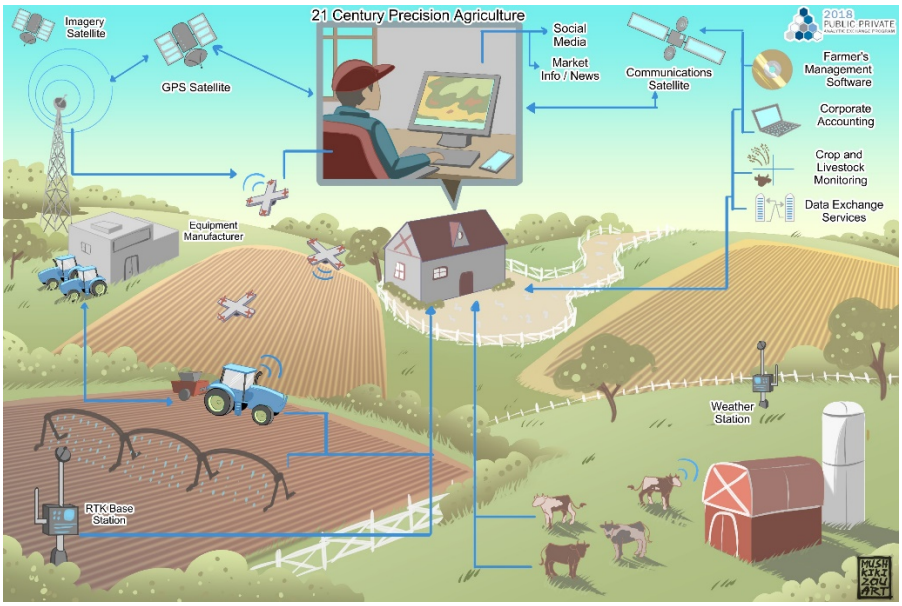
2018 Public-Private Analytic Exchange Program

Threats to Precision Agriculture



ACKNOWLEDGEMENTS

We would first like to thank the Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS) for their thoughtful support throughout the duration of the program.

We are also very thankful for the unique insight we received from contacts and interviewees who contributed their time and information to this report by educating our group on the many aspects of how precision agriculture technology is currently being used in different sectors, where the technology is heading, what are the real or perceived threats, and the safeguarding measures currently being taken. The suggestions on further areas for exploration have also helped considerably.

The people stepping up to help provide information for this project included private industry experts in row crop agriculture, viticulture, specialty crops and livestock production; crop, grain, soil and weather sensor service providers; agricultural robot and drone experts; major agricultural crop and livestock input companies including their IT security experts; major precision agriculture large equipment manufacturers; farm supply companies offering precision agriculture software services; agriculture academics and government officials; and nonprofit organizations concerned with big data and data standards.

We would like to acknowledge all the Team Members and Champions listed below for their contributions to this project and this report. This report would not have been possible without the diverse public and private sector makeup of this team spanning crop and livestock health and production interests, agricultural data analysis, and cyber security.

Team Members

Aida Boghossian	USDA, APHIS, Veterinary Services	Champion
Scott Linsky	USDA, Office of Homeland Security	Champion
Alicia Brown	CHS Inc.	Private Sector
Peter Mutschler	ResponsibleAg and CHS Inc.	Private Sector
Brian Ulicny	Thomson Reuters	Private Sector
Larry Barrett	DHS, Science and Technology Directorate	Government
Glenn Bethel	USDA, Foreign Agricultural Service	Government
Michael Matson	FBI Louisville Division	Government
Thomas Strang	USDA, APHIS, Biotechnology Regulatory Service	Government
Kellyn Wagner Ramsdell	Northern California Regional Intelligence Center	Government
Susan Koehler	USDA, APHIS, Biotechnology Regulatory Service	Government

Contents

Overview

Threats to Precision Agriculture addresses the security threats related to the adoption and impact of new digital technologies in crop and livestock production. Precision agriculture employs a variety of embedded and connected technologies that rely on remote sensing, global positioning systems, and communication systems to generate big data, data analytics, and machine learning. These technologies allow for more precise application of agricultural and livestock management inputs such as fertilizer, seeds, and pesticides, resulting in lower costs and improved yields. A consequence of this rapidly advancing digital revolution is the increased exposure to cyber and other vulnerabilities to the agricultural sector. We have highlighted the potential vulnerabilities arising from using precision agriculture, identified potential threat scenarios, and suggest possible best practices for producers and related agri-businesses.

Key Findings

The adoption of advanced precision agriculture technology and farm information management systems in the crop and livestock sectors is introducing new vulnerabilities into an industry which had previously been highly mechanical in nature. The research group visited and/or interviewed several large farms, and precision agriculture technology manufacturers located throughout the United States. The group identified that the potential threats to precision agriculture were often not fully understood or were not being treated seriously enough by the front-line agriculture producers.

Most of the information management / cyber threats facing precision agriculture's embedded and digital tools are consistent with threat vectors in all other connected industries. Malicious actors are also generally the same: data theft, stealing resources, reputation loss, destruction of equipment, or gaining an improper financial advantage over a competitor. Therefore, improper use of USB thumb drives, spear-phishing, and other malicious cyber-attacks, are readily available threat vectors for an attack; and the generally accepted mitigation techniques in other industries are largely sufficient for creating a successful defense-in-depth strategy for precision agriculture.

Precision agriculture is unique, however, because it took a highly mechanical labor-intensive industry and connected it online, dramatically increasing the attack space available to threat actors. Due to this, otherwise common threats may have unique and far-reaching consequences on the agricultural industry.

The project uncovered potential threats to the crop and livestock sectors using the *Confidentiality, Integrity, and Availability* model of information security. These threats have a potential impact to agriculture resiliency to withstand new types of disruptions which did not previously exist, or dramatically scale up the impact of legacy threats.

Confidentiality, Integrity, and Availability (CIA) are the bedrock principles of information security. Threats against precision agriculture systems can threaten any one of these. The danger is not just cyber-attacks per se, but any danger which could negatively affect CIA, such as natural disasters,

terrorist attacks, equipment breakdown, or insider threats. Based on the diverse nature of the crop and livestock sectors, different aspects of the CIA model were identified as assuming greater importance at different points in the agriculture production chain. Key threats, unique to precision agriculture or where an impact would be magnified by precision agriculture adoption, have been identified under each principle in the CIA model.

