Cybersecurity and Resiliency in Agricultural and Food Systems

Feras A. Batarseh[1], Manimaran Govindarasu[2], Monowar Hasan, Richard Hull, Doug Jacobson, Lav R. Khot, Karl Levitt, Jim Reecy, Mohammad Sadoghi, Matt Bishop, Greg Goins, Assefaw Gebremedhin, Ananth Kalyanaraman, Surya Mallapragada, Abdolhossein Sarrafzadeh, Kang Xia, Matthew C. Lange

Abstract

Cyberattacks are escalating across the agrifood sector, one of 16 critical national infrastructures designated by the U.S. Department of Homeland Security. Based on a workshop series involving more than 150 stakeholders, this paper proposes the implementation of a consortium led by regional land-grant universities with expertise in AI and cybersecurity, outlining a roadmap for comprehensive response to current/emerging agrifood cyber risks. This includes redoubling efforts in ag-cybersecurity research, education, and workforce development; creation of agrifood security testbeds; cyber threat mitigation activities including AI-driven tools for anomaly detection, intrusion response, secure equipment assembly, etc.; establishing an Agriculture Security Operations Center; and collaboration with non-university stakeholders.

[MAIN]

Cyberattacks in the U.S. were reported to cause approximately $50.5 billion in losses between 2020 and 2024[1]. In recent years, the agriculture/food ("agrifood") sector in the U.S. has been targeted by at least 30 major cyber-incidents, leading to significant financial losses[2], and apparently many attacks against small stakeholders, often unreported[3–5]. The agrifood and affiliated sectors, which account for over 5% of U.S. GDP and over 10% of U.S. employment, includes an estimated 1.9 million farms, 700,000 restaurants, 220,000 registered produce storage, food manufacturing, and processing facilities, as well as supply-chain logistics[6]. The agrifood sector has recently undergone transformative changes, partly propelled by the adoption of innovative digital/cyber technologies enabling increases in production, nutritional quality, disease resistance, safety, flavor, and reducing impacts on and vulnerabilities to climate change[7–12]. The diversity in size and type of agricultural producers, the level and types of digital technologies employed, and the low level of resources and cybersecurity knowledge across agrifood create a complex array of cybersecurity vulnerabilities and challenges for agrifood[2,13–17].

Here, we report a consensus perspective from three regionally coordinated U.S. workshops and follow-up sessions held in 2023-2024 focused on agrifood cybersecurity. Stakeholders came from farms, ag industry, government, academia, and NGOs to assess agrifood cybersecurity challenges and develop a comprehensive plan for safeguarding the U.S. agrifood sector against current and future cyber threats. Presentations were made by workshop participants, the FBI, and the Food and Agriculture-Information Sharing and Analysis Center (Food & Ag ISAC), an industry consortium providing cybersecurity resources. Breakout sessions discussed research, education and workforce challenges and opportunities, along with unique regional needs. Data from plenary discussions and breakout sessions were synthesized using an iterative thematic analysis approach. Workshop outputs were organized around predefined topical areas, with additional themes identified inductively across stakeholder groups and regions.

The workshop series outcomes are described in this paper. Several key cybersecurity issues affecting agrifood systems were identified (Section 2), and the current state of agrifood resilience was assessed (Section 3). The workshops resulted in an action plan for dramatically improving agrifood cybersecurity resilience, led by a multi-regional hub and spoke model consortium of land-

grant universities (Section 4). While the workshop series is centered on the U.S., many of the issues and approaches described here are relevant to other countries with agrifood sectors leveraging digital technologies.

THREATS, VULNERABILITIES, AND CHALLENGES OF AGRIFOOD CYBERSECURITY

The agrifood sector is marked by its immense diversity, encompassing a wide array of products alongside highly varied production, processing, and distribution needs. Stakeholders range from small-scale farmers and cooperatives to corporate agribusinesses, food processing plants, irrigation districts, and others, many of whom operate with limited technical sophistication and resources. The industry comprises numerous sub-sectors with differing levels of automation, including plant and animal breeding, agronomy, horticulture, livestock and poultry production, aquaculture, and supply chain processes including production, processing, storage, transportation, and logistics. Numerous third-party actors are also involved, including equipment distributors, crop consultants, animal immunologists, etc., who act as intermediaries between manufacturers and producers. Agrifood technology is quite heterogeneous, with a strong intermix of IT, Operational Technology (OT), CyberPhysical Systems (CPS) and Machine Learning (ML)[7–9,17]. Regional diversity presents additional challenges, e.g., automated precision agriculture equipment for row crops in the Midwest typically have different control systems than irrigation systems for fruit trees in the Northwest or leafy greens in the Southwest. Cyber vulnerabilities are compounded by the absence of physical security for components like soil sensors, animal wearables, irrigation systems, and exposed routers and edge devices[17,18]. Moreover, the sector faces a critical shortfall in cybersecurity support infrastructure[16], marked by a lack of robust policy frameworks, enforceable compliance standards, and public awareness, and by a workforce ill-equipped in agriculture-specific cybersecurity skills[3,19–21].

