agriculture

MDPI

Article

Regional Perspective of Using Cyber Insurance as a Tool for Protection of Agriculture 4.0

Maksym W. Sitnicki [1], Nataliia Prykaziuk [2], Humeniuk Ludmila [2], Olena Pimenowa [3,*], Florin Imbrea [4,*], Laura Șmuleac [4] and Raul Pașcalău [4]

[1] Management of Innovation and Investment Activities Department, Faculty of Economics, Taras Shevchenko National University of Kyiv, 01033 Kyiv, Ukraine; maksym.sitnicki@knu.ua
[2] Department of Insurance, Banking and Risk Management, Faculty of Economics, Taras Shevchenko National University of Kyiv, 01033 Kyiv, Ukraine; nprykaziuk@knu.ua (N.P.); mila_gumenyuk@knu.ua (H.L.)
[3] Department of Agronomy, Faculty of Agriculture and Biotechnology, Bydgoszcz University of Science and Technology, Al. Prof. S. Kaliskiego 7, 85-796 Bydgoszcz, Poland
[4] Faculty of Agriculture, University of Life Sciences "King Mihai I" from Timisoara, 300645 Timisoara, Romania; laurasmuleac@usvt.ro (L.Ș.); raul.pascalau@usvt.ro (R.P.)
* Correspondence: olena.pimenowa@pbs.edu.pl (O.P.); florin_imbrea@usvt.ro (F.I.)

Abstract: The digitalization of the agricultural industry is manifested through the active use of innovative technologies in all its areas. Agribusiness owners have to constantly improve their security to meet new challenges. In this context, the existing cyber risks of the agrarian industry were assessed and their classification by possible consequences, such as data theft or alteration, cyber terrorism, cyber warfare, software hacking or modification, the blocking of markets and transactions on them, was proposed. Cyber insurance is an effective tool for minimizing the likelihood of cyber incidents and for comprehensive post-incident support, with the involvement of cybersecurity specialists. An algorithm for cooperation between an agricultural company and an insurance company when concluding a cyber risk insurance contract is proposed, which takes into account the needs and wishes of insurers at each stage of the interaction. To assess the need to use cyber insurance in agriculture 4.0, a methodology has been developed to evaluate the regional characteristics of cybersecurity and the digitalization of agribusiness. The results of the study show a heterogeneous need for this tool in different regions of the world.

Keywords: agriculture 4.0; food security; cybersecurity; cyber risk; cyber insurance

Citation: Sitnicki, M.W.; Prykaziuk, N.; Ludmila, H.; Pimenowa, O.; Imbrea, F.; Șmuleac, L.; Pașcalău, R. Regional Perspective of Using Cyber Insurance as a Tool for Protection of Agriculture 4.0. *Agriculture* **2024**, *14*, 320. https://doi.org/10.3390/agriculture14020320

Academic Editor: Donatella Porrini

Received: 4 January 2024
Revised: 7 February 2024
Accepted: 13 February 2024
Published: 18 February 2024

1. Introduction

The International Covenant on Economic, Social and Cultural Rights (ICESCR), adopted by the UN General Assembly on 16 December 1966, recognizes the right of everyone to an adequate standard of living, including food and freedom from hunger [1]. The states participating in this pact should improve production methods and ensure an equitable distribution of the world's stocks, maintaining global food security. Today, the digitalization and implementation of artificial intelligence systems has a huge potential to ensure the stability of agricultural industry [2].

The development of the use of modern technologies in the agricultural sector requires a corresponding strengthening of cybersecurity in this area. Researchers note that many new technologies are not created specifically for the agricultural industry but are modified on the basis of existing ones, and therefore less attention is paid to security issues [3]. According to researchers, another feature of the transformation of the agricultural sector is manifested through the presence of a constant connection through the Internet, and therefore the systems of agricultural companies are conditionally open to cybercriminals [4].

Companies in the agrarian industry 4.0 need to start improving cybersecurity at the same time as they first use modern technology in their operations. The development of a

cybersecurity strategy begins with the assessment and identification of current risks [5]. Researchers distinguish different groups of cyber risks depending on the characteristics of the technologies involved (Table 1).

Table 1. Types of cyber risks in agricultural industry in modern scientific research.

Authors	Types of Cyber Risks	Number of Unique Types of Cyber Risks
Alahmadi, A.N.; Rehman, S.U.; Alhazmi, H.S.; Glynn, D.G.; Shoaib, H.; Solé, P. [3]	Commercially sensitive information threats; Internet of Things, robotics and aerial systems threats; Big Data and machine learning threats; supply chain threats.	6
Angyalos, Z.; Botos, S.; Szilagyi, R. [4]	Blockchain threats; IoT systems and Big Data threats; phishing threats.	3
Vatn, K.J.D. [6]	Threats to confidentiality; threats to integrity; threats to availability.	3
Okupa, H. [7]	Social engineering threats; advanced persistent threats; malware threats; denial of service threats.	4
Stephen, S.; Alexander, K.; Potter, L.; Palmer, X.-L. [8]	Threats to confidentiality; threats to integrity; threats to availability.	3
Rotz, S.; Duncan, E.; Small, M.; Botschner, J.; Dara, R.; Mosby, I.; Reed, M.; Fraser, E.D.G. [9]	The production of technologies threats; data development threats; data security threats; data ownership and control threats.	4

The correct identification of the current risks allows business owners to build an effective mechanism of protection against them. Researchers identify different approaches to minimizing such risks:

- Creating policies for mandatory identification in IT systems for company employees and limited access for one-time visitors; enhancing information security to maintain confidentiality; implementing blockchain technologies to improve data encryption and transmission channels; establishing cryptography mechanisms and management to access key creation and circulation; physical security for computer equipment, network equipment and other devices; implementing cyber incident detection systems. The measures described above can be implemented separately, but the full positive effect occurs when they are implemented in a comprehensive manner [10];
- Providing appropriate education for current and future agricultural workers, which will be the basis for improving cybersecurity in the future; strengthening interdisciplinary cooperation between the agriculture and cybersecurity sectors; creating government security standards for the agricultural sector. These measures will help to maintain the stability of food supply chains and therefore food security in general [11];
- Implementation of a scenario-based approach based on a system that assesses risk factors, safety factors and potential costs. This approach is also adapted for different agricultural scenarios and therefore already includes sub-scenarios and cases for different cases of cyber incidents [12].

Insurance is another tool for mitigating cyber risks today [13]. The process of insuring cyber risks in the agricultural sector should be considered at the macro and meso levels within the framework of global food security. For insurance companies, it is proposed to assess this type of risk based on classified threats. After the assessment, insurers need to balance the best solution for themselves and the client [14].

This paper is organized into the following sections. Section 2 outlines the process, tools and data used to assess the necessity of cyber risk insurance in the context of threats to agriculture 4.0. Section 3 discusses the theoretical foundation of this study on cyber risks in the agricultural sector 4.0 and presents regional findings. In Section 4, the obtained results

are compared to existing scientific viewpoints on the development of cyber risk insurance. Section 5 summarizes the findings and suggests future research directions.

2. Materials and Methods

2.1. Research Purpose

The purpose of this study is to develop an effective regional concept of the interaction between insurance companies and agricultural companies that use innovative technologies in their activities. To do this, it is necessary to update cyber risks and their consequences for agriculture 4.0, which will allow business owners to minimize the likelihood of their occurrence.

Scientific novelty. This article substantiates the need for cyber insurance in the agricultural industry at a regional level. A proposed index for assessing the necessity of cyber insurance in the agricultural sector across different regions of the world has been developed, drawing on the findings of the conducted research. The index is constructed by utilizing regional development indicators such as share of cyber-attacks, the National Cybersecurity Index, smart farming market share and share of agricultural output. The development of an algorithm for the cooperation between insurer and insured in the agricultural sector for insuring against cyber risks, with the assistance of cybersecurity experts, has been a topic of theoretical exploration. It has been determined that the purpose of cybersecurity experts in insurance relationships is to reduce the level of risk at every stage of their interaction.

