# Cyberbiosecurity

*Agricultural Cyberbiosecurity Education Resource Collection*

*Authored by David Smilnak, Rebekah Miller, Jaylan Day, and Dr. Hannah H. Scherer*

## What is Cyberbiosecurity?

Technological advancement is happening everywhere. The products we buy are becoming more digital and advanced every day. With **digitization** comes a new set of concerns. While doorbells still ring, they also have a camera. These cameras can often be accessed through the owner's cell phone. Can other people access that camera? How would we know? What are the risks if I access the camera footage using public Wi-Fi? As technology becomes more advanced, we as consumers need to recognize and understand the risks of unwanted surveillance or harmful activities in the everyday things we do.

Technological advancement is also bringing connections among people, information, and devices. Bluetooth, Wi-Fi, and 5G, among others, are all avenues where devices can connect with each other and interact with people, products, and processes in the real world. As digital connections become more common, the need to protect our data and information, secure remotely controlled processes, and safeguard biological material makes cyberbiosecurity more important. Cyberbiosecurity aims to understand and act on these concerns. We can do this by developing measures to prevent, protect, mitigate, and investigate threats that intersect with cybersecurity, biosecurity, and cyber-physical security.

> Cybersecurity: Protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.
>
> Biosecurity: Procedures intended to prevent the introduction and/or spread of harmful organisms in order to minimize the risk of transmission of infectious diseases to people, animals, plants, and the environment caused by viruses, bacteria, or other microorganisms.
>
> Cyber-Physical Security: Protection of physical and engineered systems whose operations are monitored, controlled, coordinated, and integrated by a computing core. Examples of cyber-physical systems include modern automobiles and medical devices.

Cybersecurity, biosecurity, and cyber-physical security are three areas of security that used to be separate from each other. As digital connections become more common, the line between them has started to blur. The digitization of industries, our personal lives, and how we interact enables us to do amazing things, but it also increases the risk of someone abusing that ability. The more technology present in any particular setting, the more pathways there are for people, like hackers, to find weaknesses in those connections to exploit. Cyberbiosecurity works to identify the weak spots between biosecurity, cybersecurity, and cyber-physical security to help safeguard our data and our systems, including our doorbells.

## Cyberbiosecurity in Agriculture

Agriculture is a unique industry with great variety and complexity. It is a focal point for food systems, textiles, government research, and biofuels. It also has a large carbon footprint, requiring many resources, including land. Because of how important agriculture is and how much land is required, agriculture benefits from digital technology. Modern agriculture is more technologically advanced than we might imagine. The use of sensors to monitor soil conditions, irrigation systems that can be controlled through smartphones, and tractors with GPS and self-driving options are just a few of the many ways technology is being utilized in agriculture. Using these types of technology helps reduce the labor-intensive practices relied on in traditional farming but also brings new security considerations.

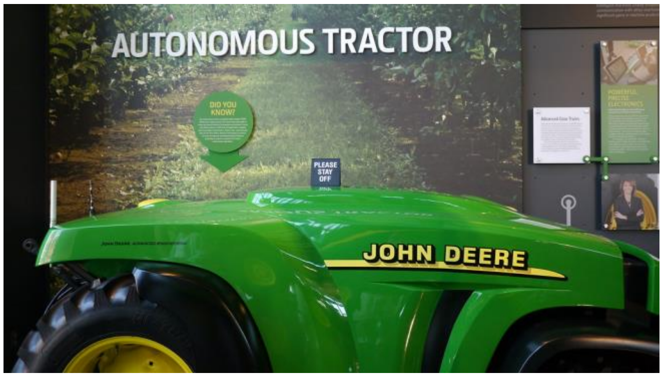

Figure 1. An autonomous tractor by John Deere. "Our Future" by adamthelibrarian is licensed under CC BY-NC-SA 2.0.

Figure 2. Sita Kumari, a farmer, uses mobile phone apps to enhance her yields and get access to markets and labor" by CGIAR System Organization is licensed under CC BY-NC-SA 2.0."

Cyberbiosecurity threats in agriculture can come in many different forms. The simplest example is a **phishing scam**. In 2017, ransomware called WannaCry hacked millions of computers, including those of many farmers. This type of attack makes a computer useless until the hacker removes the ransomware, which they often won't do until they receive money. These kinds of attacks can be devastating to smaller-scale farmers who rely on their computers to run their farms and may not have the means to pay the ransom.

