Implications of Cyberbiosecurity in Advanced Agriculture

Simone Stephen[1-2], Keitavius Alexander[1-2], Lucas Potter[3], Xavier-Lewis Palmer[2-3]
[1]Old Dominion University, Norfolk, USA
[2]CySecSol, Franklin, USA
[3]BiosView, Oswego, USA

sstep008@odu.edu
kalex019@odu.edu
lpott005@odu.edu
xpalm001@odu.edu

Abstract: The world is currently undergoing a rapid digital transformation sometimes referred to as the fourth industrial revolution. During this transformation, it is increasingly clear that many scientific fields are not prepared for this change. One specific area is agriculture. As the sector which creates global food supply, this critical infrastructure requires detailed assessment and research via newly developed technologies (Millett et al, 2019; Peccoud et al, 2018) . Despite its fundamental significance to modern civilization, many aspects of industrial agriculture have not yet adapted to the digital world. This is evident in the many vulnerabilities currently present within agricultural systems, as well as the lacking and fragmented nature of policy dictating cybersecurity stances– the field which intersects both cybersecurity and biosecurity to protect several areas within life sciences (Murch et al, 2018; Duncan et al, 2019; U.S. Department of Agriculture, 2022) . These looming oversights create dangers to advanced agricultural systems, which in turn poses risk to businesses, economies, and individuals. While there are various methods to reduce these risk factors, they ultimately depend on the careful consideration of cyberbiosecurity (CBS) by all involved. This includes the system developers, equipment engineers, and especially the end users - all of us. A conscientious team-effort can work to diminish risks and ultimately provide a safer environment for advanced agriculture and all who depend on it. This analysis explores numerous vulnerabilities within the system of advanced agriculture, discusses potential solutions to the escalating risks they present, and considers the achievable future of an advanced agricultural system which further implements the role of CBS.

1. Introduction

The United States is one of the world's leading food producers, responsible for more than $176 billion of agricultural exports in 2020 (M. Shahbandeh, 2022). The trend within the consistently high production of US agriculture is that of centralization. While the number of farms has declined from 6.8 million in 1935 to 2 million today, the average farm size has gone from 1.5 to 4.5 hundred acres (USDA 2022). This has been enabled by the changing technology of the time, the modern implications of which will be the major topic of this paper.

The cyber revolution is rapidly shaping the world and the agricultural field has begun to implement several new technologies including the internet into its environment. While these new developments have become increasingly essential, the integration of these technologies have also become a source of possible danger. With the emergence of multiple threats in the form of malicious attacks, unwanted intrusions, and sabotage within cyberspace, cybersecurity has become of critical importance within the agricultural field. Recognition of this and many other threatened fields of science has prompted the development of CBS. This new discipline is commonly described as a convergence of biosecurity, cybersecurity, and cyber-physical security. The field encompasses advancing and implementing the protection of life and medical sciences, cyber, cyber-physical, logistics network and infrastructure systems (Murch et al., 2018). As a critical infrastructure, the agricultural field has demonstrated a growing necessity for this discipline. Applications consist of safeguarding intellectual property, data integrity, availability, operation of essential systems, and overall quality of end products (Murch et al, 2018). Other functions include the restriction of access to valuable resources and data, remaining in accordance with standards, regulations, and other important documents, as well as the prevention of financial or reputational damages (Carneiro et al). These aspects could all have significant consequences not only for the industries and organizations themselves, but also their many consumers. Attacks on systems within the agricultural field could disturb the food supply chains already made fragile by the unique challenges presented during the COVID-19 pandemic (Rejeb et al., 2020). This could ultimately result in significant damage to the bioeconomy and communities (Drape et al, 2021). These factors suggest that there is a significant need for cybersecurity.

