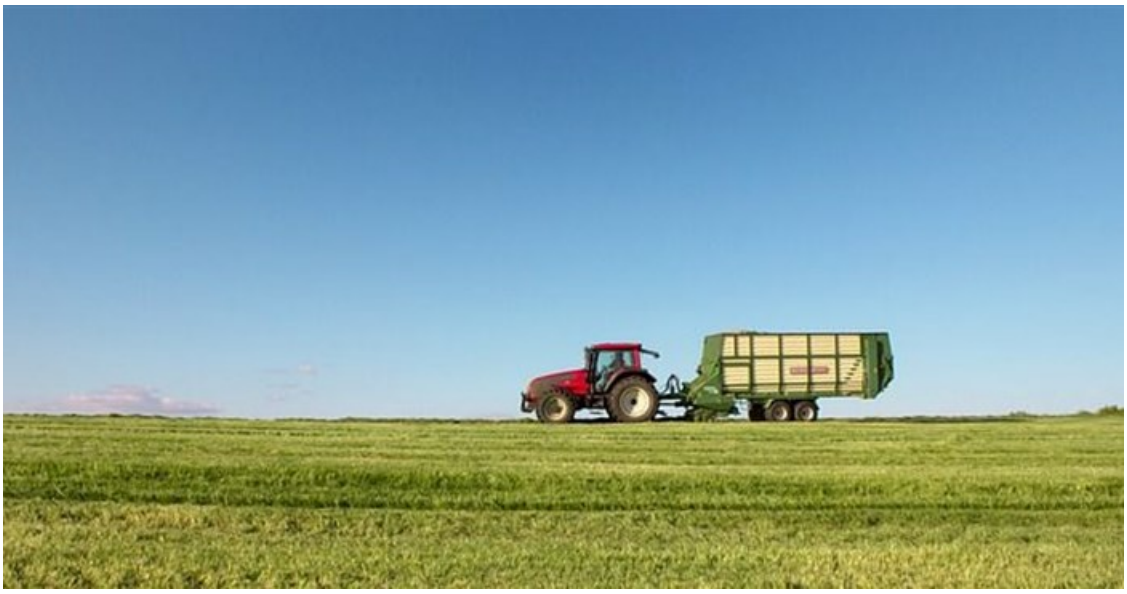
BIZCOMMUNITY

Rise of precision agriculture exposes food system to new threats

By George Grispos and Austin C. Doctor

11 Aug 2022

Farmers are adopting precision agriculture, using data collected by GPS, satellite imagery, internet-connected sensors and other technologies to farm more efficiently. While these practices could help increase crop yields and reduce costs, the technology behind the practices is creating opportunities for extremists, terrorists and adversarial governments to attack farming machinery, with the aim of disrupting food production.



Source: Mathias_Beckmann via Pixabay

Food producers around the world have been under increasing pressure, a problem exacerbated by the war in Ukraine and rising fuel and fertilizer costs. Farmers are trying to produce more food but with fewer resources, pushing the food production system toward its breaking point.

In this environment, it's understandable that many U.S. farmers are turning to modern information technologies to support decision-making and operations in managing crop production. These precision agriculture practices lead to more efficient use of land, water, fuel, fertiliser and pesticides so that farmers can grow more, reduce costs and minimise their impact on the environment.

As researchers in cybersecurity and national security at the National Counterterrorism Innovation, Technology, and Education Center, we see cause for concern. The advent of precision farming comes at a time of significant upheaval in the global supply chain and as the number of foreign and domestic hackers with the ability to exploit this technology continues to grow.

New opportunities for exploitation

Cyberattacks against agricultural targets are not some far-off threat; they are already happening. For example, in 2021 a ransomware attack forced a fifth of the beef processing plants in the U.S. to shut down, with one company paying nearly $11m to cybercriminals. REvil, a Russia-based group, claimed responsibility for the attack.

Similarly, a grain storage cooperative in Iowa was targeted by a Russian-speaking group called BlackMatter, who claimed that they had stolen data from the cooperative. While previous attacks have targeted larger companies and cooperatives

and aimed to extort the victims for money, individual farms could be at risk, too.

The integration of technologies into farm equipment, from GPS-guided tractors to artificial intelligence, potentially increases the ability of hackers to attack this equipment. And though farmers might not be ideal targets for ransomware attacks, farms could be tempting targets for hackers with other motives, including terrorists.

For example, an attacker could look to exploit vulnerabilities within fertilizer application technologies, which could result in a farmer unwittingly applying too much or too little nitrogen fertiliser to a particular crop. A farmer could then end up with either a below-expected harvest, or a field that has been over-fertilised, resulting in waste and long-term environmental ramifications.

Slow to appreciate the threat

Disruption to sensitive industries and infrastructure gives attackers higher returns for their efforts. This means that the increasing stress on the global food supply raises the stakes and creates a stronger motivation to disrupt the US agriculture sector.

Unlike other critical industries such as finance and health care, the farming industry has been slow to recognise cybersecurity risks and take steps to mitigate them. There are several possible reasons for this sluggishness.

One is that many farmers and agricultural providers haven't viewed cybersecurity as a significant enough problem compared with other risks they face such as floods, fires and hail. A 2018 Department of Homeland Security report that surveyed precision agriculture farmers throughout the US found that many did not fully understand the cyberthreats introduced by precision agriculture, nor did they take these cyber-risks seriously enough.

This lack of preparedness leads to another reason: limited oversight and regulation from government. In 2010, the US Department of Agriculture classified cybersecurity as a low priority. While this classification was upgraded in 2015, the farming sector is likely to be playing catch-up for years. While other critical infrastructure industries have developed and published numerous countermeasures and best practices for cybersecurity, the same cannot be said for the farming sector.

The Biden administration has indicated that it is willing to help farmers take steps to protect their cyber infrastructure, but as of this writing it has not released public guidelines to assist with this effort.

All-hands approach

In addition to the pressing need for policy guidance and resources from federal, state and local governments to prevent this type of cyberattack, there is room for academia and industry to step up.

From an academic research perspective, multidisciplinary efforts that bring together researchers from precision

agriculture, robotics, cybersecurity and political science can help identify potential solutions. To this end, we and researchers at the University of Nebraska-Lincoln have launched the Security Testbed for Agricultural Vehicles and Environments.

Farming equipment manufacturers and other industry organisations can help by designing and engineering equipment to account for cybersecurity considerations. This would lead to the manufacture of farming equipment that not only maximises food production yields but also minimizes exposure to cyberattacks.

ABOUT THE AUTHOR

George Grispos is Assistant Professor of Cybersecurity, University of Nebraska Omaha.

Austin C. Doctor is Assistant Professor of Political Science, University of Nebraska Omaha.