Practical value. The practical value of the study lies in the development of a regional index for determining the need for cyber risk insurance in the agricultural sector. The focus on developing this type of insurance in different regions is based on their unique characteristics, resulting from the evolution of agriculture 4.0. The suggested algorithm for utilizing cyber insurance in the agricultural sector is considered an effective risk management tool that can accurately identify the unique threats associated with the agricultural industry 4.0. This is particularly significant in the context of agricultural sector digitalization.

2.2. Research Framework

The first level of our study about the need of using cyber insurance in agriculture 4.0 is based on the identification of the risks for each of their components. The next level of research is to create an optimal classification of modern cyber risks in the agricultural sector and identify their characteristics. The third level includes the development of an algorithm for cooperation between an agricultural company and an insurance company when concluding a cyber risk insurance contract as a risk mitigation tool. The last level of research is aimed at considering the peculiarities of the development of the agricultural industry in regions and determining the level of necessity for cyber insurance in them (Figure 1).

2.3. Research Methods

This study is based on a systems approach to identify the need for cyber insurance in the agricultural sector. A comparative and historical method was used to compare the development of agriculture, innovative technologies and their synergy, which today exists in the form of modern agriculture 4.0. The use of a comparison method allows us to compare the characteristics of technological innovations used in agro-industry 4.0 and the threats they pose, and to search for similarities and differences in the current features of agribusiness in different regions of the world. The methods of analysis and synthesis were used for establishing relationships between cyber incidents and their potential impact on the agricultural sector, and for summarizing and formulating proposals for the use of cyber insurance as a tool to protect the agricultural sector 4.0. We used a monographic method to analyze the peculiarities of using modern technological innovations, with the establishment of the range of possible cyber risks and consideration of the cyber insurance process, its stages and features. The method of formalization was used to display the

stages of the algorithm of cooperation between an agricultural company and an insurance company when concluding a cyber risk insurance contract in the form of a structural and logical diagram. The results of research were determined based on methods of compiling, grouping and displaying statistical data: the grouping data on data breach success by industry; the collection and unification of information on the market share of IoT devices used in the agricultural sector; the collection and processing of information on the share of global cyber-attacks by region, National Cybersecurity Index, smart farming market share and share of agricultural output by region; the presentation of the relevant information in the form of tables and images; and the development of an approach to assess the need to use cyber insurance as a tool for protecting agriculture 4.0 depending on the specific characteristics of a region.

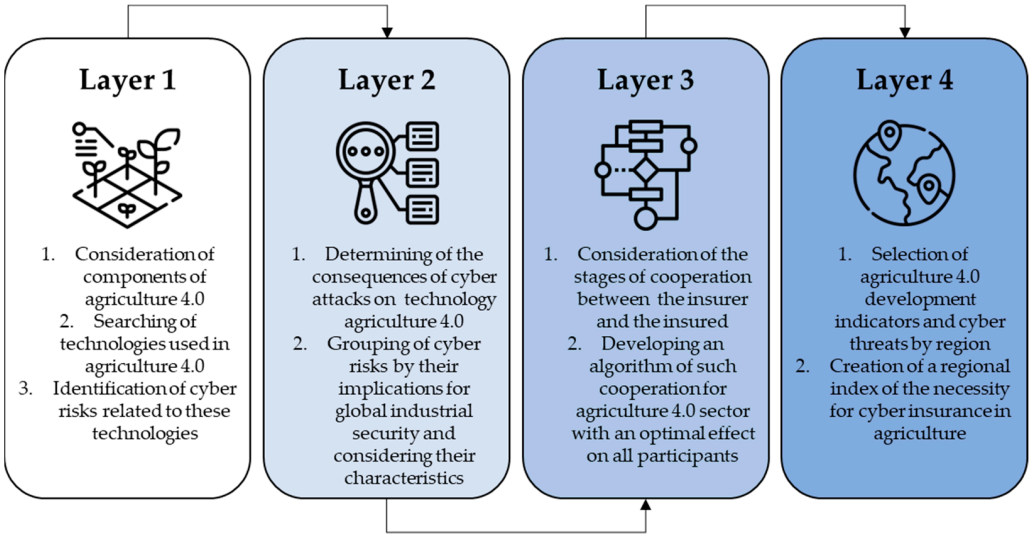

Figure 1. Research framework for the necessity of using cyber insurance in agricultural industry 4.0.

2.4. Research Materials

- In order to assess the extent to which cyber insurance is necessary in the agricultural sector, we examined the various factors that contribute to the development of cyber insurance overall. Through a regression analysis, we determined that the dependent indicator is global cyber insurance premiums (GCIP) [15], while independent indicators are industry 4.0 market size (IMS) [16] and cyber-attacks (CAs) [17] (Table 2).

Table 2. Inputs for regression analysis for GCIP, IMS, CAs.

Indicator	2018	2019	2020	2021	2022
GCIP, billion USD	4.75	5.05	5.25	7.01	11.70
IMS, billion USD	54.1	57.8	62.5	68.2	78.5
CAs, million	7.9	9.5	10.8	13.9	15.4

Source: Calculated by authors based on the GlobalData Cyber-insurance Report, Cisco Annual Internet Report, Acumen Industry 4.0 Market Report.

- The regression analysis findings reveal a consistent correlation between global cyber insurance premiums (GCIP) and industry 4.0 market size (IMS), as well as cyber-attacks (CAs) (Table 3).

Table 3. Results of regression analysis for dependent indicator GCIP.

Independent Indicators	R^2	R	F Statistic	*p*-Value	The Shapiro–Wilk *p*-Value
CAs	0.9635	0.9816	79.2049	0.002992	0.4545
IMS	0.9653	0.9825	83.5518	0.002768	0.5182

Source: Calculated by authors based on the GlobalData Cyber-insurance Report, Cisco Annual Internet Report, Acumen Industry 4.0 Market Report.

In Section 3.1.2 of the study results, based on selected indicators, we propose an index of the necessity for cyber insurance for the agricultural industry for each region of the world. In the calculation, we include the following indicators:

- The share of global cyber-attacks [18]. The data are presented as a percentage for each region, which is calculated using the formula:

$$S_{ai} = \frac{N_i}{\sum_{q=1}^{q_{max}} N_q} * 100\%, \quad (1)$$

where S_{ai}—share of cyber-attacks in the region, N_i—number of cyber-attacks on the analyzed region, N_q—the number of cyber-attacks on the q-region, q—number of regions.

- Limits of this indicator: [0%; 100%].
- National Cybersecurity Index [19]. This indicator considers the degree of progress made in protecting against cyber-attacks. This index was calculated by the NCSI project and is based on the value of denial of e-services, data integrity breach and data confidentiality breach. Limits of this indicator: [0%; 100%].
- Smart farming market share [20]. The data are presented as a percentage for each region, which is calculated using the formula:

$$S_{fi} = \frac{N_i}{\sum_{q=1}^{q_{max}} N_q} * 100\%, \quad (2)$$

where S_{fi}—market share of smart pharming market in the region, N_i– the volume of the smart farming market in the analyzed region, N_q— the volume of the smart farming market by q-region, q—number of regions.

- Limits of this indicator: [0%; 100%].
- Share of agricultural output [21]. This indicator considers the role of the region in promoting food safety. The data are presented as a percentage for each region, calculated using the formula:

$$S_{pi} = \frac{N_i}{\sum_{q=1}^{q_{max}} N_q} * 100\%, \quad (3)$$

where S_{pi}—share of agricultural output in the region, N_i– volume of agricultural output by the analyzed region, N_q—is the volume of agricultural output by the q-region, q—number of regions.

- Limits of this indicator: [0%; 100%].

The need for cyber insurance in the agricultural sector differs by region. We consider it appropriate to choose the following indicators for 2022 as indicators for comparing regions (Table 4).

Table 4. Comparative indicators of the need for cyber insurance in agricultural sector by region in 2022.

Region	Share of Cyber-Attacks, %	National Cyber Security Index, %	Smart Farming Market Share, %	Share of Agricultural Output, %
Asia–Pacific	16%	40%	10%	63%
Europe	39%	78%	21%	13%
Latin America	3%	51%	7%	7%
Middle East and Africa	1%	30%	8%	6%
North America	41%	31%	54%	10%

Source: Calculated by authors based on the Imperva cyber-attacks Statistics, NCSI report, MMR Smart Farming Market Report, Food and Agriculture Organization of the United Nations Statistics.

