Conceptual modeling to advance agrifood cybersecurity ontologies

Richard Hull[1], Matt Bishop[1], Joseph Gendreau[2], Karl Levitt[1], Mohammad Sadoghi[1], and Matthew Lange[3,*]

[1] *Computer Science Department, University of California, Davis, California, USA*
[2] *School of Veterinary Medicine, University of California, Davis, California, USA*
[3] *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 agricultural processes and the inputs they use, processing, product distribution, 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 cybersecurity attack surface, in the range and kinds 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 ontology would enable much smoother, structured information sharing between the agrifood and cybersecurity communities, and specifically support efficient data and knowledge sharing about cyber threats and defenses for the agrifood industries. This ontology 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 and previously unseen attacks on the technologies, and best practices for preventing, detecting, mitigating and deterring 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 preliminary conceptual model that can act as an initial 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 [1,2].

Proceedings of the Joint Ontology Workshops (JOWO) - Episode X: The Tukker Zomer of Ontology, and satellite events co-located with the 14th International Conference on Formal Ontology in Information Systems (FOIS 2024), July 15-19, 2024, Enschede, The Netherlands.

* Corresponding author

matthew@ic-foods.org (M. Lange)

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 $M price tags)[1–3]. 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 some amount that is difficult to detect but still impactful, e.g., 10%. An adversary intent on a long-term weakening of the US economy and food supply might pursue this kind of attack.

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, which raises the challenge of physical security for IT components since these components may not be under constant surveillance or serviced frequently. For example, a malicious actor might be able to impact the accuracy of a sensor that reports soil moisture or an attacker could disrupt the operation of a local-area 4G communications link by direct tampering, thereby enabling a cyber infiltration of numerous internet-connected devices on a farm. Furthermore, cyber-defense systems will increasingly operate without human assistance, which may make failures in those systems harder to detect. 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 mitigations and defenses 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 and then focuses on more specific ag technology classes and associated cyber vulnerabilities, attacks and defenses. Section 2 describes some of the most relevant related work, much of which the ACO will build upon. Section 3 provides some specific ways that the ACO could be used. Section 4 describes the methodology being followed. Section 5 provides an overview of portions of the preliminary concept map already developed. And Section 6 provides brief conclusions and next steps.

2. Related work

We present here some of the most important classification systems for agrifood and cybersecurity. Due to space limitations we cannot provide a comprehensive survey, but mention some of the most relevant to our investigation.

For agrifood, numerous classification systems and ontologies have been developed. Several of these have high-level classes that provide structure for the agrifood domain, but they do not provide concepts for most mid-level agricultural processes (e.g., precision irrigation or fertilization, animal feeding, food processing and packaging), nor do they expand upon details relating to real world instances of technologies used. For example, an agrifood ontology may indicate that a precision fertilizer spreader is used on a strawberry field, but does not include which sensors may be on the spreader, which communication protocols are used to control it, etc. These details are needed if we are to connect up agricultural practices with the tools, machinery and IT used to support them, and to their associated cybersecurity issues.

For example, parts of the North American Industry Classification System (NAICS), provide useful high-level classifications of agricultural domains, food manufacturing (processing) and also manufacturing of farm equipment [4]. The CGIAR Agronomy Ontology (AgrO) is largely focused on plant types, environments, inputs and yields [5]. The AgrO "agricultural implement" class has considerable overlap with the NAICS farm equipment category, and provides more subclasses. The AGROVOC Linked Open Data Dataset was developed and continues to "serve as a controlled vocabulary for the indexing of publications in agricultural science and technology" [6]. While a primary focus is on organisms, including the many plants and domesticated animals used in agriculture, AGROVOC also provides top-level concepts for "activities" (e.g., livestock feeding which includes leaves for feeding of various categories of animal). The ACO will take advantage of these classifications, and add detail, e.g., to connect agricultural domains to the technologies used by them, and to connect classes of equipment (such as feed processing equipment) to technology components they use (e.g., sensors, actuators, data communications).

