Preprint of: *van der Linden, Michalec, and Zamansky, "Cybersecurity for smart farming: socio-cultural context matters", IEEE Technology and Society Magazine (forthcoming), 2020*

Cybersecurity for smart farming: socio-cultural context matters

Dirk van der Linden, Ola Aleksandra Michalec and Anna Zamansky

Food security is a societal issue of increasing importance requiring careful consideration of the way we produce, process, and distribute food [2], [6]. Digital technologies are increasingly used to optimize processes to support these activities, and therefore, bear important implications for food security. In this article, we focus in particular on technologies used for an important aspect of such security—the effective production of sufficient food, or, *food availability*. Technology has always been an integral part of humanity's efforts to optimize food production processes. Already thousands of years ago, farming tools such as plows were used, first by humans, then with animals, to improve conditions for planting crops and thereby increase our yields. Modern food production has seen an explosion of both the amount and the sophistication of technologies we use, and has increasingly moved to sophisticated digital technologies such as robots, sensor-driven systems, drones, and automated image analysis [11].

Such digital technologies, for all the benefits they bring, also come with new challenges, including that of ensuring their "cyberbiosecurity"—ensuring there are no vulnerabilities at the intersection of their cybersecurity, cyber-physical security, and their biosecurity [27]. Recent research has highlighted the variety of cybersecurity threats and attack vectors the food sector faces (from attacks on farm data or networking and equipment, to the wider supply chain, and even terrorism, cf. [3], [14]), as well as having documented data breaches in agricultural organizations, and finding that many farmers and agribusiness owners had been affected by computer security incidents [16]. While the consequences of attacks on a digitized food sector may not be as immediately obvious as in other critical infrastructures (e.g., sudden loss of power, disruption of transport), food availability may likely be impacted as a result of cyber attacks through a delayed effect. A cyber attack may e.g., cause food production capability to be lowered and set off a ripple effect moving through the food production chain and related infrastructures of processing and distribution, until eventually consumers are faced with empty shelves in their supermarkets [21]. Both the actual technologies used for food production (*operational technology*, or, OT*)* and the computer systems that surround it (*information technology,* or, IT), need adequate protection from accidental and malicious attacks that can disrupt the food production processes. Such attacks have become increasingly common, as evidenced in increasing numbers of phishing and ransomware attacks on farms and agriculture companies, such as the ransomware attack on the U.K.'s National Milk Group in 2019[1]. However, little attention has been paid to the *socio-cultural context* in which the digital technologies for food production is developed and used, and how that may mitigate or worsen potential attack vectors and the impact of concrete threats.

[1] See: https://www.nfuonline.com/sectors/dairy/dairy-news/update-on-the-nmr-ransomware-virus-attack/

To that end, this article has two purposes: (1) to start a discussion on how the food sector is stimulated to increasingly adopt new digital technologies, without having as much opportunity to consider its cybersecurity implications, and (2) to shed light on how socio-cultural context is intertwined with the development and use of cyber secure technologies, and how unforeseen risks may arise when technologies developed in one socio-cultural context is adopted in others. We do so by analyzing the conflicting demands on use of technologies in the food sector in the U.K. on the one hand, and lack of support for its cybersecurity on the other hand, followed by an exploratory case study of what drives the development and use of a technological solution for dairy farming developed in Israel, now increasingly adopted in the U.K.

The digitized food sector: technology first, cybersecurity later?

The U.K. government, through the Department for Environment, Food and Rural Affairs (DEFRA), heavily promotes the adoption of operational precision agriculture technologies in order to stimulate increased efficiency of its food (production) sector [17]. Research has shown that such technologies exhibits rapid adoption patterns [24], meaning that once some farms adopt a particular type of technology, it is likely to quickly spread throughout the sector and be adopted by other farmers. Moreover, the sector typically favors technologies which can be readily bought and implemented 'off the shelf', which has been shown to cause rapid wide-scale adoption [28]. The food sector is thus pressured to quickly adopt new technologies both vertically (i.e., the government stimulating adoption of new technology), and laterally (i.e., competitors adopting new technology), giving it little time to perform meaningful in-depth reflections on how these technologies will change the nature of their work and what new risks and threats it may bring.