Using these indicators, we will calculate the Integral Index of the need for cyber insurance in the agricultural sector (I_{CIN}) for each of regions:

$$I_{CIN} = \overline{X} = \frac{\left(S_a + S_f + S_p\right) + (100\% - I_{NCS})}{4}, \quad (4)$$

where S_a—share of cyber-attacks in the region, S_f—smart pharming market share, S_p—share of agricultural output, I_{NCS}—National Cybersecurity Index.

It is worth specifying that such indicators as S_a; S_f are direct, as it has been established that there is a direct correlation between global cyber insurance premiums and cyber-attacks, as the higher the number of attacks, the more important it is to develop tools to minimize the consequences of them; likewise with the industry 4.0 market size, as the higher the penetration of information systems and automated systems in the region are, the more opportunities for potential cyber-attacks are opened up for attackers. Indicator S_p was identified as direct for illustrating the proportion of agricultural output, as the lack of the timely production, delivery or export of products negatively influences global food security [22].

Indicator I_{NCS} is inversely related, as the higher the level of cybersecurity, the lower the probability of a cyber incident.

- It should be noted that we chose the current USD measure for agricultural products to unify the components of the formula. The total amount of agricultural output includes crops and livestock. Therefore, the share of agricultural output is a representative cross-section of the real global volume of agricultural products (Table 5).

Table 5. Agricultural production by segment and region in 2017–2021, million USD.

Item	2017	2018	2019	2020	2021
Crops	*2,571,197*	*2,620,248*	*2,846,269*	*2,895,524*	*3,082,672*
Asia–Pacific	1,604,731	1,679,983	1,882,061	1,925,848	2,003,488
Europe	295,072	287,034	286,026	293,700	362,457
Middle East and Africa	210,004	224,532	230,356	217,169	216,342
Northern America	257,843	255,849	253,162	278,557	317,474
South America	203,546	172,850	194,663	180,251	182,912
Livestock	*1,112,905*	*1,117,987*	*1,305,721*	*1,332,435*	*1,364,798*
Asia–Pacific	592,419	607,734	781,210	809,673	800,001
Europe	211,325	214,435	211,871	212,241	228,460
Middle East and Africa	56,148	58,875	63,695	66,591	72,034
Northern America	134,690	135,773	141,073	140,921	144,861
South America	118,323	101,170	107,872	103,010	119,442
Total	*3,684,102*	*3,738,235*	*4,151,991*	*4,227,959*	*4,447,470*

Source: Calculated by authors based on the Food and Agriculture Organization of the United Nations Statistics.

- Also, during the analyzed period, we can see a stable share of agricultural output in 2021 compared to the average for the previous 3 years in the regions of the Asia–Pacific, Northern America and South America. However, the Europe region increased its share by 1 pp due to a decrease in the share of Middle East and Africa (Table 6). Therefore, we use the data for 2021 in the formula for the Necessity of Cyber Insurance for the Agricultural Industry Index.

Table 6. Share of agricultural production by region in 2017–2021, %.

Region	2017	2018	2019	2020	2021
Asia–Pacific	60%	61%	64%	65%	63%
Europe	14%	13%	12%	12%	13%
Middle East and Africa	7%	8%	7%	7%	6%
Northern America	11%	10%	9%	10%	10%
South America	9%	7%	7%	7%	7%
Grand Total, m USD	*3,684,102*	*3,738,235*	*4,151,991*	*4,227,959*	*4,447,470*

Source: Calculated by authors based on the Food and Agriculture Organization of the United Nations Statistics.

- In general, we consider all the described indicators to be equal in the formula for calculating the Necessity of Cyber Insurance for the Agricultural Industry, so we do not include weighting indicators.

3. Results

Today, we live in the fourth industrial revolution, which affects all areas of our lives. This transformation is also taking place in agriculture, which is why scientists often use the term agriculture 4.0 [23]. The characteristic features of agriculture 4.0 are the use of modern technologies and innovations, the involvement of robotics and the use of the Internet. The key difference of modern industry 4.0 is the increase in process efficiency with minimal human involvement [24].

Technological progress has a twofold impact on the transformation of the agricultural sector. Positive impacts are seen in structural changes that have deepened specialization, diversification and service provision in agricultural processes; in efficiency transformation through improved quality and increased output; and in green transformation with increased environmental protection [25]. The main drawback is the high degree of dependence of industry 4.0 stability on the level of cybersecurity of their tools or components [26]. Since most of the tools of the agricultural sector 4.0 are directly or indirectly based on technological innovations, they are potentially at risk from cybercriminals.

3.1. Cyber Risks in Digital Agricultural Sector

Precision agriculture (PA) plays a significant role in advancing the growth of agriculture 4.0, as it broadens the application of innovative technologies [27]. This strategy enables the integration of various technologies like IoT, Big Data, blockchain, AI, VR, etc., into the agriculture sector [28,29]. The digitalization of the agricultural sector is taking place through the introduction of the innovative technologies of PA in its three key areas: preparation for the production process; the production process; storage and delivery to the end consumer [30]. Each component is characterized by specific technological changes that can become potential sources of threats (Figure 2) [31–35]. Each technology is characterized by several types of cyber risks, which can be grouped into five main groups.

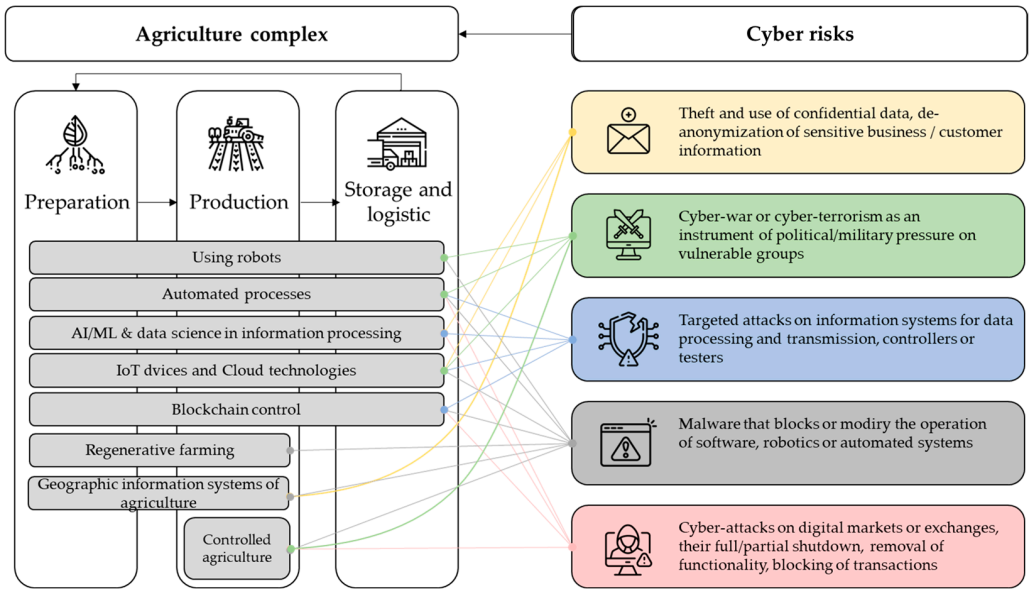

Figure 2. Cyber risk groups for key innovative tools of agricultural sector.

3.1.1. Group of Cyber Risks Aimed at Stealing and Using Confidential Information

This group of risks is realized through phishing, social engineering, spyware, ransomware or data leakage [36,37]. These attacks can be a problem for business owners and their customers, as sensitive information often includes payment information.

Business owners try to prevent information theft and train staff to work with digital systems. After the training, specialists test the level of literacy by simulating phishing attacks. For the agricultural sector, such measures had a positive impact: in 2022, only 8% of the test "failed" compared to 12% in 2021 and the average for all sectors was 11% [38].

Based on the results of research of those selected by Verizon companies in the field of data theft, the share of successful attacks in the total number of incidents in various industries was calculated (Table 7) [39]. In 2023, the most critical data breaches were for large agricultural companies (60% efficiency vs. 46% on average). Overall, 50% of agricultural companies lost data due to a cyber incident vs. 32% on average.