The FoodOn ontology focuses on food for human or domestic animal consumption, spanning from "farm to fork" [7]. It does not include a focus on crop or animal production on the farm, but it does include classes for "Food Transformation Processes" as arise in the food processing

industry. Citation [8] describes requirements for an ontology with a rich structure for processes that can be applied across the full agrifood spectrum from farm to fork. These works can provide an upper-level structure in the ACO for food processing, and may be extended to help model processes occurring on the farm and in the creation of farm inputs. Also relevant are the Food Track and Trace Ontology [9] and the Meat Enterprise and Supply Chain Ontology (MESCO) [10] that model food supply chains including processing steps.

Finally, there are multiple agrifood ontologies focused on support for data mining (e.g., [11], [12]); these may be helpful as we detail the cybersecurity issues associated with data mining and AI in agriculture.

We turn now to research on classification systems and ontologies for cybersecurity.

An invaluable family of highly detailed cybersecurity classification systems has been developed over recent years by the Mitre corporation in collaboration with various communities, including ATT&CK [13], D3FEND [14], the Common Attack Pattern Enumeration and Classification (CAPEC) [15], Common Weakness Enumeration (CWE) [16], Common Vulnerability Enumeration (CVE) [17] and Common Platform Enumeration (CPE) [18]. CAPEC provides an extensive taxonomy of attack types against software, hardware, communications, supply chain, social engineering and physical security. ATT&CK identifies a wide array of tactics that adversaries might use to gain access or disrupt operations, along with techniques to achieve those tactics. The techniques generally map to CAPEC attack patterns. D3FEND catalogs defenses against the attacks identified in ATT&CK and CAPEC. CWE identifies hardware and software weaknesses that might allow for successful attacks, and which may lead to vulnerabilities identified in CVE. Finally, the CPE identifies specific software, hardware and Industrial Control System (ICS) platforms and systems for which CVE vulnerabilities have been identified.

Because of increasing digitization, many aspects of modern agrifood can be characterized as Cyber-Physical Systems (CPS), i.e., systems that involve information, operational and communication technologies, that also interact with the physical world (e.g., see [19]). The NIST Framework for Cyber-Physical Systems identifies the basic building blocks of CPSs [20]. Citation [21] presents the SIMON framework for reasoning about the design and verification of CPS, that leverages several existing models and ontologies, including the NIST CPS framework, the Sensor Observation Sampling Actuator Ontology (SOSA) [22], CAPEC, and the model underlying the Structured Threat Information eXpression (STIX) language [23], among others. The SIMON framework also includes a Cyber Threat Information (CTI) ontology that draws from three sources: CVE, the Exploit Database [24], and Metasploit [25,26]. The SIMON framework enables the efficient integration of multiple models and ontologies to reason about a given CPS context (e.g., traffic management). Citation [27] develops a framework similar to SIMON, but aimed at supporting reasoning about the impacts of cyber attacks on various CPS scenarios. In contrast to those works,, our goal with the ACO is to provide a comprehensive, unified ontology, with links to other existing models and ontologies, that supports reasoning about a wide area of concerns across the full agrifood supply chain.

The IoTSec ontology focuses on cybersecurity for IoT systems, with an emphasis on IoT devices and machine-to-machine (M2M) communication [28,29]. The top-level classes include Asset, Vulnerability, Threat (essentially different kinds of cyber attack) and SecurityMechanism (to reduce risk of attack). The IoTSec is highly relevant to our envisioned ACO, given the increasing digitization of most farm operations, and also because the upper ontology applies to

non-IoT contexts. For example, the underlying intent of the IoTSec Threat class is basically the same as the CAPEC notion of Types of Attack. The ACO will exploit this relationship, thereby providing rich detail (for both IoT and non-IoT technologies) for its Threat class, and linkages from there to D3FEND, ATT&CK, CAPEC, etc. The IoTSec ontology was developed primarily for enterprise applications, and is thus directly relevant to food processing operations. Some adjustments will be required to fit with unique requirements on farms, because, e.g., communications may take place over large distances (e.g., with a tractor), and where animals may damage equipment (e.g., collar-mounted sensors).

The Unified Cybersecurity Ontology (UCO) [30,31] is an ambitious project to provide a framework in which multiple ontologies that correspond to specific aspects of security can be created and selectively combined. Thus, in principle, by appropriate composition and pruning, an ontology that represents the vulnerabilities, attacks, and defenses associated with a particular operational system can be captured.