Key Threats

Threats to Confidentiality

Data privacy is a top concern when implementing precision agriculture. Farmers are very protective of their information, such as yield data, land prices, and herd health. Loss or misuse of the data can have dramatic financial and emotional impacts on farmers. There is also a potential reputational loss for equipment and software manufacturers. Four unique threats were identified under the confidentiality standard.

Intentional theft of data collected through decision support systems (DSS) or the unintentional leakage of data to third parties. There has been an explosion of DSS and farm information management systems (FIMS), primarily mobile apps, designed to support farmers. Many have been built by start-ups or university extension programs which outsource their programming, and may not provide updates or patching. Privacy controls, user agreements, third party applications, and system update procedures are haphazard at best. Some DSS apps could be malicious by design to steal data. This is the most likely threat to the confidentiality standard.

Intentional publishing of confidential information from within the industry such as from a supplier to damage the company or cause chaos. Like the 2014 Sony cyber-attack, public release of information such as confidential pricing and market data of farmers from a supplier, could have catastrophic impacts for the supplier as it would destroy trust and cause customer loss. This is the most impactful threat to the confidentiality standard.[1]

Foreign access to unmanned aerial system (UAS) data. Major UAS equipment manufacturers in the precision agricultural market are dominated by foreign built systems. A foreign government having access to sensor collection from a UAS provider could create national security issues. A foreign government being able to aggregate important agricultural information on the United States, or identify and image critical infrastructure is also a potential threat.

Unscrupulous sale of confidential data. Confidential data could be used against farmers on the commodity market, which for farmers is a zero-sum game. This project identified at least one insider

[1] In December 2014, malicious actors associated with North Korea hacked into Sony Pictures' internal systems and stole confidential documents. The malicious actors then publicly posted these documents, which included salary information, internal gossip, and details of films still in development. The release of the information caused severe reputational harm to Sony Pictures.

threat example of a company being approached with offers to sell their data under the table to commodity brokers or hedge funds.

Threats to Integrity

Precision agriculture has aggressively moved into "smart farming" with the introduction of massive sensor nets being built in the crop and livestock sectors. Data collection and exploitation is a valuable tool assisting in real-time farming and livestock decisions. As precision agriculture increasingly adopts equipment automation, robotics, machine learning, and edge computing, threats to data integrity are manifesting in ways never contemplated in the agriculture sector.

Intentional falsification of data to disrupt crop or livestock sectors. The presence of a virulent animal disease within the nation's livestock herd, or an unapproved genetic modification can cause massive economic disruption, complex foreign trade issues, and real impacts to food security. It potentially will take extensive time and massive resources to confirm and control a disease outbreak in livestock through laboratory and field work. A malicious actor, publicly releasing false data mimicking actual farm data prior to or during a livestock disease outbreak like foot-and-mouth disease, could take months to resolve to the satisfaction of the agriculture and foreign trade markets. The same scenario would apply in crops with the allegation of a crop disease, or improper mixing of restricted GMO products into the food supply chain. This is the highest impact threat identified under the Integrity standard, and the highest impact threat identified overall. It is an easy threat to potentially manifest as it does not rely on original access to real data.

Introduction of rogue data into a sensor network which damages a crop or herd. In the highest value crop sectors, such as vegetables, fruits, and nuts, smart sensor implementation is deepest. These sensors are often connected via cellular, Bluetooth, or Wi-Fi networks, and many rely on edge computing to make decisions at the source. Introduction of rogue data into these networks could, either intentionally or through faulty sensors, result in issues like under or over watering of a crop, destroying it. The same scenario could apply to "smart" farm buildings being built to manage livestock herds. Faulty sensors which disrupt an HVAC system, for example in an automated livestock barn, could potentially result in adverse health impacts or the loss of animals.

Insufficiently vetted machine learning modeling. Machine learning techniques are beginning to be tested and deployed in advanced precision agriculture applications in both the crop and livestock sectors. Insufficiently modeled algorithms, "100-year storm" data outliers, and inherent biases in the data which creep into the predictive models can all have unintended and adverse effects. This is an evolving, near horizon threat, the consequences of which are only beginning to take shape, but one which the project assessed would grow in importance over time.

Threats to Availability

Farming and livestock operations are heavily equipment reliant. Major farm equipment is, a system of systems, relying on complex embedded tools, and a sophisticated suite of communication and guidance systems. Threats to equipment availability manifest from both cyber-related issues, and natural

disasters. What became evident was the impact to equipment loss is very uneven and is heavily timing dependent.

Timing of equipment availability. For every crop sector, there are very narrow and precise windows for planting and harvesting where equipment must work. Losing the equipment during those key windows, could prevent planting during the optimal planting window, or delay harvest resulting in the loss of crop quality. If a malicious actor could identify a vulnerability in a piece of equipment and disrupt thousands of machines at once, or a poorly designed patch was released at the wrong moment which locked up significant amounts of equipment, it could have an impact on food security and severe reputational loss to the equipment manufacturer. This is the highest impact threat in the availability standard.

Disruption to positioning, navigation, and timing (PNT) systems – space based. The signal spectrum is becoming increasing crowded. In the United States, protected spectrum near the Global Positioning System (GPS) signal is being released for 5G broadband use with the potential for GPS signal disruption. In other countries the bandwidth specifics may be different, but the crowding issue is the same and farmers routinely face some sort of guidance signal loss. In addition, most guidance systems also rely on GLONASS and other foreign systems. Access to these systems could be denied during a crisis or conflict, limiting the ability necessary to fully exploit precision agriculture equipment. This is a cross-sector threat as PNT is used in almost every sector; but it was identified as a core competency of successful precision agriculture applications, therefore it has a high impact potential.

Disruption to PNT systems – ground based. Real-time kinematic (RTK) positioning is a technique used to enhance the precision of position data derived from satellite-based systems. It allows precision agriculture to move from sub-meter precision to centimeter precision for seed planting, agricultural input application, and row crop alignment. RTK requires base stations to process and refine space-based signals. Loss of multiple base stations could impact precision agriculture applications at the county or multi-county level. Major natural disasters can take out base stations on a large scale, as seen with Hurricane Maria in Puerto Rico.

Disruption to communication networks. Farming operations are inherently rural. Precision agriculture is built on distributed sensor networks requiring ever increasing levels of data transfer. Reliable rural broadband is a limiting factor for precision agriculture adoption, and loss of signal, for any reason, including net neutrality concerns, could have a devastating loss on equipment availability. Farmers rely on a hodgepodge of cellular, Bluetooth, and Wi-Fi networks, and still heavily rely on USB drives to manually transfer data. Signal loss and data bandwidth limits common in rural communications networks are a major weak point for precision agriculture. It is the most likely threat impacting the availability standard.