Table 7. Data breach efficiency of agricultural sector and related industries in 2023 by company size.

Industry	Total	Small	Large	Other
Agriculture	50%	0%	60%	50%
Finance	26%	54%	60%	24%
Healthcare	83%	82%	100%	82%
Retail	47%	53%	64%	44%
Transportation	30%	62%	52%	27%
Other	30%	53%	39%	29%
Average	32%	54%	46%	30%

Source: Calculated by authors based on the Data Breach Investigations report.

The simplest but most basic recommendations for improving the data security of agricultural companies and their customers are to use high-security passwords at all stages of their operations [40]. The data transfer process itself should also be secured and use modern tools for encrypting information flows [41].

3.1.2. Cyber-Warfare and Cyber-Terrorism as Instruments of Political/Military Pressure on Vulnerable Groups

The risk group aims to undermine the stability of food security and create related political or military pressures. The key tools of cyber-warfare and cyber-terrorism in the agricultural sector can be categorized into three main areas:

- Supply chain disruption: cyber-attacks can cause changes in supply chains, redirecting raw materials or finished products [42];
- Deterioration in product quality: cyber-attacks on production monitoring and testing systems implemented to reduce access to food for vulnerable populations [43];
- Misrepresentation of product information: cybercriminals can spread disinformation about the quality or quantity of products, provoking panic among the population, or interfere with monitoring results, with the possible deletion or falsification of data [44].

It is difficult to prevent the occurrence of such risks, as such incidents are most often sponsored by certain countries or large organizations. The targets of this type of cyber-attack are groups of organizations or suppliers, not individual agricultural companies. A massive approach causes instability and panic among the population, increasing pressure on the leadership of organizations or states [45].

3.1.3. Targeted Attacks on Data Processing and Transmission Systems, Controllers or Testers

These risks are aimed at identifying weaknesses in the protection of data transmission channels and the reading and control devices themselves [46]. The key feature of cyber-attacks in this group is the focus on distorting, replacing or deleting information about certain product indicators. Individual companies with a low level of cyber defense and those using unencrypted data and communication channels are targeted.

Often, attackers attack IoT devices that are organized in a network of thousands of devices but controlled through a single system [47]. Information from devices is transmitted and stored in clouds [48]. Therefore, the attackers' access to a single system gives them control over all devices for monitoring and testing the environment and products.

Today, the IoT market in the agricultural sector is estimated at USD 14.83 billion (+9% vs. 2022 and +18.6% vs. 2021) and is projected to grow to USD 28.56 billion in 2030 [49]. The regional distribution of the market for 2022 is heterogeneous: the Asia–Pacific (a region with a high level of digitalization) holds the largest share, Europe is in second place and North America is in third (Figure 3) [49].

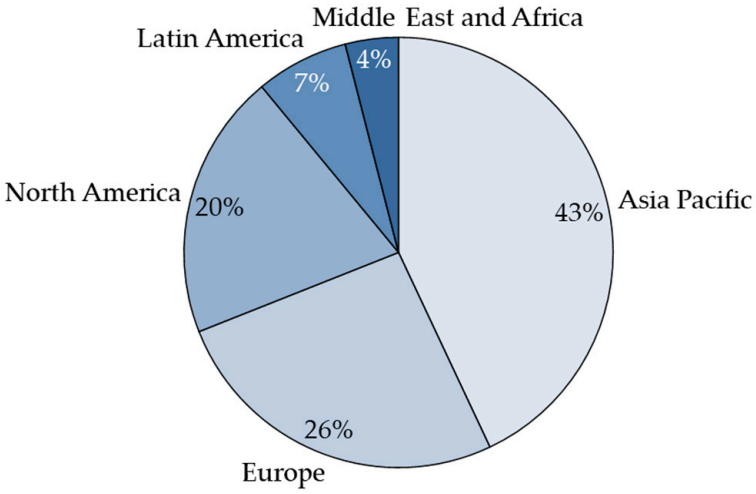

Figure 3. Regional split of agricultural IoT market in 2022. *Source: Calculated by authors based on the Precedence Statistics of the Internet of Things (IoT) in Agriculture Market*.

IoT devices are the basis for the development of agriculture 4.0 and are included in the strategy for the optimization and transformation of the agricultural sector in the European Union [50]. Accordingly, the expansion of the use of these devices requires the development of methods to improve their cybersecurity, to minimize risks and losses in the event of cyber incidents.

3.1.4. Malware That Blocks or Alters the Operation of Software, Robotics or Automated Systems

The automation of the agricultural industry has greatly relieved human labor and expanded the range of available tools for information processing. When malware enters an information system, it starts infecting neighboring systems and blocks their operations [51]. With a high level of automation and robotics applications, these harmful injections can completely stop the process of the production, processing or transportation of products [52].

The global market for robotics 2023 in the agricultural industry is estimated at USD 13.7 billion (+23.4% vs. 2022 and +50.5% vs. 2021) and is forecast to reach USD 20.6 billion by 2025 [4]. Regional development varies somewhat: North America is the leader in this area due to a number of transformation programs for large organizations; the European Union is second, due to a smaller volume of agro-industrial facilities; the Asia–Pacific is third due to sufficient human resources, which are cheaper compared to the transition of production to automated systems (Figure 4) [53].

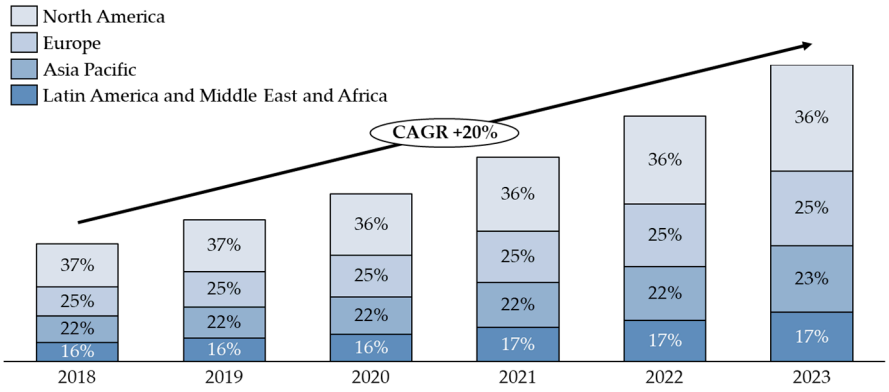

Figure 4. Regional split of agricultural robotics market 2018–2023. *Source: Calculated by authors based on the Researchdive Statistics of the Agriculture Robot Market.*

This growth rate of the robotics market confirms the vector of the agricultural industry's movement towards a digital business format. As part of this transformation, business owners should expand their cyber defense tools by hiring specialists in this area, creating cyber defense departments within their companies and purchasing cyber insurance policies [54].

3.1.5. Cyber-Attacks on Digital Markets or Exchanges, Their Full/Partial Shutdown, Removal of Functionality, Blocking of Transactions

We consider cyber-attacks on digital markets and exchanges (i.e., platforms for buying/selling finished goods and procurement materials) to be a separate group of cyber risks. The consequences of such incidents can be expressed through the following:

- Deterioration in the financial performance of the agricultural sector, and therefore a decrease in investment flows. Often, such attacks block bidding and transactions and therefore delay the supply of food to certain groups of companies or end users [55];
- Removing exchange instruments that block the ability to track prices and trade efficiently. Also, changes in trade profile settings can lead to the mass blocking of transactions as potentially fraudulent.

3.2. Cyber Insurance as a Tool to Protect Agricultural Industry 4.0

Cyber insurance is a component of an effective risk management strategy and an important tool for the preventive protection of organizations against cyber-attacks [56]. The issue of cybersecurity has become especially relevant during the COVID-19 pandemic, when most companies switched to a remote work format and automated their business processes [57]. Digitalization continues and uses more and more innovative technologies.

Proof of this is the involvement of artificial intelligence in some business processes. However, the uncontrolled use of tools such as ChatGPT or other AI chatbots can help attackers gain access to insecure information systems or data [58].