Citation [32] develops an ontology to facilitate software development that incorporates cybersecurity defense features starting at design time, rather than as an afterthought. This, along with an analog for hardware, will be useful in ACO. Citation [33] develops a dependency model for Supervisory Control and Data Acquisition (SCADA) systems that can facilitate goal-oriented risk assessment. SCADA systems arise in various aspects of agrifood, including food processing and water management systems (both regional and on farm). Citation [34] develops a more generic ontology focused on risk of cybersecurity attacks.

To summarize, on the one hand, there is a wealth of knowledge and practice about the cyber risks, mitigations, etc., associated with the kinds of technologies used in agrifood, along with mature ontologies and classification systems. On the other hand, there is a lack of machine-accessible mid- and low-level information about the equipment used across agrifood. A key goal of our work in the creation of an ag-cybersecurity ontology is to model the mid- and low-level agrifood details and thereby solidify the linkages between the agrifood and cybersecurity models. This will provide the foundation for streamlined and easy access to relevant cybersecurity information for individual stakeholders in the overall agrifood supply chain, to enable them to establish cyber defenses, and identify and mitigate attacks if they do happen.

3. 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.

To illustrate, 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 (including CAPEC, CWE, CVE), and also from sources related to a variety of other areas, such as crop yields, soil conditions, weather projections, biohazards, 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.

This kind of querying capability can be accomplished along the lines described in the Integrated Knowledge and Learning Environment [35]. 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 [36] to specify linkages between multiple ontologies for the different knowledge sources, SPARQL [37] for exploring and navigating the linked ontologies, and Vega-Lite [38] 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 development, 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 passwords, routine software patches, and secure firewalls. The ACO can also be used during runtime, to help with analysis and reasoning about observed anomalies and intrusions, including immediate threats and longer-term suspicious behavior sequences. In addition, the ACO can be used to construct

[2] Communication with Joseph Gendreau, UC Davis.

incident response playbooks that balance mitigating damage during a cyber security incident with ongoing operation of the agribusiness [39], including the aspects of crop and animal health.

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 agrifood 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 [40,41]. These SOCs will maintain a comprehensive and growing knowledge base with user-friendly querying capabilities. The ACO 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 ACO will enable effective information sharing between the SOCs and other interested stakeholders, because the ACO will provide an authoritative vocabulary and structure for the breadth of agrifood cybersecurity information, useful both for human communication and automated processing.

4. 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 [42–44]. This paper reports on the first step of the effort, which is focused on the development of a concept map that includes a subset of the overall domain, incorporating selected high-level classes from the agrifood and cybersecurity domains, and illustrating how the two are interconnected. 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 agrifood and Cybersecurity. As noted in Section 2, we have found that a major challenge is the lack of mid-level details in agrifood models and ontologies about the implements and processes used. These details must be incorporated in order to link agrifood activity to the detailed listings of cybersecurity risks, mitigations and defenses as found in CAPEC, D3FEND, etc.

To allow for a very direct focus on the essential features of the interplay between agrifood and Cybersecurity, we started 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.

5. Preliminary concept map

Our preliminary concept map draws primarily from the NAICS categories [4] involving farm and food processing activities, and the IoTSec ontology [28,29] that addresses key aspects of cyber risks in technology-rich systems. The two figures included here show a subset of the

concepts used, to illustrate the structure of the concept map without overwhelming the reader with detail.

Figure 1 shows examples of agrifood classes based on the NAICS categories on the left and includes animal agriculture, horticulture, and food processing. Each of the systems used in agriculture have a one-to-many "usesSystem" relation to examples of cyber physical systems used in agrifood, shown in the middle-right of the concept map. The cyber physical systems shown here are broad categories, and may have their own subtypes in future iterations of this concept map (e.g., PasteurizationSystem would have a subtype for milk and a subtype for food preservation). These CPS classes then have a one-to-many "usesAsset" relation to examples of asset classes inspired by the IoTSec ontology. While neither the list of CPS classes nor the list of asset classes is exhaustive, future work including surveys of systems used on farms and integration of other cybersecurity vocabularies, like CAPEC, will allow for a more complete framework linking agrifood classes at all levels to corresponding technology classes and their cyber risks.