Foreign supply chain access to equipment used in precision agriculture. In addition to issues with data integrity, foreign-manufactured equipment could potentially be remotely disabled in bulk either through built in firmware backdoor access or through malicious code sent to equipment during times of crisis or during key planting or harvesting windows.

Smart livestock production facility failure. Increasingly complex, internet connected buildings that house and manage livestock open vast new attack surfaces such as HVAC or feed systems for malicious cyber actors, software failure, or human error, which could result in potential livestock loss.

Key Controls

While the threats to precision agriculture technologies are unique, the baseline security controls necessary to mitigate these threats are consistent with security controls in other industries. Below are some of the key security controls employed in other industries with applicability and utility in securing precision agriculture technologies and their users. These controls are derived from the Center for Internet Security's Critical Security Controls and guidance from industry practitioners.

- **Implement Email and Web Browser Protections:** Email is the primary vector for attackers to gain network footholds. Email security greatly reduces the attack surface, thereby protecting precision agriculture systems and users. Threats are also regularly encountered while browsing the web. Allowing only authorized web browsers with various scripts disabled further protects precision agriculture companies and users.

- **Limit and Control Network Ports, Protocols, and Services:** Unsecured ports, protocols, and services may allow a remote attacker to gain access to critical systems. Limiting these communications pathways to only authenticated and authorized systems mitigates several threat vectors. A critical control is only allowing remote desktop access through virtual private networks (VPNs) or other encrypted pipelines.

- **Inventory and Control Hardware Assets:** This control encourages network owners to inventory all devices as a means of establishing authorized devices and detecting unauthorized devices. This control is often not implemented at the farm level, but is essential at the precision agriculture vendor level.

- **Inventory and Control Software Assets:** Like the inventory of hardware assets, this control calls for organizations to inventory the various software packages. This control helps determine what security updates may be necessary. Software inventories can also be used to determine authorized and unauthorized software running on precision agriculture systems.

- **Account Monitoring and Control:** Establishing levels of access for authorized users can also greatly increase the security of precision agriculture data and systems.

- **Separate Operational Technologies and Business Operations:** Separating operational technologies like fertilizer distribution machinery and tractors from traditional business networks is critical for mitigating risk to the physical machinery. This separation can be facilitated by virtual local area networks (VLANs), firewalls, and cyber-defined demilitarized zones.

Many of the key threats to precision agriculture relate to data security issues not completely addressed by the above controls. Farmers may benefit from adopting some data security controls.

- **Data Recovery Capabilities:** Precision agriculture companies and users rely on vast data sets whose loss renders much of the technology ineffective. Establishing a plan and maintaining equipment to backup data as it is collected is invaluable in the event of data loss. A plan for implementing data backups after a loss is equally important.

- **Data Protection:** Data recovery is important to continued functionality, but organizations can also prevent data loss in the first place by employing database management tools, encryption, and access control.

- **Understanding Data Ownership:** A critical area of concern for precision agriculture users is understanding who owns what data. Contracts with precision agriculture vendors may change data ownership and impact the privacy of data to which farmers believe they have exclusive rights. Understanding these contracts is critical for securing farm data.

As precision agriculture companies increasingly face technological threats, developing various controls such as incident response and physical security would provide deterrence.

- **Incident Response and Management:** Developing these capabilities early may allow for more rapid recovery from major threats to precision agriculture.

- **Implement Physical Controls:** Defense-in-depth strategies of security emphasize the use of physical security controls to augment cyber security controls. Agriculture in general is multifaceted which thus far has not uniformly implemented these controls. Farmers and precision agriculture manufacturers may consider adding physical security controls restricting access to key technology areas.

Use of these controls and other standard cybersecurity practices can enhance CIA standards without degrading user experience. Additional guidance on best practices can be found at the Center for Internet Security (CIS) Controls Guide. The US Industrial Control System Computer Emergency Response Team (ICS-CERT) also offers guidance on securing critical operational technology.

What is Precision Agriculture?

Precision in agriculture is not a new concept. Livestock and crop farmers have always sought out or developed methods to decrease production costs and increase outputs. From mechanical planters used for seed placement and population, to milking machines and scales to measure feed, agriculturalists have been collecting data and making decisions with that data. Modern precision agriculture, integrating the utilization of satellites and computers didn't begin until the second half of the 20th century.

Precision agriculture is using technology to improve input efficiency and collect output data to facilitate future production decisions. The minimization of inputs results in the least negative effects on the environment. It allows farmers to apply the optimal amount of nutrients, seed, and pesticides in the right location, at the right time, using the right product and right amount to maximize crop yield and save on labor and time. Precision livestock farming (PLF) is the use of advanced technologies to optimize animal production. It allows farmers and ranchers to consistently collect information at the animal level

to recognize sick animals, increase feed efficiency, and save on labor, feed costs, and time. This is enabled by technologies that allow for the customization by animal for functions such as automated milking systems, electronic feeding, and health monitoring.

In both crop and livestock agriculture, precision agriculture provides environmental benefits by reducing required inputs, minimizing energy use, and reducing waste. Due to its tendency to reduce labor and inputs, precision agriculture also provides economic benefits to farmers.

Farmers have always made multiple decisions related to production and planting factors to maximize profits. These decisions include seed (crop type, seed variety); planting (seed density, depth, and spacing); and chemical applications of fertilizer, herbicide, pesticide and nitrogen (timing, application rates, and placement). Farmers integrate multiple technologies to provide actionable information. In precision agriculture, decisions are made related to the factors of productions at a hyper-local scale. This is enabled by combining information from many sensors that precisely map multiple attributes before planting, during planting, during growing, and during harvest. The multiple observations can be combined by modeling, resulting in a detailed prescription (recipes) that minimize costs and maximize yields. These prescriptions result in variable rate applications that are implemented by specialized precision agriculture equipment.

To accomplish this, a large amount of digital data must be collected, analyzed, and stored. There is exponential growth in application development in agriculture which allows farmers to use the integrated GPS in devices like smartphones and tablets for data visualization and data collection. Applications for weather, the recording of field notes, and soil and crop growth information can be linked to site specific information for better decision capabilities.