According to GlobalData, the global cyber insurance premium market has been growing over the past ten years, with growth accelerating in 2020–2021 under the influence of the COVID-19 pandemic; the CAGR came to 28% [15]. Typical cyber insurance policies cover first-party and third-party risks in the following areas: data confidentiality/retention/recovery; security of data transmission channels and communication facilities; integrity and security of information systems and software; ensuring a high level of reputation and its restoration in the event of insurance cases [59].

As already mentioned, the agrarian industry is actively digitizing and increasing digital tools in the processes of preparation, production and delivery to the end consumer. Accordingly, company management is faced with the task of creating a cyber risk protection strategy that takes into account all the specifics of their business. We believe that the best cybersecurity practices that should be developed in the agricultural sector are as follows:

- Develop a cybersecurity culture in which all business owners and their employees are familiar with the basic rules and principles of information systems. In addition, the entities in this area should strengthen cooperation with other critical industry entities [60];
- Establishing cybersecurity departments within organizations or engaging specialists in this area to monitor and improve the security of IT systems [44];
- Use of cyber risk insurance policies as an effective tool for the timely prevention and identification of risks, as well as ensuring a set of post-incident measures in case of their occurrence [61].

3.2.1. Development of an Algorithm for Cooperation between an Agricultural Company and an Insurance Company When Concluding a Cyber Risk Insurance Contract

The classic participants in insurance relations are the insurer, the insured, insurance intermediaries and the regulator; however, the emergence of cyber insurance has added experts specializing in the field of cybersecurity [62]. We have developed an algorithm for cooperation between an agricultural company and an insurance company when concluding a cyber risk insurance contract (Figure 5).

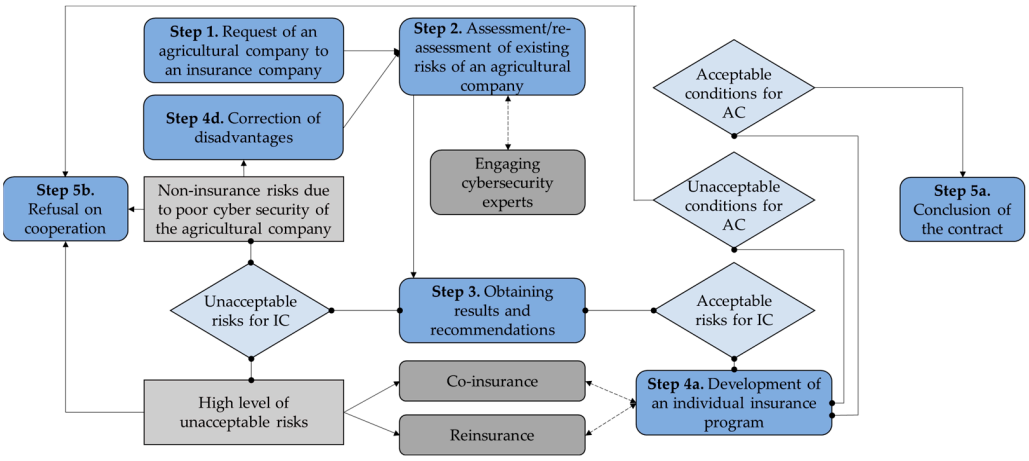

Figure 5. Algorithm of cooperation between an agricultural company and an insurance company when concluding a cyber risk insurance contract.

1. Step 1. Request of an agricultural company to an insurance company. After deciding about the need for cyber risk insurance, agribusiness owners start looking for insurers that provide the following services. After selecting one or more options, the process of negotiations between the parties to the insurance relationship begins;

2. Step 2. Assessment of existing risks of an agricultural company. The other party, the insurance company, begins to assess the current state of the agricultural company, its IT infrastructure, employee awareness, information security and data transmission channels. Based on the information collected, the risk is quantified. To monitor the required indicators, an insurance company may engage cybersecurity experts;
3. Step 3. Obtaining results and recommendations. After receiving the results of the inspection, the insurer determines the level of risk: acceptable or unacceptable for insurance. Also, at this stage, the insurer, either independently or with the involvement of cybersecurity experts, creates a roadmap for correcting disadvantages to improve the protection of the agricultural company;
4. Step 4. (a) If the risks are acceptable to the insurer, an individual insurance plan is developed based on the client's needs. (b) If the risks are high, the insurance company may accept the object for insurance, while transferring part of the risk to reinsurance. The insurer makes the decision to reinsure independently and is not obliged to notify the client. In this case, an individual insurance plan is developed based on the client's needs. (c) In a case where the risks are big or excessive and therefore unacceptable, an agricultural company is offered coinsurance for the following risks. If such conditions are agreed upon, the insurance company begins to work with co-insurance partners and develops an individual insurance plan based on the client's needs. If the client refuses this option, then a refusal to cooperate is recorded. (d) If the risks are unacceptable due to the unsatisfactory state of cybersecurity, the agricultural company is requested to correct the problems based on the recommendations received. If an agricultural company agrees to correct the problems, it undergoes a second inspection (Step 3). If an agricultural company refuses to correct the problems, a refusal to cooperate is recorded;
5. Step 5. After the development of an individual insurance policy with the required coverage and tariff, the agricultural company decides whether the proposed option is suitable for it. (a) If the terms and conditions are acceptable to the agricultural company, an agreement is concluded. (b) If the conditions are unacceptable to the agricultural company, a refusal to cooperate is recorded.

The role of cybersecurity experts in the insurance process is being transformed from just a third party. They make the decision on whether to provide insurance for the cyber risks of an agricultural company due to possessing the specific expertise needed. Furthermore, throughout the algorithm's progression, experts in cybersecurity actively recognize chances to mitigate unsystematic risks. Already, after signing the insurance contract, cybersecurity experts provide control over the protection of agricultural companies from cyber risks thanks to continuous monitoring of their condition and 24/7 support [63].

The simplest option of coverage and tariff of a cyber insurance policy is calculated based on existing information about losses from a cyber-attack in a particular industry [64]. Since cyber threats are constantly being modified, we offer a selection of cyber policy coverage based on the classification of cyber risks by consequence vectors (described in Section 3.1).

One of the forms of mandatory coverage for most agricultural companies is insurance against a group of risks associated with malware that blocks or changes the operation of software, robotics or automated systems. This approach is due to the fact that, at all stages of agro-industrial activity, systems or devices are used that are characterized by the following risks.

We consider insurance against the theft and use of confidential data, and the deanonymization of sensitive business or customer information, to be another form of mandatory coverage. While human involvement is not completely excluded from the company's activities, it is worth considering the possibility of human error.

Coverage of such risk groups as targeted attacks on information processing and data transmission systems, controllers or testers; cyber-attacks on digital markets or exchanges, their full/partial shutdown, removal of functionality or blocking of transactions; and cyber-

war or cyber-terrorism as a tool of political/military pressure on vulnerable groups should be added to policies depending on the specifics of an individual client and the scope of their activities.

3.2.2. Regional Need to Develop Cyber Insurance for Agricultural Sector 4.0

According to the results of the calculation, the highest I_{CIN} is in the North America region, due to the highest proportion of cyber-attacks, smart farming and the average National Cybersecurity Index (NCSI). The Asia–Pacific region is in second place, as it has the highest share of agricultural products and low levels of smart farming and cyber-attacks. The third position is occupied by Europe, as, despite the highest NCSI, it receives 39% of cyber-attacks. In the fourth position are the Middle East and Africa, due to low NCSI. In the last place is Latin America, where the average NCSI level is overlapped by low shares of other indicators (Figure 6).