Cyberattacks on agrifood might leverage security weaknesses across hardware, networking, software, and advanced machine learning (ML) algorithms[17,22–24], and also weaknesses in the cybersecurity culture[13,17]. Successful attacks can lead to substantial financial loss, supply chain disruptions, and public health challenges due to: reduced productivity, loss and/or disease in crops and livestock; food safety hazards; equipment malfunction or damage; data corruption or theft; compromised decision support; and/or ransomware disruptions. The following illustrates cyber vulnerabilities across agrifood.

Opportunistic Attacks: These exploit easily accessible vulnerabilities—e.g., unpatched systems, weak credentials, or phishing-prone users—without prior targeting of specific organizations[17]. Such attacks are the typical entry point for malicious actors to exploit additional vulnerabilities described below. Small-/medium-sized agrifood operations are especially vulnerable because of low levels of cybersecurity awareness and education, poor cybersecurity hygiene, and operating at thin margins[3,20,21].

Plant Ag: Infield sensors measuring soil and plant nitrogen and moisture levels, and pest pressure levels, enable the application of the right amounts of fertilizer, water, herbicides, or pesticides. If sensor data is corrupted, decision support systems can misguide farmers[17,22,25]. Furthermore, sensors not physically protected may be vulnerable to tampering, potentially creating a pathway for attacks on connected critical system components.[18]

Row Crop Ag: Row crop farming tasks require completion within specific time windows, and most of the large equipment used for planting, spraying, and harvesting relies on GPS real-time kinematics for guidance. Disrupted communication channels between this equipment and satellites, cellular

data, or Bluetooth can lead to widespread crop loss[17,25]. At a smaller scale, a mobile GPS spoofing attack might impact multiple farms across a flat terrain.

Animal Ag: Sensors in livestock barns enable control of heating and ventilation, feed and water supply, and animal health monitoring. Cyberattacks might corrupt sensor data or control systems, leading to decreased productivity, or animal harm or loss[17,25].

ML in Ag: Machine learning models for forecasting, prediction, and control are used widely in precision agriculture. Tampering of sensing devices, or the ML algorithms and their data pipelines, could result in substantial disruptions in the amounts of inputs (e.g., water, fertilizer), or to subtle alterations causing suboptimal agricultural performance that farmers might attribute to other factors[17,18].

Food Processing: In recent years, ransomware attacks have disabled numerous regional and national food processors for multiple days, leading to significant food loss and supply chain disruption[2,14,19]. In general these attacks disrupt IT systems, which leads to shutting down the OT systems and halting production.

Insider Threats: Insider threats[13,26] can originate from farm workers, employees, or contractors through intentional misuse of access to equipment, data, or services. Insider threats could also be unintentional, e.g., if installation of a new component disrupts the farm intranet and creates firewall gaps.

Ag Infrastructure: Agriculture relies on a range of geographically distributed infrastructure, including weather stations and agricultural mesonets, and reservoirs and irrigation canals, mostly networked to the cloud, connected to power grids, and operated by diverse regional and federal managers. Malicious attacks on any component could significantly impact operations across the entire network[2,27].

Public Opinion: Carefully staged disinformation campaigns could dramatically impact the food supply chain[28]. For example, a rumor alleging that beef cattle in the Midwest have contracted mad cow disease might be fabricated from stolen data about herd demographics, and take weeks for the government to discount. Demand for beef might collapse, impacting the downstream beef market, leading to wasted beef and straining alternative food source supply chains[25].

AGRIFOOD CYBER RESILIENCE LANDSCAPE IN THE U.S.

This section describes U.S. government and industry initiatives around cybersecurity, overviews a basic framework for cybersecurity resilience, and explores weaknesses in current agrifood cybersecurity preparedness.