Field precision agriculture is enabled by precision geolocation, remote sensing, and the mapping of soils, nutrients, crop conditions and the location of weeds and pathogens. On the ground this is accomplished with farm machinery that utilizes Variable Rate Technology (VRT), yield monitoring, Auto-Steering, guidance, navigation, and on-board computers and networking capabilities. Below are descriptions of these technologies in crop and livestock production.

Crop Production

Since the mid-2000s precision agriculture techniques, GPS, differential global positioning system (DGPS) precision location - including satellites, continuously operating reference stations (CORS), and RTK satellite navigation have grown in use and accuracy. Other techniques such as: overhead imagery (multispectral imagery from satellites, planes, and UAS), VRT / variable rate application (VRA), and ground-based sensor collection are other items being developed and in use.

Today precision agriculture is used by a wide variety of farming operations and agricultural practices. This is primarily due to the reduction in cost of precision agriculture technology in the last six years. Farmers no longer purchase guidance systems as the technology is integrated into their farm equipment. This allows a farmer the capability of guidance and controlling of equipment at a much lower cost with a wider range of capabilities. This integrated precision agriculture technology has an unlock fee with varying rates for the capabilities desired.

Location Technologies

A major enabling technology is being able to measure location with centimeter accuracy using RTK. The accuracy of RTK is directly proportional to the distance between the rover and the base station. Farmers must have RTK receivers on farm equipment. They may use existing CORS stations, subscribe to a vendor's RTK base stations, use a neighbor's RTK; or own their own base stations. The base station sends corrected carrier phase information to equipment in real time. Each tractor requires a receiver to communicate with the base station (either by radio antennae or over the internet via cellular service). Activities like auto-steer and guided precision planting, cultivating, controlled traffic, spraying, land leveling, and strip tillage require this level of accuracy to be effective. Threats to this technology include malicious jamming and spoofing technologies that block or alter GPS signals or communications to the tractor.

In-Situ Monitoring and Data Collection

- **Precision Soil Sampling**: Both grid soil sampling and proximal sensors are used in precision agriculture to measure or estimate various soil parameters and characteristics at precise locations. The results are used to create maps for such activities as variable rate fertilizer applications, variable planting rates, and other technology that is dependent on soil types.
- **Proximal Sensors for Soil and Plant Status:** Many different types of sensors operating close to or in contact with soil and plants are used to precisely monitor in real-time the status of properties relative to soil and crop health and management while concurrently recording GPS data.
- **Electromagnetic Induction (EMI) mapping of apparent electrical conductivity (ECa)**: These can be used in conjunction with soil sampling for separating variations in soil texture, porosity, water-holding capacity/drainage, soil cation exchange capacity, depth to clay pan or rock, and soil temperature at a given time and year to year trends.
- **Soil Moisture Sensors**: These can be linked to automated or semi-automated irrigation systems with alerts to notify farmers when to activate them or when there is anomaly to indicate a possible leak.
- **Visible- Near-Infrared Reflectance Spectroscopy (VNIRS)**: VNIRS measurements over a crop canopy can be used to measure the health and nitrogen status. Crop sensors can be mounted or integrated onto tractors to inform on-the-go VRAs of crop inputs such as nitrogen, to detect the presence of weeds on bare ground or between crop rows to inform herbicide applications, or to inform vigor or quality of biomass.

Farm Equipment

- **Auto-Steering and Guidance:** Auto-steering and guidance relies on high-precision GPS technology. A digital record is created of where the rows are planted, to facilitate subsequent operations such as spraying, fertilization or weeding along the same route. This technology has generated advances in new equipment such as small and large field robots, like those used for

thinning and weed control and autonomous tractors and sprayers that precisely apply crop inputs.

- **Section Control:** Farm implements that apply inputs like seed, fertilizer or pesticides are enabled by integration of the field row map into the implement's software. Automatic row shut-offs are activated at specific points or sections to avoid overlap of input application on intersecting rows.

- **Variable-Rate Technology (VRT):** VRT is divided into two types, prescription-based and sensor-based. Prescription based application is decided pre-application while sensor based decisions are made during the application. Prescription based requires an RTK or GPS device. Sensor-based is done instantaneously based on sensor data, and can be implemented without a GPS receiver. VRA facilitates the application of crop inputs specific to locations or zones in a field, as opposed to uniform amounts across an entire field that occur without VRA. In prescription based VRT, a GPS device and receiver and "prescription" map developed from previously collected data are used to guide the material rate adjustment. VRT can also be based on continuous proximal sensing which allows for variable rate adjustments on-the go. More recently, sensor-based systems using imagery, AI, and machine learning to distinguish crops from weeds or other active sensing are integrating this information in real time for direct precision weed control and crop thinning. Both section control and VRT can use special nozzles and injection systems for proper timing and rate adjustments.
- **Yield Monitors:** Yield monitors are sensors connected to an on-board computer that electronically record crop yield as biomass flow or weight while the harvester operates. Such

devices are used for grain, forage and horticultural crops. When coupled with a GPS system to capture spatial information in the field, yield maps can be displayed in GIS systems or farm management software to help identify low and high performing areas of the field to inform decisions on how best to parse inputs to maximize profits.

Remote Sensing Technologies

Remote sensing technologies are used to monitor crop conditions. Remote sensing is based on the interaction of electromagnetic radiation with soil and plant material captured as images with sensors that are mounted on various platforms such as satellites, aircraft, or UAS. Precision agriculture applications involve identifying and collecting images using reflectance information from the visible and near infrared bands from either bare soil (to discern patterns of soil moisture, organic matter etc.) and from crop canopies (to estimate crop health/biomass, nutrient deficiencies, crop damage etc.).

Scouting services are usually sold as a commercial service to farmers as part of integrated pest management. Farms with large field sizes can use free sources from medium resolution satellite. These can be supplemented with imagery from commercial sources. Farmers and crop scouts may also use UAS to obtain the highest spatial resolution observations of plants. Sensors on small satellites and miniaturized for UAS are increasing in number and capabilities that can provide added value in crop scouting; these include multi-spectral, hyperspectral, Radar, Light Detection and Ranging (LIDAR), and thermal imaging.

Machine Learning

Machine learning algorithms can be integrated into decision support tools and are increasingly popular and powerful in many areas, including precision agriculture. Machine learning algorithms are purely about identifying statistical correlations, not causal explanations. All machine learning algorithms share a common strategy. Machine learning algorithms take a (large) number of examples of some kind of entity or situation, for example crop yields, along with data describing various aspects of that entity or situation, the relevant *features (*e.g. soil conditions, weather conditions) that are thought to predict the outcome. The data used to train the model is called the *training data*.