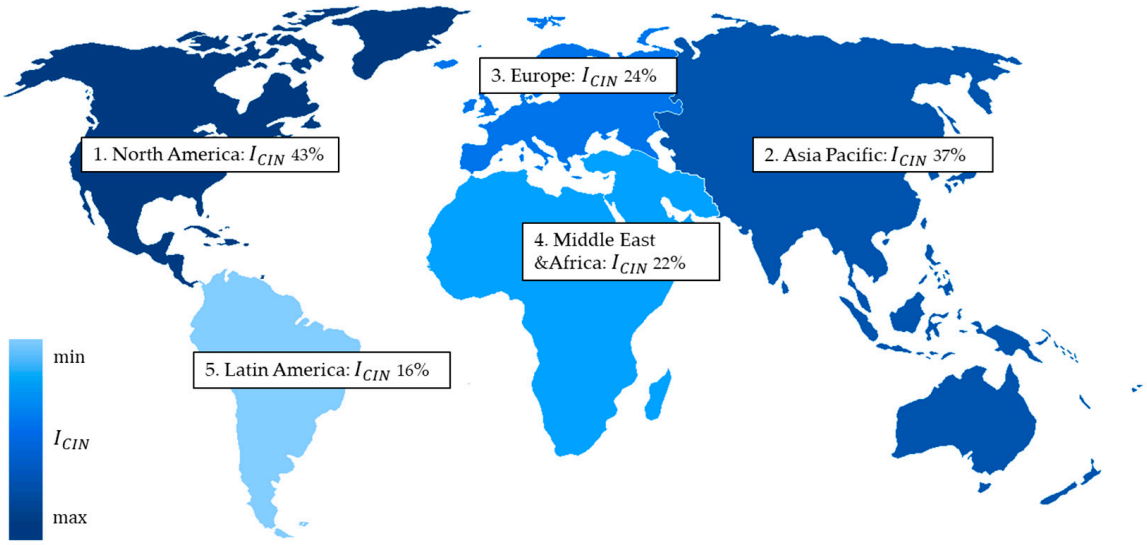

Figure 6. Map of the necessity of cyber insurance for agricultural industry based on 2022 numbers.

Differences in the way digitization is implemented in various regions within the agricultural sector have resulted in varying outcomes on the calculated index. As a result, it is important to tailor cybersecurity strategies to each region's specific characteristics and requirements. Therefore, if the agricultural company chooses to use cyber insurance as a risk management solution, insurers and cybersecurity experts should collaborate to develop customized insurance products based on the recommended algorithm.

4. Discussion

The initial hypothesis of our study was the uneven distribution of the need to develop cyber insurance for the agricultural industry in different regions of the world. According to the results, the values of the index I_{CIN} are in a range from 16% to 43%. That is, the spread between the minimum and maximum values is 27 pp, which corresponds to our hypothesis.

The assumption that there is a high need for the development of cyber insurance for the agrarian industry in North America was confirmed by the impact of the largest share of the smart farming market (54%), the largest share of cyber-attacks (41%) and the average of the National Cybersecurity Index (31%).

The second and third positions also conformed with the initial hypothesis: the Asia–Pacific region has the highest share of agricultural production (63%) and an average of National Cybersecurity Index (40%). Therefore, ensuring a high level of cybersecurity in the region is a high priority. The Europe region has the highest level of National Cybersecurity Index (78%), offset by a high share of cyber-attacks (39%), while the shares of smart farming and agricultural production are average (21% and 13% respectively).

An unexpected conclusion was that we could see the Middle East and Africa region in the fourth position and Latin America in the last, fifth position. Although Africa's agrarian industry has a development plan and continues to improve, the share of agricultural production is the lowest (6%) [65,66]. However, the market share of smart farming is higher (8%) than in Latin America (7%), which is reinforced by the inverse National Cybersecurity Index (30% vs. Latin America 51%). Accordingly, the Latin American region has the lowest need to develop cyber insurance for the agricultural industry at this stage due to low rates of cyber-attacks, its small share of the smart farming market and agricultural output and the average level of its National Cybersecurity Index. After the saturation of the agricultural industry with innovative technologies in Latin America, the level of need will increase.

Based on the obtained results, the need for cyber insurance increases with the increase in digitalization of a certain sector. Cyber insurance is seen by scientists as a means of investing in their own cybersecurity, as it not only provides financial protection but also lowers the chances of experiencing cyber incidents [45]. Cyber insurance is also defined as a tool to protect against indirect losses, such as fines and sanctions imposed by market regulators [67]. However, it is worth considering the possibility of the insured investing in cybersecurity, as the sole use of cyber insurance can cause significant losses for the insurance company [68].

An alternative opinion is that cyber insurance is useless in the event of a cyber-war or a targeted act of terrorism, since losses from such cases are catastrophic for all participants in insurance relations [69]. Therefore, the other side of cyber insurance is its profitability for insurance companies, whose goal is to make a profit [70]. The establishment of cyber insurance ought to prioritize the optimization of advantages for all involved parties, while adequately addressing their respective requirements [71].

The vector of research in this area is an in-depth study of the need for cyber insurance in the context of different countries. This will allow insurers to understand the importance of implementing this type of insurance at the local level and agricultural companies to include such a tool in a set of measures to improve cybersecurity. It is clear that technological development will continue, so the Agricultural Cyber Insurance Needs Index can be updated and supplemented in accordance with new challenges and threats in cyberspace.

This study also provides a framework for cooperation between agricultural companies and insurance companies during the cyber insurance process. Future research areas may be narrowed to consider the insurance of specific cyber risks in the agricultural sector.

5. Conclusions

The future development of the agrarian industry depends on the efficiency and timeliness of the technological innovations in it. In the context of growing cyber threats, agribusiness owners need to be able to detect and neutralize them. However, it is impossible to completely eliminate the likelihood of a cyber incident due to the constant nature of the technological process. In this case, cyber insurance is a tool to minimize losses from cyber-attacks. This type of insurance should take into account the peculiarities of agriculture 4.0 and its importance for global food security. In this paper, we have developed an algorithm for cooperation between an agricultural company and an insurance company when concluding a cyber risk insurance contract, which is client-centric, as it takes into account the requirements and wishes of the client at each stage of the interaction. Peculiarities of agricultural development and cybersecurity differ in different regions of the world. Therefore, the need for cyber insurance for the agricultural sector differs from region to region. The proposed index of the necessity of cyber insurance for the agricultural industry allows us to compare regions and understand future development vectors. The study shows that the North American region is in the greatest need of developing cyber insurance for the agricultural industry, as it has the largest share of smart farming but a low level of National Cybersecurity Index. At the same time, the smallest level of cyber insurance is required for the agrarian industry in Latin America, as it accounts for a small share of agricultural production, cyber-attacks and the smart farming market. Therefore,

the creation of personalized insurance products according to the proposed algorithm is a promising vector for the development of regional cyber insurance markets.

Author Contributions: Conceptualization, M.W.S., N.P., L.H., O.P., F.I., L.Ș. and R.P.; methodology, M.W.S., N.P., H.L. and O.P.; validation, M.W.S., N.P., H.L. and O.P.; formal analysis, M.W.S., N.P., H.L. and O.P.; investigation, M.W.S., N.P., H.L. and O.P.; data curation, M.W.S., N.P., H.L. and O.P.; writing—original draft preparation, M.W.S., N.P., H.L. and O.P.; writing—review and editing, M.W.S., O.P., F.I., L.Ș. and R.P.; visualization, N.P. and H.L.; supervision, M.W.S. and O.P.; project administration, M.W.S. and O.P.; funding acquisition, F.I., L.Ș. and R.P. All authors have read and agreed to the published version of the manuscript.

Funding: The APC of this paper was funded by a project grant (Code 6PFE) under the scheme "Increasing the impact of excellence research on the capacity for Innovation and Technology Transfer within USV Timisoara" Romania.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The article contains the necessary data to support the findings of this study.

Acknowledgments: The APC of this paper was funded by a project grant (Code 6PFE) under the scheme "Increasing the impact of excellence research on the capacity for Innovation and Technology Transfer within USV Timisoara" Romania and was achieved by the Named scholarship of the Verkhovna Rada of Ukraine for young scientists—doctors of science for 2023, state registration grant project number 0123U103631.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. International Covenant on Economic, Social and Cultural Rights. 1966, Volume 3. Available online: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-3&chapter=4&clang=_en (accessed on 16 November 2023).
2. Marvin, H.J.P.; Bouzembrak, Y.; van der Fels-Klerx, H.J.; Kempenaar, C.; Veerkamp, R.; Chauhan, A.; Stroosnijder, S.; Top, J.; Simsek-Senel, G.; Vrolijk, H.; et al. Digitalisation and Artificial Intelligence for Sustainable Food Systems. *Trends Food Sci. Technol.* **2022**, *120*, 344–348. [CrossRef]
3. Alahmadi, A.N.; Rehman, S.U.; Alhazmi, H.S.; Glynn, D.G.; Shoaib, H.; Solé, P. Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors* **2022**, *22*, 3520. [CrossRef]
4. Angyalos, Z.; Botos, S.; Szilagyi, R. The Importance of Cybersecurity in Modern Agriculture. *J. Agric. Inform.* **2021**, *12*, 1–8. [CrossRef]
5. Amin, Z. A Practical Road Map for Assessing Cyber Risk. *J. Risk Res.* **2017**, *22*, 32–43. [CrossRef]
6. Vatn, K.J.D. Cybersecurity in Agriculture: A Threat Analysis of Cyber-Enabled Dairy Farm Systems. Master's Thesis, NTNU–Norwegian University of Science and Technology, Trondheim, Norway, 2023. Available online: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3082225 (accessed on 16 November 2023).
7. Okupa, H. Cybersecurity and the Future of Agri-Food Industries. Master's Thesis, Kansas State University, Manhattan, KS, USA, 2020. Available online: https://hdl.handle.net/2097/40529 (accessed on 16 November 2023).
8. Stephen, S.; Alexander, K.; Potter, L.; Palmer, X.-L. Implications of Cyberbiosecurity in Advanced Agriculture. In Proceedings of the 18th International Conference on Information Warfare and Security, Baltimore, MD, USA, 9–10 March 2023; Volume 18, pp. 387–393. [CrossRef]
9. Rotz, S.; Duncan, E.; Small, M.; Botschner, J.; Dara, R.; Mosby, I.; Reed, M.; Fraser, E.D.G. The Politics of Digital Agricultural Technologies: A Preliminary Review. *Sociol. Rural.* **2019**, *59*, 203–229. [CrossRef]
10. Yang, X.; Shu, L.; Chen, J.; Ferrag, M.A.; Wu, J.; Nurellari, E.; Huang, K. A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 273–302. [CrossRef]
11. Drape, T.; Magerkorth, N.; Sen, A.; Simpson, J.; Seibel, M.; Murch, R.S.; Duncan, S.E. Assessing the Role of Cyberbiosecurity in Agriculture: A Case Study. *Front. Bioeng. Biotechnol.* **2021**, *9*, 737927. [CrossRef]
12. Riaz, A.R.; Gilani, S.M.M.; Naseer, S.; Alshmrany, S.; Shafiq, M.; Choi, J.-G. Applying Adaptive Security Techniques for Risk Analysis of Internet of Things (IoT)-Based Smart Agriculture. *Sustainability* **2022**, *14*, 10964. [CrossRef]
13. Marotta, A.; Martinelli, F.; Nanni, S.; Orlando, A.; Yautsiukhin, A. Cyber-Insurance Survey. *Comput. Sci. Rev.* **2017**, *24*, 35–61. [CrossRef]
14. Prykaziuk, N.; Lobova, O.; Motashko, T.; Prokofieva, O.; Diachuk, H. Optimization of the Mechanism of Natural and Climate Risk Insurance at the Macro- and Meso-Levels of the National Economy. *Stud. Appl. Econ.* **2021**, *39*, 4655. [CrossRef]
15. GlobalData. *Cyber Insurance—Thematic Intelligence*; GlobalData: London, UK, 2023; Available online: https://www.globaldata.com/store/report/cyber-insurance-theme-analysis/ (accessed on 16 November 2023).

16. Acumen Global Industry 4.0 Market Report: Los Angeles, CA, USA. 2022. Available online: https://www.globenewswire.com/en/news-release/2022/10/21/2539262/0/en/Industry-4-0-Market-Size-Will-Attain-USD-261-9-Billion-by-2030-growing-at-16-3-CAGR-Exclusive-Report-by-Acumen-Research-and-Consulting.html (accessed on 6 February 2024).
17. Cisco Annual Internet Report (2018–2023) White Paper: CA, USA. 2020. Available online: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed on 6 February 2024).
18. Imperva. Available online: https://www.imperva.com/ (accessed on 16 November 2023).
19. NCSI. Available online: https://ncsi.ega.ee/compare/ (accessed on 16 November 2023).
20. Maximize Market Research. *Smart Farming Market—Global Industry Analysis and Forecast (2023–2029)*; Maximize Market Research: Narhe Pune, India, 2023; Available online: http://www.maximizemarketresearch.com/market-report/global-smart-farming-market/22769/ (accessed on 16 November 2023).
21. Food and Agriculture Organization of the United Nation Statistics. Available online: https://www.fao.org/faostat/en/#data/QV (accessed on 16 November 2023).
22. Van der Linden, D.; Michalec, O.A.; Zamansky, A. Cybersecurity for Smart Farming: Socio-Cultural Context Matters. *IEEE Technol. Soc. Mag.* **2020**, *39*, 28–35. [CrossRef]
23. Abbasi, R.; Martinez, P.; Ahmad, R. The Digitization of Agricultural Industry—A Systematic Literature Review on Agriculture 4.0. *Smart Agric. Technol.* **2022**, *2*, 100042. [CrossRef]
24. Cunha, L.; Silva, D.; Maggioli, S. Exploring the Status of the Human Operator in Industry 4.0: A Systematic Review. *Front. Psychol.* **2022**, *13*, 889129. [CrossRef]
25. Deng, F.; Jia, S.; Ye, M.; Li, Z. Coordinated Development of High-Quality Agricultural Transformation and Technological Innovation: A Case Study of Main Grain-Producing Areas, China. *Environ. Sci. Pollut. Res.* **2022**, *29*, 35150–35164. [CrossRef]
26. Da Silveira, F.; Lermen, F.H.; Amaral, F.G. An Overview of Agriculture 4.0 Development: Systematic Review of Descriptions, Technologies, Barriers, Advantages, and Disadvantages. *Comput. Electron. Agric.* **2021**, *189*, 106405. [CrossRef]
27. Trivelli, L.; Apicella, A.; Chiarello, F.; Rana, R.; Fantoni, G.; Tarabella, A. From precision agriculture to Industry 4.0: Unveiling technological connections in the agrifood sector. *Br. Food J.* **2019**, *121*, 1730–1743. [CrossRef]
28. Yarashynskaya, A.; Prus, P. Precision Agriculture Implementation Factors and Adoption Potential: The Case Study of Polish Agriculture. *Agronomy* **2022**, *12*, 2226. [CrossRef]
29. Monteleone, S.; Moraes, E.A.d.; Tondato de Faria, B.; Aquino Junior, P.T.; Maia, R.F.; Neto, A.T.; Toscano, A. Exploring the Adoption of Precision Agriculture for Irrigation in the Context of Agriculture 4.0: The Key Role of Internet of Things. *Sensors* **2020**, *20*, 7091. [CrossRef]
30. Yaqot, M.; Menezes, B.C.; Al-Ansari, T. Unmanned Aerial Vehicles in Precision Agriculture towards Circular Economy: A Process System Engineering (PSE) Assessment. *Comput. Aided Chem. Eng.* **2021**, *50*, 1559–1565. [CrossRef]
31. Dey, K.; Shekhawat, U. Blockchain for Sustainable E-Agriculture: Literature Review, Architecture for Data Management, and Implications. *J. Clean. Prod.* **2021**, *316*, 128254. [CrossRef]
32. Yépez-Ponce, D.F.; Salcedo, J.V.; Rosero-Montalvo, P.D.; Sanchis, J. Mobile Robotics in Smart Farming: Current Trends and Applications. *Front. Artif. Intell.* **2023**, *6*, 1213330. [CrossRef]
33. Bland, R.; Ganesan, V.; Hong, E.; Kalanik, J. Trends Driving Automation on the Farm; McKinsey & Company. 2023, p. 9. Available online: https://www.mckinsey.com/industries/agriculture/our-insights/trends-driving-automation-on-the-farm (accessed on 16 November 2023).
34. Demestichas, K.; Peppes, N.; Alexakis, T. Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors* **2020**, *20*, 6458. [CrossRef]
35. Keshavarz, M.; Sharafi, H. Scaling up Climate-Smart Regenerative Agriculture for the Restoration of Degraded Agroecosystems in Developing Countries. *Sustain. Prod. Consum.* **2023**, *38*, 159–173. [CrossRef]
36. Bendovschi, A. Cyber-Attacks—Trends, Patterns and Security Countermeasures. *Procedia Econ. Financ.* **2015**, *28*, 24–31. [CrossRef]
37. Ghiasi, M.; Niknam, T.; Wang, Z.; Mehrandezh, M.; Dehghani, M.; Ghadimi, N. A Comprehensive Review of Cyber-Attacks and Defense Mechanisms for Improving Security in Smart Grid Energy Systems: Past, Present and Future. *Electr. Power Syst. Res.* **2023**, *215*, 108975. [CrossRef]
38. ProofPrint. *2023 State of the Phish*; ProofPrint: Toronto, ON, Canada, 2023; p. 35. Available online: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2023.pdf (accessed on 16 November 2023).
39. 2023 Data Breach Investigations Report; Verizon. 2023, p. 89. Available online: https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf (accessed on 16 November 2023).
40. Hazrati, M.; Dara, R.; Kaur, J. On-Farm Data Security: Practical Recommendations for Securing Farm Data. *Front. Sustain. Food Syst.* **2022**, *6*, 884187. [CrossRef]
41. Anand, S.; Sharma, D.A. AgroKy: An Approach for Enhancing Security Services in Precision Agriculture. *Meas. Sens.* **2022**, *24*, 100449. [CrossRef]
42. Ben Hassen, T.; El Bilali, H. Impacts of the Russia-Ukraine War on Global Food Security: Towards More Sustainable and Resilient Food Systems? *Foods* **2022**, *11*, 2301. [CrossRef]
43. Elhabashy, A.E.; Wells, L.J.; Camelio, J.A. Cyber-Physical Attack Vulnerabilities in Manufacturing Quality Control Tools. *Qual. Eng.* **2020**, *4*, 676–692. [CrossRef]
44. Leclair, J. *Protecting Our Future, Volume 2: Educating a Cybersecurity Workforce*; Hudson Whitman Press: New York, NY, USA, 2015.

