLP Methodologies and Graph Neural Network." *Engineering Science and Technology, an International Journal* 52 (April): 101675.

Sontowski, Sina, Maanak Gupta, Sai Sree Laya Chukkapalli, Mahmoud Abdelsalam, Sudip Mittal, Anupam Joshi, and Ravi Sandhu. 2020. “Cyber Attacks on Smart Farming Infrastructure.” In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, 135–43. IEEE.

Syed, Zareen, Ankur Padia, Timothy W. Finin, M. Mathews, and A. Joshi. 2016. “UCO: A Unified Cybersecurity Ontology.” *Workshops at the Thirtieth*, February. https://doi.org/10.13016/M2862BG1V.

Toro, Sabrina, Anna V. Anagnostopoulos, Sue Bello, Kai Blumberg, Rhiannon Cameron, Leigh Carmody, Alexander D. Diehl, et al. 2023. “Dynamic Retrieval Augmented Generation of Ontologies Using Artificial Intelligence (DRAGON-AI).” *arXiv [cs.AI]*. arXiv. http://arxiv.org/abs/2312.10904.

Tu, Yamei, Xiaoqi Wang, Rui Qiu, Han-Wei Shen, Michelle Miller, Jinmeng Rao, Song Gao, et al. 2023. “An Interactive Knowledge and Learning Environment in Smart Foodsheds.” *IEEE Computer Graphics and Applications* 43 (3): 36–47.

Venkata, Rohith Yanambaka, Rohan Maheshwari, and Krishna Kavi. n.d. “SIMON: Semantic Inference Model for Security in Cyber Physical Systems Using Ontologies.” In *Conference: ICSEA 2018 : The Thirteenth International Conference on Software Engineering Advances*.

Window, Marc. 2019. “Security in Precision Agriculture : Vulnerabilities and Risks of Agricultural Systems.” https://www.diva-portal.org/smash/get/diva2:1322203/FULLTEXT02.