This also applies to the area of advanced agriculture. For the purposes of this work, Advanced Agriculture is defined as the technology-enabled development of data-driven agricultural systems involving food production, technological food processes, animal feed, bioenergy, agrofuels, and bio-based products (Kanski, 2020). This is often innovative research with the aim of maximizing efficiency, productivity, availability, and sustainability of farming methods (Kanski, 2020). However, despite advanced agricultural systems also having a significant effect on global food supply chains and the bioeconomy, they are remarkably ill-equipped for cyber-attacks. This is evident in an article by Christine Whitt in 2021 stating that at least 80% of the agricultural and food operation in the United States is generated by small family farms, ranches, and food producers (Whitt, 2021). This is an issue because these agricultural sectors receive practically no consideration regarding the security of cyber/IT infrastructure (Whitt, 2021, cited in Drape & Murch, 2022). This is especially an issue as advanced agriculture also commonly involves information sharing for the purpose of facilitating improved data interpretation. Restricting this exchange of data complicates the design of produce generated for specific consumer demands as well as the value chain, and can ultimately heighten CBS risks (Duncan et al., 2020). CBS risks in this field are numerous and increasing every day as technological developments continue to be implemented. These vulnerabilities could allow for significant damage to the confidentiality, integrity, and availability of digital information within agricultural systems. It is crucial for CBS to be further implemented into advanced agricultural systems to safeguard the bioeconomy, food supply chain, and ultimately communities around the world. This work will examine the vulnerabilities within these systems, possible threats, the implications of these threats, and discuss solutions towards reducing risks and aspects of future integration of CBS within advanced agriculture. The major areas of these issues in the farming environment are noted in figure 1 below.

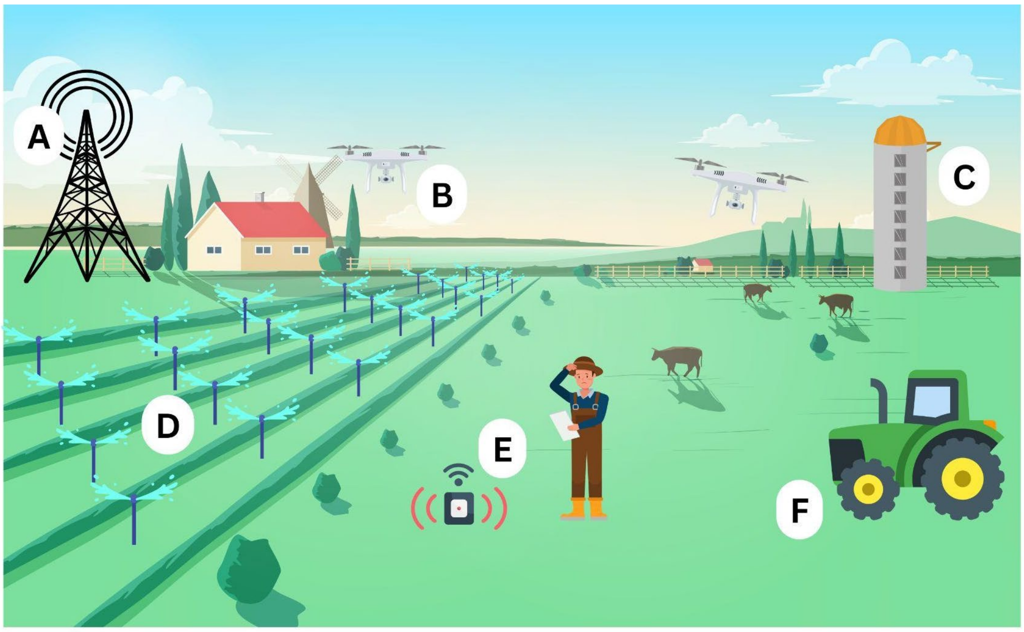

Figure 1: This is an image of a modern farm implementing advanced agricultural aspects. (A) Cyber attacks on the electrical power grids could cease all farm operations that require electricity. (B) Cyber attacks targeting drones used on farms. These attacks could result in the deterioration of the quality of the soil, increasing the difficulty of producing and maintaining a large quantity of agricultural goods (Croptracker). (C) Cyber attacks could target the agricultural sensors and climate controls of storage silos. (D) Cyber attacks on water distribution/irrigation systems. (E) Cyber attackers could target agricultural sensors tracking information regarding: the amount of sunlight received, amount of humidity, compression and density of soil, climate of environment surrounding, soil air penetration, farming activity conducted on soil, and similar data regarding the soil (Geopard, 2022). (F) Cyber attacks targeting technology used as tools or equipment on farms could result in farming becoming more difficult.

