An NCC Group Publication

Cyber Security in UK Agriculture

Key Contacts

Lawrence Baker, NCC Group

Richard Green, Harper Adams University

Contributors

Lawrence Baker	NCC Group	Security Consultant
Prof Karl Behrendt	Harper Adams University	Elizabeth Creak Chair in Agri-Tech Economic Modelling
Dr James Bell	Harper Adams University	Senior Lecturer, Food Technology and Innovation department
Matt Butler	Harper Adams University	Researcher, Engineering department
Dr Richard Byrne	Harper Adams University	Senior Lecturer, Land, Farm and Agribusiness Management department
Parmjit Chima	Harper Adams University	Head of Engineering Department
Dave Clare	Harper Adams University	Senior Lecturer - Electronics & Mechatronics
Sam Durham	National Farmers Union	Chief Land Management Adviser
Dr Jane Eastham	Harper Adams University	Associate Head of Department, Food Technology and Innovation department
Kit Franklin	Harper Adams University	Agricultural Engineering Senior Lecturer
Jonathan Gill	Harper Adams University	Mechatronics Researcher & UAV Pilot
Dr Richard Green	Harper Adams University	Principal Lecturer, Engineering department
Dr Ivan Grove	Harper Adams University	Principal Lecturer Applied Agronomy, Crop and Environment Sciences department
Mike Gutteridge	Harper Adams University	Associate Researcher, Engineering Department
Debbie Heeks	Harper Adams University	Research Support and Project Administrator, Engineering department
Graham Higginson	Harper Adams University	Lecturer, Engineering department
Richard Hooper	Harper Adams University	Pig unit manager
Neil Jones	NCC Group	Security Consultant
Sophia McCall	NCC Group	Security Consultant
Alexander Miles	Harper Adams University	Aquaculture Researcher
Dr Jim Monaghan	Harper Adams University	Reader - Fresh Produce and Horticulture / Director of the Fresh Produce Research Centre
Dr Sven Peets	Harper Adams University	Lecturer, Engineering department
Megan Platt	Harper Adams University	Associate Researcher, Engineering Department
Prof Mark Rutter	Harper Adams University	Professor of Applied Animal Behaviour, Animal Production, Welfare and Veterinary Sciences department
Dr Kreseda Smith	Harper Adams University	Research Grants Administrator
Simon Thelwell	Harper Adams University	Associate Head of Department, Director of Rural consultancy, Land, Farm and Agribusiness Management department
Martin Wilkinson	Harper Adams University	Senior Lecturer in Farm Finance & Economics, Land, Farm and Agribusiness Management department

Harper Adams University

About Harper Adams University

As the population grows, so do our demands on the planet. Managing this resource has never been so important.

Since it was founded in 1901, Harper has been designed to meet this challenge. Set on a 635-hectare farm, we are the UK's leading specialist university tackling the future development of our planet's food production, processing, crop and animal sciences, engineering, land management and sustainable business.

Website: http://www.harper-adams.ac.uk/

nccgroup

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, trusted to protect and secure our customers' critical assets.

Home to the world's leading cyber scientists we continually invest in research and innovation, pushing boundaries to protect customers and society from the ever-changing threat landscape.

We are committed to developing the future generation of cyber scientists, analysts and professionals, offering internships, graduate placements and sponsorship of national education programmes as well as participating in guest lecture opportunities.

NCC Group has its global headquarters in Manchester, UK and has circa 1,800 colleagues in 12 countries with an established and significant presence in Australia, North America and Europe as well as the UK.

Website: https://www.nccgroup.trust

Executive Summary

This whitepaper addresses the cyber security threat to agriculture and the wider food network. The food industry is a critical, complex and interconnected global network utilising a diverse range of digital technologies. This forms a large attack surface and a range of threat scenarios. Public perception and behaviours are important factors when considering the likely severity of these threat scenarios.

The food network is resilient to disruption and there are no conceivable cyber threat scenarios with a severity level high enough to cause direct and immediate starvation. However, there are threat scenarios that could result in significant financial harm to the industry, social unrest and suffering to livestock. The most severe risks lie within food distribution and storage, and food standard systems. Large food processors are high-risk targets for cyber criminals and any disruption to their operations could affect a large number of farmers and growers that supply them. The issues of ownership, data privacy and security have to be addressed to avoid abuse and inequality.

The interactions between the food sector and other critical infrastructure pose additional threat scenarios, where a simple, less targeted cyber attack could cause extensive damage to other economically vital infrastructure.

The mitigations for much of the food sector are similar to those required for other industry sectors and can be managed with standard approaches and business processes. Securing farms poses some unique challenges, including low awareness of cyber security in the farming community. Relying on farmers to adopt generic guidance on how businesses can protect themselves is likely to prove ineffective by itself.

The cyber threat will increase in severity and likelihood as new technologies are adopted by the agri-food sector. Not only should we be preparing for this growing cyber threat in order to protect the day-to-day functioning of the food industry but also to ensure that they do not delay the adoption of technologies that are urgently needed by mankind. There are specific actions that can address the issues raised in this whitepaper and it is recommended that these be considered by the industry.

Contents

1 Introduction 7
- **1.1** Purpose and Scope 7
- **1.2** The Importance of Agriculture 8
- **1.3** Digitisation and the Emerging Cyber Threat 9

2 The Food Network 10
- **2.1** Food Network Stakeholders 12
  - 2.1.1 Consumers 12
  - 2.1.2 Farms 12
  - 2.1.3 Processors 13
  - 2.1.4 Wholesalers, Retailers and Food Outlets 13
  - 2.1.5 Farm Suppliers and Advisors 14
  - 2.1.6 Government and Non-Governmental Organisations 14
  - 2.1.7 Logistical Companies and Food Distribution 15
- **2.2** Severity Based on Food Type 16
- **2.3** Food Network Technologies 17
- **2.4** Threat Actors 17
- **2.5** Threat Scenarios 18
  - 2.5.1 Leaking of Confidential Farm Data 18
  - 2.5.2 Loss of Availability of Distribution and Storage Systems 19
  - 2.5.3 Loss of Availability of Processing Systems 20
  - 2.5.4 Compromised Integrity of Food Assurance Systems 20
  - 2.5.5 Farm Vehicle Collisions with Power CNI Assets 21
  - 2.6 Future Cyber Threat Landscape 22

3 Cyber Security Threats on Farms 24
- **3.1** Focus on Farms 24
- **3.2** Current Farm Technologies and Potential Threat Scenarios 25
  - 3.2.1 Farm Management Software 25
  - 3.2.2 Agricultural Ground Vehicles 26
  - 3.2.3 Unmanned Air Systems 28
  - 3.2.4 Remote Connected Sensors 29
  - 3.2.5 Livestock Farming Infrastructure 30
  - 3.2.6 Aquaculture Infrastructure 31
- **3.3** Future Technology Trends and their Cyber Security 32
  - 3.3.1 Data Analytics 32
  - 3.3.2 Autonomous Ground Vehicles (AGV) 33
  - 3.3.3 Unmanned Air Systems (UAS) 34
  - 3.3.4 Remote Connected Sensors 34

4 Agricultural Ground Vehicle Attack Surface 35

5 Conclusion 38

6 Recommendations 39

7 References 40

Glossary

AEF	Agricultural Industry Electronics Foundation
AGV	Autonomous Ground Vehicle
AHDB	Agriculture and Horticulture Development Board
APHIS	Animal and Public Health Information System
ARAMS	Animal Reporting And Movement Service
BCMS	British Cattle Movement Service
BVLOS	Beyond Visual Line Of Sight
CAN	Controller Area Network
CAP	Common Agricultural Payments
CESAR	Construction and Agricultural Equipment Security and Registration
CNI	Critical National Infrastructure
COTS	Commercial Off-The-Shelf
CPNI	Centre for the Protection of National Infrastructure
DAERA	Department of Agriculture, Environment and Rural Affairs
Defra	Department for the Environment, Food and Rural Affairs
DfT	Department for Transport
ECU	Electronic Control Unit
EU	European Union
FBI	Federal Bureau of Investigation
FSA	Food Standards Agency
GNSS	Global Navigation Satellite System
HMRC	Her Majesty's Revenue and Customs
HVAC	Heating, Ventilation, and Air Conditioning
ICO	Information Commissioner's Office
IoT	Internet of Things
IP	Internet Protocol
IPAFFS	Import of Products, Animals, Food and Feed System
JIT	Just-In-Time
NFU	National Farmers Union
NGO	Non-Governmental Organisations
NIS	Network and Information Systems
OEM	Original Equipment Manufacturer
POE	Power over Ethernet
RAS	Recirculatory Aquaculture Systems
RFID	Radio Frequency IDentification
RTK	Real-Time Kinematic
SCADA	Supervisory Control and Data Acquisition
TRACES	TRAde Control and Expert System
UAS	Unmanned Air System
UK	United Kingdom
US	United States
USA	United States of America
V2X	Vehicle to Everything
VRT	Variable Rate Technology

1 Introduction

1.1 Purpose and Scope

This whitepaper addresses the cyber security threat to agriculture and the wider food network. The perspective and primary focus is the United Kingdom but the majority of observations on the structure of markets, technologies and related issues are largely applicable to other countries. Furthermore, some of the recommended actions identified in this whitepaper, such as standards, require international collaboration.

This whitepaper is the output of a collaborative effort between Harper Adams University and NCC Group. It collates the viewpoints of industry specialists gathered from a series of workshops, with references to other sources that reinforce or supplement these viewpoints. This whitepaper is not a comprehensive study of cyber security in the agricultural industry – to completely threat model the food network and assess all risks would require a significant undertaking, involving input from multiple stakeholders, which is beyond the scope of this whitepaper. The intention of this whitepaper is to outline the current security posture of the agricultural industry, expected near-to-medium-term changes and recommended actions to mitigate these cyber risks.

The wider food network was studied to provide context to agricultural cyber threats, the criticality they pose and to enable identification of the most critical areas of concern at a national level. A more detailed study is made of farms, which are of particular interest due to bespoke technologies, market forces and behaviours. This whitepaper also studied the attack surfaces of one key agricultural technology – agricultural ground vehicles – chosen due to their ubiquity and the assumption that they are high-risk assets.

1.2 The Importance of Agriculture

Agriculture is essential for modern society and is arguably the most important invention of all time. The flourishing of international trade and the adoption of intensive agricultural practices post-World War II have both resulted in dramatic changes to the industry and the UK landscape. This has contributed towards the decrease in the industry's share of UK GDP to only 0.7%, while the proportion of the UK population it employs is now just 1.47% of the workforce[1]. For less developed countries these proportions are far higher, increasing the global averages to 3.9% of global GDP and 26% of the global workforce[2]. The wider food industry is far larger, representing 17% of UK manufacturing [3] and employing 3.7 million people, if wholesale, retail and catering supply chains are included[4].