45. Oluwaseun, A.D.; Olugbemi, O.T.; Anani, O.A.; Hefft, D.I.; Wilson, N.; Olayinka, A.S.; Ukhurebor, K.E. Cyberespionage: Socioeconomic Implications on Sustainable Food Security. In *AI, Edge and IoT-Based Smart Agriculture*; Academic Press: Cambridge, MA, USA, 2022; pp. 477–486. [CrossRef]
46. Ayrour, Y.; Raji, A.; Nassar, M. Modelling Cyber-Attacks: A Survey Study. *Netw. Secur.* **2018**, *3*, 13–19. [CrossRef]
47. Xu, J.; Gu, B.; Tian, G. Review of Agricultural IoT Technology. *Artif. Intell. Agric.* **2022**, *6*, 10–22. [CrossRef]
48. A Novel Technology for Smart Agriculture Based on IoT with Cloud Computing. Available online: https://ieeexplore.ieee.org/abstract/document/8058280 (accessed on 15 November 2023).
49. Precedence Research. *Internet of Things (IoT) in Agriculture Market*; Precedence Research: Ottawa, ON, Canada, 2022; Available online: https://www.precedenceresearch.com/iot-in-agriculture-market (accessed on 16 November 2023).
50. European Commission. *Industry 4.0 in Agriculture: Focus on IoT Aspects*; European Commission: Brussels, Belgium, 2017; p. 6. Available online: https://ati.ec.europa.eu/reports/technology-watch/industry-40-agriculture-focus-iot-aspects (accessed on 16 November 2023).
51. Yascaribay, G.; Huerta, M.; Silva, M.; Clotet, R. Performance Evaluation of Communication Systems Used for Internet of Things in Agriculture. *Agriculture* **2022**, *12*, 786. [CrossRef]
52. Watson, M.R.; Shirazi, N.; Marnerides, A.K.; Mauthe, A.; Hutchison, D. Malware Detection in Cloud Computing Infrastructures. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 192–205. [CrossRef]
53. ResearchDive. *Agriculture Robot Market Report*; ResearchDive: New York, NY, USA, 2020; p. 210. Available online: https://www.researchdive.com/52/agriculture-robot-market (accessed on 16 November 2023).
54. Nikander, J.; Manninen, O.; Laajalahti, M. Requirements for Cybersecurity in Agricultural Communication Networks. *Comput. Electron. Agric.* **2020**, *179*, 105776. [CrossRef]
55. Tosun, O.K. Cyber-Attacks and Stock Market Activity. *Int. Rev. Financ. Anal.* **2021**, *76*, 101795. [CrossRef]
56. Tsohou, A.; Diamantopoulou, V.; Gritzalis, S.; Lambrinoudakis, C. Cyber Insurance: State of the Art, Trends and Future Directions. *Int. J. Inf. Secur.* **2023**, *22*, 737–748. [CrossRef]
57. Pranggono, B.; Arabo, A. COVID-19 Pandemic Cybersecurity Issues. *Internet Technol. Lett.* **2020**, *4*, e247. [CrossRef]
58. Sebastian, G. Do ChatGPT and Other AI Chatbots Pose a Cybersecurity Risk? *Int. J. Secur. Priv. Pervasive Comput.* **2023**, *15*, 320225. [CrossRef]
59. Baker, T.; Shortland, A. Insurance and Enterprise: Cyber Insurance for Ransomware. *Geneva Pap. Risk Insur. Issues Pract.* **2023**, *48*, 275–299. [CrossRef]
60. Duncan, S.E.; Reinhard, R.; Williams, R.C.; Ramsey, F.; Thomason, W.; Lee, K.; Dudek, N.; Mostaghimi, S.; Colbert, E.; Murch, R. Cyberbiosecurity: A New Perspective on Protecting U.S. Food and Agricultural System. *Front. Bioeng. Biotechnol.* **2019**, *7*, 63. [CrossRef]
61. Development of Large-Scale Farming Based on Explainable Machine Learning for a Sustainable Rural Economy: The Case of Cyber Risk Analysis to Prevent Costly Data Breaches. Available online: https://www.tandfonline.com/doi/full/10.1080/08839514.2023.2223862 (accessed on 12 November 2023).
62. Wolff, J.; Lehr, W. Roles for Policy-Makers in Emerging Cyber Insurance Industry Partnerships. In Proceedings of the TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy 2018, Washington, DC, USA, 20–22 September 2018. [CrossRef]
63. Camillo, M. Cyber risk and the changing role of insurance. *J. Cyber Policy* **2017**, *1*, 53–63. [CrossRef]
64. Romanosky, S.; Ablon, L.; Kuehn, A.; Jones, T. Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk? *SSRN Electron. J.* **2017**, *6*, 38. [CrossRef]
65. Jellason, N.P.; Robinson, E.J.Z.; Ogbaga, C.C. Agriculture 4.0: Is Sub-Saharan Africa Ready? *Appl. Sci.* **2021**, *11*, 5750. [CrossRef]
66. Badiane, O.; Makombe, T. *The Theory and Practice of Agriculture, Growth, and Development in Africa*; The United Nations University World Institute for Development Economics Research (UNU-WIDER): Helsinki, Finland, 2014. [CrossRef]
67. Ganbayar, U.; Yautsiukhin, A.; Martinelli, F.; Massacci, F. Optimisation of cyber insurance coverage with selection of cost effective security controls. *Comput. Secur.* **2021**, *101*, 102121. [CrossRef]
68. Bartłomiej, B.; Dankiewicz, R.; Ostrowska-Dankiewicz, A. The role of insurance in cyber risk management in enterprises. *Humanit. Soc. Sci.* **2019**, *26*, 19–33. [CrossRef]
69. Mazzoccoli, A.; Naldi, M. Robustness of Optimal Investment Decisions in Mixed Insurance/Investment Cyber Risk Management. *Risk Anal.* **2019**, *40*, 550–564. [CrossRef]
70. Harner, C.; Beck, C.; Fleisher, B. Cyber: Navigating the War Exclusion Issue. *Risk Manag.* **2020**, *7*, 8–11.
71. Pal, R.; Golubchik, L.; Psounis, K.; Hui, P. Improving Cyber-Security via Profitable Insurance Markets. *ACM SIGMETRICS Perform. Eval. Rev.* **2018**, *45*, 7–15. [CrossRef]