2. Hardware

With digital transformation affecting more fields than before, the agricultural field continues to develop technological mechanisms and devices to incorporate into their systems. This includes a multitude of sensor nodes used to attain environmental and livestock data, unmanned vehicles and other robotics used for precise automation of routine field tasks, and the integration of IoT platforms for the use of controlling, interacting, and monitoring of a system of connected devices (Bacco et al., 2019). These developments improve many aspects of the system such as efficiency, productivity, and manageability. For this reason, these new mechanisms and equipment have largely become a necessity. However, the implementation of these new devices also creates many weaknesses within the system. The first component of vulnerability within these systems to be discussed is hardware. In advanced agriculture at the field level, this can take the form of actuators, sensors, and vehicles. These can be used for monitoring critical environmental parameters, executing farming functions, and delivering automated transport (Alahmadi et al., 2022; Saiz-Rubio & Rovira-Más, 2020). While these technologies provide great utility and convenience, not enough attention is given to these devices. Many of these hardware devices do not include an integrated security mechanism to examine their usage, status, or memory access which is essential in securely storing cryptographic keys (Alahmadi et al.,2022). This in turn makes them vulnerable to certain threats.

One of the most common known threats are trojans which are a kind of malicious misuse that can impact system hardware components through covert modification of devices. This could severely alter the intended function of devices or even go as far to stop a function or resource from operating in a denial-of-service attack (Jang-Jaccard & Nepal, 2014). A possible example of this threat causing problems in an agricultural context could be stuxnet-like malware causing the overwatering of crops within a farming system (Wolf, 2014). Another increasing exploitation of hardware is the illegal cloning of devices to contain malware which can cause harm and information leaks (Jang-Jaccard & Nepal, 2014). A possible instance of this would be an attacker discreetly administering a cloned fertilizer spreader with irregular distribution intended to cause under or over fertilization of crops. Another common threat to hardware being side-channel attacks. These are attacks made through exploiting information extracted from the data leakage of a physical cryptosystem. This can take the form of exploiting timing, power consumption, electromagnetic emissions, and thermal signatures which deliver valuable data capable of revealing the encryption standard as well as the keys to crack the encryption (Alahmadi et al., 2022). This can cause the leakage of very sensitive data which can be used or manipulated by attackers. Ultimately, these many vulnerabilities within the hardware of advanced agriculture can cause serious harm and demand to be addressed and appropriately secured.

3. Software

Despite hardware attacks having greater capacity for system influence, the manipulation of software vulnerabilities constitute a significant amount of cyber-attacks. These commonly occur via malware, a form of malicious software that can cause inconvenience, loss, or damage. It is usually loaded into a system, unknown to the system owner, to compromise it for an attacker's gain. It can come in the form of worms, viruses, ransomware, spyware, and bot executables that can be injected to affect nodes and devices (Jaccard & Nepal, 2014; Leclair & Ramsay, 2015). Other causes of software vulnerability within agricultural systems are attacks on applications, such as software update attacks which are executed by interrupting the update procedure of installed software. Another example is buffer overflow attacks, which take advantage of coding errors to overwrite memory and compromise systems. Application attacks also include SQL injection, which is the use of code injection techniques to deceive a database server into executing malicious SQL code that is injected into a database input field. A possible example of this would be an attacker using SQL injection to penetrate and exploit a logistics system into transporting crops to different places than intended or to steal private data from storage systems. These attacks all have the massive potential to cause damage to computer systems (Yazdinejad et al., 2021).

As farms and related research facilities continue to integrate technology, the risk of these attacks increases significantly. Yet, despite recognition of these dangers, many agricultural systems are not prepared for protecting against these attacks. It has been found that in some farming systems, anti-virus software was only installed on most computer systems instead of all, while in others, there were different anti-virus programs downloaded on different workstations. It was also found that some of these systems utilized the same computer systems for both on-farm integration and web-browsing. This also takes place within the agricultural research field in which many projects promote the improved use of technology, but neglect safety in their models

(Windows, 2019). This is evident in how a research study by Kim et al. (2018, cited in Windows, 2019) had been written on the use of farm as a service, sensors, AI usage, and the Internet of Things without any mention of the possible threats and dangers presented. It has also been seen in a paper by Walter et al. (2017, cited in Windows, 2019) that even if dangers are incorporated into articles, they are seen as incidental instead of potential attack points to be taken advantage of by attackers . This demonstrates that despite the rising integration of technology within these agricultural systems, there is a blatant lack of security practices set in place. Ultimately, these vulnerabilities within both the hardware and software applications of advanced agricultural systems demand the implementation of safety measures to create a more secure environment.