In 2017, the U.K. Government explicitly called to defend the food sector from deliberate attacks, including "*cyber enabled industrial espionage, or hacking—gaining unauthorized access to computer systems, perhaps with malicious intent*" [18]. Yet, even though there is a relevant EU Directive on security of network and information systems for critical national infrastructure (the "NIS" Directive), the U.K. Government has not included the food sector to fall within its remit. While farmers and other stakeholders in the food sector have explicitly called for the NIS directive to apply to the food sector in order to increase cybersecurity standards, doing so is postponed until the legislation's first re-evaluation [19]. Moreover, while relevant Publicly Available Specifications (PASs) sponsored by the U.K. Government [18] describe several cyber threats that the food sector needs to deal with (e.g., DDOS attacks on web-based ordering systems, loss of GPS-based navigation, ex-filtration of sensitive data due to phishing emails), little guidance is yet given to how to safely and effectively adopt novel technologies while explicitly understanding what consequences the assumptions of their design entails. There is thus a clear threat to the food sector from massive disruption as a result of cyber attacks, as

technologies are increasingly adopted and quickly spread throughout the sector, without allowing for the time to consider its impact on security (i.e., technology first, cybersecurity later). Because the U.K. produces almost half of the food it consumes [30] this may be even more critical, as disruptions in internal food production will make the food sector not resilient to cope with disruptions from attacks.

Cyber attacks against the food sector may target both the operational technology (i.e., the actual technologies 'in the field'), as well as the information technology (i.e., the computer systems used to control and manage those technologies). Moreover, such technologies adopted by the U.K. food sector may have been originally developed anywhere in the world. Technology is not developed in a vacuum, but it is a subject to socio-cultural differences in how we approach and value both problems and their solutions (cf. [20]). Thus, the way technologies were developed may have been guided by completely different assumptions and attitudes, whether stemming from the culture of the society it was developed in, or the culture from the organization and sector within that society. As a result, technological solutions that make sense in one socio-cultural context may not make sense in another (cf. [33]). This makes it all the more critical for a sector where technologies are rapidly adopted and diffused. We, therefore, ought to understand how the assumptions and expectations from a particular socio-cultural context where the innovation was originally developed may or may not transfer well to its new location.

However, most of the existing research on cybersecurity in the food sector does not yet address these assumptions and demands, instead focusing on technical aspects, or proposing frameworks focused on data analytics and economic incentives. For example, Chi et al. proposed a framework incorporating the detection of false positives in sensor data, implementation of access control, and using encryption [8]. Other industrial reports focus primarily on *perceived* risks and threats (e.g., [5]), which has led to researchers offering quantitative prediction models for vulnerability of technologies in the food sector [34]. Hecht et al., on the other hand, have offered one of the few in-depth qualitative work identifying a wider variety of factors contributing to (lack of) resilience in the urban food supply chain [15], noting the importance of the social environment and organizational culture. The food sector displays multiple systemic qualities: complexity, interconnectedness, path-dependency, non-linearity; so goes the argument for the societal challenges surrounding innovation in that sector [32]. Cybersecurity, privacy, transparency of data, sustainability, safety and equitable access—all these issues depend on each other and ought to be considered in their broader socio-cultural context to improve resilience of a sector as a whole [26]. This article will demonstrate how opening up a debate on the socio-cultural dimensions of cybersecurity in food production innovation will inevitably lead to re-conceptualizing cybersecurity away from purely technical issues and solutions.

In summary, ignoring the interdependencies between the elements of the food system could lead to a potential "perfect storm"' of conditions to affect the U.K.'s food availability should malicious actors be able to successfully disrupt food and agriculture processes by exploiting vulnerabilities in operational precision agriculture technologies or the information technology

controlling it—similar to the impact the WannaCry ransomware attack had on the the U.K.'s National Health Service [9].

Case study—precision dairy farming

With this case study, we aimed to construct a snapshot of the different considerations and attitudes towards cybersecurity across different stakeholders of the food sector, focusing specifically on the dairy farming sector in Israel. We focus on this case because the dairy industry leads the technology in precision livestock farming [25], and Israel is a global leader in the dairy industry (cf. [29]), which makes it particularly relevant to understand how new innovative technologies may come about. In our analysis, we compare case study data from Israel (technology developers and early adopters) with the political and commercial context of the UK, where the efforts to mobilise early-adoption of precision agriculture are taking place [10].