Mathematical algorithms are then used to determine ways of predicting the outcomes based on the input features that minimize the cost of errors. The training algorithm iteratively determines weights on features that minimize the prediction error. For example, the algorithm might determine weights on input features such as soil and weather conditions that yields the least error in predicting crop yields.

Machine learning algorithms result in a *model* that enables predictions based on previously unseen combinations of features. The accuracy of the produced models based on the input for cases not in the training data can then be evaluated. If the test data is sufficiently like the training data, the results should be comparable.

In traditional machine learning, the features are specified by the engineer. Poorly chosen features inhibit predictive models. In contemporary *deep learning* algorithms, some of which are beginning to be used in precision agriculture as well, the features that form the basis of the prediction are induced by the algorithm, generally requiring orders of magnitude more data. For example, the algorithm might

learn to make predictions based on subtle clusters of image features at the pixel level. Because deep learning features are represented as weights on multi-layered network nodes, they are difficult to understand. This means that it is often very difficult to explain why deep learning models work or where they might fail.

Precision agriculture can utilize machine learning algorithms in various ways. For example, machine learning algorithms can be used to categorize the health of a plant or animal, based on features such as vital statistics or other sensor-driven measures. Machine learning algorithms can also predict the amount of fertilizer to apply to a patch of land to maximize yield. Alternatively, machine learning algorithms could be used to estimate plant water stress detection or to assess soil erosion.

Machine learning employed in precision agriculture is susceptible to the same threats as other applications of machine learning. Machine learning algorithms make mistakes, and it is important to understand their accuracy. Machine learning can predict or categorize things incorrectly, either because the test data is sufficiently unlike the training data, or insufficient training data was provided to generalize the model, or external factors important to the prediction were not included in the model, or simply because no machine learned model is completely general and 100% accurate. As such, a machine learned model can wrongly characterize unhealthy plants as healthy or healthy animals as unhealthy. If it has mischaracterized the current situation, it may make incorrect predictions about how well a plant or animal will do under specific conditions. In adversarial situations, machine learning algorithms can even be trained to make bad predictions through manipulation of the training data.

Decision Support Systems (DSS)

Farmers increasingly have access to an array of quantified data from sensors, cameras, and other devices. These DSS are primarily designed to operate on mobile platforms, such as phone, tablets, and in-cab virtual terminals. Traditional decision support systems ingest these data points and either simply integrate them into a dashboard that enables farmers to make decisions based on the data, or applies algorithms and models to the data input to suggest outputs, based on scientific or statistical models.

Livestock Production

Like crop production, livestock production has small profit margins. This makes the growth, development, reproduction, and well-being of each animal critically important for a profitable enterprise. PLF has lagged behind crop production mainly due to the cost and lack of awareness among livestock producers. The main purpose of PLF systems is to collect relevant information frequently and cost effectively while improving animal welfare and minimizing environmental impact.

Current technologies such as robotic milkers, wearable sensors, radio frequency ID ear tags, and feed sensors allow producers to monitor individual animal feed consumption, feedlot movement, temperature, lameness, milk production, meat composition and quality, antibiotic use, weight gain, and environmental data—with minimal human intervention.

However most livestock producers see initial cost, uncertain economic returns, and technology complexity as limiting factors but the technology has proven to provide good returns on investments.

Some examples of employed technologies include:

- Image processing and scales automatically records body weight and body condition scoring.
- Automatic feeding systems stores and mixes different feed components; and distributes onto a feeding table or provides individualized animal feed.
- Wearable sensors and biosensors implanted on animals to detect their sweat constituents, measure body temperature, observe behavior, detect stress, analyze sound, detect pH, and records cows' movements to aid in the detection diseases and lameness in cattle.
- Microphones monitors respiratory infections in pigs by characterization of cough sounds and localization of sick pig coughs. Noise sensors may be important to determine the effect of environment (heat) on chick health.

The bio-sensing technologies combined with advances in the internet of things (IoT) paradigm will provide real-time dissemination of data collected from the farms. Many applications have been developed for handheld devices to reduce the effort of recording data manually. Solar-powered receivers mounted on livestock can collect data that is transmitted to a central server. The final data can be viewed on a custom dashboard or the livestock producer's office computer.

Currently only a few countries (China, Brazil, US, Australia, and those in the European Union), have commercial facilities that use PLF. But considerable effort and progress has been made from universities, organizations, and governments around the world doing research to develop better technological solutions for livestock management.

Precision livestock farming will increase production, decrease labor costs while minimizing the environmental footprint of livestock. The international market for wearable technology for animals is expected to grow from around $1 billion to $2.5 billion in the next decade. The highest percentage of manufacturers of this unique technology is in China and the USA.

Who is Impacted by Precision Agriculture and How Are They Impacted

Agriculture is the world's largest and most diverse industry. No two operations are alike based on management style, the crop produced, and soil and water availability.

The agricultural sector is vitally important to the country's overall economic and food security. The country's relatively small rural population supplies food for the entire country and provides economic exports globally. A smaller family farm may not have all the technology, but will still utilize various aspects of precision agriculture such as soil maps to apply pesticides and fertilizers when and where it is needed. Larger scale farms with more automated machinery will gather additional data points in their fields and roll this data up into precision agricultural platforms that function as decision support tools.

Current statistics indicate the world population is hovering around 7.5 billion people and is expected to reach 8.5 billion by 2030, 9.7 billion in 2050 and over 11 billion by 2100. To feed this sheer number of people, precise food production is critical. Precision agriculture will help manage this problem.

In addition to a hungry population, the following groups are strongly impacted by the use or misuse of precision agriculture technologies:

- **Farmers, Livestock Producers, and Laborers**: Farmers, livestock producers, and farm laborers are impacted by precision agriculture through increased efficiencies and increased cost. Precision agriculture uses technology to improve production, increase efficiency, and reduce labor cost but the initial investment is costly. Where in the past farmers relied on mechanical skills to keep equipment operating, precision agriculture requires them to learn how to integrate computer systems and evaluate data integrity. In most cases, precision agriculture is forcing the farmers to rely more on outside service more. Failure to adopt new technologies puts farmers into a competitive disadvantage. Being able to evaluate which technologies will return on their investment is a critical skill for today's farmers. A lower demand for low skilled labor (thinning, weeding, picking) in specialty crop production is a likely impact from utilizing precision

agriculture technology. Another impact may be the creation of better paying, more permanent jobs for those who become trained in servicing and using this equipment and software.