The U.S. government contributes towards cybersecurity resilience primarily through the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), which leads cross-sector risk management, incident response coordination, threat information sharing, and implementation of the National Cybersecurity Strategy. The National Institute of Standards and Technology (NIST) has developed widely adopted frameworks and guidelines, e.g., the NIST Cybersecurity Framework 2.0 (CSF)[29], and supports numerous cybersecurity-targeted databases, e.g., the National Vulnerability Database. The FBI tracks and disseminates information about cyber attacks and malicious actors. Some U.S. states also foster cybersecurity resilience. Several U.S. agencies have a history of supporting cybersecurity research, including NSF, DHS, DoD, DOE, and more recently, USDA. Notably, the National Strategic Research Institute (NSRI) at the University of Nebraska serves as a trusted partner to the DoD, providing essential engineering, research and development capabilities, including in cybersecurity. The DHS supports the National

Counterterrorism Innovation, Technology, and Education Center (NCITE), also based at the University of Nebraska, which is a premier provider of counterterrorism research, technology and workforce development programs.

For agrifood, CISA works with the USDA and FDA; programs include the Food and Agriculture Sector-Specific Plan, voluntary vulnerability assessments, information-sharing partnerships, and cyber hygiene services[6]. FBI field offices organize regional Ag Cybersecurity workshops, and the FBI held a national-level workshop in Nebraska in 2024[4]. In mid-2025 two bills[30,31] focused on agrifood cybersecurity were introduced into the U.S. Congress, with sister bills in the Senate. One[31] would require the USDA to establish a consortium of 5 land-grant universities, similar to the workshop consensus recommendations presented here.

Industry plays a central role in supporting cybersecurity resilience for agrifood through technology development, standards adoption, information sharing, and participation in information-sharing organizations and public–private partnerships. Large agrifood companies, equipment manufacturers, input suppliers, and food processors increasingly integrate cybersecurity safeguards into their products and workforce training. John Deere hosts the annual CyberTractor hack-o-thon event focusing on training and workforce development, in partnership with Iowa State University. Many of the larger equipment manufacturers routinely add known cyber vulnerabilities into the Common Vulnerability Enumeration (CVE), provide patches, and maintain technical advisories about mitigations. Nevertheless, the workshop consensus and outside experts[2,20,32] stress the importance of substantially increasing industry investments into agrifood cyberresilience.

Effectively safeguarding agrifood operations from cybersecurity threats requires deliberate, holistic efforts along several interacting dimensions[33]. Following the spirit of the NIST CSF 2.0[29], Figure 1 illustrates a continuous loop of activities used to prevent or minimize the effects of cyberattacks. Key steps include preventative measures (e.g., strong password controls, network segmentation) and continually watching for anomalies that might indicate cyberattacks. Also essential is establishing mitigation and incident response plans, and performing forensics to understand how attacks succeeded. Risk assessments and cost-benefit analysis can guide investments into overall system resilience. Distinctive aspects of agrifood add a layer of concerns on top of this generic framework.

Unfortunately, the tools and techniques available to malicious actors continue to expand (viz., generative AI and LLMs), leading to new kinds of attacks that are more challenging to detect/mitigate[34]. Concomitantly, agrifood technology continues to expand, broadening attack surfaces and severity. These factors emphasize the need for ongoing research, education and workforce development related to all cybersecurity dimensions in Figure 1.