We performed a qualitative study using in-depth semi-structured key informant interviews [23] and site visits, interviewing key stakeholders to build a picture of the cybersecurity situation for dairy farming in Israel over the span of two weeks. As it is challenging to conduct interview-driven studies in commercial sectors where the aim is to get participants to reveal critical information about the security of products they develop or use [12], [13], we opted to build an in-depth case study, building rapport with key informants, and using multiple data points obtained through interviews at different times. We selected participants according to the different roles they play in the context of precision farming and their ability to provide further insight into key issues perceived by colleagues in their field (i.e., using them as *key informants* to further understand attitudes and requirements from these type of stakeholders). We interviewed the chief technoloy officer (CTO) of a leading commercial vendor which provides sensor equipment to farms, a farmer using the vendor's technology able to speak of other colleagues' attitudes and opinions, and a risk analyst from an international strategy firm tasked with analyzing cybersecurity of various sectors. We spoke to interviewees multiple times, and performed site visits to a farm using the vendor's product to gain a better understanding of the developed technology. Due to the sensitive nature of discussing security concerns of a commercially available product, we do not disclose the identities of the interviewees or their organizations. We obtained approval from our Institutional Review Board (IRB) before any empirical work began. We did not capture any personal information from interviews.

Participants were read an informed consent form, and verbally consented to participating in the study. We used a common interview guide based (shown in the Appendix) on questions and items from recent work on secure development [1] and precision agriculture cybersecurity frameworks [8], [34], tailoring the questions to each participant to account for their different roles and relation to the food sector and/or the dairy farming technology. Interviews took place at different sites or via online calls. One researcher conducted all interviews, sometimes accompanied by a second researcher, which we did in order to build up rapport and trust given

the potentially sensitive nature of these discussions focusing on security of technology they developed and used. Due to the potentially sensitive topic of the interviews did not record participants, instead taking notes to inform further analysis of findings. No reimbursement was given for participants.

Using the notes taken during the interviews, two authors iteratively discussed the findings, developing a conceptual framework of the key concepts raised by participants. They did so focused on fostering discussion and building towards a shared understanding of key points discovered in the interviews, to uncover the attitudes towards cybersecurity across stakeholders, guided by Barbour's reflection on qualitative research noting that "what is ultimately of value is the content of disagreements and the insights that discussion can provide for refining coding frames." [4]

The descriptive case study is structured in three parts, discussing (1) what the technology developed by the vendor does, (2) what its key requirements are from the vendor and user perspectives, and (3) how the technology is used and how cybersecurity considerations from both vendo and user follow from that.

Description of the technology for sensor-driven dairy farming

The vendor is a leading commercial company which provides sensor-driven technologies for precision farming, used by dairy farms across the world ranging in size from e.g., 50 to 400 cows. The technological solution, is, to put it simplified, a sensor-based system for the monitoring of data relevant to health and welfare of livestock. The operational technology consists of physical sensors which are worn by individual cows, capturing e.g., activity data and vital signs. This data is then relayed towards a central information system where farmers can monitor all captured data. The software analyzes this data to provide further decision-making support on important livestock performance aspects which may impact the quality of the produced milk, giving indicators for e.g., stress levels, feeding patterns, or metabolic changes.

Requirements for the technology—data is everything

If one thing became apparent from our interviews, it is that *data is everything*. From the vendor's point of view, data quality is central in developing an efficient system for dairy farming, as the data forms the basis to inform any of the farmers' decision-making. Most development thought and effort thus goes towards the sensors, assessing what kinds of data can be acquired of the cow, and how these data can be of value to farmers. Data quality, is thus the name of the game, and development of the technology focuses on capturing as much meaningful actionable data to support understanding livestock physiology and behavior.

This aligns well with the priorities of farmers, whose main focus is to use data to understand their livestock—tracking individual cows to know when to inseminate, generating patterns of feed intake, understanding behavioral factors affecting their health and welfare. Effectively, the

farmer noted that they and their colleagues make all decisions based on aggregated data, so their priority is to get high quality data, and as much of it as possible.

The farmer we interviewed was relatively new to the profession, having been a dairy farmer only for the past three years. Of those three years, he has always used sensor technologies, never considering it a challenge to implement and use it, noting that *"farmers have always used technologies to understand their cows for as long as they have existed."* The farm they work at has been in business for over 15 years. Different kinds of technologies have come and gone since then, with farm management adopting new technologies when it allowed them to obtain more data about their cattle. Their requirements are to obtain more and more data, effectively to build a detailed model of each individual cow from birth, to analyze how they will behave, and whether they will become an effective dairy cow. When pressed on what future technologies could, or should, hold, the answer was similar: more, detailed data, going to the level of individual genetic information of each cow. They explained this would be great from a business point of view, as the cost involved in raising a cow to adulthood is significant, and, should they not be as productive as desired, selling them as meat cows only allowed to recoup some of the expenses involved in raising them.