Figure 2 shows a partial view of the cybersecurity side of the preliminary concept map; the overall structure is drawn from the IoTSec ontology. The color-coded classes in the upper left of Figure 2 correspond to the color-coded classes on the right of Figure 1. When viewed together, these figures illustrate the basic approach that the ACO will use to link agrifood technologies (including at the low-level) with cybersecurity models and ontologies. This will enable the ACO to take advantage of existing cyber security vocabularies to identify and reason about specific weaknesses and vulnerabilities present in agrifood tools and processes, which will in turn allow for substantially improved cyber mitigations and defenses by the agrifood industry.

6. 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 (ACO), namely, the creation of a preliminary 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 risks. 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, agrifood productivity, market conditions, etc.; and (ii) enabling the seamless incorporation of cybersecurity concerns into the full operational lifecycle of using agrifood technologies.

Immediate next steps include fleshing out the concept map described in Section 5, to include lower levels of detail on both the agrifood and cybersecurity sides. This will be done in parallel with the development of "Cybersecurity Technology Landscapes" for various agrifood sectors, to ensure that the ACO is grounded in reality. Likewise, further assessment and mapping of the linkages between the subclasses of agrifood technologies, the cyberinfrastructure components they use, and their combined inherent cyber risks is needed. Further review of the literature and of analysis of extant source vocabularies, including ontology resources, to ensure correctness and completeness is critical.

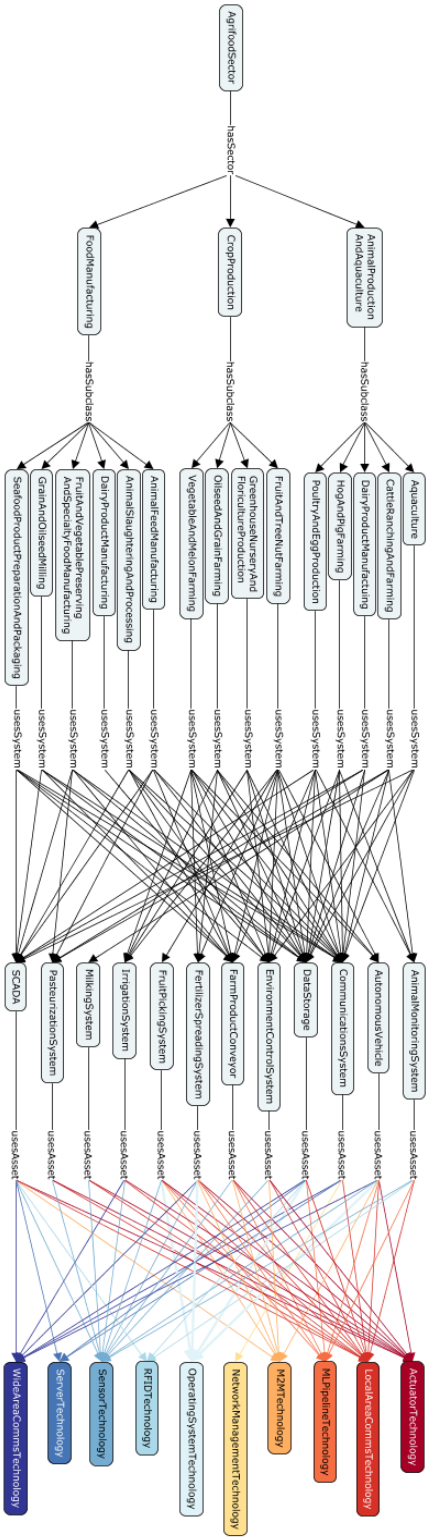

Figure 1: Partial, top-level view of the agrifood portion of preliminary concept map for agrifood cybersecurity.