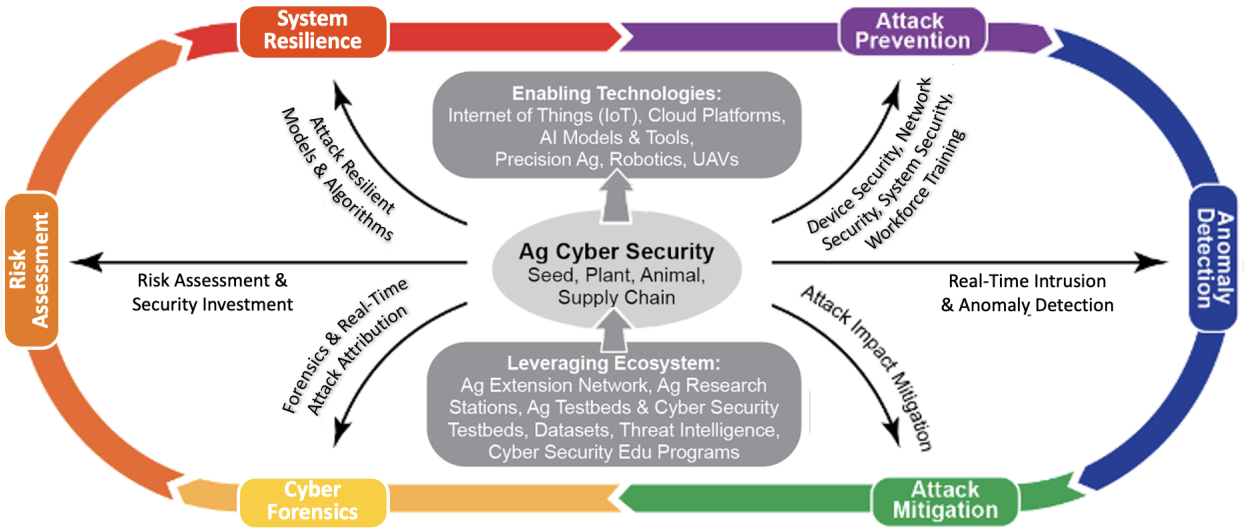

Figure 1: *A holistic cybersecurity framework for agrifood.*

The existing literature indicates that the level of agrifood cybersecurity awareness and preparedness is shockingly low. One Illinois-based survey[3] found that about half of farmers had been impacted by a cybersecurity incident, but only 14% were using firewall software; another[21] found that "beginner" farmers were more likely to use computer technology than more experienced farmers, but they lacked education on cybersecurity risks/mitigations. A UK-based study[35] found that online cybersecurity information can be difficult and confusing for small and medium-sized stakeholders to access and apply to their contexts. Another UK-based survey[20] of mostly small food processing companies found that only half had implemented antivirus software on all computers, and only 25% of employees across the surveyed companies had received cybersecurity training. A recent literature survey[19] on the food supply chain reports increasing automation with vulnerabilities at every stage, and determined that cyber risks are not adequately addressed. These findings highlight the need for cybersecurity education and skills development as foundational for strengthening the sector's resilience.

A PATH FORWARD

The workshop participants call for the creation of a national, geographically distributed Agriculture Cybersecurity Consortium (ACC) based on strong partnerships, including farms, coops, agri-business, cybersecurity businesses, government, NGOs, and academia. The ACC would undertake synergistic activities around three pillars: cutting-edge research and technology transfer, developing research infrastructure and testbeds, and strengthening educational and extension outreach programs (Figure 2). An optimal choice for leading this consortium would be land-grant universities that have strong cybersecurity and AI research programs. Land-grant universities were established by the Morrill Acts of 1862 and 1890[36] to provide practical education in agriculture, science, and engineering. These universities have a history of groundbreaking research in agricultural technologies, extensive undergraduate and graduate agrifood programs, and Extension programs focused on bringing basic and advanced agricultural information/practices to the current and future workforce. Land-grant university Extension programs have long-term, trusted, collaborative relationships across agrifood, enabling deep understanding of regional stakeholder concerns, and opportunities to engage stakeholders in various educational modalities. With cybersecurity and AI research programs in the mix, land-grant universities are well positioned to conduct and disseminate cybersecurity research, education, and training tuned to the agrifood sector. Finally, land-grant

universities provide an open, scientifically driven environment that will foster vibrant collaboration with other organizations and stakeholders.