Given the focus on data, basic cybersecurity efforts proposed in literature (e.g., [8], [34]) are important to consider, such as at least ensuring (1) abnormal measurement detection, (2) access control, and (3) encryption. Detection of abnormal measurements is indeed seen as vital by the developer given the data-driven nature of the technology and significant development efforts go towards it. Access control is currently implemented, but limited to sensitive data, such as current research or commercial data. However, most, if not all data is freely shared owing to the socio-cultural origin of the agriculture sector in Israel, leading stakeholders to not perceive significant threats that a malicious actor could carry out with livestock data. Encryption, however, is not as widely used, likely due to similar attitudes of data being freely shared and perceptions of that it would be counterproductive to avoid easy access to it.

Using the technology—not all threats are perceived equally by vendors and users

We further built a more accurate understanding of what threats the food sector in general, and digitized food production organizations (such as precision livestock farming) in particular, face in Israel. We interviewed a managing research director of cybersecurity, who focused on modeling and understanding cyber attacks and risks, including those present in critical infrastructures, including the food sector.

The primary threat faced by food production companies is similar to that in many other contexts. There is little evidence of malicious nation state actors or their proxies engaged in cyber attacks, but there is real-world evidence of attacks conducted by smaller scale cyber criminals motivated by economic incentives (i.e., theft of data perceived as commercially sensitive, or blackmailing).

As one could expect from the smaller scale, these do not focus on the operational technologies used by the food sector, as developing and conducting attacks against new technology requires an investment of time and effort to understand the hardware, build attacks, and find appropriate vectors to conduct them. Instead, attackers attempt typical attacks like ransomware and phishing to affect the information technology layer and blackmail the operators of this IT layer into making payments to unlock the hardware or avoid release of sensitive data. However, a more direct threat vector has been used as well, where cyber criminals attempt to compromise the digital infrastructure of farms through lateral movements, again attacking the information technology layer primarily (to the point of overruling almost any other attack vector) through insecure configuration. That is, attackers will attempt to log in to IT systems using standard credentials, or attempt to abuse management systems such as auto-backup scripts with embedded credentials. The key threat to technologies in the food sector faced in Israel is thus towards the *information technology (IT) layer*, coming primarily from an *economic* perspective.

From interviewing the vendor of the system we studied, these attack vectors seem particularly salient, as only one real threat was perceived: *real-time data loss*, by whatever means. Should the system crash, whether due to software bugs, environmental factors, or cyber attacks, this would be a major problem. Given that data is stored on the information technology layer, it thus seems that the existing attack vectors indeed pose a threat to the cybersecurity of the technology.

Looking at the farmers using the technology, understanding of what they do to ensure their cybersecurity, and more importantly, whether they share the same attitude towards data loss being critical paints a more nuanced picture. In interviews with users of the sensor technologies, we found that they were not as worried about data loss, whether data itself leaking by accident or being maliciously extracted. Furthermore, the farmer mentioned that to their knowledge other colleagues in the field did not worry about this either, even though they admitted to having a central local server that holds all their real-time and historical data. When asked why they did not consider data loss to be a threat, they noted two key things:

1. unlike the vendor, they are not worried about loss of real-time data, as this is used for day-to-day operations rather than long-term analysis and decision making; and
2. they simply do not consider the data as commercially sensitive. In fact, they shared it freely: "*if a veterinarian calls and asks for the data, they get it. If a researcher calls and asks for the data, they get it.*"

Farmers did note the impact that a loss of real-time data would have on their ability to immediately react to their cows, but, besides having never experienced such data loss before, noted they knew how to run their farm, and that years of experience in day-to-day work meant that they perceived the impact of not having this data on the productivity and welfare of their livestock as negligible. On the historical, or aggregated data, they explained that loss of such data is certainly an issue that has to be dealt with, as this data informs their decision-making. However, dealing with it was considered trivial because relevant data could simply be obtained from colleagues, as there is an existing culture of being open and sharing with such data.