- **Industries that Support Agriculture (Inputs)**: Precision agriculture gives the input side of the industry (fertilizer and pesticide suppliers, seed companies, equipment providers, consulting, feed suppliers, and financial institutions) tremendous tools to help the farmer and increase customer efficiencies. Fertilizers, pesticides and the equipment to apply them precisely are very expensive and the expertise to run the equipment is limited. This has helped increase the custom application business significantly in this country. Unfortunately, when weather conditions are challenging, there are not enough machines and people available to meet the demand. Financial Institutions have access to more accurate performance numbers and farm plans which provides an additional level of risk management for their organization. Due to high costs of equipment and the added expenses for expertise to analyze precision agriculture data, farm sizes are increasing and consolidating. This consolidation of farms could expose a bank to bigger risk and can trigger catastrophic conditions for the organization.

- **Organizations that Support Agriculture**: The organizations that support agriculture vary from the local farm organizations, to the county-level extension offices, to the trade associations, to the vocational schools and universities, to the various government agencies. These organizations contribute in many ways to the success of farm and livestock operations. In addition, some groups have even joined forces as consortiums to develop best practices and standards into agricultural operations. For example, Ag Vo Tech programs in schools provide the training required to utilize precision agriculture technology. One of the limiting factors in the advancement of precision agriculture is the lack of technology skilled individuals who understand agriculture. The US educational system will be critical in finding and developing this talent. These organizations are also very important in maintaining the integrity within the system from regulation to research. Precision agriculture technology can be used inappropriately to profit from the farmers efforts. Our government agencies and trade associations are an important agent in identifying and blocking these efforts.

- **Industries that Rely on Outputs or Data from Agriculture**: Precision agriculture is extremely important for the output side of production that depend on crop yields and livestock products to produce products at the retail level. Food processors, grain dealers, commodity brokers, energy producers, manufacturers, and crop insurers all heavily depend on accurate data and quality final products to ensure the safety of the food products reaching the market is significant. Consumers are also demanding integrity in the products they are buying and this data.

- **Human and Animal Health and Safety**: Disease and contamination can devastate a food processor or distributor. Precision agriculture allows closer tracking of crops and animals through every step of production. Precision agriculture provides the tools needed by producers and regulatory officials to improve the health of herds and the safety of the food that we buy.

Hypothetical Threat Scenarios

The following are eight hypothetical threat scenarios under the various *CIA* standards. The threat scenarios variously attack precision agriculture's embedded and digital tools to impact data confidentiality, data integrity, and availability of equipment. Identified impacts scale from the individual farmer up to the national-security level which impact the United States' food security. At least one scenario under each standard is based in whole or in part on real life examples uncovered during the project.

Confidentiality Scenarios

Scenario 1

A farmer co-op provides services to their members. Like a credit union, the co-op exists for the benefits of the members. A co-op collects highly sensitive yield data and purchase prices, and costs of feed, fertilizer and herbicides sold to farmers. Many co-ops are also aggressively entering the precision agriculture market from an agronomy standpoint, offering detailed consulting and prescription plans for members, which requires the members to provide access to sensitive land use information.

- A co-op accidently exposes their internal data on an unsecured, Internet facing computer.
- An insider threat steals and publishes internal data.
- An outside malicious actor targets the co-op in a cyber network operation and steals and publishes internal data.

In all three sub-scenarios, the result is the same. Highly confidential data of farmer co-op members is exposed, and any / all discrepancies in price and purchase information is available to all members. Agronomy data on individual farms, important for land purchase / lease issues, and crop insurance, is also exposed. This type of "Sony Hack" would cause significant financial and reputational loss to a co-op, and potentially hundreds or thousands of members, because an agricultural co-op is built upon an explicit trust model of equality of its membership.

Scenario 2

Foreign companies dominate the commercial UAS markets. Their cloud service could be configured to store sensor data in the foreign country and under local laws be available to a foreign government.

- A foreign government exploits access to sensor data regardless of user agreements consumers have with the company to review millions of sensor images being generated by agricultural UASs. A foreign government could then exploit the data to create higher fidelity assessments of US agricultural yields, and potentially actionable intelligence useful in trade negotiations.

- In addition, foreign governments could identify critical infrastructure located in rural areas and obtain high-fidelity sensor data on that infrastructure as a by-product of farm use of UAS sensor collection.

Integrity Scenarios

Scenario 3

A major crop disease infestation or virulent animal disease creates immediate, cascading effects resulting in economic loss from destroyed crops or animals, and often significant foreign trade issues as countries ban meat or vegetable imports until the crisis is contained. A scenario attacking data integrity which implies there was a crop or animal disease outbreak was identified as one of the highest potential impact scenarios by experts interviewed in the crop and livestock sectors.

A cyber threat actor protesting the use of antibiotics in meat wants to attack the livestock industry. The terrorist conducts a cyber network operation targeting large US cattle operations which rely on open range feeding across thousands of acres, and steals the herd data collected to monitor/manage the health of the herds. They modify the data to look like the herds have foot and mouth disease, and dump the data on the Internet.

It could take weeks to confirm through laboratory and field work that the “activist” data “revealing” an outbreak was fake and there was no disease outbreak. Mitigation would take a 100 percent accountability of all cattle in those herds, compared against data backups, to verify that foot and mouth had not occurred. An integrity (perception/trust) attack of this type could have the potential for large industry stock market losses, negatively impact exports and public trust due to the difficulty in proving a negative in the face of realistic looking fake data.

Scenario 4

Rogue data ingested into sensor networks tied to automated decision support systems or a machine learning system could have dramatic, adverse effects in a short amount of time.

- A farmer has fields planted across multiple counties. The farmer deploys remote weather stations to the fields with soil moisture sensors, connected to water pivots, to automate water systems. A soil moisture sensor fails, or is maliciously hacked by a neighbor, and the sensor indicates watering is continuously needed, triggering the pivot when not needed, and flooding a field.

- Fully automated robotic milking barns are a potential game changer for larger dairy herds. Cows need milking 2-3 times a day, seven days a week. This does not allow for any down time for a dairy farmer – ever. This automation extends not just to the robotic milking machines, but the industrial internet of things (IoT) systems used for building management and maintenance of the barn housing the herd. A failure of an IoT sensor managing the environment of the barn, or one deliberately manipulated to provide false readings to programmable logic controllers, could

cause a dramatic shift in temperature or feeding conditions in a barn in a very short amount of time, negatively impacting herd health and milk production.