4. Threats/Exploitation

4.1 Threats to confidentiality, integrity, availability

The agriculture industry is reliant on secure technologies to maintain, produce, and transport livestock, farm goods, and more. In the future farmer-free farms may exist and be operated by artificial intelligence and robotic systems with only minimal human intervention. Taking insights from Demestichas et al (2020), smart farming setups can have numerous points at which privacy losses and data breaches can occur Demestichas et al., 2020). For instance, a smaller farmer may rely on a mobile computing-based platform for predictions on what crops to grow and when, and false information may cause real-world consequences insofar as crop failure or suboptimal yields. However, a larger agricultural operation may be a more completely autonomous operation, like a smart farming environment. In either case, the real-world necessity and purpose of smart operations make suspensions of network activity dire (Demestichas et al., 2020). Operations with more points of failure and less layering of protective operations can have more opportunities for hardware-based attacks and malfunctions (Demestichas et al., 2020). Digital adversaries seek to gain unauthorized access to machinery and software to gain access to information, databases, and intellectual property. As this industry develops and adapts and advances more capable and hi-tech, developments in cyber defenses should be established. The Frontiers article, “Assessing the Role of Cyberbiosecurity in Agriculture, A Case Study”, stated that:“Smart technologies, while beneficial, have the potential to be exploited by hackers to disrupt the farms using them and the downstream users relying on the supply chain. Potential risks that are attributed with precision agriculture and smart technologies include: false sensor data, data and machinery access control, and data encryption (i.e., ransomware attacks)” (Chi et al., 2017, cited in Drape, 2021).

Cyber threats may also attempt to disrupt agricultural production through means of advanced cyber attacks such as artificial intelligence attacks. AI attacks will search for vulnerabilities more efficiently, and quickly than a cyber attack led by a human. AI cyber attacks also develop massive databases on vulnerable corporate smart farms. A new generation of cybercriminals has emerged, one that is both subtle and secretive, which will influence the future of cybersecurity. “The new generation of cyber threats will be smarter and capable of acting independently with the help of AI. Future cyberattack methods will be able to be aware of their surroundings and make informed decisions based on the target environment” (Guembe et al., 2022). By learning the pattern of repeated behavior of agriculturally focused attacks and their targets, defense actors can make more educated decisions on how to counter malicious ones who may aim to infiltrate, block access, and change or delete information utilized to compute and control operations related to agricultural operations.

4.2 Who benefits from these Exploitations

Exploitation of security vulnerabilities of softwares, machinery, and digital agriculture tools can be beneficial to numerous parties who hold a stake in the bioeconomy, from local to national (brands, governments, cyber criminal organizations, and industries) who view categories and subcategories of agriculture as a threat to their own. Resources such as vegetation, seeds, irrigation systems, cattle in livestock, foods, and fuels are valuables to threats. Stolen data from vulnerable digital and hardware infrastructure and framework can be utilized to attack individuals, companies, corporations, and more. Insights from Alahmadi et al (2022) suggest that relationships between producers of agricultural products and those who trade them are important security intersections to examine. Through the monitoring of parameters that trading competitors use to gauge production efficiency, an actor can isolate weak links in a region’s bioeconomy (Alahmadi et al., 2022). Competitors use data gained through cyber attack to exploit vulnerable farms more and develop larger scale attacks to farms with more advanced cyber defenses. On a national scale, this can be a route to disrupting competing bioeconomies in order to change the state of competition. Expanded to a war-time scenario, this could be a route by which countries asymmetrically compete with their enemies, to the dismay and harm of citizens caught in between. Competition in this vein, through attacking bioeconomies and their supports, have the potential to shorten conflicts, but a huge problem with this is dealing with the after-effects restoring the damaged systems. It is hoped that sufficiently designed agricultural security systems can mitigate this possibility.