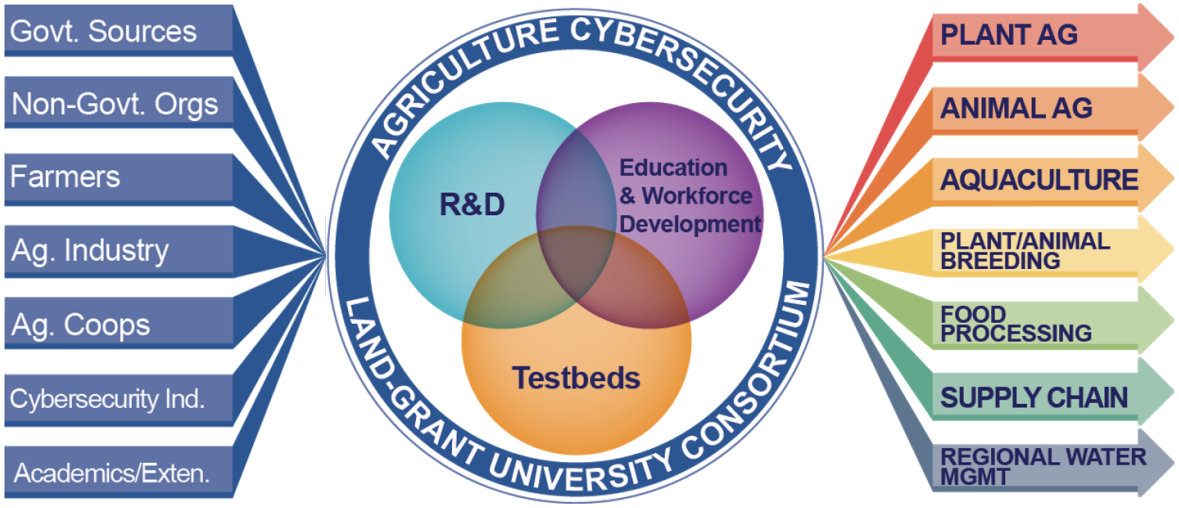

Figure 2: *Agriculture Cybersecurity Consortium ecosystem with three pillars.*

We now consider the three pillars of ACC activity in turn.

Multidisciplinary Research and Development: The ACC would need to pursue strong, broad, and continuous academic research programs geared toward agrifood. The program could address the entirety of the holistic approach shown in Figure 1. Promising research areas include: expanding the use of AI and other emerging technology to support automated detection, defense against, and prevention of, future attacks[24,37]; developing computationally cheaper and easier-to-install authentication methods; improving identification of hardware, firmware, and software security flaws[38]; designing hardware, firmware, and software with built-in security safeguards[39]; developing farming testbed and ecosystems for risk assessment[40], including the use of controlled honeypots to assess adversarial capabilities[41]; exploring the use of permissioned, consortium-based distributed ledger technologies to support tamper-evident data management[42–44]; knowledge management tools to bring cybersecurity best practices information to agrifood stakeholders[45–47], and understanding investment strategies for reducing cyber risk[48]. Much of this research would be performed at land-grant and other research universities with government support from the USDA and others; additional research might be performed by industry.

Research Infrastructures and Testbeds: Establishing research infrastructures and public-private, industry-driven testbeds would bolster the interdisciplinary nature and effectiveness of an ACC. These facilities could support advanced cybersecurity research and collaborative spaces for experts from academia, the agribusiness industry, and others. The testbeds could include real ag components susceptible to cyberattacks, providing real-world scenarios for experimentation and validation of cybersecurity solutions. At least two such testbeds are described in the recent literature[40,41], but these efforts must be substantially expanded. Testbeds for ag cybersecurity could be leveraged for hands-on learning opportunities for students and agrifood professionals, and for demonstrations to the general public. The testbeds could help with developing evidence-driven policies, standards, or guidelines for agrifood. The testbeds could be developed and maintained by Land-grant and other research universities, USDA Agricultural Research Service (ARS) laboratories, USDA Agricultural Experiment Stations, regional irrigation districts, and/or industry consortia, with government support and possibly industrial partnerships.

Educational Programs and Workforce Development: This pillar aims to fundamentally change the cybersecurity culture in agrifood and foster a new generation of professionals equipped with state-of-the-art agrifood cybersecurity awareness, knowledge, and skills[49]. Formal and non-formal education curricula could be developed for all levels and for agrifood practitioners. Extension educators could be trained to deliver practical cybersecurity programs tailored to farm operations and culture, including hands-on technical instruction on topics such as VPNs, network segmentation, and firewalls. Facilitated exercises such as Cybersecurity Incident Management Exercises (CIME) can provide experiential learning that focuses on managing disruptions, maintaining operations, and coordinating response[50]. Education and workforce development initiatives would also need to encompass third-party actors in the agrifood ecosystem. The ACC would focus on sharing and disseminating educational and training modules across regions, demonstration of realistic attack-defense use-cases using the testbeds, threat information sharing, etc. This would be a natural extension of numerous university-led stakeholder workshops and other engagements already held with industry and government leaders, including the workshop series described here. Government funding would be needed to support these initiatives, presumably led by the USDA.