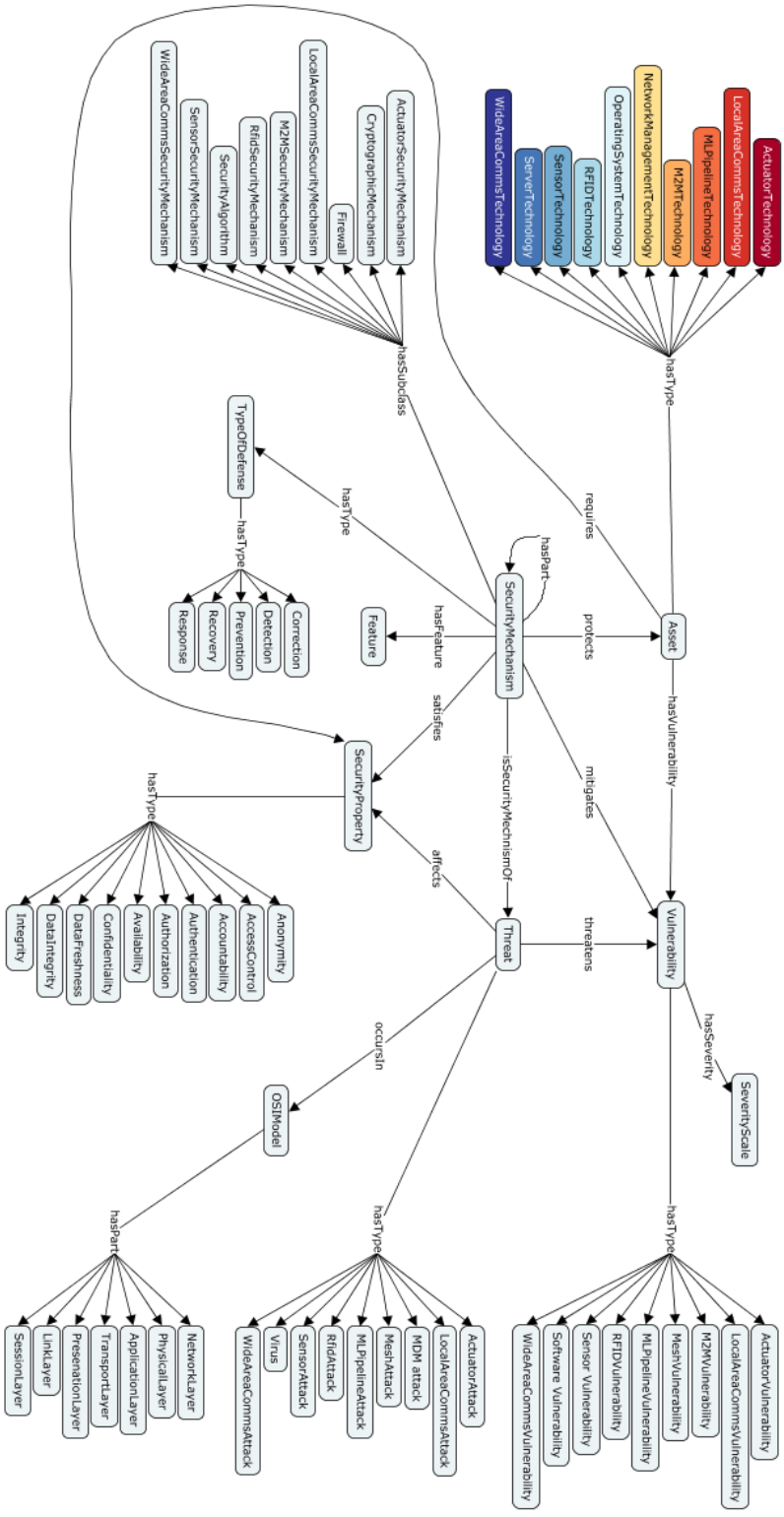

Figure 2: Partial, top-level view of the cybersecurity portion of preliminary concept map for agrifood cybersecurity. (Links between various leaf nodes are not shown.)

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 [45]).

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

References

[1] Kulkarni A, Wang Y, Gopinath M, Sobien D, Rahman A, Batarseh FA. A Review of Cybersecurity Incidents in the Food and Agriculture Sector. arXiv [cs.CR]. 2024. Available: http://arxiv.org/abs/2403.08036

[2] Sontowski S, Gupta M, Chukkapalli SSL, Abdelsalam M, Mittal S, Joshi A, et al. Cyber Attacks on Smart Farming Infrastructure. 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC). IEEE; 2020. pp. 135–143.