The environmental impact of agriculture is significant – it contributes to 10% of UK greenhouse emissions[5] and some farming practices negatively impact ecosystems. At a global level, the UN estimates that agricultural production accounts for 70% of freshwater consumption, 38% of land use and 14% of greenhouse gas emissions. It identifies agriculture and food consumption as one of the most important drivers of environmental pressures, especially habitat change, climate change, water use and toxic emissions[6].

With 70% of UK land used for agricultural purposes, the industry is responsible for shaping and maintaining most of the UK's landscapes, including areas of cultural heritage. Although few people are directly involved in agriculture, it is predominantly favourably perceived by the general public, who appreciate living near rural green spaces and associate it as beneficial for wellbeing[7].

A romanticised view of agriculture and rural society influences consumer choice as well as the attitudes and decisions of those that work in the industry. The latter influences the cyber threats that the industry faces and will be touched on later in this whitepaper.

The food sector is one of 13 sectors classified as a Critical National Infrastructure (CNI) by the UK Government. It has an important influence on water supply, which is itself a CNI. Unlike other CNI sectors, there is little regulatory oversight to ensure resilience and availability. A possible explanation for this is within the findings of a Centre for the Protection of National Infrastructure (CPNI) report in 2010[4], though it should be noted that this was focused on the risks of flooding and other natural disasters rather than cyber security. This found there to be no single point of failure due to the size and diversity of food supply chains from domestic and international suppliers. It concluded that while consumer choice would be impacted, the overall availability of food would not be impacted. The CPNI report further identifies the food sector as being highly dependent on other critical infrastructure sectors, notably energy, transport, water and communications.

No specific guidelines or policies were introduced to build resilience following the findings of the 2010 CPNI report, with the onus placed on individual companies to review business continuity arrangements and incident plans.

The UK is not alone in its stance on the food sector – a joint Capgemini and Wageningen University whitepaper on cyber security in the agrifood sector notes that in 2015 the Dutch Government decided not to label agrifood processes as vital[8].

1.3 Digitisation and the Emerging Cyber Threat

The changes brought about by the ongoing digital revolution are also being realised within the food network. In agriculture, terms such as 'smart farming' and 'precision farming' are used to reference emerging information technologies and operational technologies that promise to revolutionise how we produce food. An unfortunate consequence of increasing digitisation is a growing cyber security threat – the number of UK firms experiencing cyber attacks is increasing, with more than 60% of firms having reported one or more attacks in 2019, compared to 45% in 2018[9]. It is inevitable that agricultural and food firms face a growing cyber security risk.

As alluded to in the previous section, the response by governments to cyber threats in the food industry has been light-touch. The 2016 EU Directive on the Security of Network and Information Systems (NIS), which aims to improve cyber security across sectors that are vital to EU economies, does not include the food sector.

The US Government, as with other industry sectors, has taken a more proactive attitude towards the cyber security risks in the food sector. The Federal Bureau of Investigation (FBI) issued a notice to the cktaUS food and agriculture sector warning of the risks to cyber security from smart farming in 2016[10]. A 2018 study for the USA Department of Homeland Security identified a number of technologies and cyber threat scenarios relating to precision agriculture[11].

It is difficult to determine the current number of cyber attacks that the food sector is currently experiencing due to the lack of systems for accurately reporting incidents. A research article assessing cyber security practices in the United States agriculture industry identified 11 out of 621 documented breaches having occurred against agricultural organisations[13]. More anecdotally, HSBC recently issued a warning to UK farmers about cyber criminals targeting them for fraud attacks[12]

2 The Food Network

To identify and assess cyber security threats to the food sector, it is helpful to first map out the stakeholders that form the food supply chain and their interdependencies. A simplified view of the food network is shown in Figure 1, which is centred on the farm, ends at the consumer and includes supporting organisations that span the length of the supply chain.

It is worthwhile noting that the UK is about 60% self-sufficient for food[1] and the interconnectedness of foreign markets means that the majority of these organisations could be foreign-based. There are also varying levels of horizontal and vertical integration within different subsectors of the food network. Greater integration generally improves efficiency, as was concluded by a UK Parliament Select Committee on Environment, Food and Rural Affairs report into the dairy industry[14]. It also increases the adoption of new technologies, as concluded by researchers from the universities of Copenhagen, Manchester and Saskatchewan[15].

There has been increasing connectedness in the agricultural supply chain, with the term 'Agriculture 4.0' being used to describe the digitisation of the sector, similar to the term 'Industry 4.0'. An ecosystem exists for agricultural data, for example with data being shared between agricultural Original Equipment Manufacturers (OEM), agronomy firms and veterinary service providers. This is currently fuelling debate within the sector about data ownership.

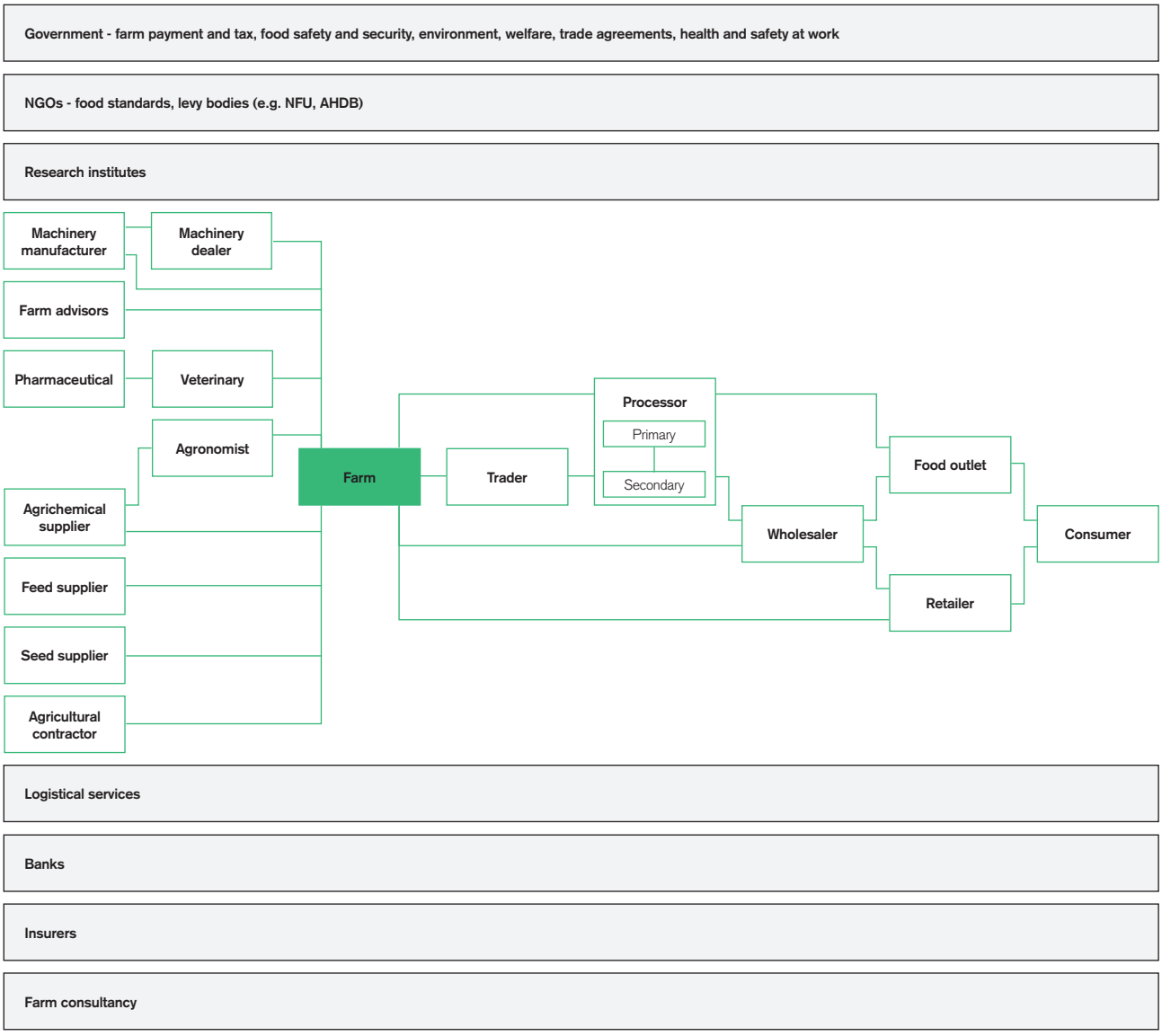


Figure 1: simplified food network

2.1 Food Network Stakeholders

There are certain aspects of the different types of stakeholders in the food network that are of relevance for understanding the cyber security posture of the sector. These are summarised within this subsection.

2.1.1 Consumers

Arguably, the most influential entity within the food network is the consumer. Consumer demand is highly influenced by price but food safety, reputation, animal welfare and environmental impact are also important influential factors. A 2018 National Farmers Union (NFU) Mutual Food Fraud report highlights that the cost of food fraud to the UK food industry could be as much as £12 billion each year and that consumer confidence is decreasing[16]. In general, EU welfare standards are significantly higher than in other countries, with the UK exceeding the EU baseline in some aspects[17].

To satisfy consumer demand for organic produce, about 20% of farms are organic, though this demand is dependent on the disposable income of consumers.

2.1.2 Farms

There is a large range of UK farm sizes from tiny holdings of less than two hectares, through to larger family farms that are typically between 50 and 200 hectares, to trust companies and charities with more than 3000 hectares. About three quarters of farmed land is owned by large farms, with greater than 100 hectares, comprising 22.4% of UK farms[5].

Following World War II, there has been a trend toward increasing farm size to benefit from economies of scale for both farmed land and livestock. Historically, this has typically been through farmers buying up neighbouring farms. In the past 15 years there has been a significant increase in the number of large farm businesses that either own land or rent land from farmers. At the same time, there has been increasing specialisation.

The majority of farms are family owned and run small or micro businesses. They are typically run as sole traders or partnerships with little outside involvement, with farmers typically relying on long-term personal relationships with farm advisors and agronomists. The structure of farming creates barriers for new entrants, supporting high levels of succession within farming families and encouraging farmers to continue working into retirement[18]. This has led to an increasing average age of UK farmers, with only 3% under the age of 35 and 30% aged 65 or over[5]. Many farmers view the profession as a lifestyle and as such, can make decisions that are not necessarily the best for the success of their businesses. This has hindered the adoption of improved farming practices and raised concerns about the level of professionalism within agriculture.

A 2017 Department for Environment, Food and Rural Affairs (Defra) report shows that the income of farm businesses varies greatly[1], with only 25% of UK farms being profitable in the absence of farm subsidies. For some farms, up to 50% of all money received is from subsidies, with small farmers being particularly vulnerable[5]. In general, farms are asset rich but cash poor – a report commissioned by The Prince's Countryside Fund warns of a cash flow crisis within agriculture[19]. To generalise, larger farms tend to be more business focussed and willing to invest in new technologies, and farms that are run more like businesses tend to be more profitable.