They perceived this attitude towards data sharing to be grounded in the history of the agriculture sector in Israel, where farming has effectively descended from kibbutzim [singular -kibbutz -]: ideological collective communities hoping to spread socialism and equality "to all corners of the land" [22]. These communities were primarily centered around agriculture, and built on an utopian ideology of social responsibility and sharing of labor [31]. Over time, and in part due to economic crisis as well as increasing individualism, many agricultural kibbutzim became privatized, and detached from the original utopian visions, but, nonetheless, had a lasting effect on the attitude of people working in the sector. Thus, while in modern times the agriculture sector is no longer exclusively built on collective farming models, the open attitude of the people involved in the agriculture sector has prevailed. Shared responsibility is effectively seen as shared benefits, especially when it comes to data analysis. Dairy farms provide data to a central authority, which allows for more insights than any individual farmer could generate on their own with their livestock. Almost all dairy farms in the country participate in this, and benefit from the research and analysis performed centrally to understand their own cows better. As such, they are happy to share data, and do not consider it a threat if other farmers learn details of their operations (whether livestock data or even financial data), even meeting up yearly to compare and learn from each other.

Instead, farmers' primary concerns in terms of potential cyber attacks were not focused on the access to data held in their farm's IT layer per sé, but rather on the accuracy of the data captured by the operational technology, the actual physical sensors. They noted that it would be a major problem if sensors were somehow compromised and subsequently provide erroneous data without them realizing so, as this would lead to making decisions on faulty data, potentially impacting productivity and welfare of the livestock. However, they perceived this as very unlikely, assuming it to require physical access, and relevant know-how of the hardware itself. Indeed, this kind of cyber attack is unlikely given the known threat actors in this context, as corrupting data would decrease its potential value for anyone involved. Commercial sabotage could thus be a main driver for such attacks, although in this socio-cultural context such attacks would not make sense as farmers freely share data and collaborate, rather than compete. Given the dairy farmers' propensity for sharing files, and learning from each other, this thus seems an unlikely threat, as it only reduces potential value for any actors involved (less worthwhile data to learn from, whereas affected target can still learn from untampered data shared by others). Another critical aspect supporting the cybersecurity of the technology is that farmers in this culture are open to the vendor gaining access to their information technology in order to configure the operational technology. That is, they happily grant access to their systems in order to allow the vendor to set up and configure the technology—reducing the risk of poorly configured systems that are more susceptible to data breaches.

This combination of the socio-cultural origin of the agriculture sector and its lasting effect on the attitudes of farmers in terms of data sharing on the one hand, and the primary attack vector being focused on holding data ransom does not mean that this attack vector as used by cyber criminals is suddenly gone—they will still attempt to attack IT layers and steal data. But the

impact of this primary threat is significantly reduced, as farmers would have no incentive to pay for e.g., unlocking encrypted data as a result of ransomware attacks, because other farmers would stand likely in solidarity with them and freely share the data they would need to continue operations.

Discussion—where it was made matters

Due to its success in increasing dairy farmers' productivity, the sensor technology has been increasingly adopted outside of Israel. However, due to the cultural origins of the agriculture sector and its effect on farmers' attitudes, key cybersecurity threats faced by the technology are effectively mitigated (i.e., ransomware threats focused on 'locking' away data fail because day-to-day data is not seen as vital, and long-term data is freely shared across the sector). This may not be the case in other countries where the agriculture sector may have developed in different ways, with radically different social origins.

Returning to the U.K. context, in our interview the vendor noted complications with the technology's initial adoption in the U.K., as farmers' attitudes towards data sharing are far less open. Sensor data is perceived to be more commercially sensitive, as the sector does not engage in similar open sharing as in Israel, evidenced by the vendor's experiences, and e.g., industrial reports focused on the U.K. context noting the "leaking of confidential farm data", including livestock health and economic indicators, as a major threat [3]. This difference in attitude means that unlike in Israel, farmers may be less likely to allow the vendor access to their information technology layer to setup and configure the operational technology, *increasing the risk of poor configurations being abused as a threat vector*, and more critically, *increase the impact of such risks*, as farmers in the U.K. more likely cannot fall back on other farmers' willingness to share data. We thus argue that threats that did not make sense in one socio-cultural context, also suddenly become relevant again. Compare for example the threat of commercial sabotage, which was mitigated in Israel due to the sector *collaborating* rather than *competing*, now is no longer mitigated, being a more valid threat, and thereby likely also attracting increased attention from cyber criminals as an opportune attack vector.