The envisioned ACC could play a central role in establishing and supporting a national, regionally distributed Security Operations Center (SOC) dedicated to agrifood cybersecurity. Working closely with academia, government and industry, the SOC could share information about agrifood cyber threats, technology vulnerabilities and cybersecurity resilience. The ACC could support the SOC by sharing research innovations, technologies and testbeds. The SOC framework could copy long-standing national cyber assistance organizations, e.g., the DHS CISA Computer Emergency Readiness Team or the CMU CERT Division. It might be established as a dedicated national non-profit, a Federally Funded Research and Development Center (FFRDC), or a national non-profit cooperative consortium.

To be most effective, an ACC could be organized in a tiered hub and spoke model. Such models are based on a central hub that collaborates with five regional centers (midwest, northwest, northeast, southwest, and southeast), which are themselves coordinating hubs for regional or local partners. Each regional hub would engage regional and local partners, develop testbeds, undertake agrifood-focused cybersecurity research, and promote regionally customized education and workforce development. One of the regional hubs could serve a dual role as national coordinator. The tiered hub and spoke model has been shown effective in several initiatives, including the National Plant Diagnostic Network (NPDN) and the USDA Climate Hubs program.

CONCLUSIONS

Establishing and maintaining the ACC envisioned in this article will require sustained federal and state investment and strong public-private partnerships. However, the cost of inaction—measured in disrupted food production, food contamination, economic loss, and threats to national security—is far greater. As digital technologies, AI-driven systems, and interconnected supply chains continue to transform agrifood, cybersecurity must be treated as a foundational element of agrifood innovation and resilience, analogous to biosecurity. By proactively integrating research, education, workforce development, and testbeds through a national consortium model, the U.S. can move from reactive crisis management toward anticipatory, national-level resilience. The framework outlined here provides a scalable blueprint for the U.S., and also for other digitally enabled agrifood systems worldwide.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the assistance of Julie Kuhlman, Iowa State University (ISU), for her numerous contributions to this manuscript, including assistance with structuring, revisions, and feedback on technical writing. The work of ISU researchers was funded in part by the ISU Presidential Interdisciplinary Research Initiative.The work of IC-FOODS researchers was supported in part by NSF Award Number 2112606 AI Institute for Intelligent CyberInfrastructure with Computational Learning in the Environment (ICICLE)

REFERENCES

1. Federal Bureau of Investigation (FBI) Internet Crime Report 2024. Preprint at https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
2. Kulkarni, A., Wang, Y., Gopinath, M., Sobien, D., Rahman, A., Batarseh, F., “A review of cybersecurity incidents in the food and agriculture sector”, Journal of Agriculture and Food Research, Volume 23, 2025, 102245, ISSN 2666-1543, https://doi.org/10.1016/j.jafr.2025.102245.
3. Andrew Geil, Glen Sagers, Aslihan D. Spaulding and James R. Wolf. Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *Int. Food Agribus. Manag. Rev.* **21**, 317–334 (2018).
4. Protecting Critical Infrastructure: FBI Agriculture Threats Symposium in Nebraska highlights safety measures to safeguard the nation’s critical food infrastructure. *FBI: News* https://www.fbi.gov/news/stories/agriculture-threats-symposium-in-nebraska-highlights-safety-measures-to-protect-nations-critical-food-infrastructure (2024).
5. Martin, D. Threat of agriculture-related cybercrime is rising: Cybersecurity protocols are just as important as biosecurity. *Farmtario* (2024).
6. Fact Sheet: Food and Agriculture Cybersecurity Checklist and Resources. *CISA: America’s Cyber Defense Agency* https://www.cisa.gov/resources-tools/resources/food-and-agriculture-cybersecurity-checklist-and-resources (2025).
7. M. S. Farooq, S. Riaz, A. Abid, K. Abid and M. A. Naeem. A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access* **7**, 156237–156271 (2019).
8. Wolfert, S., Ge, L., Verdouw, C. & Bogaardt, M.-J. Big Data in Smart Farming – A review. *Agric. Syst.* **153**, 69–80 (2017).
9. Ray, P. P. Internet of things for smart agriculture: Technologies, practices and future direction. *J.*

Ambient Intell. Smart Environ. **9**, 395–420 (2017).