Awareness of cyber security in the farming community is believed to vary widely but is generally considered low – the NFU has not received significant interest from its members on cyber security. Data privacy, physical theft by organised criminal gangs and concern about animal welfare activists are key concerns.

2.1.3 Processors

There can be multiple layers of processors within a food supply chain, depending on the product and level of integration. In general, primary processing is highly consolidated for bread, dairy, poultry and potatoes, where big processor conglomerates are able to exert significant influence on the farmer through mechanisms such as contract farming. The opposite is true for eggs, where the market is dominated by a small number of primary producers who pack and sell directly to retailers. Any disruption to the operations of a large processing conglomerate could have a significant impact on the market. Secondary processors are less consolidated, being made up of many small businesses.

2.1.4 Wholesalers, Retailers and Food Outlets

As with processors, the level of vertical integration in a food supply chain varies between food type and wholesalers, retailers and food outlets. Retailers have an important and direct influence on food standards, reflecting the preferences and demands of the consumer.

2.1.5 Farm Suppliers and Advisors

An aspect of particular note within the vast breadth of agricultural suppliers is the recent accumulation of farm datasets. OEMs and agrichemical firms are attempting to increase market share or add new revenue streams by mining agricultural data, such as offering services related to precision agriculture or equipment aftermarket. The ownership of data is a contentious issue, with the farming community concerned about data privacy[20].

The 'right to repair' is a key issue within the farming community. The complexity and increased use of electronics within agricultural equipment means that OEMs can tie users to their aftermarket services by controlling the availability of spares, maintenance manuals and equipment. The issue is particularly pronounced in the USA, with some farmers 'hacking' their tractors to bypass the OEM[21]. This introduces a new attack vector, for example through malicious software posted on internet forums discussing the 'right to repair'. Although the EU has recently taken steps to address the issue – with new rules to protect the 'right to repair' due to come into force in April 2021 – these do not cover agricultural equipment[22].

2.1.6 Government and Non-Governmental Organisations

Government policy and regulation shape the structure of the food network. They also provide vital operational services through online portals, such as the following:

- Rural payments, as part of the EU Common Agricultural Payments (CAP), which is managed by the Rural Payment Agency
- Tax collection and VAT repayment, which is managed by Her Majesty's Revenue and Customs (HMRC)
- British Cattle Movement Service (BCMS) – a database of all bovine animals, which is maintained by the Rural Payment Agency
- Animal and Public Health Information System (APHIS) which is an equivalent database to the BCMS for Northern Ireland and is maintained by the Department of Agriculture, Environment and Rural Affairs (DAERA)
- Animal Reporting and Movement Service (ARAMS) – a database for tracking the movement of sheep, goats and deer within England, which is maintained by a third party on behalf of Defra
- ScotEID and EIDCymru – databases equivalent to ARAMS and managed by the Scottish and Welsh governments respectively. ScotEID is also used for tracking the movement of pigs
- The Import of Products, Animals, Food and Feed System (IPAFFS) – a service to notify UK authorities on the planned import of animals, animal products, high-risk food or animal feed of non-animal origin from outside of the EU, which is maintained by the Animal and Plant Health Agency
- TRAde Control and Expert System (TRACES) – a web-based veterinarian certification tool for controlling the import and export of live animals and animal products within and without the EU, which is maintained by the European Commission

The tracking of pig movement in England and Wales is via an online portal to the eAML2 system, managed by the Agriculture and Horticulture Development Board (AHDB), which is a levy board that represents farmers, growers and others in the agricultural supply chain. Note that there are alternatives to using online portals for accessing eAML2 and Government managed services.

While the Food Standards Agency (FSA) is responsible for food safety and food hygiene, Non-Governmental Organisations (NGO) – such as the Assured Food Standard that licenses the red tractor quality mark – set, promote and regulate food quality through farm assurance schemes. Separate certification bodies perform the enforcement and auditing of these assurance schemes.

Defra is the lead Government department for the food sector CNI, apart from food contamination where the Food Standards Agency has the lead role. They jointly produce PAS 96, a guide for business in the food and drinks industry on how to defend against deliberate attack, including cyber security[23]. This provides generic advice on cyber risk management and governance and board level responsibilities.

2.1.7 Logistical Companies and Food Distribution

Food distribution and storage connects the various entities in the food network. This often requires specialist vehicles and warehouses with controlled environments to avoid spoilage and achieve compliance to food standards. Competitive pressures from the largest supermarkets are driving efficiency improvements, resulting in a Just-in-Time (JIT) food supply chain, reduced stock holdings and consolidation within the distribution network. This requires on-the-minute coordination and sophisticated processes and systems.

The move toward JIT supply chains has reduced resilience to transport disruption, creating a clustering of strategic distribution centres within the 'distribution triangle' of central England and longer recovery times following panic buying[24]. Based on a full fact estimate, there was approximately 10 days' worth of food stocks in 2012[25].

Transport is included within NIS regulations but road logistical service providers are not within scope.

2.2 Severity Based on Food Type

The severity of cyber security threats to the food network varies between food types, with higher severity for fresh produce, meat and poultry and low severity for cereals. Note that this does not consider the severity to individual organisations within the food network.

Fresh produce is a higher-risk food type due to a higher relative food safety risk to the consumer, low storability potential and high-value. For example, the value per hectare of strawberries can be 10 times that of grain. The harvest window is smaller than for cereals, so any disruption to harvesting equipment during this period could affect yields. Disruption to the production of fresh produce in the UK could have a significant effect on market prices.

Disruption to UK production of cereals would have a relatively low impact on the wider food network. This is because grain has a high storage potential, relatively low value and market prices are driven by global demand and supply, of which the UK is only a small producer. The harvesting window lasts a few weeks so any disruption to harvesting equipment during this period could affect the yields on a large number of farms.

The severity of risks to the meat and poultry supply chain are considered to be moderate. There are significant food safety risks to be managed for meat and poultry and they tend to be high-value produce. Their storage potential varies but is generally low for much of the associated produce.

Aquaculture is a rapidly growing subsector globally but comparatively slow within the UK, which farms a narrow range of species. As with meat and poultry, there are significant food safety risks to be managed, they tend to be high-value produce, and the storage potential varies but is low for much of the associated produce.

2.3 Food Network Technologies

The food network utilises a broad range of technology types. In addition to standard enterprise technologies, the following systems are prevalent within the food network:

- Online portals for rural payments and livestock movement tracking
- Supervisory control and data acquisition (SCADA) production systems
- Heating, ventilation, and air conditioning (HVAC) systems in intensive livestock farms, production lines, warehouses and distribution vehicles
- Agriculture machinery (e.g. farm vehicles, milking parlours)
- Livestock tracking wearables
- Smart agriculture sensors (e.g. soil moisture, weather station)
- Farm management software
- Logistics management software
- Farm databases (gathered by agrichemical and OEM companies) and big data analytics
- Food distribution vehicle telemetry

2.4 Threat Actors

Cyber threat actors can be generalised into the following categories:

- Nation-states
- Cyber criminals
- Hacktivists
- Terrorist groups
- Thrill seekers
- Insider threat

Of particular note for the food network are nation-states, cyber criminals and hacktivists. As the food sector is a CNI, it is a potential target for states wishing to weaken the UK.

The guidance from Defra and FSA for defending against deliberate attacks[23] predominately identifies cyber threats originating from cyber criminals. The findings from Hiscox research into cyber attacks suggest that UK farms and secondary processors are particularly vulnerable to cyber criminals because smaller businesses tend to be less prepared[9]. While rural crime is a key concern of farmers, being at its highest levels for years, the top issues are the theft of all-terrain vehicles, tools, machinery and livestock [26].

There are a number of emotive subjects that could motivate hacktivists, the foremost being animal welfare, but also from within the farming community. The latter might wish to target agrichemical firms and OEMs over data privacy and 'right to repair' concerns or target buyers that are perceived as abusing a dominant position.

2.5 Threat Scenarios

A number of previous studies have identified various threat scenarios:

- A study for the US Department of Homeland Security identified threat scenarios relating to precision agriculture[11]
- A joint Capgemini and Wageningen University study identified threat scenarios to the Dutch food sector[8]
- A joint Lloyds of London and University College London study identified threat scenarios related to the use of Internet of Things (IoT) devices[27]

Threat scenarios determined by this study are detailed below, but this only includes those that were judged to be a significant threat to the UK food sector or other CNI. This is not an exhaustive list and it should be noted that a subsequent section of this whitepaper presents lower-level threat scenarios for farms.

While the adoption of precision agriculture technologies has resulted in the emergence of a multitude of new attack surfaces and threat scenarios, few of these threat scenarios have a severity that would significantly affect the UK food network, at least in the short-term, as UK crop yields are among the best in the world.

Precision agriculture will enable relatively limited increases in absolute production levels but can lead to improved efficiency and reduced environmental impact. Hence, cyber attacks that deny availability to precision agriculture resources will only have modest consequences, assuming that farmers are able to revert to non-precision methods. Similarly, precision agriculture technologies for livestock generally improve efficiency, standardisation and welfare, but the impact of their loss to the wider food network would generally be modest.

The longer-term impact of cyber attacks on precision agriculture could be more damaging. As discussed in a later subsection, there are huge challenges facing the food network and precision agriculture is one of the approaches to addressing these. Adoption of new agricultural methods and technologies takes time – undermining farmer confidence could reduce the rate of adoption, exacerbating the challenge as well as potentially harming the competitiveness of the UK food sector.

2.5.1 Leaking of Confidential Farm Data

Companies such as farm consultancies, farm advisors, agrichemical firms and OEMs maintain databases containing information about farms. These can contain sensitive information about yield quantities and prices, costs of agrichemicals, feed and equipment, livestock and crop health and pesticide use.

Leaking of this confidential data could occur due to an insider attack leading to theft and publishing of data, accidental public exposure by a company or a deliberate outsider attack on the network of a company hosting an agricultural database. While a number of motivations for an attack exist, specific reasons include:

- Animal welfare activists wishing to 'expose' evidence of abuse
- Misuse of data, for example to understand potential market drivers or to identify struggling farms with underutilised land that could be bought at lower than the standard market price

The accumulation of these large datasets and the information that can be gleaned from big data analytics is an emotive subject within the farming community. There is anecdotal evidence of a company providing free online farm management services to South American farmers, misusing acquired data to identify struggling farms and then offering to purchase blocks of land from them at significantly below their calculated true value.

While legislation in the UK may make this type of misuse by the firms acquiring the data less likely, the potential for leaked information to be misused by a third party still exists. The reputational impact of a data leak would be substantial and could hold back the adoption of this technology, either through farmers choosing alternative providers that promise not to harvest data or the imposition of overly prohibitive regulation.

2.5.2 Loss of Availability of Distribution and Storage Systems

Food storage and distribution relies on various technologies to achieve a Just-in-Time system and meet food standards. While the network is tolerant to the loss of individual assets, the loss of availability of key IT systems for a large distributor would likely have a significant impact because any non-digital fall back system would be unable to achieve an equivalent level of performance.