Thus, it seems that adoption of technologies built in one socio-cultural context into another comes with consequences for its cybersecurity, if key assumptions for the safe and secure operation of the system *in-context* are not made explicit. This case study has raised only one example of such socio-cultural factors, notably, the openness of a sector to share, rather than compete, and how it changes the impact of cyber attacks. This changes the way that risks should be analyzed. Typically, risks are assessed by quantifying their *impact* (from, say, negligible to catastrophic) and their *likelihood* of occurring (from, say, rare to certain) (cf. [7]). For example, if we know cyber criminals are actively using ransomware attacks to lock up IT layers in the food sector, *and* we assume that devices in that layer are poorly protected against key delivery vectors (e.g., people are not trained to detect phishing, firewalls and antivirus are not kept up to date), we could say it has a high likelihood. But what would the impact be? If they

succeed in an attack, and lock up data, farmers would effectively shrug, replace the computer rather than pay the ransom, and go about their day, using data willingly shared by other farmers. More realistically, the likelihood of the attack is affected by the socio-cultural context of the technology as well, as farmers are happy to allow the vendor to securely configure the technology, thereby reducing the likelihood of a poor configuration being abused as a threat vector.

The *socio-cultural context* in which technology is situated thus has an effect on the impact of a cyber attack. But the very likelihood of it from the attackers' point of view may also be affected, as cyber criminals will (eventually) realize their actions are fruitless in this context, making them drop such attack vectors for better opportunities. Thus, in order to assess the socio-culturally dependent risk of a cyber attack, both impact and likelihood need to be understood in context of the sector and the attitude of people within it. This raises an important call for research in protection of national infrastructures, or indeed, any sector to better understand digital technologies and their cybersecurity in the socio-cultural context they are situated: *what socio-cultural factors of technology development and use may alter, for better or worse, the impact and likelihood of cyber attacks?*

Acknowledgments.

This research was supported by a grant from the Ministry of Science & Technology, Israel (MOST), and by the Cabot Institute Innovation Fund. The Cabot Institute for the Environment is a diverse community of 600 experts, united by a common cause: protecting our environment and identifying ways of living better with our changing planet. Together, we deliver the evidence base and solutions to tackle the challenges of food security, water, low carbon energy, city futures, environmental change and natural hazards and disasters.

Author biographies

Dirk van der Linden is Lecturer (Assistant Professor) at Northumbria University, U.K. His research interests include software engineering, cyberpsychology, and technology for animals. Contact him at: dirk.vanderlinden@northumbria.ac.uk.

Ola Aleksandra Michalec is Research Associate at University of Bristol, U.K. Her research interests include policy and politics, science and technology studies, and partnership building. Contact her at: ola.michalec@bristol.ac.uk.

Anna Zamansky is Associate Professor at University of Haifa, Israel. Her research interests include information systems and technology for animals. Contact her at: annazam@is.haifa.ac.il.

References

1. H. Assal and S. Chiasson, "Security in the Software Development Lifecycle". In *Proc. 14th Symposium on Usable Privacy and Security*, pp. 281-296, 2018.
2. W. de Amorim et al., "Urban challenges and opportunities to promote sustainable food security through smart cities and the 4th industrial revolution". *Land Use Policy*, 87, pp. 104065, 2019.
3. L. Baker and R. Green, "Cybersecurity in UK Agriculture". NCC Group Whitepaper, 2019.
4. R. Barbour, "Checklists for improving rigour in qualitative research: a case of the tail wagging the dog?" *BMJ*, 322(7294), pp. 1115–1117, 2001.
5. M. Bogaardt et al., "Cybersecurity in the Agrifood sector". Technical Report. Capgemini Consulting, 2016.
6. H. Charles et al., "Food security: the challenge of feeding 9 billion people". *Science*, 327(5967), pp. 812-818, 2010.
7. Y. Cherdantseva et al., "A review of cybersecurity risk assessment methods for SCADA systems". *Computers & Security*, 56, pp. 1-27, 2016.
8. H. Chi et al, "A Framework of Cybersecurity Approaches in Precision Agriculture". In *Proc. of the ICMLG2017 5th International Conference on Management Leadership and Governance*. pp. 90–95, 2017.
9. A. Dwyer, "The NHS cyber-attack: A look at the complex environmental conditions of WannaCry". *RAD Magazine*, 44, 512, pp. 25-26, 2018.
10. T. Duckett et al., "Agricultural Robotics: The Future of Robotic Agriculture". Technical Report, UK-RAS Network White Papers, ISSN 2398-4414, 2018.
11. H. van Es and J. Woodard, "Innovation in agriculture and food systems in the digital age". In *The Global Innovation Index 2017 - Innovation Feeding the World*, pp. 97-104, 2017.
12. M. de Goede, E. Bosma, P. Pallister-Wilkins (Eds.), "*Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*". Routledge, 2019.
13. C. Grey, "Security studies and organization studies: Parallels and possibilities". *Organization*, 16(2), pp. 303-316, 2009.
14. M. Gupta et al., "Security and Privacy in Smart Farming: Challenges and Opportunities". *IEEE Access*, 8, pp. 34564-34584, 2020.
15. A. Hecht et al., "Urban Food Supply Chain Resilience for Crises Threatening Food Security: A Qualitative Study". *Journal of the Academy of Nutrition and Dietetics*, 119(2), pp. 211-224, 2019.
16. A. Geil et al., "Cybersecurity on the farm: an assessment of cybersecurity practices in the United States agriculture industry". International Food and Agribusiness Management Review, 21(3), pp. 317-334, 2018.
17. HM Government, "A UK Strategy for Agricultural Technologies". Technical Report, 2013.

18. HM Government, "PAS 96:2017 – Guide to protecting and defending food and drink from deliberate attack". Technical Report, 2017.
19. HM Government (Department for Digital, Culture, Media and Sport), "Security of Network and Information Systems – Government response to targeted consultation on Digital Service Providers". Technical Report, 2018.
20. G. Hofstede, "*Culture's consequences: International differences in work-related values*". Sage, 1984.
21. D. Ivanov, A. Dolgui, and B. Sokolov, "The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics". *International Journal of Production Research*, 57(3), pp. 829-846, 2019.
22. Y. Kislev, "Agricultural cooperatives in Israel: Past and present". In *Agricultural Transition in Post-Soviet Europe and Central Asia after 20 Years*, pp. 281-302, 2015.
23. P. Lavrakas, "Key informant." In An Encyclopedia of Survey Research Methods, pp. 2455, 2008.
24. J. Lowenberg-DeBoer and B. Erickson, "Setting the record straight on precision agriculture adoption". *Agronomy Journal*, 111(4), pp. 1552-1569, 2019.
25. E. Maltz, "Novel technologies: sensors, data and precision dairy farming", In Proc. North American Conference on Precision Dairy Management, pp. 1-15, 2010.
26. A. Michalec, "An exploratory study of the contributions to low carbon policy making in Bristol using WEF Nexus as a heuristic device". PhD Disseration, 2020.
27. R. Murch et al., "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy", *Frontiers in Bioengineering and Biotechnology*, 6, pp. 1-6, 2018.
28. E. Pierpaoli et al., "Drivers of precision agriculture technologies adoption: a literature review". *Procedia Technology* 8, pp. 61–69, 2013.
29. Reuters, "RPT-Milking it: Israel leads the way in dairy tech", May 19, 2015.
30. H. de Ruiter et al., "Global cropland and greenhouse gas impacts of UK food supply are increasingly located overseas". *Journal of The Royal Society Interface* 13(114), pp. 1-10, 2016.
31. T. Simons and P. Ingram, "The kibbutz for organizational behavior". *Research in Organizational Behavior*, 22, pp.283-343, 2000.
32. J. Schiere et al., "System thinking in agriculture: an overview". In *Emerging challenges for farming systems–lessons from Australian and Dutch agriculture*, pp. 87-105, 2004.
33. S. Vatanasakdakul, W. Tibben, and J. Cooper, "What prevents B2B eCommerce adoption in developing countries?: a socio-cultural perspective." *In Proc. 17th Bled eCommerce Conference*, pp. 1-15, 2004.
34. J. West, "A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies". *Journal of Agricultural & Food Information*, pp. 1–24, 2018.

Appendix

Interview guide

- What are your main priorities during the [development / use] of this technology? (in order of priority)
- Do your priorities change when a deadline approaches?
    - Why do you feel they [don't] change?
    - What about when a competitor seems to [develop / use] similar technology?
- What do you feel are the key challenges in [developing /using] precision agriculture technology?
- What about security of this technology? Is it something you worry about?
    - Can you think of anything in particular that made you think so?
    - How does security fit into your priorities?
- To what extent do you [build in / verify] the following functionality? What do you feel are your main challenges in doing so?
    - abnormal measurement detection
    - access control
    - encryption