5. What Implications Could Mean For Development/Safety of Advanced Agriculture

An agricultural industry that does not address current and future threats is likely to face harsh consequences from adversaries that have prepared these potential threats. The exploitation of automation and remote controls of machinery that can be used to maintain and supervise farms could be used to sabotage produce and ruin a potential energy source in the future. The agricultural industry could become a key player in the energy industry. Photosynthesis plays an important role in agriculture not only for the production of energy rich foods; also for future avenues to combat climate change. Synthetic and genetically engineered photosynthesis could be a prominent source of oxygen and $CO2$. Researchers are eyeing new plant engineering techniques that could improve crop yields and improve food security. (Baslam et al., 2020.) However, with growing concerns of climate and renewable energy, energy and developmental resources located and operated at smart farms could be hacked. Technologies including genetically engineered vegetation could face threats who seek to steal and ruin production though hardware or software attacks. Synthetic photosynthesis and genetically modified plants could be the future of agriculture; however, development and resource allocation must take place to secure placement for new technologies in agriculture. This risk must also be balanced in the midst of macro-level induced issues that endanger agricultural resources. For example, during the COVID-19 pandemic simple vegetation seedlings were difficult to come across. This has caused seed shortages which are expected to also affect the value chain (Nchanji et al., 2021). Similar environmental conditions could occur in a future experiencing extreme consequences of climate change. During these incidents, cyber threats can exploit technological vulnerabilities to gain access and control resources such as the genetically modified seedlings. Advanced genetic engineering technologies could be used as a weapon to steal resources from farms. One hypothetical, future example may be in the form of an engineered DNA stealing parasite that could be a threat to the confidentiality of targeted farms. In the case of Claude dePamphilis, professor of biology, parasitic plants who stole and weaponized genetic information from host plants were found (Swayne, 2016). What may follow from this possibility is the ability of malicious actors one day enlisting biological agents to steal or compromise unique GMO intellectual property. This hypothetical type of attack would not be one that is easily detectable via legacy visual means such as cameras or satellites. A solution to this may lie within passive monitoring systems installed throughout farms. This could also be supported by active monitoring methods through sequencing of samples taken through swabbing, plant cuttings, insect collection, and routine soil examinations that monitor changes in genetic material within these farm environments. We may look to innovations shown in dynamic, rapid integrated monitoring systems in the future.

6. Developing Thoughts on the Future of Advanced Agriculture

As the fourth industrial revolution proceeds to shape the world, the advanced agricultural field will continue to implement technology. To provide the world's growing population with sufficient food and energy products while also combating climate change, the advanced agricultural sector must continue to integrate technology to maximize efficiency. The World Population Prospects project (2015, cited in Goedde et al., 2020) that the population is to reach 9.7 billion by 2050. This in turn, prompts the need for a 70% increase in calories available for consumers according to a report by the United Nations on World Resources Institute (2013, cited in Goedde et al., 2020). The United Nations has also stated that the water supply will be 40% below global water demand by 2030 (2016, cited in Goedde et al., 2020). These projections in combination with the rise of environmental pressures and urge for sustainable agricultural practices suggest the need for further technological integration to resolve these imminent issues. This can take the form of further implementation of smart devices, plant propagation and cultivation technologies, intelligent automated mechanisms, and effective data analysis (Dhar, 2022). These technologies can also consist of more advanced tools like sentinel satellites and drones to provide photos for mapping of spatial variability. These maps could then be used to measure things like crop harvest, humidity levels, topography, and resources in the area (Gorli, 2017). These innovations can aid in ultimately increasing development, diminishing waste, and improving profit margin within the advanced agricultural field (Eashwar & Chawla, 2021). However, they may just be the beginning of an increased utilization of technology. It has been predicted by OnFarm, the creator of a connected farm IoT platform, that the average farm in 2050 will generate about 4.1 million data points per day. This is a 190,000-point increase from the year 2014 (Gorli, 2017).

This demonstrates that the amount of technology implemented into agricultural systems will increase dramatically in years to come. However, the question remains as to whether the advanced agricultural field will be able to properly integrate CBS practices in preparation for this impending innovation. As cyber-attacks are inevitable, CBS will be essential to the future success and security of the agricultural supply chain and bioeconomy, and it would be advantageous to increase and improve security to avert successful attacks rather than in reaction to them (Van der burg et al., 2019).

7. Conclusion

The recent developments in agricultural systems and other similar life sciences have established new technologies which in turn introduce a multitude of new cybersecurity threats. Recognition and detection of these susceptibilities fall under CBS. This work first goes on to describe the relevance, significance, and many vulnerabilities within advanced agricultural systems. Threats to confidentiality, availability, and integrity and potential actors of these threats were then presented to provide a landscape of the many dangers within these spaces. Beyond this, the possible consequences of these threats affecting further development of advanced agricultural systems was established to demonstrate the significance of applying relevant CBS perspectives. The work then finally discussed upcoming world developments prompting the demand for further innovation within agriculture, providing additional incentive for CBS practices in the future. Ultimately, this paper highlights the dangers involved in unprotected advanced agricultural systems and calls for further analysis and awareness of CBS while strongly suggesting the need for solutions.