The more technologically dependent agriculture gets, the more advanced the cyberbiosecurity threats can be. In the livestock industry, herd genetics are a crucial part of a successful ranch. As more data is stored digitally, it could be at risk of manipulation if a hacker got access to it. If this happened, a herd's true genetic data could be lost, causing ranchers to miss breeding windows or leaving genetic records unknowingly inaccurate. This is also a matter of national security. Agricultural data is incredibly important for the economy and for food systems. If a foreign government dominates a budding industry and stores that data exclusively within their country, they can control access to that data. While security concerns have always been present on the farm, **precision agriculture**, the **Internet of Things**, **artificial intelligence**, and **big data** make security gaps harder to find, harder to manage, and potentially more detrimental.

Cyberbiosecurity tries to consider the relationships between cyber, biological, and physical concerns to make security as strong as needed. Farms aren't the only place where cyberbiosecurity concerns can impact agriculture. Cyberbiosecurity can include safeguarding the food supply system, protecting financial and personal data stored in cooperatives, securing intellectual property, processes that produce seed varieties, genealogical and veterinary information on livestock, and securing potentially harmful pathogens and pests at research facilities.

## Conclusion

As technology evolves, cyber threats will change as well. Cyberbiosecurity aims to keep up with cyber threats that pose a risk to our cybersecurity, biosecurity, and cyber-physical security. The largest intersection in those areas is you. Human error or negligence is a big weakness in cyberbiosecurity. Often, we might not even be aware of the risk we pose. While the security measures we decide to use may depend on the situation, below are some common security measures we can implement.

1. Check automated systems frequently to make sure they are operating as intended.
2. Secure data with multiple factors: passwords and two-factor authentication.
3. Provide training to employees; do not assume people know the risks.
4. Control access to systems and keep devices secured.

5. Update systems frequently; system updates often include security patches.
6. Backup and secure critical data.

## Glossary

**Artificial Intelligence**: Advanced algorithms that receive input and alter their behavior similar to the way the human brain works.

**Big Data**: Data sets that are increasingly large and complex, in which we can find helpful trends that would not otherwise be apparent.

**Digitization**: Adaptation of a system, process, etc. to be operated with the use of computers and the internet.

**Internet of Things (IoT)**: The connectivity between different computers, sensors, products, and processes via the internet.

**Phishing Scam**: A type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source—an internet service provider, a bank, or a mortgage company.

**Precision Agriculture**: A farm management technique that uses observations and measurements to optimize production.

## Additional Resources

Phishing Attacks in the Agricultural Industry https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/phishing-attacks-in-the-agriculture-industry/#gref

## References

Ramsey, F., & Seyyedhasani, H. (2021). Cyber attacks in agriculture: protecting your farm and small business with cyberbiosecurity.

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). https://www.frontiersin.org/articles/10.3389/fbioe.2019.00063

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*, *6* (39). https://doi.org/10.3389/fbioe.2018.00039

U.S. Department of Homeland Security (2023). *Cyber Physical Systems Security*. https://www.dhs.gov/science-and-technology/cpssec

## About the authors

This resource was developed by faculty and students at Virginia Tech: David Smilnak, Ph.D. Candidate in the Department of Agricultural, Leadership, and Community Education; Rebekah Miller, Ph.D. Student in the Department of Food Science and Technology; Jaylan Day, Undergraduate Student in the Department of Chemistry; and Dr. Hannah Scherer, Associate Professor and Extension Specialist in the Department of Agricultural, Leadership, and Community Education, Virginia Tech.

## Acknowledgments

This resource was developed, in part, with the help and expertise of the Center for Advanced Innovation in Agriculture (CAIA) through a CAIA-Graduate Student Association writing workshop held in 2022. Jordan Wilson contributed to an earlier version of this work.

This work was supported, in part, through the CCI Southwest Virginia Node Cyberbiosecurity Seed Grant program and the USDA National Institute of Food and Agriculture, Women and Minorities in Science, Technology, Engineering, and Mathematics Fields (WAMS) Grants Program, award #2020-38503-31950. Technical and publishing support was provided by the Open Education Initiative of the University Libraries at Virginia Tech.

## About this project

Cyberbiosecurity is an emerging field that focuses on creating security measures for digital aspects of our food and agriculture systems, creating a structure and opportunity for a safe food system that can meet the large needs of a growing population and world. This educational resource was developed as part of a project to support formal and non-formal agricultural educators in integrating cyberbiosecurity topics and research-based strategies for engaging middle-school-aged girls in STEM into their educational programs.

The entire resource collection can be accessed here: https://doi.org/10.21061/cyberbiosecurity

The project is an outreach effort of the Virginia Tech Center for Advanced Innovation in Agriculture.

## Did you know that you can customize and share your version of this Open Educational Resource?