The type of technologies that could be targeted include:

- Loss of HVAC systems in storage warehouses
- Loss of SCADA systems, such as equipment used to move goods
- Loss of availability or integrity of logistics software
- Remote immobilisation of distribution vehicles (e.g. via telemetry systems)

The vulnerability of the food supply chain to distribution issues was evident in the recent and much published issues that KFC experienced when it changed its food distributor in the UK[28]. One example of the reliance on HVAC systems is potatoes, which need to be stored in a refrigerated environment and can no longer be sold if stored at room temperature for a couple of days or more.

While a number of motivations exist, specific reasons include:

- Targeting of live transportation of poultry by 'extreme' animal welfare activists who believe that animals are better off dead than living in a farmed environment. As poultry transportation relies on forward movement of the vehicle to provide ventilation, immobilisation of the vehicle over a sufficient period can lead to death of animals via overheating or asphyxiation
- Nation-state attacks to economically and socially weaken another state
- Organised criminal gangs manipulating markets by influencing the share price of publicly listed companies

There is sufficient food in the supply chain to last around 10 days and any cyber attack on the food distribution network is highly unlikely to result in starvation. However, the food network is susceptible to food scares and there is a non-linear relationship between supply and the price of food. There is a realistic possibility of significant financial harm and social unrest resulting from this type of attack.

2.5.3 Loss of Availability of Processing Systems

Food processors can use automated SCADA systems on their production lines, which are often exposed to the internet. These systems are vulnerable to cyber attacks. While a number of motivations exist, specific reasons include:

- Targeting of meat and poultry abattoirs by animal welfare activists wanting to cause financial and reputational harm
- Ransomware attacks by cyber criminals

The loss of a facility's production system in a food sub-sector dominated by a few large companies could result in high financial harm to the affected company and the farms that supply it.

2.5.4 Compromised Integrity of Food Assurance Systems

Several of the food assurance systems have web portal interfaces to databases that allow users to view or submit information relating to the movement of livestock, food and animal products, and accreditation of organisations within the food network. Specific motivations include:

- Targeting of livestock farms and meat and poultry processors by animal welfare activists. This could be by direct financial harm to the victims or by attempting to change consumer habits by undermining consumer confidence in meat and poultry safety or animal welfare standards
- Exposure of the falsification of records by unscrupulous processors, who may be attempting to profit through non-conformance to food standards
- Nation-state attacks to economically and socially weaken another state

A cyber attack that reduced the availability of a food assurance system is unlikely to cause substantial disruption to the food network as fall-back systems generally exist. A cyber attack on the integrity of the food assurance systems could undermine consumer confidence, which would have a high financial impact on food companies and potentially a significant impact to the wider economy. The high economic cost of food scares is illustrated by the 2011 Spanish cucumber scare, where fresh produce from Spain was incorrectly blamed for a deadly outbreak of E. coli in Germany. One estimate of the cost to the Spanish economy was 200 million per week[29].

2.5.5 Farm Vehicle Collisions with Power CNI Assets

Modern farm vehicles contain networked digital micro-controllers, making use of automotive standard Electronic Control Units (ECUs) linked with Controller Area Network (CAN) buses. Farm vehicles can be equipped with auto-steer, which uses Global Navigation Satellite Systems (GNSS) to autonomously control the direction of travel. Though less common, there are farm vehicles that have autonomous speed control, though a driver is still required to take control e.g. to avoid obstacles or turn at a headland. As discussed in a subsequent section, there are a number of attack surfaces that could be exploited in order to carry out a cyber attack. The high levels of momentum and traction of these vehicles can result in catastrophic collisions with people or other assets.

While a number of motivations exist, specific reasons include:

- Terrorism – attacking buildings and roads to cause injury, death and destruction
- Nation-state attacks against the electrical power CNI assets, with power pylons and electrical substations in and around farmland potentially targeted

The presence of a driver in these vehicles significantly reduces the likelihood of this type of attack occurring. However, it is believed that there is a residual risk due to: i) the torque generated at full power, if maliciously demanded, possibly exceeding the brake forces that the driver can command; ii) the ability of a driver to respond within sufficient time if a malicious command was requested while in close proximity to the target.

2.6 Future Cyber Threat Landscape

The digitisation of the food sector will continue over the next three decades, driven by a number of factors:

- Pervasiveness of digitisation
- Brexit
- Consumer-driven standards
- Demographic changes
- Sustainability
- Increasing demand
- Climate change and ecological damage

The rapid rate of digitisation within society will continue and its pervasiveness will spread to the food sector, whether this is to achieve improved efficiencies, to exploit new revenue streams or because standard parts used within the sector come with the technology by default. There is growing interest in the use of big data to analyse and monetise the ever-increasing quantity of data that connected devices are sharing.

Brexit could potentially accelerate the adoption of new methods and technologies if a reduction in subsidies increases the need for business competitiveness. Increased vertical integration, improved streamlining and efficiency, and decisions based on actual market returns are required in order for UK agriculture to succeed post-Brexit[30].

Consumer demand will continue to drive food standards. The NFU Mutual Food Fraud report 2018 highlights that Brexit could detrimentally affect public confidence, with consumer confidence being lower for the global food chain than UK-sourced food[15]. Technology offers potential solutions to improve the traceability of food and monitoring of animal welfare, for example by blockchain algorithms, livestock worn trackers, environmental sensors and multi-spectral cameras coupled with machine learning algorithms.

The trend of an increasing average age for farmworkers is not a UK-only phenomenon – it is a global issue that developing countries, such as some in Africa, are also experiencing as younger members of society move to urban areas to seek better opportunities[31]. The resulting lack of suitably skilled farmworkers will drive the demand for increased automation, such as Autonomous Ground Vehicles (AGV) and automatic milking parlours. Some forecasts predict that half of dairy herds in north west Europe will be milked by automatic milking parlours in the future[32].

Finally, but by far the greatest global challenge facing the food sector, is the transformation needed to provide food for a growing population in a sustainable manner while adapting to the effects of climate change and ecological damage. The global population is expected to increase to over 50 billion by 2050, requiring a corresponding increase in food production of 70%, while at the same time climate change, ecological damage and water scarcity threatens the productivity of the food system. If previous trends continue, a growing global middle class will demand increased meat in their diet. With meat being an inefficient food source, this increases the challenge of achieving a sustainable food system. Technology, while not being a panacea, is part of the solution[33], which is recognised by the UK Government and supported through its Industrial Strategy Challenge Fund.

With the UK's high utilisation of suitable farmland for agriculture and world-class yields, there is only so much new technologies can do to increase UK productivity. However, there is variation, so benefits can be achieved through raising levels of adoption of best practices and increasing standardisation. Reducing or eliminating soil compaction with smaller farm vehicles, such as those used in the Hands Free Hectare project, for which Harper Adams is a key sponsor[34], and through autonomous Unmanned Air Systems (UAS), is one promising opportunity.

Increasing digitisation can significantly improve agricultural efficiency and sustainability through precision use of agrichemicals and irrigation, though in the UK only fresh produce typically requires irrigation.

This increase in digitisation will result in increased exposure to existing security vulnerabilities and new emerging threats. With regards to appraising new technologies, the UK governments 2011 'The Future of Food and Farming' final report[33] states that:

- The safety of new technology needs to be rigorously established, with open and transparent decision-making
- Risks need to be appropriately weighed against the potential costs of not utilising new technology
- Governance for new technologies needs to consider how it may alter the relationship between commercial interests and food producers

In keeping with these findings, we need to manage cyber security risks introduced from increasing digitisation in the food sector with appropriate governance. The impact on food producers needs to be appropriately considered and the security of new technologies tested in line with security industry best practice.

3 Cyber Security Threats on Farms

3.1 Focus on Farms

As explored in the previous section, the majority of high severity threat scenarios do not lie within farms. The vulnerable technologies, and means for hardening them, are common to other industry sectors, including SCADA-type systems, enterprise network infrastructure and web applications. Vulnerabilities in food distribution vehicles present some novelties, and the interactions and sharing of responsibilities between the food and transport CNIs need to be appropriately considered.

Farms can use diverse and tailored technologies in unique environments that present numerous novel threat scenarios. The increasing average age of farm workers and the tendency for farms to be small or micro enterprises means that they are particularly vulnerable. The current light-touch approach by Defra of providing generic business guidance for protecting against cyber attacks is likely to have limited effectiveness, as evidenced by the low levels of cyber security awareness in the farming community.

While cyber attacks against farms may not have a significant impact on the wider food network, they could hamper efforts to transform the food sector to address the huge global challenges humanity faces in the coming decades. Hence, this section examines agricultural technologies and identifies potential threat scenarios in order to understand the current security landscape for farms.

3.2 Current Farm Technologies and Potential Threat Scenarios

The technologies and threat scenarios contained in the following sub-sections are not intended to be a comprehensive list, but should provide a good indication of the breadth and type of cyber attacks that need to be considered in order to adequately protect a farm.

3.2.1 Farm Management Software

Farm management software aids the farmer in managing and optimising the operations of a farm. It provides functionality such as traceability, insight and means to improve profitability, and tracking and monitoring of farm workers and assets. The software can run on a PC, tablet or phone, and can be hosted locally or in the cloud.

Some software packages can interface directly with industry portals such as BCMS and ARAMS, and services from farm advisors, agronomic firms and satellite service providers (e.g. Landsat). They can integrate with precision agriculture devices such as Unmanned Air Systems (UAS), weather stations and other remote sensors.

A cyber attack could result in the following scenarios:

- Leaking of confidential data that puts the business at a competitive disadvantage
- Leaking of confidential data that is misused by prospectors wishing to buy underperforming land at below market price
- Leaking of confidential data that aids organised criminal gangs in stealing farm assets
- Loss of integrity resulting in financial loss due to reduced yields or production efficiency, putting the business at a competitive disadvantage
- Loss of availability resulting in financial loss due to reduced yields or production efficiency. This would likely only have a limited effect on an individual farm, with fresh produce being at higher risk due to smaller harvesting windows. Attacking multiple users via software updates or a cloud-hosting platform would magnify the impact, which could motivate cyber criminals to target service providers with ransomware-type attacks

3.2.2 Agricultural Ground Vehicles

There are a wide range of farm vehicles, with the more common types broadly categorised as follows:

- Tractors and implements
- Harvesters
- Sprayers
- Telescopic handlers
- All-terrain vehicles
- Farm robots

German OEMs dominate the European market for tractors and harvesters. Modern farm vehicles have followed the automotive industry in the use of Commercial Off-The-Shelf (COTS) ECUs linked with a CAN bus to control much of their functionality. A high-end tractor can have in excess of 20 ECUs. Manufacturer-approved diagnostic kits are required for connecting to the CAN bus to carry out servicing and repairs. Farm vehicle servicing staff are typically lower paid than those in the automotive industry, raising potential concerns about dealers being able to retain those with adequate cyber security awareness.