References

Alahmadi, Adel N., et al. “Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture.” *Sensors*, vol. 22, no. 9, 2022, p. 3520., https://doi.org/10.3390/s22093520.

Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. Electronics. 2022; 11(1):16. https://doi.org/10.3390/electronics11010016

Bacco, Manlio, et al. “The Digitisation of Agriculture: A Survey of Research Activities on Smart Farming.” *Array*, vol. 3-4, 2019, p. 100009., https://doi.org/10.1016/j.array.2019.100009.

Baslam, M., Mitsui, T., Hodges, M., Priesack, E., Herritt, M., Aranjelo, I., & Saenz-Saez, A. (2020). Photosynthesis in a Changing Global Climate: Scaling Up and Scaling Down in Crops. Frontiers in Plant Science, 11(1664-462X). https://doi.org/10.3389/fpls.2020.00882

Carneiro, Renata, et al. “Cyber Attacks in Agriculture: Protecting Your Farm and Small Business with Cyberbiosecurity.” *VCE Publications | Virginia Tech*, 14 July 2021, https://www.pubs.ext.vt.edu/content/pubs_ext_vt_edu/en/FST/FST-387/FST-387.html.

Chi, H., Welch, S., Vasserman, E. and Kalaimannan, E., 2017. A framework of cybersecurity approaches in precision agriculture. In proceedings of the ICMLG2017 5th International Conference on Management Leadership and Governance (pp. 90-95). Reading, UK: Acad. Conf. Publ. Int.

Croptracker (n.d.). Croptracker - Drone Technology In Agriculture. [online] www.croptracker.com. Available at: https://www.croptracker.com/blog/drone-technology-in-agriculture.html.

Demestichas, K., Peppes, N., & Alexakis, T. (2020). Survey on Security Threats in Agricultural IoT and Smart Farming. Sensors, 20(22), 6458. https://doi.org/10.3390/s20226458

Dhar, Payal. “Cybersecurity Report: ‘Smart Farms’ Are Hackable Farms.” *IEEE Spectrum*, IEEE Spectrum, 19 Sept. 2022, https://spectrum.ieee.org/cybersecurity-report-how-smart-farming-can-be-hacked.

Drape, Tiffany, et al. “Assessing the Role of Cyberbiosecurity in Agriculture: A Case Study.” *Frontiers in Bioengineering and Biotechnology*, vol. 9, 2021, https://doi.org/10.3389/fbioe.2021.737927.

Drape, Tiffany A., and Randall Murch. “Leveraging Cyberbiosecurity to Safeguard Agriculture and Food.” *VTechWorks Home*, Virginia Tech, 1 Oct. 2022, https://vtechworks.lib.vt.edu/handle/10919/112168.

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., ... & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting US food and agricultural system. *Frontiers in bioengineering and biotechnology*, *7*, 63.

Duncan, Susan E., et al. “Securing Data in Life Sciences—a Plant Food (Edamame) Systems Case Study.” *Frontiers in Sustainability*, vol. 1, 2020, https://doi.org/10.3389/frsus.2020.600394.

Eashwar, S, and Paras Chawla. “Evolution of Agritech Business 4.0 – Architecture and Future Research Directions.” *IOP Conference Series: Earth and Environmental Science*, vol. 775, no. 1, 2021, p. 012011., https://doi.org/10.1088/1755-1315/775/1/012011.

GeoPard Agriculture. (2022). “What are precision agriculture sensors.” [online] Available at: https://geopard.tech/blog/what-are-the-types-of-sensors-used-in-agriculture/#.

Goedde, Lutz, et al. “Agriculture's Connected Future: How Technology Can Yield New Growth.” *McKinsey & Company*, McKinsey & Company, 11 Nov. 2020, https://www.mckinsey.com/industries/agriculture/our-insights/agricultures-connected-future-how-technology-can-yield-new-growth.

Gorli, Ravi, and G. Yamini. "Future of smart farming with Internet of things." *Journal of Information Technology and Its Applications* 2.1 (2017).

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. Applied Artificial Intelligence, 1–34. https://doi.org/10.1080/08839514.2022.2037254

Jang-Jaccard, Julian, and Surya Nepal. "A Survey of Emerging Threats in Cybersecurity." *Journal of Computer and System Sciences*, vol. 80, no. 5, 2014, pp. 973–993., https://doi.org/10.1016/j.jcss.2014.02.005.