10. Su, X., Sutarlie, L. & Loh, X. J. Sensors, biosensors, and analytical technologies for aquaculture water quality. *Research* **2020**, 8272705 (2020).
11. Awais, M., Wang, X. & Ashraf, M. U. Mitigation and adaptation strategies in climate-smart agriculture: A review for sustainable production. *Climate Smart Agriculture* **3**, 100097 (2026).
12. Abbasi, R., Martinez, P. & Ahmad, R. The digitization of agricultural industry – a systematic literature review on agriculture 4.0. *Smart Agricultural Technology* **2**, (2022).
13. GIAC Cyber Security Discussion Paper. *USDA Agricultural Marketing Service* https://www.ams.usda.gov/about-ams/giac-may-2024-meeting/cybersecurity (2024).
14. Food & Ag ISAC. Farm-to-Table Ransomware Realities: Exploring the 2025 Ransomware Landscape and Insights for 2026. Preprint at https://www.foodandag-isac.org/ (2026).
15. DHS, FDA, USDA. Food and Agriculture Sector-Specific Plan - 2015. *Cybersecurity & Infrastructure Security Agency* https://www.cisa.gov/resources-tools/resources/food-and-agriculture-sector-specific-plan-2015 (2015).
16. Pascual, J. Farm protection from cyberattacks almost non-existent. *Farmers Forum* (2022).
17. Mohammad Ashik Alahe, Lin Wei, Young Chang, Sainath Reddy Gummi, James Kemeshi, Xufei Yang, Kwanghee Won, Mazhar Sher. Cyber security in smart agriculture: Threat types, current status, and future trends. *Comput. Electron. Agric.* **226**, (2024).
18. Pasca, E. M., Delinschi, D., Erdei, R., Baraian, I. & Matei, O. D. A vulnerable-by-design IoT sensor framework for cybersecurity in smart agriculture. *Agriculture* **15**, 1253 (2025).
19. Jones R, Feoktistov D. Cybersecurity vulnerabilities in the food supply chain and their impact on food security: a systematic literature review. *Global Smart Food Systems* **1**, 1–27 (2025).
20. Alqudhaibi, A. *et al.* Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. *Discov. Food* **4**, (2024).
21. A. D. Spaulding, J. R. Wolf. Cyber-Security Knowledge and Training Needs of Beginning Farmers in Illinois. in *2018 Agricultural & Applied Economics Association Annual Meeting* (2018).
22. Sontowski S, Gupta M, Chukkapalli SSL, Abdelsalam M, Mittal S, Joshi A, Sandhu R. Cyber Attacks on Smart Farming Infrastructure. in *2020 IEEE 6th International Conference on Collaboration and*

Internet Computing (CIC) 135–143 (2020).

23. Alahmadi, A. N. *et al.* Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors* **22**, (2022).
24. M. A. Ferrag, L. Shu, O. Friha, X. Yang. Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions. *IEEE/CAA j. autom. sin.* **9**, 407–436 (2022).
25. CISA. Cybersecurity Threats to Precision Agriculture. *Cybersecurity & Infrastructure Security Agency (CISA)* https://www.cisa.gov/news-events/alerts/2018/10/03/cybersecurity-threats-precision-agriculture, https://policycommons.net/artifacts/1571846/threats-to-precision-agriculture/2261625/ (2018).
26. Mahlous, A. R. Security analysis in smart agriculture: Insights from a cyber-physical system application. *Comput. Mater. Contin.* **79**, 4781–4803 (2024).
27. Amin, S., Litrico, X., Sastry, S. & Bayen, A. M. Cyber security of water SCADA systems—part I: Analysis and experimentation of stealthy deception attacks. *IEEE Trans. Control Syst. Technol.* **21**, 1963–1970 (2013).
28. Chowdhury, A., Kabir, K. H., Abdulai, A.-R. & Alam, M. F. Systematic review of misinformation in social and online media for the development of an analytical framework for agri-food sector. *Sustainability* **15**, 4753 (2023).
29. National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework (CSF) 2.0. Preprint at https://www.nist.gov/cyberframework, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (2024).
30. Finstad, B. H.R.1604 - Farm and Food Cybersecurity Act of 2025 (a bill introduced in the U.S. Congress). Preprint at https://www.congress.gov/bill/119th-congress/house-bill/1604 (2025).
31. Nunn, Z. H.R.4046 - Cybersecurity in Agriculture Act of 2025 (a bill introduced in the U.S. Congress). Preprint at https://www.congress.gov/bill/119th-congress/house-bill/4046 (2025).
32. Malone, T. Why cybersecurity must be a top priority for agribusiness in 2025. *Purdue University: Center for Food and Agriculture Business.* https://agribusiness.purdue.edu/2025/02/20/why-cybersecurity-must-be-a-top-priority-for-agribusiness-in-2025 (2025).