[3] Window M. Security in Precision Agriculture : Vulnerabilities and risks of agricultural systems. 2019. Available: https://www.diva-portal.org/smash/get/diva2:1322203/FULLTEXT02

[4] North American Industry Classification System (NAICS). In: United States Census Bureau [Internet]. [cited 5 Aug 2024]. Available: https://www.census.gov/naics/

[5] Medha Devare, Elizabeth Arnaud, Mari-Angélique Laport, Céline Aubert. AgrO: The Agronomy Ontology. In: CGIAR Platform for Big Data in Agriculture [Internet]. [cited 5 Aug 2024]. Available: https://bigdata.cgiar.org/resources/agronomy-ontology/

[6] Caracciolo C, Stellato A, Morshed A, Johannsen G, Rajbhandari S, Jaques Y, et al. The AGROVOC Linked Dataset. Semant Web. 2013;4: 341–348.

[7] Dooley DM, Griffiths EJ, Gosal GS, Buttigieg PL, Hoehndorf R, Lange MC, et al. FoodOn: a harmonized food ontology to increase global food traceability, quality control and data integration. NPJ Sci Food. 2018;2: 23.

[8] Dooley DM, Weber M, Ibanescu L, Lange M, Chan L, Soldatova L, et al. Food process ontology requirements. Semantic Web. 2022. doi:10.3233/sw-223096

[9] Pizzuti T, Mirabelli G, Sanz-Bobi MA, Goméz-Gonzaléz F. Food Track & Trace ontology for helping the food traceability control. J Food Eng. 2014;120: 17–30.

[10] Pizzuti T, Mirabelli G, Grasso G, Paldino G. MESCO (MEat Supply Chain Ontology): An ontology for supporting traceability in the meat supply chain. Food Control. 2017;72: 123–133.

[11] Ngo QH, Kechadi T, Le-Khac N-A. OAK: Ontology-Based Knowledge Map Model for Digital Agriculture. Future Data and Security Engineering. Springer International Publishing; 2020. pp. 245–259.

[12] Fuentes V, Martin T, Valtchev P, Diallo AB, Lacroix R, Leduc M. DCPO: The dairy cattle performance ontology, a tool for domain modelling and data analytics. Available: https://library.wur.nl/WebQuery/wurpubs/fulltext/585046#page=65

[13] Mitre Corporation. ATT&CK Website. [cited 5 Aug 2024]. Available: https://attack.mitre.org/
[14] Mitre Corporation. D3FEND web page. [cited 5 Aug 2024]. Available: https://d3fend.mitre.org/
[15] Mitre Corporation. Common Attack Pattern Enumeration and Classification (CAPEC) website. [cited 5 Aug 2024]. Available: https://capec.mitre.org/
[16] Mitre Corporation. Common Weakness Enumeration (CWE) website. [cited 5 Aug 2024]. Available: https://cwe.mitre.org/
[17] Mitre Corporation. Common Vulnerability Enumeration (CVE) website. [cited 5 Aug 2024]. Available: https://cve.mitre.org/
[18] NIST. Official Common Platform Enumeration. In: NIST National Vulnerability Database [Internet]. [cited 5 Aug 2024]. Available: https://nvd.nist.gov/products/cpe
[19] Kumar K, Behal S, Bhandari A, Bhatia S. Security and Resilience of Cyber Physical Systems. CRC Press; 2022.
[20] D. A. Wollman, M. A. Weiss, Y. Li-Baboud, E. R. Griffor, and M. J. Burns. Framework for cyber-physical systems. 2017.
[21] Venkata RY, Maheshwari R, Kavi K. SIMON: Semantic Inference Model for Security in Cyber Physical Systems using Ontologies. Conference: ICSEA 2018 : The Thirteenth International Conference on Software Engineering Advances.
[22] Janowicz K, Haller A, Cox SJD, Le Phuoc D, Lefrançois M. SOSA: A lightweight ontology for sensors, observations, samples, and actuators. Journal of Web Semantics. 2019;56: 1–10.
[23] Barnum S. Standardizing cyber threat intelligence information with the structured threat information expression (stix). Mitre Corporation. 2012;11: 1–22.
[24] OffSec Company. The Exploit DB. [cited 5 Aug 2024]. Available: https://www.exploit-db.com/
[25] Metasploit. [cited 5 Aug 2024]. Available: https://www.metasploit.com/
[26] Holik F, Horalek J, Marik O, Neradova S, Zitta S. Effective penetration testing with Metasploit framework and methodologies. 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI). IEEE; 2014. pp. 237–242.
[27] Rohith Y. Venkata, Patrick Kamongi, Krishna Kavi. An ontology-driven framework for security and resiliency in cyber physical systems. Thirteenth Intl Conf on Software Engineering Advances (ICSEA). 2018. pp. 13–19.
[28] Mozzaquatro BA, Jardim-Goncalves R, Agostinho C. Towards a reference ontology for security in the Internet of Things. 2015 IEEE International Workshop on Measurements & Networking (M&N). IEEE; 2015. pp. 1–6.
[29] Mozzaquatro BA, Agostinho C, Goncalves D, Martins J, Jardim-Goncalves R. An Ontology-Based Cybersecurity Framework for the Internet of Things. Sensors . 2018;18. doi:10.3390/s18093053
[30] Unified Cyber Ontology (UCO) web page. In: UCO Community [Internet]. [cited 5 Aug 2024]. Available: https://unifiedcyberontology.org/
[31] Syed Z, Padia A, Finin TW, Mathews M, Joshi A. UCO: A Unified Cybersecurity Ontology. Workshops at the thirtieth. 2016. doi:10.13016/M2862BG1V
[32] Shaked A. A model-based methodology to support systems security design and assessment. Journal of Industrial Information Integration. 2023;33: 100465.