Modern farm vehicles can come equipped with telematics units, which send diagnostic and usage data to the OEM but can also include harvester yields and geo-location. A common use case for this functionality is to provide diagnostic alerts to the OEM for servicing. The telematics systems on some vehicles are capable of sending control commands to the vehicle to enable remote deactivation or to optimise combine thresher settings.

With the cost of GNSS systems, including Real-Time Kinematic (RTK) solutions, steadily decreasing, their use on farm vehicles is now commonplace. In some vehicles, these systems are used to autonomously steer the tractor – otherwise known as auto-steer – which increases efficiency by reducing overlap. It also enables tracking of vehicles, the mapping of soil composition, crop health, weeds and yields, and site-specific application of agrichemicals via Variable Rate Technology (VRT). GNSS systems were initially installed as add-ons by third parties but are now commonly integrated by OEMs.

With auto-steer systems a driver is still in control of the throttle and brake, and is responsible for avoiding obstacles such as electricity pylons, and turning at headlands. Some vehicles enable the driver to pre-programme the turn operation and replay it. There are only a few examples of commercially available systems that allow a limited control of forward speed in tractors, including: i) balers controlling the rate of input of hay or straw; ii) combine harvesters managing the offloading of grain into a trailer – this system also provides command inputs to the tractor's auto-steer.

Tractor implements can include their own microcontrollers and come equipped with a variety of sensor types. These sensors may be used to directly control VRT or robotic inter-row and intra-row weeding systems. Various communication technologies and protocols are in use to connect a tractor to an implement. An attempt to adopt an industry standard through ISO 11783, commonly known as ISOBUS, has had partial success. Connected implements are typically controlled by the driver using a virtual terminal, which initially were offered by third-parties but are now increasingly being integrated by tractor OEMs. It is possible for a COTS tablet to be installed to provide an additional display but these are believed to be currently limited to displaying information only.

Dedicated sprayers are typically bespoke or batch produced by small suppliers. While the cyber security awareness of these suppliers is likely to be low, these vehicles are less likely to have any form of connectivity that could form an exploitable attack surface.

The use of AGVs is currently limited to niche applications. Small autonomous tractors for orchards and vineyards are commercially available, with a key benefit being reduced exposure of human operators to spray chemicals. A variety of small robots for intensive livestock farms are commercially, including robot washers for piggeries and robot scrapers and feed pushers for dairy farms. These have wireless links to internet-connected base stations.

Agricultural vehicles have historically had low levels of physical security, driven by the desire for convenient access by farm workers. There is a significant level of agricultural vehicle theft, with equipment being targeted by organised criminal gangs and sold abroad[26]. The industry has responded in recent years with OEMs installing chipped keys (that can be programmed to work on multiple vehicles), GNSS trackers, remote deactivation and the Construction and Agricultural Equipment Security and Registration (CESAR) marking scheme. Keyless entry systems are not in use, so the industry has avoided the recent security issues that the automotive industry is experiencing with this technology[35]. There has been a recent spate of thefts targeting tractor GNSS systems[36], which could suggest that thieves are targeting easier high-value assets. The NFU has also heard of GNSS jamming equipment being used to circumvent GNSS trackers.

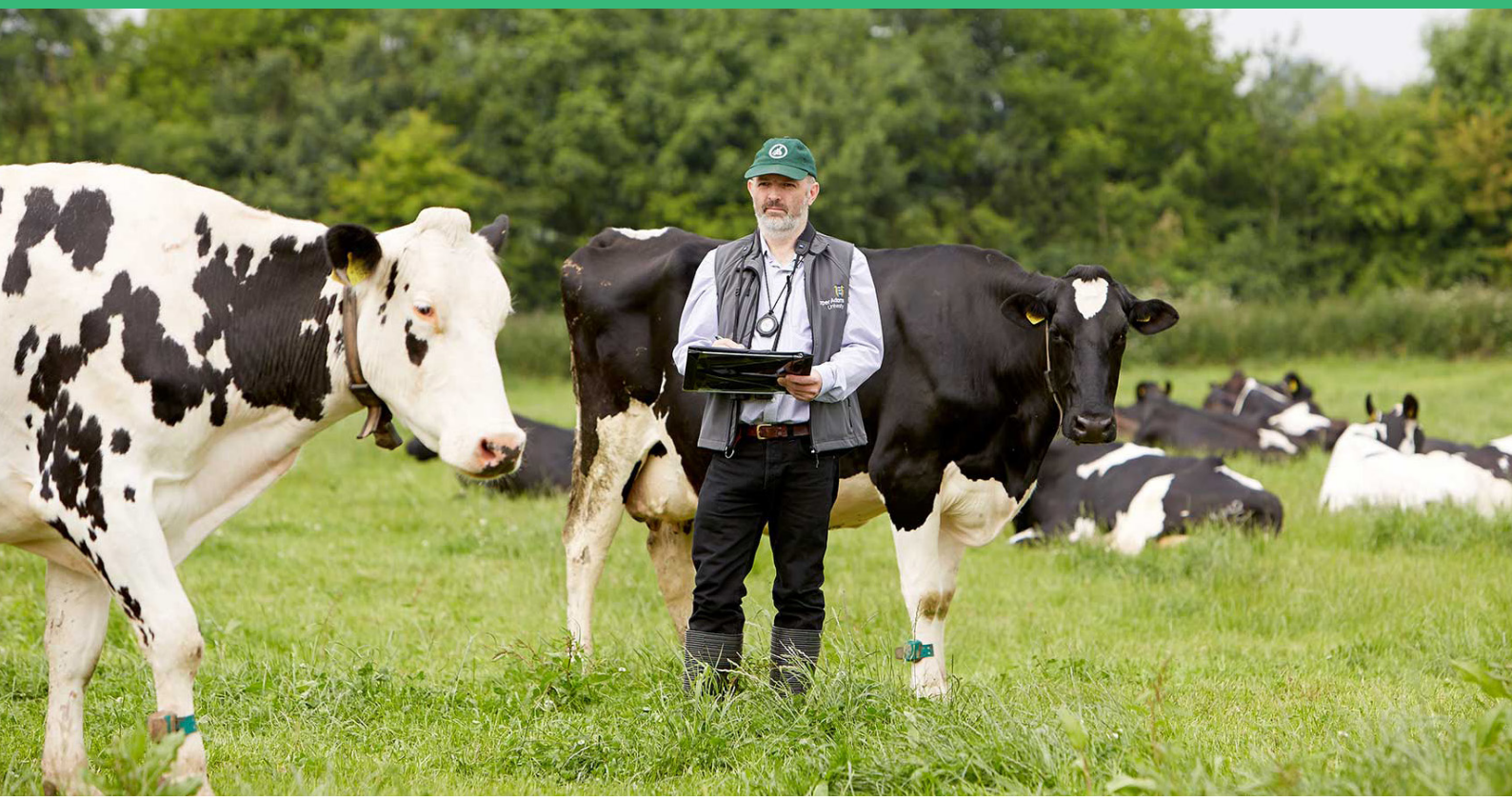
A cyber attack could result in the following scenarios:

- Leakage of telematics data leading to the disclosure of confidential information on production efficiency, crop health and yields, which puts the farm at a competitive disadvantage
- Unauthorised access to the telemetry system allowing an attacker to command sub-optimal combine harvester thresher settings. This could result in reduced yields and loss of income to the farmer, putting them at a competitive disadvantage. It is likely that the operator would notice yields that are significantly lower than expected, but with a limited harvesting window, the ability to rectify this within sufficient time may be limited
- A malicious script being planted on an ECU that provides malicious commands to the throttle and auto-steer. The presence of a driver in these vehicles reduces the likelihood of collision. However, it is believed that there is a residual risk due to: i) the torque generated at full power, if maliciously demanded, exceeding the brake forces that the driver can command; ii) the ability of a driver to respond within sufficient time if a malicious command was requested while in close proximity to the target. Terrorists could use this to attack buildings and roads to cause injury, death and destruction, though they would likely lack the required expertise. A nation-state sponsored attack would have the expertise but could be more interested in targeting electrical power CNI assets, such as power pylons and electrical substations in and around farmland
- A ransomware attack carried out by an organised criminal gang, leading to the installation of malicious ECU software update that ‘bricks’ the ECU, immobilising the farm vehicle. This would require a replacement ECU to be fitted in order to return the vehicle to service. The severity, and likelihood of a ransom being paid would increase if timed to occur during a critical period in the season, such as during the harvest window
- Connection to the CAN bus diagnostic port allowing an immobilisation system to be circumvented, resulting in theft of vehicles by organised criminals. Note that physical access to the farm vehicle cab could be achieved through vehicles not being locked, or through a physical locking system that is simple to overcome

3.2.3 Unmanned Air Systems

The use of Unmanned Air Systems (UAS), or drones, in agriculture in the UK is limited to remote sensing using multispectral sensors. Regulatory restrictions on Beyond Visual Line Of Sight (BVLOS) operations and spraying of chemicals from UAS have limited their applications and adoption within agriculture. In China, where regulations are less restrictive, fleets of autonomous UAS spray fields, with the primary driver being the elimination of poor health and safety practices.

Due to the limited application of UAS in UK agriculture and low levels of autonomy, they do not currently present any significant cyber security threat.



3.2.4 Remote Connected Sensors

Remote connected sensors typically fall within two categories:

- Agronomic sensors
- Livestock sensors

Agronomic sensors include typical weather station measurements such as air pressure, temperature and humidity, wind speed and direction, and rainfall. They can also measure soil moisture, temperature and salinity, leaf wetness and solar radiation. Moisture sensors are more common on fresh produce farms, where irrigation may be required. These sensors can utilise different wireless standards including ZigBee, LoRaWAN and 2G/3G/4G mobile networks.

Livestock sensors are typically limited to dairy herds due to equipment costs, used to monitor feeding, rumen health, lameness, oestrus and calving. The most common type are activity and rumination sensors that contain tri-axis accelerometers, which are worn on neck collars, ear tags or nose halters. Rumen sensors located within the animals' stomachs can monitor temperature, pressure and acidity. Calving sensors, mounted to the tail, use tail movement to predict imminent calving. Leg-mounted pedometer sensors can provide further insight into animal health and activity.

These sensors can be used by vendor-specific applications or integrated with third-party farm management software.

The loss of confidentiality of agronomic sensor data is unlikely to constitute any form of threat. Similarly, the leaking of livestock sensor information, for example by animal welfare activists attempting to expose animal welfare issues, while undesirable is not necessarily a significant cause for concern. Indeed, additional use of livestock sensors and transparency has been proposed as a means for improving animal welfare and increasing consumer confidence. The loss of availability of the system is unlikely to pose a significant risk either, as the farmer can revert to alternative methods.