33. Haque, M.A., Shetty, S., Gold, K., Krishnappa, B. Realizing Cyber-Physical Systems Resilience Frameworks and Security Practices. in *Security in Cyber-Physical Systems. Studies in Systems, Decision and Control* (ed. Awad, A.I., Furnell, S., Paprzycki, M., Sharma, S.K.) 1–37 (Springer International Publishing, Cham, Switzerland, 2021).
34. Shandilya, S. K. *et al.* GPT based malware: Unveiling vulnerabilities and creating a way forward in digital space. in *2023 International Conference on Data Security and Privacy Protection (DSPP)* 164–173 (IEEE, 2023).
35. Khan, N. , Furnell, S. , Bada, M. , Nurse, J. R. C. , Rand, M. Assessing Cyber Security Support for Small and Medium-Sized Enterprises. in *Human Aspects of Information Security and Assurance. HAISA 2024; IFIP Advances in Information and Communication Technology, vol 721.* (Springer, Cham., 2025). doi:10.1007/978-3-031-72559-3_11.
36. Act of July 2, 1862 (Morrill Act), Public Law 37-108, which established land grant colleges, 07/02/1862; Enrolled Acts and Resolutions of Congress, 1789-1996; Record Group 11; General Records of the United States Government; National Archives. Preprint at https://www.archives.gov/milestone-documents/morrill-act.
37. Ferrag, M. A., Shu, L., Djallel, H. & Choo, K.-K. R. Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. *Electronics (Basel)* **10**, 1257 (2021).
38. Reps, T. Program analysis via graph reachability. *Information and Software Technology* **40**, (1998).
39. Gupta, S., Rahnama, S., Linsenmayer, E., Nawab, F. & Sadoghi, M. Reliable Transactions in Serverless-Edge Architecture. in *2023 IEEE 39th International Conference on Data Engineering (ICDE)* 301–314 (IEEE, 2023).
40. Freyhof, M., G. Grispos, S.K. Pitla, C. Stolle. Towards a Cybersecurity Testbed for Agricultural Vehicles and Environments. in *Proc. 17th Midwest Association for Information Systems Conference (MWAISC)* (2022). doi:10.48550/arXiv.2205.05866.
41. Thilakarathne, N. N., Bakar, M. S. A., Abas, P. E. & Yassin, H. A novel cyber threat intelligence platform for evaluating the risk associated with smart agriculture. *Sci. Rep.* **15**, 3904 (2025).
42. Gupta, S., Hellings, J. & Sadoghi, M. *Fault-Tolerant Distributed Transactions on Blockchain*. (Morgan & Claypool, San Rafael, CA, 2021).

43. I. Homoliak, S. Venugopalan, Q. Hum, P. Szalachowski. A Security Reference Architecture for Blockchains. in *2019 IEEE International Conference on Blockchain (Blockchain)* 390–397 (2019).
44. LF Decentralized Trust. Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric. Preprint at https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study (2019).
45. R. Hull, M. Bishop, J. Gendreau, K. Levitt, M. Sadoghi, M. Lange. Conceptual Modeling to Advance Agrifood Cybersecurity Ontologies. in *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)* (2024).
46. Venkata, R. Y., Maheshwari, R. & Kavi, K. SIMON: Semantic inference model for security in Cyber Physical Systems using Ontologies. in *ICSEA 2019: The Fourteenth Intl. Conf. on Software Engineering Advances* (2019).
47. Tu, Y. *et al.* An interactive knowledge and learning environment in smart foodsheds. *IEEE Comput. Graph. Appl.* **43**, 36–47 (2023).
48. Gordon, L. A. & Loeb, M. P. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.* **5**, 438–457 (2002).
49. G. Grispos, L. Mears, L. Loucks, W. Mahoney. Cultivating Cybersecurity: Designing a Cybersecurity Curriculum for the Food and Agriculture Sector. in *20th International Conference on Cyber Warfare and Security (ICCWS 2025)* (2025).
50. Schultz, M. & Scarbrough, L. Cybersecurity Initiative Protects Iowa Farmers and Rural Businesses: Building a safer digital future for Iowa agriculture. *Iowa State University Extension and Outreach* https://www.extension.iastate.edu/news/cybersecurity-initiative-protects-iowa-farmers-and-rural-businesses (2025).