[33] Cherdantseva Y, Burnap P, Nadjm-Tehrani S, Jones K. A Configurable Dependency Model of a SCADA System for Goal-Oriented Risk Assessment. NATO Adv Sci Inst Ser E Appl Sci. 2022;12: 4880.
[34] Oliveira Í, Sales TP, Baratella R, Fumagalli M, Guizzardi G. An Ontology of Security from a Risk Treatment Perspective. Conceptual Modeling. Springer International Publishing; 2022. pp. 365–379.
[35] Tu Y, Wang X, Qiu R, Shen H-W, Miller M, Rao J, et al. An Interactive Knowledge and Learning Environment in Smart Foodsheds. IEEE Comput Graph Appl. 2023;43: 36–47.
[36] Moxon S, Solbrig H, Unni D, Jiao D, Bruskiewich R, Balhoff J, et al. The Linked data Modeling Language (LinkML): A general-purpose data modeling framework grounded in machine-readable semantics. ICBO. 2021; 148–151.
[37] DuCharme B. Learning SPARQL: Querying and Updating with SPARQL 1.1. "O'Reilly Media, Inc."; 2013.
[38] Satyanarayan A, Moritz D, Wongsuphasawat K, Heer J. Vega-Lite: A Grammar of Interactive Graphics. IEEE Trans Vis Comput Graph. 2017;23: 341–350.
[39] Shaked A, Cherdantseva Y, Burnap P, Maynard P. Operations-informed incident response playbooks. Comput Secur. 2023;134: 103454.
[40] IT-ISAC Home Page. [cited 5 Aug 2024]. Available: https://www.it-isac.org/
[41] Security Operations Center. In: (United States) Shared Services web site [Internet]. [cited 5 Aug 2024]. Available: https://ussm.gsa.gov/fibf-cyb-soc/
[42] Toro S, Anagnostopoulos AV, Bello S, Blumberg K, Cameron R, Carmody L, et al. Dynamic Retrieval Augmented Generation of Ontologies using Artificial Intelligence (DRAGON-AI). arXiv [cs.AI]. 2023. Available: http://arxiv.org/abs/2312.10904
[43] Kommineni VK, König-Ries B, Samuel S. From human experts to machines: An LLM supported approach to ontology and knowledge graph construction. ArXiv. 2024;abs/2403.08345. doi:10.48550/arXiv.2403.08345
[44] Sanju Saravanan K, Bhagavathiappan V. Innovative agricultural ontology construction using NLP methodologies and graph neural network. Engineering Science and Technology, an International Journal. 2024;52: 101675.
[45] Manimaran Govindarasu, 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.