Cyber attack scenarios that could be of significant severity are:

- Loss of integrity of animal sensors so that they provide inaccurate oestrus information. This could result in missed breeding cycles, with financial impact on a farm. Motivations include manipulation of the market by cyber criminals and animal welfare activists wishing to financially harm the livestock industry
- Loss of integrity of moisture sensors, resulting in inadequate irrigation of fresh produce and reduced yields, which puts the farm at a competitive disadvantage

3.2.5 Livestock Farming Infrastructure

The level of digitisation of livestock farms is lower than for crop farms but there is still a diverse mixture of technologies in use within the infrastructure. These can be broadly categorised into the following:

- Feeding
- Milking
- Segregation gates
- Animal monitoring
- HVAC

The greatest use of digitisation and automation occurs in dairy and poultry farms. On dairy farms, the greater scope for reducing manual labour, particularly during unsociable hours, has been a driver for digitisation. Intensively farmed pig farms are also adopting digital technologies. Grazing livestock, such as sheep farms and open farmland pig farming, generally has low levels of digitisation.

Mechanised feed and watering systems have been in use for decades but recently, more advanced solutions have been introduced that tailor feed to the individual animal. The benefit of doing this is increased efficiency and improved standardisation of carcass sizes. The most tailored solutions occur in dairy farms, where automated milking parlours tailor feed quantities for individual animals. Animals are identified via Radio Frequency Identification (RFID) tags, typically in the form of an electronic ear tag. In intensive pig farms, systems exist that can separate different sized animals into sub-groups based on their mass relative to the group mean and tailor feed to each subgroup to minimise the standard deviation of mass.

The severity of cyber attacks against feed systems is low: they contain little or no confidential data and incorrect feed sizes would have a minor impact on efficiency, yields and animal welfare before being detected. A loss of availability could be managed by reverting to more manual methods.

The milking period varies between animals and over time. Automatic milking parlours, which operate all the time, allow for optimal milking periods that improve yields and animal welfare. These systems can detect possible health issues, alerting farmers and segregating animals. The milk from a cow undergoing treatment for mastitis is automatically discarded to avoid drugs entering the food chain. The milk is collated in a refrigerated storage vessel ready for collection, with an automated cleaning cycle performed following a collection. These systems are connected to the internet, allowing remote monitoring and software patching by OEMs.

The severity of cyber attacks against automatic milking parlours could be significant. Loss of integrity or availability could result in the spoiling of batches of milk or reduced yields per animal. Milk production is demand-driven, so if a cow is not milked it will eventually dry off and only produce milk again following the next breeding cycle. The ability for a farm to revert to an alternative means for milking strongly influences the severity of any loss of availability of an automatic milking parlour.

HVAC systems are often necessary on poultry farms to avoid asphyxiation from excessive ammonia and carbon dioxide levels as well as avoiding overheating. These systems can include ammonia and carbon dioxide concentration sensors, and temperature sensors. Some intensive pig farm buildings may require active ventilation systems to maintain health and avoid overheating if natural ventilation is inadequate. Dairy farms are encouraged to avoid active ventilation in favour of ensuring that building designs provide adequate natural ventilation.

Animal monitoring solutions currently consist of infrared and visible light Internet Protocol (IP) camera systems, typically using Wi-Fi or Power over Ethernet (POE) data links. These are used for monitoring calving pens and lambing sheds but can also be used as security cameras.

Cyber attack scenarios of significant severity include:

- Unauthorised access to IP cameras, enabling criminal gangs to plan and time theft of farm assets for maximum success. Malicious disabling of IP cameras would reduce the likelihood of thieves being apprehended
- Loss of integrity of automatic milking parlours, resulting in incorrect dumping of milk by the milking machine, contamination of the milk storage vessel with cleaning product or spoiling of milk through incorrect refrigeration settings, which would impact yields and competitiveness of the farm
- Loss of availability of automatic milking parlours resulting in an inability to milk cows and cows drying off, leading to significant financial harm to dairy farms. Dairy farms or OEMs could be targeted with a ransomware-type attack by cyber criminals or by animal rights activists
- Loss of integrity or availability of HVAC systems, leading to large losses of poultry or pigs, particularly if targeted on a hot day, resulting in significant financial harm to farms. Farms could be targeted with ransomware-type attacks by cyber criminals or by extreme animal rights activists

3.2.6 Aquaculture Infrastructure

While the application of science in aquaculture is advanced, there is only limited digitisation of the farming processes. The types of technologies used include:

- Environmental control
- Feeding
- Fish grading
- Vaccination

The amount of environmental control depends on the type of farming – Recirculatory Aquaculture Systems (RAS) are the most sophisticated, controlling acidity, oxygenation, temperature, lighting and ammonia levels. Some automated feeding systems use various sensors to monitor feed demand and adjust the quantities accordingly.

On larger fish farms, fish grading is automated, typically using different mechanical approaches to separate fish by size and using infrared sensors to count fish. Vision-based fish grading systems are starting to become commercially available, though these are used post-slaughter. Similarly, the vaccination of larger fish can be performed automatically, with commercial solutions using vision systems.

The various aquaculture equipment can be monitored by a single software solution or implemented as a SCADA system.

A loss of integrity or availability of the environmental control systems on a RAS farm is the most obvious threat scenario. This could lead to reduced yields or a large loss of animals, causing significant financial harm to the farm. They may be targeted by a ransomware-type attack by cyber criminals, extreme animal rights activists or wild fishery farmers that blame aquacultures for spreading lice and genetic introgression within their stock.

3.3 Future Technology Trends and their Cyber Security

The digitisation of agriculture will continue over the coming decades, driven by the various challenges detailed in section 2.6. This section explores future agricultural technology and the impact it may have on cybersecurity, though it is recognised that forecasting technological change can be fraught due to its chaotic nature.

Cyber attacks may become increasingly severe as wellas increasingly common due to several factors:

- A reduction of available fall-back systems, including the skills required to use them
- Introduction of common mode failures as systems become increasingly integrated
- Emergent threats for the super-system

The use of diverse suppliers and solutions can reduce risks but the potential increase in unit and maintenance costs may deter farm businesses if the costs of cyber attack are not appropriately considered. This mitigation also requires OEMs to adopt common standards and support interoperability, something that they may not be willing to do of their own accord. For some equipment types or for smaller farms it may not be possible to diversify the systems. Therefore, the appropriate management of cyber security risks in these products will become even more important.

Increasing connectivity between different agricultural systems can lead to unexpected behaviours from the larger system. System integrators use approaches such as system engineering methodologies to manage this behaviour. By drawing a comparison with commercial aerospace – an industry that has already had to deal with the integration of a multitude of systems across international boundaries – various national and international organisations work together to define regulations and standards. These organisations help integrate the systems, achieving high levels of availability and safety. Similar coordination may be necessary in the food sector.

The following subsections explore a number of rapidly evolving technologies in further depth.

3.3.1 Data Analytics

The integration and sharing of data between different entities in the food network will continue to grow, with farm management software being a key node in this network. Exploitation of this with big data analytics and artificial intelligence will drive improved efficiency and yields. Machine learning algorithms that utilise mobile phone cameras will support the monitoring and diagnosis of crop health, weeds and pests. This increased sharing of data will continue to fuel concerns over data privacy and the risk of misuse. To address these concerns there needs to be increased transparency over how data is used, the sharing of benefits between all stakeholders and confidence in the cyber security of these products. The Information Commissioner's Office (ICO) provides useful guidance on data protection[37] that is relevant to agriculture.

3.3.2 Autonomous Ground Vehicles (AGV)

Farm vehicles are expected to become increasingly connected and autonomous, with one estimate from Research and Markets suggesting that there will be a demand for over 60 thousand autonomous tractors by 2025[38]. The move toward AGVs is appealing as it can reduce labour costs and ameliorate a shortage in skilled farmworkers. Fresh produce farms are likely to be early adopters as labour contributes toward a more significant proportion of their costs.

Depending on the cost of equipment, AGVs potentially enable the move toward using fleets of small tractors by decoupling farm vehicle size and operating costs. Historically agricultural vehicles have increased in size to improve productivity but have now reached a practical limit, with the use of large vehicles causing soil compaction, which reduces yields. Up to 90% of energy used for cultivation is to repair the damage caused by compaction.

The adoption of fully autonomous tractors may currently be limited more by legal concerns than technological readiness. Fendt demonstrated a technology where an unmanned tractor works in parallel with a manned tractor in 2015. The Hands Free Hectare trial, for which Harper Adams University is a key partner, has demonstrated the ability to farm crops entirely with autonomous vehicles.

The cyber security threat to AGVs is substantial. While no significant new threat scenarios over current technologies have been identified, the increased attack surface and lack of a driver constantly monitoring the vehicle means that the likelihood and severity of cyber threats are elevated. Thorough testing of the cyber security of AGVs is necessary and ideally, security standards for the industry would be agreed and adhered to throughout the lifecycle of the product. Examples of applicable automotive standards include SAE J3061[39], PAS 1885:2018[40] and the in-development ISO/SAE CD 21434[41] – the latter includes the Agricultural Industry Electronics Foundation (AEF) as a cooperating organisation.

3.3.3 Unmanned Air Systems (UAS)

The mass adoption of UAS in agriculture will occur once regulations pass permitting them to spray agrichemicals and conduct autonomous BVLOS operations, noting that this technology is already in use in other countries. Their ability to carry out farm operations with little manual effort while avoiding soil compaction or physical damage to crops offers efficiency benefits over existing methods.

Other possible applications include the use of UAS to herd sheep and linking of a UAS to a tractor to provide multispectral sensor data for site-specific application of agrichemicals. Harper Adams University is planning trials for the latter.

The widespread adoption of UAS poses a number of cyber threats but these are largely generic rather than specific to agriculture. Hence, these cyber threats are not considered by this whitepaper. The only agricultural-specific cyber threat of significant severity is the hijacking of an autonomous spraying drone to dump chemicals. Significant financial damage could be caused if fresh produce farms or aquacultures were targeted. The severity of this threat scenario is mitigated by the banning of agrichemicals capable of causing significant harm to humans and water companies filtering water supplies for agrichemicals.

Cyber security issues of UAS and associated infrastructure will have to be addressed but no specific solutions are expected to be required for agriculture.

3.3.4 Remote Connected Sensors

There is considerable interest in the benefits that IoT devices could bring to agriculture. A likely application is the control of sector-specific irrigation on fresh produce farms, currently limited by the power supply. The development of low-cost biodegradable sensors offers one potential solution to this problem.

The use of sensors on individual livestock is expected to spread from dairy to pigs and possibly other species as the cost of sensors reduces and consumers demand improved animal welfare standards. An NFU-commissioned report into animal welfare[17] highlighted that animal welfare and public perception can be improved through additional data collection. A publication from the UK cross-government programme on food security research[42] raised the possibility of individual fish being monitored.

With regards to how cyber threats could change, if moisture sensors are used to directly control irrigation then the severity of a loss of integrity of the system is likely to increase. If there is a loss of confidentiality for systems that provide geo-tagged data for grazing livestock, organised criminal gangs could abuse this information to improve their success at stealing livestock.