Scenario 5

Embedded and digital tools in livestock production are beginning to generate massive amounts of near real-time data in support of individual animal health and breeding decisions. A malicious actor could alter data or algorithms in livestock or thoroughbred management software about a competitor's breeding stock, causing them to miss breeding gestation windows for high-value animals and causing significant financial loss.

Availability Scenarios

Scenario 6

Crop producers have narrow, inflexible timeframe for planting and harvesting where major equipment is critical. Equipment malfunction during planting and harvesting was identified as a unique circumstance where attacks against precision agriculture embedded tools creates one of the highest impact threats facing precision agriculture.

- An individual farmer receives a bad software patch just before planting, degrading the planter's precision capability, but leaving the mechanical tractor operable. The farmer could fall back on less precise manual row planting, but because of the extremely tight precision tolerances in row width and depth required to successfully plant 40,000 corn seeds per acre, the farmer must stop his planting season until his precision capability is restored, possibly missing the entire planting window, or sacrifice yield potential to plant a crop using only mechanical means at 20,000 seeds per acre.

- Hundreds of farmers purchase diagnostic software on pirated software markets to jailbreak their tractors and sprayers and conduct diagnostic work on-site instead of taking their equipment to a dealership for service. Unbeknownst to the farmers, there is an exploitable vulnerability in the software, or a built in backdoor. When planting season starts hundreds of tractors are exposed to malicious actors who could:

    - Brick up equipment, possibly for ransom, resulting in planting loss of hundreds of thousands of acres of row crops, and creating massive reputational loss to the equipment manufacturer.

    - Use online connected equipment as an access point into other networks for traditional cyber operations to target a farmer's network or third-party data collectors.

Scenario 7

Foreign-built agricultural equipment could have built-in firmware access to support updating and other remote access needs, or have remote access tools (RATs) installed by a foreign government as part of a supply chain interdiction attack. A foreign government could remotely disable agricultural equipment

during critical planting and harvesting windows in a destructive equipment attack targeting the US agriculture sector.

Scenario 8

Natural disasters can have a dramatic, if temporary impact, on guidance and communication systems. Like the island-wide loss of CORS stations during hurricane Maria in 2017, which impacted RTK-level sub-centimeter precision capability, other natural disasters can disrupt guidance and communications at the local, regional, or state level. As communication systems are not as redundant and resilient in rural areas, it takes less of a natural disaster to have a significant impact on a farmer's ability to employ precision tools if the disaster strikes at the wrong time.

Best Practices to Protect and Build Resilience into Precision Agriculture

Adoption of information security standards for precision agriculture is important for the future success of precision agriculture, along with industry efforts for equipment interoperability and data use / privacy.

Industry recognized critical security controls highlighted earlier could protect against many threats to precision agriculture. Vetted best practices, borne from hard experience learned in other sectors which have proceeded agriculture in the digital revolution, offer a proven path for data security.

Efforts to build industry standards for equipment interoperability, data transfer between proprietary systems, and privacy / user standards, also build confidence and strengthen the integrity of precision agriculture technologies. Improving the resiliency of guidance and communication systems, and redundancy in embedded tool technology strengthen resilience in precision agriculture systems to withstand chronic stresses and acute shocks.

The project identified three key areas to protect systems and data, and build resilience into precision agriculture infrastructure.

- Embrace and implement recognized information security critical security controls to maintain and protect embedded and digital tools used in precision agriculture. Many if not most of these controls are items designed to be implemented by equipment and software service providers of precision agriculture technology to the ultimate end-user, the farmer. However, many of these controls are also good cybersecurity practices for individual farmers on their personal networks. Taken together, they provide good defense-in-depth to protect against threats, and mitigate impacts when incidents inevitably occur. The 20 Center for Internet Security's Critical Security Controls designed by cyber industry experts as part of a comprehensive information security regime are:
    - Inventory of authorized and unauthorized devices.
    - Inventory of authorized and unauthorized software.
    - Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers.
    - Continuous vulnerability assessment and remediation.

- Controlled use of administrative privileges.
- Maintenance, monitoring, and analysis of audit logs.
- Email and web browser protections.
- Malware defenses.
- Limitation and control of network ports, protocols, and services.
- Data recovery capability.
- Secure configurations for network devices such as firewalls, routers, and switches.
- Boundary defense.
- Data protection.
- Controlled access based on the need to know.
- Wireless access control.
- Account monitoring and control.
- Security skills assessment and appropriate training to fill gaps.
- Application software security.
- Incident response and management.
- Penetration tests and red team exercises.

- Continue development of agricultural industry standards, both technical ISO standards for data and equipment, and privacy / use standards for data generated by precision agriculture applications. Transparency standards on how information is generated, used and shared strengthen all three pillars of the *CIA* information security model.

    i. Continuing industry efforts to expand and improve upon the CANbus and ISOBUS standards critical for equipment interoperability.
    ii. Continuing industry and non-profit efforts through organizations like AgGateway to build standards for exchange of digital information between DSS / FIMS programs.
    iii. Continuing efforts through organizations like the Ag Data Coalition and Open Ag Data Alliance to build best practices for data use and privacy.

- Building resiliency into rural navigation, communication, and embedded tool applications by developing multiple communication and computer processing paths such as 5G cellular, Wi-Fi, satellite, cloud services, and edge computing. This includes alternative technologies, such as lidar or cameras mounted on equipment to create dual or tri-sensor modes for navigation and guidance, to compensate for temporary guidance loss or degradation. This resiliency supports the core technologies upon which all other precision agriculture applications are anchored.

Areas for Additional Research

During this research, several topic areas emerged that were outside of the scope of this research, but nonetheless warrant further exploration. Below is a selection of these topics

- ***Threats to Food & Animal Feed Processing and Manufacturing***: This research did not examine threats to facilities and companies engaged in the processing and manufacturing of foods or animal feed. This area is likely susceptible to many of the same threats as precision agriculture in addition to threats more commonly seen in the critical manufacturing sector. This includes a

lack of proper supply chain management for livestock feed products to ensure they are from approved sources. If computer systems are tracking these ingredients and system failures occur, feed ingredients from countries with high threat foreign animal diseases could be a potential risk for disease agents in contaminated feed and infect U.S. livestock. As with precision agriculture, these threats are only likely to increase as adoption of technologies and trade increases.