Kanski, Ian. "Center for Advanced Agriculture and Sustainability." *Harrisburg University*, 1 Oct. 2020,https://www.harrisburgu.edu/about/centers-institutes/center-for-advanced-agriculture-and-sustainability/.

Kim, S., Lee, M. and Shin, C. (2018). IoT-Based Strawberry Disease Prediction System for Smart Farming. Sensors, 18(11), p.4051. doi:10.3390/s18114051.

LeClair, Jane, and Sherri W. Ramsay. *Protecting Our Future: Educating a Cybersecurity Workforce*. Hudson Whitman/Excelsior College Press, 2015.

Millett, K., Dos Santos, E., & Millett, P. D. (2019). Cyber-biosecurity risk perceptions in the biotech sector. *Frontiers in bioengineering and biotechnology*, *7*, 136.

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. *Frontiers in bioengineering and biotechnology*, 39.

Nchanji, E., Lutomia, C., Chirwa, R., Templer, N., Rubyogo, J., & Onyango, P. (2021). Immediate impacts of COVID-19 pandemic on bean value chain in selected countries in sub-Saharan Africa. Agricultural Systems, 188(0308-521X), 103034. https://doi.org/10.1016/j.agsy.2020.103034

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: from naive trust to risk awareness. *Trends in biotechnology*, *36*(1), 4-7.

Rejeb, et al."Covid-19 and the food chain? Impacts and future research trends." *LogForum* 16.4 (2020).

Saiz-Rubio, Verónica, and Francisco Rovira-Más. "From Smart Farming towards Agriculture 5.0: A Review on Crop Data Management." *Agronomy*, vol. 10, no. 2, 2020, p. 207., https://doi.org/10.3390/agronomy10020207.

Samori, I. A., Palmer, X. L., Potter, L., & Karahan, S. (2023). Commentary on Biological Assets Cataloging and AI in the Global South. In Proceedings of SAI Intelligent Systems Conference (pp. 734-744). Springer, Cham.

Shahbandeh, M. (22 Aug 2022). U.S. agriculture - statistics & facts. Retrieved from: https://www.statista.com/topics/1126/us-agriculture/#topicHeader__wrapper

Szefer, Jakub, et al. "Cyber Defenses for Physical Attacks and Insider Threats in Cloud Computing." *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, 2014, https://doi.org/10.1145/2590296.2590310.

United Nations (2015). The World Population Prospects: 2015 Revision | Latest Major Publications - United Nations Department of Economic and Social Affairs. [online] Un.org. Available at: https://www.un.org/en/development/desa/publications/world-population-prospects-2015-revision.html.

U.S. Department of Agriculture. (1 Dec 2022). Farming and Farm Income. Retrieved 15 Dec 2022: https://www.ers.usda.gov/data-products/ag-and-food-statistics-charting-the-essentials/farming-and-farm-income/

U.S. Department of Agriculture . (2022, June 2). Animal Health Surveillance in the United States. USDA APHIS | Animal Health Surveillance in the United States. Retrieved September 20, 2022, from https://www.aphis.usda.gov/aphis/ourfocus/animalhealth/monitoring-and-surveillance

Van der Burg, Simone, et al. "Ethics of Smart Farming: Current Questions and Directions for Responsible Innovation towards the Future." *NJAS: Wageningen Journal of Life Sciences*, vol. 90-91, no. 1, 2019, pp. 1–10., https://doi.org/10.1016/j.njas.2019.01.001.

Vinatzer, Boris A., et al. "Cyberbiosecurity Challenges of Pathogen Genome Databases." *Frontiers in Bioengineering and Biotechnology*, vol. 7, 2019, https://doi.org/10.3389/fbioe.2019.00106.

Whitt, Christine. www.usda.gov. (n.d.). "A Look at America's Family Farms." [online] Available at: https://www.usda.gov/media/blog/2020/01/23/look-americas-family-farms.

Windows, Marc. "Security in Precision Agriculture ." *Diva Portal*, Luleå University of Technology, 2019, http://www.diva-portal.org/smash/get/diva2:1322203/FULLTEXT02.

Wolf, Marilyn. "Cyber-Physical Systems." *High-Performance Embedded Computing*, 2014, pp. 391–413., https://doi.org/10.1016/b978-0-12-410511-9.00008-3.

Yazdinejad, Abbas, et al. "A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures." *Applied Sciences*, vol. 11, no. 16, 2021, p. 7518., https://doi.org/10.3390/app11167518.