With manufacturers rushing to bring new features to market, basic cyber security considerations are frequently being ignored[43]. The cyber security of IoT devices is currently being scrutinised, with recently proposed legislation aimed at addressing the problem[44]. The proposal includes the introduction of a labelling system to aid users in understanding security. In addition to complying with any legislation, IoT OEMs should adopt industry best practice and consider the security development lifecycle from initial design stages.

4 Agricultural Ground Vehicle Attack Surface

Agricultural ground vehicles have a number of significant threat scenarios and a relatively complex attack surface. The attack surface for current, highly-connected vehicles and hypothetical near-future commercial AGVs capable of conducting crop farming entirely autonomously are detailed within this section, in Figure 2 and Figure 3 respectively.

The attack surface for a current high-end agricultural ground vehicle is similar to that for road vehicles, with key differences including:

- Interfaces with implements
- Standalone infotainment systems
- Driver assist being more reliant on GNSS than machine vision systems

The most noteworthy change to the attack surface for a near-future AGV is the addition of Vehicle-to-Everything (V2X) communication systems, for example ground infrastructure that autonomously resupplies the vehicle with agrichemicals.

Current Farm Vehicle Attack Surface

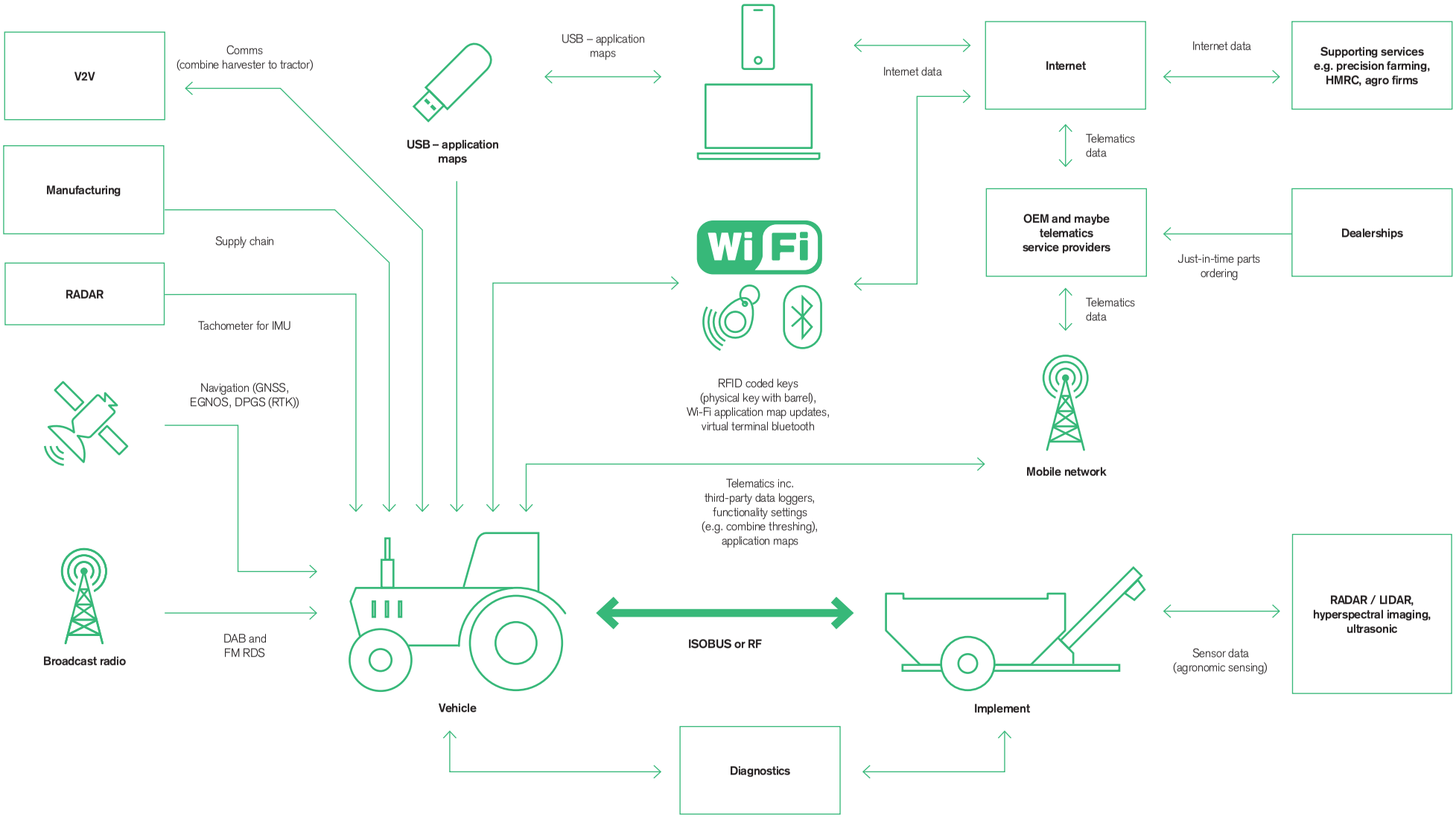


Figure 2: current farm vehicle attack surface

Autonomous Ground Vehicle Attack Surface

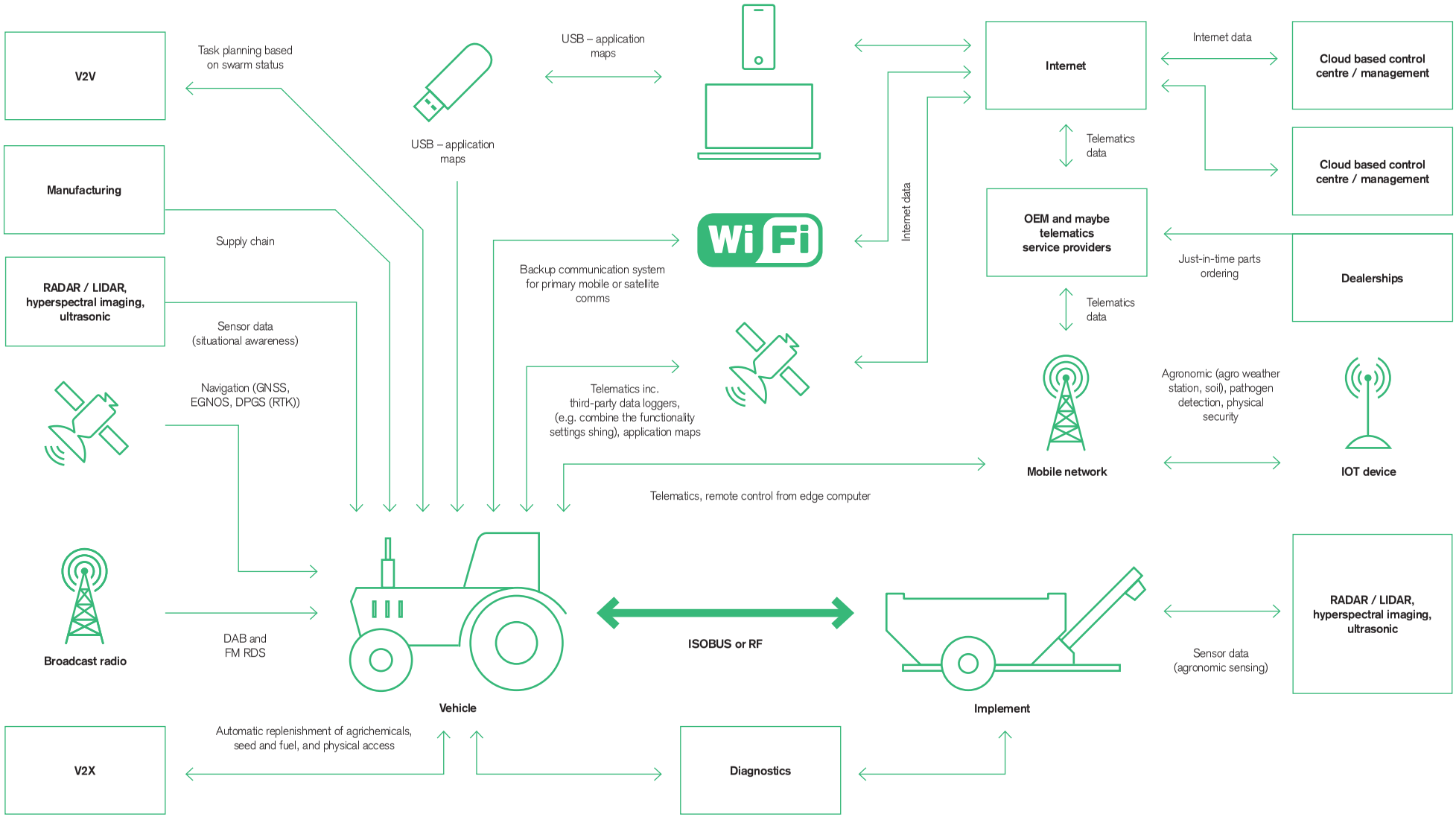


Figure 3: autonomous ground vehicle attack surface

5 Conclusion

The food industry is a critical, complex and interconnected global network utilising a diverse range of digital technologies. This forms a large attack surface and a range of threat scenarios. However, given the wide variety of food types available to the consumer, diverse food chains and a high number of micro, small and medium sized businesses, it is resilient to disruption. There is no conceivable cyber threat scenario with a severity level high enough to cause direct and immediate starvation. There are, however, threat scenarios that could result in significant financial harm to the industry, social unrest and suffering to livestock.

The most severe risks lie within food distribution and storage, and food standard systems. Public perception and behaviours are important factors when considering the likely severity of threat scenarios. Any undermining of public confidence in food standards can result in massive financial losses for the afflicted subsector, as consumers avoid certain food types or supply chains. Food scares can result in panic buying, magnifying and spreading the effect of any disruption to food supply. The continuous pressure for improved efficiency within food distribution from large retailers could lead to further consolidation of distributors and smaller stockpiles, increasing risk.

Large food processors are high-risk targets for cyber criminals and any disruption to their operations could affect a large number of farmers and growers that supply them. The drive to improve efficiencies in food production will likely lead to further integration, further increasing this risk.

The subject of data protection within agriculture is unlikely to disappear anytime soon as the volume and variety of accumulated data grows and machine learning and artificial intelligence are applied in increasingly sophisticated ways to provide new insights – and revenue streams – for those that have access to it. The issues of ownership, data privacy and security have to be addressed to avoid abuse and inequality.

The interactions between the food sector and other critical infrastructure pose additional threat scenarios. Malicious control inputs into farm vehicles fitted with auto-steer could be used to target electric power distribution. A simpler, less targeted terrorist attack could aim to cause injury, death and destruction.

The mitigations for much of the food sector are similar to those required for other industry sectors – the cyber security of enterprise networks, web applications, cloud hosted services and SCADA systems can be managed with standard approaches and business processes. Indeed this is the approach that Defra and FSA have adopted. It is worthwhile considering that cyber attacks against some businesses can cause far more harm and warrant additional scrutiny.