- ***Impact of US Not Adopting Precision Agriculture***: Countries including Brazil, Australia, European Union and China are quickly adopting precision agriculture technologies. US agriculture failing to adopt these technologies at similar rates could diminish the US role in the global agriculture market.

- ***Cybersecurity of Commodities and Insurance Markets***: Several of the key threats identified in this research concerned attempted market manipulation by threat actors. This research examined that threat from the side of the data producers, but data security of the markets themselves warrants further examination.

- ***Threat Introduced by Limited Number of Precision Agriculture Technology Providers***: Competition in certain aspects of the precision agriculture technology industry is low. This leaves farmers beholden to a few companies, regardless of their security practices. This is especially evident in UAS used in precision agriculture as most companies developing UAS for precision agriculture are Chinese firms.

Resources

- 2010 ICPA Presentation –precision agriculture equipment limitations: http://www.aces.edu/anr/precisionag/documents/2010ICPAPresentation-PAEquipmentLimitations.pdf

- AG Web Powered by Farm Journal, Farmers Reveal Their Favorite Apps: https://www.agweb.com/mobile/article/farmers-reveal-their-10-favorite-apps/

- AgGateway: http://www.aggateway.org

- Agricultural Data Coalition: http://agdatacoalition.org/

- Agricultural Aerial Remote Sensing Standards Council: https://agrscouncil.org/

- American Farm Bureau Federation, Privacy and Security Principles for Farm Data: https://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data

- AU Signal Processing Group. 2018. RoboWeedMaps. https://vision.eng.au.dk/roboweedmaps/ *(Includes links to several publications using images, machine learning, and neural networks to identify and map weeds)*

- Berenstein R, Ben Shahar O, Shapiro A, Edan Y. Grape clusters and foliage detection algorithms for autonomous selective vineyard sprayer. Intel Serv Robotics 3:233-243.

- Byrum, J. 2017. Putting a price on farm data. AgFunder News. https://agfundernews.com/putting-price-farm-data.html

- CEMA 2017. Digital Farming: what does it really mean? European Agricultural Machinery.http://www.cema-agri.org/page/digital-farming-what-does-it-really-mean

- CIS - Center for Internet Security: https://www.cisecurity.org/controls/

- Daniels J. 2018. From strawberries to apples a wave of agriculture robotics may ease the farm labor crunch. https://www.cnbc.com/2018/03/08/wave-of-agriculture-robotics-holds-potential-to-ease-farm-labor-crunch.html

- Delmar Cengage Learning, History of Precision Agriculture: http://www.delmarlearning.com/companions/content/140188105X/trends/history_pre_agr.asp

- IG Inside GNSS, GNSS and Precision Farming: http://insidegnss.com/gnss-and-precision-farming/

- International Organization for Standardization: https://www.iso.org/home.html

- Kamilaris, Andreas & Prenafeta Boldú, Francesc. 2018. Deep Learning in Agriculture: A Survey. Computers and Electronics in Agriculture. 147. 10.1016/j.compag.2018.02.016.

- Ledbetter, K. 2018. Texas A&M AgriLife researchers push drones to 'Read The Weeds'. Texas A&M Today. April 4, 2018 https://today.tamu.edu/2018/04/04/texas-am-agrilife-researchers-push-drones-to-read-the-weeds/

- Mulla, D. J. 2013. Twenty-five years of remote sensing in precision agriculture: Key advances and remaining knowledge gaps. Biosystems Engineering. 114:358-371.

- NASA Earth Observatory Precision Agriculture: https://www.earthobservatory.nasa.gov/Features/PrecisionFarming/

- NASA Global Positioning System History: https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html

- Nguyen A, Yosinski J, Clune J. Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images. In Computer Vision and Pattern Recognition (CVPR '15), IEEE, 2015. http://www.evolvingai.org/files/DNNsEasilyFooled_cvpr15.pdf

- O'Grady MJ and O'Hare GMP. 2017. Modelling the smart farm. Information Processing in Agriculture 4:179-187. https://www.sciencedirect.com/science/article/pii/S2214317316301287

- Open Ag Data Alliance: http://openag.io

- Pivoto D, Waquil PD, Talamini E, Pauletto C, Finocchio S, Dalla Corte VF ,Mores GDV. Scientific development of smart farming technologies and their application in Brazil. Information Processing in Agriculture 5:21-32. https://www.sciencedirect.com/science/article/pii/S2214317316301184

- Robbins JA. 2018. Small unmanned aircraft systems (sUAS): An emerging technology for horticulture. *In* Horticultural Reviews 45. Ed. by Ian Warrington, John Wiley and Sons, Inc. publisher.

- SANS: https://www.sans.org/critical-security-controls
- Schepers A. 2012. Using thermal imagery for agriculture. http://cornerstonemapping.com/wp-content/uploads/2016/04/NeATA_thermal_2012_web_ver.pdf
- Schimmelpfenning, David, Farm Profits and Adoption of Precision Agriculture: https://www.ers.usda.gov/publications/pub-details/?pubid=80325
- Smithsonian The National Museum of American History Precision Farming: http://americanhistory.si.edu/american-enterprise-exhibition/new-perspectives/precision-farming
- The John Deere Journal, John Deere hands-free guidance system continues its evolution: https://johndeerejournal.com/2016/03/terry-picket-first-gps-unit/
- University of Missouri, Precision Agriculture Feeding the Future: https://artifactsjournal.missouri.edu/2017/06/precision-agriculture-feeding-the-future/
- Update on the 2014 Sony Cyber Attack Investigation: https://www.fbi.gov/contact-us/field-offices/sandiego/news/press-releases/update-on-sony-investigation
- van Es, HM, Woodard JD, Glos M, Chiu LV, Dutta T, and Ristow A. 2016. Digital Agriculture in New York State: Report and Recommendations. Cornell University, Ithaca, NY. https://fieldcrops.cals.cornell.edu/extension-outreach/meeting-and-training-archives/2015-precision-agriculture-workshop/
- Wanstreet, R. 2018, March 8. America's farmers are becoming prisoners to agriculture's technological revolution. *Motherboard.* Available at https://motherboard.vice.com/en_us/article/a34pp4/john-deere-tractor-hacking-big-data-surveillance
- Wolfert, Sjaak, et al. "Big data in smart farming–a review." *Agricultural Systems* 153 (2017): 69-80.
- Zhang C and Kovacs JM. 2012. The application of small unmanned aerial systems for precision agriculture: a review. Precision Agriculture 13:693-712. https://link.springer.com/article/10.1007%2Fs11119-012-9274-5