Smart Farming: Cyber Security Challenges

Luís Barreto
Instituto Politécnico de Viana do Castelo
Instituto de Telecomunicações, Aveiro and ARC4DIGIT
Valença, Portugal
lbarreto@esce.ipvc.pt

António Amaral
Instituto Politécnico de Viana do Castelo
Centro Algoritmi and ARC4DIGIT
Valença, Portugal
antonioamaral@esce.ipvc.pt

***Abstract*—The diffusion of new digital technologies renders digital transformation relevant to nearly every economic activity sector, including in the agriculture sector. Farming and how farmers work is changing, the use of Information and Communications Technology (ICT) together with the increased use of the Internet of Things (IoT) is developing a concept that is called Smart Farming. Smart Farming benefits are tremendous, smart data can be used for seed traits and to treat soil conditions, the use of new technologies can offer unprecedented conveniences and improve the management and quality of agriculture farming. The use of new information systems and services will be more and more used to sustain and improve operations, competitiveness, and profitability in the agriculture sector. However, the massive use of technology comes with inherent security risks and vulnerabilities, and the sector finds itself targeted as never before. In this paper, using an empirical methodology, are highlighted some reflections regarding the security challenges that Smart Farming systems face.**

***Keywords*—Smart Farming, cybersecurity challenges, farms of the future**

I. Introduction

The benefits of using Information and Communications Technologies (ICT) together with the increasing use of the Internet of Things (IoT) in developing precision farming, also called Smart Farming, are tremendous. Using drones, robots, smart energy meters, smart security devices, smart data for seed traits and to treat soil conditions, these and other new systems offer unprecedented conveniences and improvements to managing the agriculture farming quality. New interconnected systems combined for monitoring, controlling and enhanced automation will drastically change the available infrastructures and services in the new farms. This means that the agriculture sector will depend more and more on information systems to sustain and improve operations, the competitiveness level, and its profitability.

Despite the massive benefits gained with the use of technology it also holds inherent risks, and the sector finds itself targeted as never before, thanks to its intellectual property being coveted by foreign competitors and hacktivists [1]. Most food and agriculture companies still are not investing in cybersecurity, but the prospects of cyber agroterrorism are beginning to concern the sector. A sophisticated terrorist attack could wreck any food and agriculture company as a trusted food supplier and undermine domestic confidence in the all food supply chain. It is clear that the sector's growing digitization drives new opportunities for terrorists, allowing them to attack places that previously have been too remote or difficult to strike. Cyber terrorism is a relatively low-cost venture with high payoff potential, making the risks of agroterrorism too large to ignore [2]. This means that an extreme, coordinated cyber attack on agricultural companies would have deep human and financial consequences. Thus, it is important to develop awareness in the smart farming sector about the importance of cybersecurity and the security challenges that arise from the massive use of technology in the agriculture sector.

In this paper are highlighted some reflections, regarding the challenges of smart farming emphasizing the security threats and issues, in order to raise the underlying awareness required, using an empirical methodology. This paper is organized as follows: in section II, it is introduced the concept of smart farming and its applications; in section III, it is presented an overview of the security threats and challenges that the use of smart farming poses, including an overview of the major security threats; conclusions and further developments are presented in section IV.

II. Smart Farming

Every day, the world is facing challenges. These challenges are also present in the agriculture and farming sector. Smart Farming involves the use of Information and Communications Technology (ICT) and, in particular, the Internet of Things (IoT) and related big data analytics to improve agricultural operations and processes. In general, the main purpose of Smart Farming is the emergence of digital and electronic monitoring of crops, as well as those related to the environment, soil, fertilization, and irrigation conditions [3]. Smart Farminhg uses smart networking, mobility, the flexibility of agricultural operations and their interoperability, integration with customers and suppliers and the adoption of innovative business models [4].

Smart Farming relies on intelligent networks based on cyber-physical systems (CPS). A CPS can have its operations monitored, coordinated, controlled and integrated by a computer and communication system, allowing the interaction with the physical world using a set of networked agents [5]. These network agents include: sensors, actuators, control processing units, and communication devices (Fig. 1).

978-1-5386-7097-2/18/$31.00 ©2018 IEEE

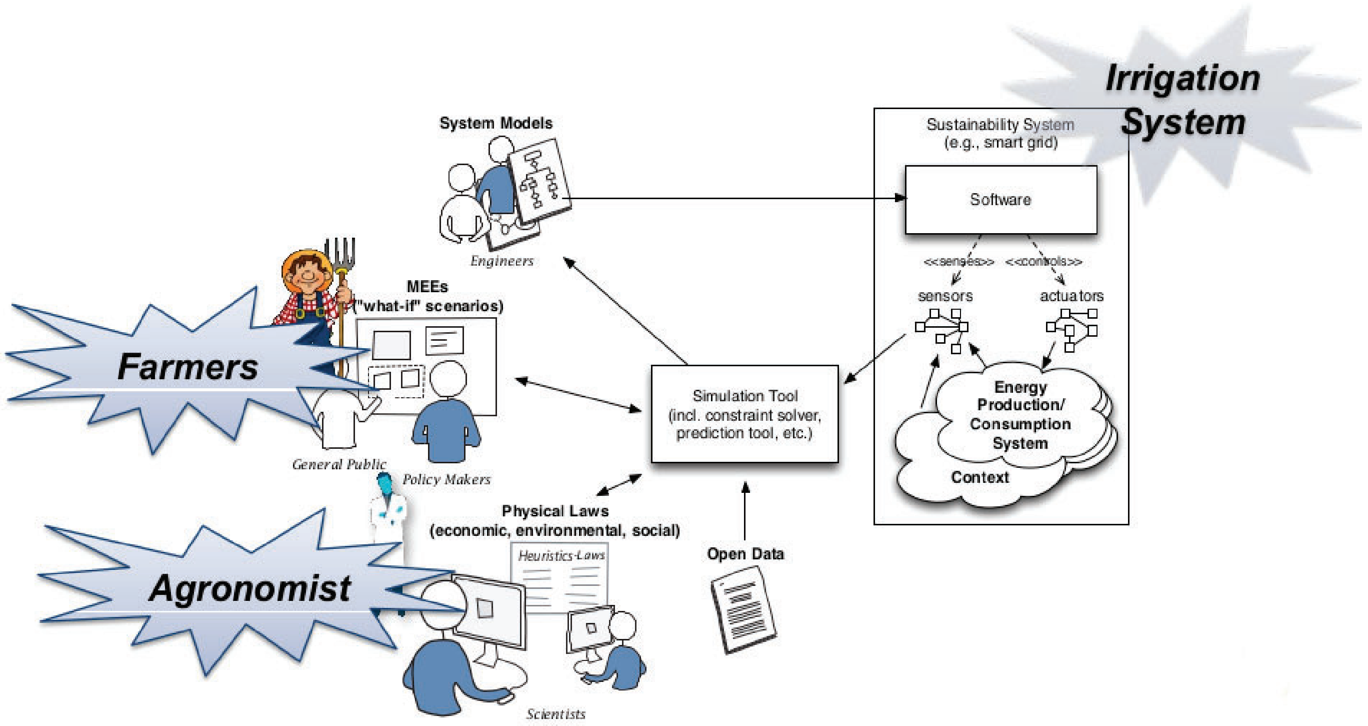
Irrigation System
Sustainability System (e.g., smart grid)
Software
<<senses>>
<<controls>>
sensors
actuators
Energy Production/ Consumption System
Context
System Models
Engineers
MEEs ("what-if" scenarios)
Farmers
General Public
Policy Makers
Simulation Tool (incl. constraint solver, prediction tool, etc.)
Physical Laws (economic, environmental, social)
Heuristics-Laws
Agronomist
Open Data
Scientists

Fig. 1 Farming System Modeling. Source: [6]

For example, sensors can collect information such as soil moisture, fertilization, weather oscillations and transmit it, in real-time, through a cellular wireless network providing farmers real-time access to information and analysis on their land, crop, livestock, logistics and machinery and then actuators can perform a previously programmed action [7]. This enables the smart farm to improve its operational performance by analyzing the data collected and acting upon it in ways that could increase productivity or streamline operations. Nevertheless, it must be considered that the increased innovation and production of these technologies means that even premium equipment will soon be supplanted by superior models, thus reducing the price of older equipment that would still bring many benefits to currently offline farms. The use of these technologies also exposes and increases the probability of bad data usage and of information and network security flaws. In order to have a better understanding of the benefits related to Smart Farming IoT technology, please look at Fig. 2, where it is pointed the main applications and how they could help improve farming and agriculture.

Given the huge variety in of niche equipment needed to successfully run a modern-day farm, it will come as no surprise that the IoT technology available to the agricultural industry today is just as varied and also has the benefits generated of being able to be made to a specific requirement. This requires the much-needed precision farming equipment needs in order to optimize and streamline traditional agricultural operations while also being able to feedback information on. This requires the much needed precision farming equipment needs in order to optimize and streamline traditional agricultural operations while also being able to feedback information on. To better understand the advantages that Smart Farming IoT technology can bring, let's look at where they could be applied and how they could help improve farming and agriculture.

A. *Water Management*

It is well known that one of the most common features needed at any farm is the irrigation system. The data collected from remote sensors can be used and analyze by farmers or other virtual technicians, through a laptop, tablet or smartphone, allowing them to define adequate strategies, regarding the water resources management, towards selecting the best distribution/irrigation approach and if it should be directed or not, during how much time and with which type of pressure.

B. *Fertigation*

The use of the IoT can be used for remotely controlled fertigation solutions. Fertigation is the process of injecting fertilizers, soil amendments and other products needed into soil [9]. This way, farmers could remotely control the fertigation system, allowing them to monitor the fertilizer concentrations and other environmental conditions in the soil using remote sensors, like, (e.g. pH values) and actively adjust the amount of fertilizer required level if needed.

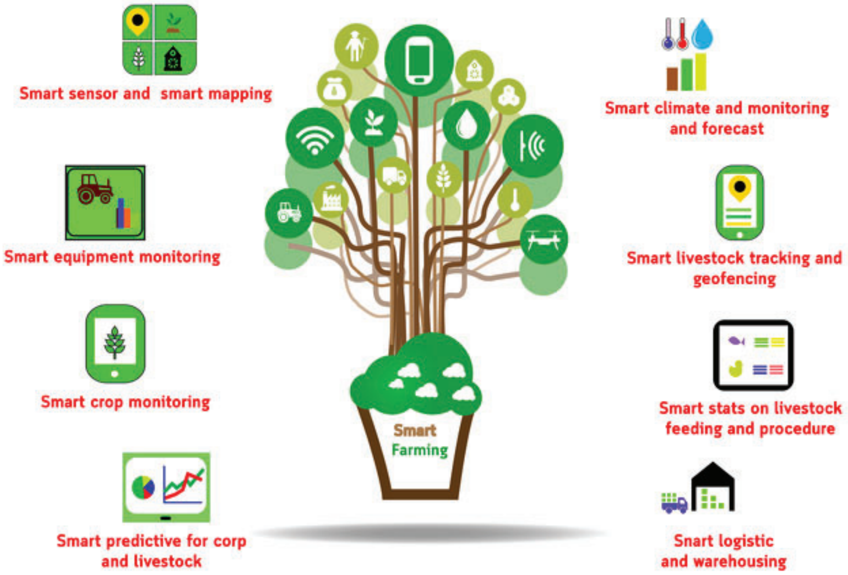
Smart sensor and smart mapping
Smart equipment monitoring
Smart crop monitoring
Smart predictive for corp and livestock
Smart Farming
Smart climate and monitoring and forecast
Smart livestock tracking and geofencing
Smart stats on livestock feeding and procedure
Snart logistic and warehousing

Fig. 2 Smart Farming Applications. Source: [8]

C. Livestock Safety and Maturity Monitoring

With IoT-enabled sensors producing real-time livestock data using GPS positioning, permits farmers to keep track of the wander-off animals. With the development of new biometric sensors, such systems can also provide real-time biomedical data on livestock such as body temperature, pulse and even tissue resistivity. Large farm owners can utilize mobile/wireless IoT applications to collect data regarding the location, well-being, and health of their cattle. The information obtained can then be used to identify sick animals allowing to take active actions for preventing the disease spreading as well as to promote the adequate actions to overcome any problem in the shortest time and with a lower level of impact. It also lowers labor costs as cattle can be easily and precisely located with the help of IoT based sensors. For high-value livestock, or even for the breed of new animals, new clients could have the option to monitor their future animals before being bought and follow up its development over time, tracking all the parameters of its development.

D. Crop Communication

As the world population increases and the global weather changes to being more extreme, farms will need to adapt and to maintain the global crop requirements. Smart Farming IoT solutions can be developed and deployed to enhance production, to reduce waste and costs and to improve resource consumption. The ability to monitor the condition of the soil in which the latest crop is planted through a smartphone will improve resource management by farmers.

E. Drilling, Seeding and Spraying

The use of drones in agriculture is becoming more and more popular and of extreme utility with major applications in Smart Farming IoT. Autonomous tractors, remotely controlled, built to do functions such as drilling, seeding and spraying are already being developed and deployed [10].

F. Aerial Crop Monitoring

Monitoring a vast field to expose issues related to soil variation, fungus and irrigation is quite challenging and costly to be achieved in a timely period. But due to cheap drones, equipped with different types of sensors, of controlled costs, combined with powerful processors, GPS and radio technologies, farm monitoring is more affordable and much more accurate and precise. Therefore, farmers can use time series animations to keep an eye on development of their crop and soil variation issues leading to more efficient crop management, as well as the increasing of the level of production and quality standards.

G. Supply Chain Monitoring

IoT sensors can also be applied in several parts of the product value chain increasing the products quality. It is possible to decouple de physical flows from information aspects of the operations [11], [12]. Supply chain monitoring does no longer require physical proximity, which implies that the path or route followed by the physical products from source/origin to the destination is no longer dependent on the location of the partners executing activities of control and coordination [13]. Using new IoT based solutions supply chains can be monitored, controlled, planned and optimized remotely [14], [15], [16].

III. The security challenges in smart farming

Nowadays, the possibilities for cybercrime increases every day. New forms of cyber terrorism attacks are being registered, and with the use of ICT an IoT in the agriculture is increasing the level of exposition of this sector. Therefore, the agriculture sector is becoming more vulnerable to cyber attacks against its infrastructures and its production facilities [17]. Combating this requires a multi-disciplinary effort that spans hardware and software through policies definition and people - all of it aimed for preventing cybercrime occurrence in the first place, or mitigating its impact when it happens. This is the practice of cybersecurity [18]. Farmers and their employers must be aware that as technology evolves and is further integrated into our work and lives, the opportunities for abuses grow. For example, an IoT system that controls the production of crops with genetically modified organisms (GMO), can be attacked and the GMO fundamentals can be changed to be harmful to the human beings. Thus, it is important to be aware of and prepared for the major security threats that Smart Farming could face. Therefore, it is important to know the major security threats that Smart Farming needs to handle and that the different stakeholders need to focus on and try to mitigate its impacts. The methodology used was an empirical one, through the analysis of the information and experiences collected in the Internet Security Alliance [19], the European Cyber Security Organisation (ECSO) [20] and the National Institute of Standards and Technology (NIST) [21].

A. The major security threats facing smart farming

1) Security and privacy issues: The data collection process in IoT is more passive and more pervasive, which turns out to be a challenge to ensure privacy, resulting in users being less aware of whether and when they are being tracked. The locational data, used in all GPS systems, can be a key security concern. The use of the GPS systems increases the access to origin and location data details, which allows the attackers to specifically know what farm and what specific crop can be attacked [22]. Therefore, the agriculture data is becoming more sensitive, as well as the confidentiality of the data is becoming more critical. The advancement of IoT creates new challenges in a world where farmers and farms are becoming more and more dependent on connected devices and services towards enhancing its productivity and its products' quality. Privacy issues will increase with the explosion of the IoT. For that reason, the exposure of personnel's private information to any cyber attack is a potentially severe threat that should be seriously and carefully considered.

2) Social Engineering: It is commonly accepted that Humans are inherently complex and a multi-faceted creature with own agendas, influences, faults, beliefs, and priorities. Due to that fact, each ones complexities, personal characteristics and overall influences could conditionate the judgement criteria and the rational thinking, which sometimes increases the level of confidence and the relaxation to values that could be harmful. Due to our human necessities, the most protected system can be breached through social engineering - also known as the hacking of people [23]. No amount of technical information of any system can be so severely compromised, as a user can innocently click on an email link, or being convinced to give up login details over the phone by someone pretending to be from the IT department of an IoT supplier. It must be noticed, that cybersecurity isn't just about technological cyber defenses: people must be also considered when tackling this problem. Every user needs a basic understanding of what is a cyber threat and how it could be recognized - this is a factor that comes under the umbrella of digital literacy. Digital literacy is still very low in the agriculture sector, and every day more awareness is needed.

3) Ransomware: Ransomware has become a significant threat to any business and individuals worldwide. With the increasing use of ICT and IoT in the agriculture sector, this is becoming also a threat to be aware. Attackers can use any form of ransomware to encrypt farm and famers data, rendering them unreadable until a ransom is paid [24]. Data on GMOs and pesticides use can also be destroyed through a ransomware system. To tackle such situations robust data back-up and recovery plan must be implemented. Back-ups should be placed in a separate and secure location so that attackers cannot readily access them from local networks.

4) Denial of Service (DoS): Smart Farming relies on the interconnection of IoT devices and on its Internet services. The more effective is the interconnection, more comprehensive is the interconnectivity, more effectual and thrift is the connection, as well as more authentic is the quality of service in IoT. Since a large number of nodes and groups exist in IoT this may result in denial of service (DoS) attacks. The purpose of the DoS is to disable the system making it useless. This can be accomplished by a device that broadcasts signals used for malicious purposes and can disrupt or block the working IoT devices. There are many possibilities to perform DoS attacks including the possibility of placing the information in Faradays cage [25]. Using IoT in improving farming and agriculture has as a consequence that cloud computing also has an important role in the Smart Farming concept, thus allowing attackers to use and explore system vulnerabilities using DoS. This damage can be extremely costly to any new high tech farm. Those attacks can imply material damage (servers and sensors need to be replaced and reprogrammed; network needs to be reconfigured; systems need to be replaced and restarted) but also operational and financial damage (service interruption, new training for farm operators and the definition of new metering infrastructures) [26]. DoS attacks are often unforeseeable and very difficult to control, and the best defense is the prevention of such attacks.

5) Cyber-Espionage, Agroterrorism, Confidential Information and Intellectual Property: Agricultural production and operations will only increase dependency on software and hardware applications vulnerable to cyberattacks and cyber espionage. Smarter and more robust automation will expand into food processing. The increased level of connectivity creates vulnerabilities that the agriculture sector hasn't fully contended with, especially not in the operational environment. Organized groups of cyber-criminals with excellent skills are targeting the agriculture sector, towards hacking sensitive information and intellectual property. One of such scenarios is the use of malware to destroy farm control systems, which would cause food production to come to a screeching halt for a period of time. Also, using cyber espionage, nations are making efforts to illegally get of other nations agricultural technology. Particularly data from genetic engineering, improved seeds and fertilizers as well as information related to organic insecticide and irrigation equipment. While most recent cases of intellectual property espionage were done by the old-fashioned way, it's naive to assume cyber espionage will not become a major element of commercial espionage [2].

More and more, the possibility of cyber terrorism in the agriculture sector, known as *agroterrorism*, is concerning the sector. A simple agroterrorism attack could destroy any smart farm willingness' of being a trusted food supplier and undermine any gained confidence in the food supply chain. The increased use of digital an interconnect system in the agriculture sector brings with new opportunities for terrorists to attack places that previously were too remote or difficult to strike. Cyber terrorism is a relatively low-cost venture with high payoff potential, making the risks of agroterrorism too large to ignore. Therefore, it is important to find solutions that guarantee trust and transparency within the smart farming concept, as well as the protection of the critical know-how [27]. Data loss prevention solutions associated with strong encryption algorithms and protocols must be considered in order to protect high value and sensitive data assets.

6) Supply Chain: The use of digital systems and IoT enables to connect different organizational environments, making it possible to make the supply chain more efficient and more integrated. Taking an integrated approach to the whole agriculture/food supply chain is one of the surest ways to create sustainable jobs and value added in rural areas. The agriculture sector also deals with products that often have a very short shelf life in uncertain conditions in high quantities, and in some products, the supply can be uncertain [15], [16]. Agricultural products like fruits, vegetables, meats and dairy are highly impacted by delays, temperature variations and other environmental factors as they travel from farms through processing and distribution centers to customers. The supply chain visibility and efficiency is a big part of running a profitable agricultural business and supporting it with a flexible and compete IoT systems can help to optimize the highly complex supply chain for agriculture. However, it must be noticed that using such systems introduces potential security vulnerabilities in every stage of the supply chain, making the optimization of the supply chain with technology quite a challenge [16].

Security vulnerabilities can be identified in the supplier, which is vulnerable to phishing attacks and the stolen of privileged credentials, resulting in mass data exposure. But the most important vulnerabilities are the ones that arise at the top of the supply chain, allowing to spread to the rest of the organizational processes through its dependent systems. The security mechanisms that can help to prevent a supply chain exposure and attack are: security awareness, control access through authentication mechanisms, cryptographic processes (using, for example, blockchain technology [28]).

B. Securing the Farms of the Future

With the IoT looking set to revolutionize not just farming and agriculture but many global industries, more and more businesses and organizations are looking to build stable foundations for this new, evermore interconnected world. As with any internet-based technology, Smart Farming IoT applications and technologies are vulnerable to cyber threats from hostile attackers.

This means that, when thinking of securing smart farms, it is important for farmers to use preconceived and established security frameworks. One such framework is presented in Fig. 3. The framework refers to six fundamental areas for cyber risk management: Legal and Compliance, Operations and Technology, Human Factors, Business Continuity and Crisis Management, and Leadership and Governance.

Also and in a broader context, not exclusively for the agriculture sector the European Parliament has recently (April of 2016) published and approved Directive 2016/679, requiring all European organizations to prove their capability to protect their organizational processing activities and the free flow of personal data between Member States [30].

IV. Conclusions and Future Developments

In this paper, we addressed some reflections and challenges regarding some of the considered major security threats facing smart farming, as well as the challenges to overcome those security threats in a proper way. It must be noticed that security, in the context of any business activity, means more financial investment without a necessary return of investment (ROI). This is why usually security flaws are tackled after any critical security incident occurs that is reflected in huge and dramatic impacts on any activity. This way of tackling security flaws is costly and most of the times does not convey a permanent solution. Thinking of Smart Farming, and in the future of agriculture, this increases the impacts that cybersecurity brings. Smart farming opposes new challenges, especially in the technological and cyber security domains, being essential that all the involved in the process are aware of that. Cyber security processes are now widely discussed, and the importance of protecting all Information and Communications Technology (ICT) systems will propel the development of new smart farming systems, making them more secure and safer throughout all its value chain.

The guidance and the work developed by specialists will be extremely important to highlight the different approaches and possibilities that the agriculture sector will be able to implement and carry out in the future agriculture. It must be noticed, however, that it will continue to be extremely important to compile and to benchmark the solutions seeking better results that might benefit the level of security of all stakeholders within the different agriculture chain of processes.

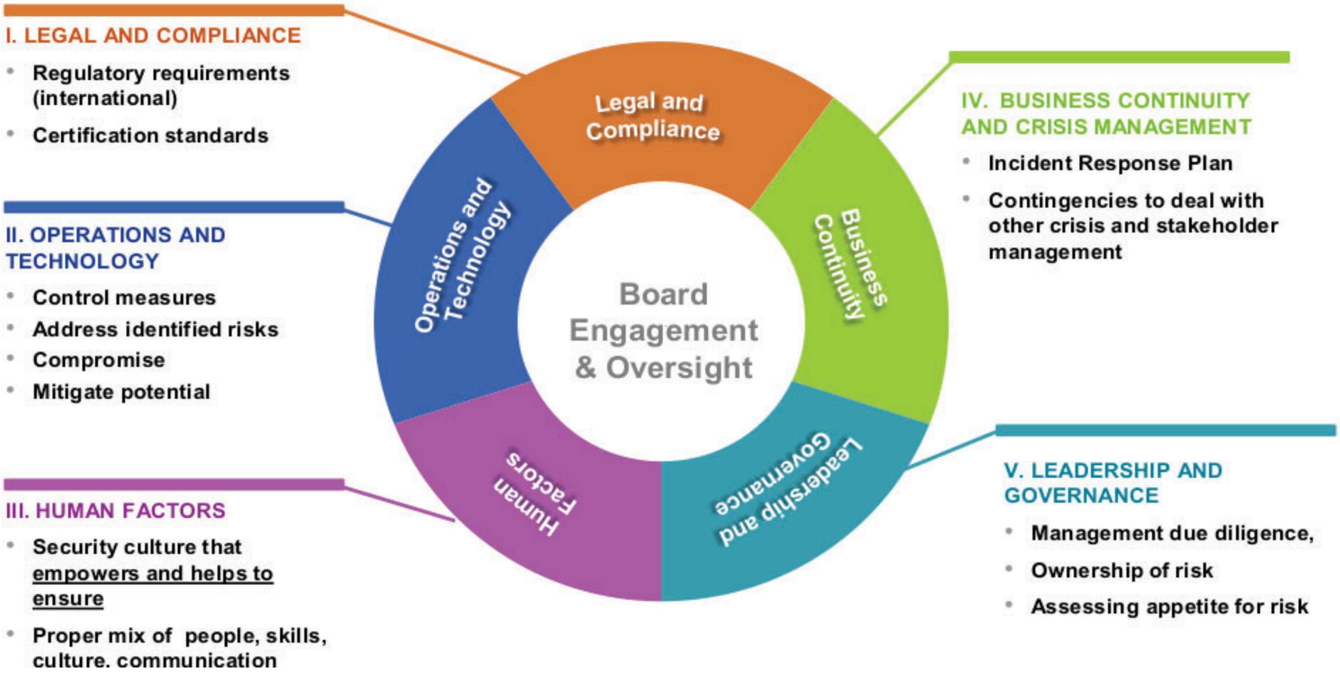
I. LEGAL AND COMPLIANCE
Regulatory requirements (international)
Certification standards
II. OPERATIONS AND TECHNOLOGY
Control measures
Address identified risks
Compromise
Mitigate potential
III. HUMAN FACTORS
Security culture that empowers and helps to ensure
Proper mix of people, skills, culture. communication
IV. BUSINESS CONTINUITY AND CRISIS MANAGEMENT
Incident Response Plan
Contingencies to deal with other crisis and stakeholder management
V. LEADERSHIP AND GOVERNANCE
Management due diligence,
Ownership of risk
Assessing appetite for risk
Legal and Compliance
Business Continuity
Leadership and Governance
Human Factors
Operations and Technology
Board Engagement & Oversight

Fig. 3 Cyber Risk Management Framework. Source: [29]

Therefore, it is intended to study some specific case-studies about security policies and strategies developed in some organizations within the Smart Farming paradigm. Such studies will be important to develop a multi-layered framework with the identification of stakeholders, phases, processes, technical requirements and respective level of integration, as well as the policies, for efficiently securing smart farms in the European territory context. It is also intended to analyze the developed solutions to achieve the necessary security and awareness, within the multi-layered framework, in the different areas of Smart Framing applications previously presented.

Acknowledgment

Applied Research Centre for Digital Transformation (ARC4DigIT) R&D Unit of the Instituto Politécnico de Viana do Castelo- http://arc4digit.ipvc.pt.

References

[1] Deloitte, “Hacktivism: A Defender’s Playbook,” Tech. Rep., 2016.

[2] J. Olcott, “Input to the Commission on Enhancing National Cybersecurity: The Impact of Security Ratings on National Cybersecurity,” Internet Security Alliance, Tech. Rep., 2016.

[3] P. P. Jayaraman, A. Yavari, D. Georgakopoulos, A. Morshed, and A. Zaslavsky, “Internet of Things Platform for Smart Farming: Experiences and Lessons Learnt,” *Sensors (Switzerland)*, vol. 16, no. 11, pp. 1–17, 2016.

[4] A. Kamilaris, F. Gao, F. X. Prenafeta-Boldu, and M. I. Ali, “Agri-IoT: A Semantic Framework for Internet of Things-Enabled Smart Farming Applications,” *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*, no. October 2017, pp. 442–447, 2017.

[5] L. Barreto, A. Amaral, and T. Pereira, “Industry 4.0 Implications in Logistics: An Overview,” *Procedia Manufacturing*, vol. 13, pp. 1245 – 1252, 2017, manufacturing Engineering Society International Conference 2017, MESIC 2017, 28-30 June 2017, Vigo (Pontevedra), Spain. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2351978917306807

[6] B. Combemale and J.-M. Bruel, “Modeling for Smart Cyber-Physical Systems: Application to Farming Systems,” in *2016 Workshop in Software and System Engineering for Cyber-Physical System*, ser. Workshops in Models for CPS design. CPSE Labs, Toulouse, 2016.

[7] P. C. H. Chavan and P. V. Karande, “Wireless Monitoring of Soil Moisture , Temperature & Humidity Using Zigbee in Agriculture,” *International Journal of Engineering Trends and Technology (IJETT)*, vol. 11, no. 10, pp. 493–497, 2014.

[8] S. Ravindra. (2018, May) The Impact of IoT on Agriculture. [Online]. Available: https://technofaq.org/posts/2018/05/the-impact-of-iot-on-agriculture/

[9] R. Raut, H. Varma, C. Mulla, and V. R. Pawar, “Soil Monitoring, Fertigation, and Irrigation System Using IoT for Agricultural Application,” in *Intelligent Communication and Computational Technologies*, Y.-C. Hu, S. Tiwari, K. K. Mishra, and M. C. Trivedi, Eds. Singapore: Springer Singapore, 2018, pp. 67–73.

[10] S. K. Shah, “A Review : Autonomous Agribot For Smart Farming,” *International Journal of Industrial Electronics and Electrical Engineering*, vol. 4, no. 2, pp. 12–15, Feb. 2016.

[11] M. P. Clarke, “Virtual Logistics: An Introduction and Overview of the Concepts,” *International Journal of Physical Distribution & Logistics Management*, vol. 28, no. 7, pp. 486–507, 1998. [Online]. Available: https://doi.org/10.1108/09600039810247461

[12] C. Verdouw, A. Beulens, and J. van der Vorst, “Virtualisation of Floricultural Supply Chains: A Review from an Internet of Things Perspective,” *Computers and Electronics in Agriculture*, vol. 99, pp. 160 – 175, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0168169913002135

[13] B. Yan, P. Shi, and G. Huang, “Development of Traceability System of Aquatic Foods Supply Chain Based on RFID and EPC Internet of Things,” *Transactions of the Chinese Society of Agricultural Engineering*, vol. 29, no. 15, pp. 172–183, 2013. [Online]. Available: https://www.ingentaconnect.com/content/tcsae/tcsae/2013/00000029/00000015/art00021

[14] C. Verdouw, J. Wolfert, A. Beulens, and A. Rialland, "Virtualization of Food Supply Chains with the Internet of Things," *Journal of Food Engineering*, vol. 176, pp. 128 – 136, 2016, virtualization of Processes in Food Engineering. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S026087741530056X

[15] M. Dougados, S. Ghioldi, R. V. Doesburg, and K. Subrahmanya, "The Missing Link Supply Chain and Digital Maturity Digital Technologies Offer a Shot in the Arm for Traditional Supply Chains," Cap Gemini, Tech. Rep.

[16] C. Verdouw, A. Beulens, H. Reijers, and J. van der Vorst, "A Control Model for Object Virtualization in Supply Chain Management," *Computers in Industry*, vol. 68, pp. 116 – 131, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0166361514002164

[17] G. Weimann, "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism*, vol. 28, no. 2, pp. 129–149, 2005. [Online]. Available: https://doi.org/10.1080/10576100590905110

[18] A. C. Society, "Cybersecurity Opportunities, Threats Challenges," Tech. Rep. November, 2016.

[19] (2018, Aug) Internet Security Alliance. [Online]. Available: https://isalliance.org/

[20] (2018, Aug) European Cyber Security Organisation. [Online]. Available: https://ecs-org.eu/

[21] (2018, Aug) National Institute of Standards and Technology. [Online]. Available: https://www.nist.gov/

[22] A. S. Elmaghraby and M. M. Losavio, "Cyber Security Challenges in Smart Cities: Safety, Security and Privacy," *Journal of Advanced Research*, vol. 5, no. 4, pp. 491–497, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.jare.2014.02.006

[23] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced Social Engineering Attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113 – 122, 2015, special Issue on Security of Information and Networks. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212614001343

[24] X. Luo and Q. Liao, "Ransomware: A New Cyber Hijacking Threat to Enterprises," in *Handbook of Research on Information Security and Assurance*. IGI Global, Jan 2009, pp. 1–6. [Online]. Available: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-59904-855-0.ch001

[25] J. Vacca, *Computer and Information Security Handbook*, 3rd ed. Elsevier, May 2017.

[26] F. Schreier, "On Cyberwarfare," *DCAF Horizon Working Paper*, no. 7, pp. 1–133, 2012. [Online]. Available: http://www.dcaf.ch/Publications/On-Cyberwarfare

[27] M. Whitman, "Enemy at the Gate: Threats to Information Security." vol. 46, pp. 91–95, 01 2003.

[28] (2018, Aug) Blockchain in Transport Alliance: BiTA. [Online]. Available: https://bita.studio/

[29] P. Aasness and M. K. Delvo, "Cyber Data Attacks: Are Farmers and Agribusiness Exempt?" AGRIGROWTH, Tech. Rep., 2016. [Online]. Available: https://www.dorsey.com/newsresources/events/videos/2016/10/{~}/media/53172b99d8b843c897805a42d93844e1.ashx

[30] E. Parliament, of the processing of personal data, and on free movement of such data, *General Data Protection Regulation-GDPR*, online, European Union Std., Apr 2016. [Online]. Available: https://eur-lex.europa.eu/