The threat to farms differs from the rest of the food sector. Firstly, there are diverse and tailored technologies in unique environments that present numerous novel threat scenarios. A broad range of attack surfaces, attack vectors, motivations and threat scenarios have been discussed in this whitepaper. Secondly, the increasing average age of farm workers, the tendency for farms to be small or micro enterprises and small margins means that they are less likely to be prepared for cyberattacks. Awareness of cyber security in the farming community is low and relying on farmers to adopt generic guidance on how businesses can protect themselves is likely to prove ineffective by itself.

The cyber threat will increase in severity and likelihood as new technologies are adopted by the food sector. The motivation for increasing digitisation extends beyond merely that of competitiveness – improving agricultural technology is one of the means for achieving the fundamental shift that is required by the global food network to adapt to population growth, demographic changes, climate change, ecological damage and water scarcity. Not only should we be preparing for this growing cyber threat in order to protect the day-to-day functioning of the food industry but also to ensure that they do not delay the adoption of technologies that are urgently needed by mankind.

6 Recommendations

There are specific actions that can address the issues raised in this whitepaper. It is recommended that the following actions be considered by the industry:

1. Defra and the FSA to work with research institutes and security specialists to improve understanding of the cyber security posture of the food network, including interactions between the different subsystems and emergent system effects. Collaboration with the Department for Transport (DfT) may be required for the assessment of cyber threats within the food distribution system.

2. Defra and FSA to review whether the cyber security of large food sector companies should face additional scrutiny to appropriately reflect the severity of cyber attacks directed against them.

3. The CPNI to consider the cyber threat of farm vehicles used to target CNIs, such as electric power distribution.

4. Defra, DfT, agricultural OEMs and security specialists to collaborate to ensure that cyber security knowledge, intelligence, standards and best practice are shared between the transport sector and farm vehicle manufacturers.

5. Defra, NFU, ADHB, agricultural OEMs, research institutes and security specialists to collaborate to review and produce policies, guidance and standards for agriculture. Consideration of user behaviours is necessary in order to implement the most effective means for improving security. For example, extending the proposed labelling scheme for IoT devices to aid users in understanding security[43] to other types of equipment and raising awareness within the farming community.

6. Defra to review policies relating to data privacy in the agriculture sector in order to clarify data ownership, promote transparency, share benefits and avoid misuse.

7. Defra, FSA, food sector OEMs, research institutes and security specialists to research the cyber security of technologies in order to identify vulnerabilities and fixes.

7 References

1. "Agriculture in the United Kingdom 2017" DEFRA https://www.gov.uk/government/statistics/agriculture-in-the-united-kingdom-2017
2. "Employment in agriculture (% of total employment) (modelled ILO estimate)", International Labour Organization, ILOSTAT database. Data retrieved in September 2018 https://data.worldbank.org/indicator/SL.AGR.EMPL.ZS
3. "The Food and Drink Industry - Economic contribution and growth opportunities", June 2017, by Grant Thornton on behalf of the Food and Drink Federation https://www.fdf.org.uk/publicgeneral/FDF-GT-Exec-Summary.pdf
4. "Sector Resilience Plan for Critical Infrastructure 2010", March 2019, UK government Cabinet Office policy paper https://www.gov.uk/government/publications/2010-sector-resilience-plan
5. "AGRICULTURE IN THE UK - NIESR General Election 2017 – Briefing No. 4", 26th May 2017, by Alastair Bailey, Sophia Davidova and Ulrike Hotop, funded by the Nuffield Foundation, https://www.niesr.ac.uk/sites/default/files/publications/NIESR GE Briefing Paper No. 4 - Agriculture in the UK_0.pdf
6. "Assessing the environmental impacts of consumption and production: Priority products and materials", International Resource Panel (2010), United Nations Environment Programme http://www.resourcepanel.org/reports/assessing-environmental-impacts-consumption-and-production
7. "Farming loved but misunderstood, survey shows", 23 August 2012, https://www.cam.ac.uk/research/news/farming-loved-but-misunderstood-survey-shows
8. "Cybersecurity in the Agrifood sector: Securing data as crucial asset for agriculture", Capgemini Consulting and Wageningenur University https://www.capgemini.com/consulting-nl/wp-content/uploads/sites/33/2017/08/02-029.16_agrifood_pov_consulting_web.pdf
9. "More than half of British firms 'report cyber attacks in 2019", BBC News 23rd April 2019, https://www.bbc.co.uk/news/business-48017943
10. Private Industry Notification PIN 160331-001 Smart Farming May increase Cyber Targeting Against US Food and Agriculture Sector https://info.publicintelligence.net/FBISmartFarmHacking.pdf
11. "Threats to Precision Agriculture", 2018 Public-Private Analytic Exchange Program https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf
12. "HSBC issues fraud warning as UK farmers targeted by cyber criminals", 15th April 2019, Farmers Guardian, https://www.fginsight.com/news/news/hsbc-issues-fraud-warning-as-uk-farmers-targeted-by-cyber-criminals-83806
13. "Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry", 26th February 2018, by Andrew Geil, Glen Sagers, Aslihan D. Spaulding, James R. Wolf, https://www.wageningenacademic.com/doi/abs/10.22434/IFAMR2017.0045
14. "4 The structure of the dairy supply chain: how efficient is the UK dairy industry?", Select Committee on Environment, Food and Rural Affairs Ninth Report, 8th June 2004, https://publications.parliament.uk/pa/cm200304/cmselect/cmenvfru/335/33507.htm
15. "Innovation and integration in the agri-food industry", April 2010, by Kostas Karantininis, Johannes Sauer and William Hartley Furtan, https://www.research.manchester.ac.uk/portal/en/publications/innovation-and-integration-in-the-agrifood-industry(549a3ae7-42ce-4e33-a864-cee6c94097b3).html
16. "Food Fraud Report" 2018, NFU Mutual, https://www.nfumutual.co.uk/globalassets/news-and-stories/pdfs/nfu-mutual-food-fraud-report-2018.pdf
17. "Farm Animal Welfare Global Review Summary Report" February 2018 by the Evidence Group on behalf of the NFU https://www.nfuonline.com/sectors/animal-health/animal-health-rh-panel/farm-animal-welfare-global-review-summary-report/
18. "Future Of Farming Review Report", 9th July 2013, Defra, https://www.gov.uk/government/publications/future-of-farming-review-2013-report
19. "The cash flow crisis in farming and its implications for the wider rural economy", April 2016, produced by the Andersons Centre and commissioned by The Prince's Countryside Fund, https://www.princescountrysidefund.org.uk/research/the-cash-flow-crisis-in-farming
20. "Big data means big profits, risks for farmers", 11th May 2014, USA Today, https://eu.usatoday.com/story/money/business/2014/05/11/gannett-big-data-means-big-profits-for-farmers-but-trust-concerns-loom/8970299/
21. "Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware", 21st March 2017, Motherboard, https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware
22. "Climate change: 'Right to repair' gathers force", 9th January 2019, BBC, https://www.bbc.co.uk/news/science-environment-46797396

23. “PAS 96:2017 - Guide to protecting and defending food and drink from deliberate attack”, 4th edition, November 2017, produced by the Department for Rural Affairs and the Food Standard Agency https://www.food.gov.uk/sites/default/files/media/document/pas962017.pdf

24. “Resilience in the Food Chain: A Study of Business Continuity Management in the Food and Drink Industry - Final Report to the Department for Environment, Food and Rural Affairs”, July 2006, Dr Helen Peck, http://randd.defra.gov.uk/Document.aspx?Document=FO0102_8522_FRA.doc

25. “Is the UK’s food supply hanging in the balance?”, 4th June 2013, Full Fact, https://fullfact.org/economy/uks-food-supply-hanging-balance/

26. “Taking the Fight Forward - Rural Crime Report 2018”, NFU Mutual, https://www.nfumutual.co.uk/news-and-stories/rural-crime-2018-infographic/

27. Networked world “Risks and opportunities in the Internet of Things”, A Lloyd’s emerging risk report https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/networked-world

28. “3 Supply Chain Lessons From the KFC Fowl-Up”, 1st March 2018, Forbes, https://www.forbes.com/sites/kevinomarah/2018/03/01/three-supply-chain-lessons-from-the-kfc-fowl-up/#523728f31cb1

29. “E. coli cucumber scare: Spain angry at German claims”, 31 May 2011, BBC. https://www.bbc.co.uk/news/world-europe-13605910

30. “Brexit Perspectives: What can we learn from NZ?”, 15th January 2019, ADHB, https://ahdb.org.uk/news/brexit-perspectives-what-can-we-learn-from-nz

31. “Food security for sustainable development and urbanization: Inputs for FAO´s contribution to the 2014 ECOSOC Integration Segment, 27-29 May”, FAO, http://www.un.org/en/ecosoc/integration/pdf/foodandagricultureorganization.pdf

32. “Milking automation is gaining popularity”, 15th January 2015, Dairy Global, https://www.dairyglobal.net/Milking/Articles/2015/1/Milking-automation-is-gaining-popularity-1568767W/

33. “Foresight. The Future of Food and Farming (2011) Final Project Report”, The Government Office for Science, London, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/288329/11-546-future-of-food-and-farming-report.pdf

34. “Press Release 5 - Automated Harvest Time 06/09/2017”, 11th September 2017, HandsFree Hectare, http://www.handsfreehectare.com/press-releases/press-release-5

35. “Six new cars rated ‘poor’ for security in theft-risk survey”, 21st March 2019, BBC, https://www.bbc.co.uk/news/business-47655330

36. “GPS equipment worth thousands stolen from tractors”, 20th March 2019, Farmers Weekly, https://www.fwi.co.uk/news/crime/gps-equipment-worth-thousands-stolen-from-tractors

37. “Big data, artificial intelligence, machine learning and data protection”, version 2.2, 4th September 2017, Information Commissioner’s Office, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

38. “Autonomous Tractors Market by Power Output (Up to 30 HP, 31–100 HP, 101 HP and Above), Crop Type (Cereals & Grains, Oilseeds & Pulses, Fruits & Vegetables), Farm Application, Component, and Region - Global Forecast to 2025”, February 2018, Research and Markets, https://www.researchandmarkets.com/research/5gkkxh

39. “J3061_201601: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”, 14th January 2016, SAE International, https://www.sae.org/standards/content/j3061_201601/

40. “PAS 1885:2018: The fundamental principles of automotive cyber security. Specification”, December 2018, British Standards Institution, https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

41. “ISO/SAE CD 21434: Road Vehicles -- Cybersecurity engineering”, under development, International Organization for Standardization, https://www.iso.org/standard/70918.html

42. “The UK Aquaculture industry” July 2014, Insight Issue https://www.foodsecurity.ac.uk/publications/insight-issue-four-uk-aquaculture-industry.pdf

43. “IoT security: Why it will get worse before it gets better”, 7th November 2018, ZDNet, https://www.zdnet.com/article/iot-security-why-it-will-get-worse-before-it-gets-better/

44. “Plans announced to introduce new laws for internet connected devices”, 1st May 2019, https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices