Cybersecurity and smart innovation for rural resilience: Moldova's strategic transition to green and digital villages

Anatolie BABIN,
Academy of Economic Studies of Moldova, Chisinau, Republic of Moldova
anatolii.babin@ase.md

Sergiu TUTUNARU,
Academy of Economic Studies of Moldova, Chisinau, Republic of Moldova
tutunaru@ase.md

Ion COVALENCO,
National Research and Educational Network of Moldova, Chisinau, Republic of Moldova
ion.covalenco@renam.md

Abstract
In the context of rapid digital transformation, both urban and rural communities are rethinking their development strategies through the adoption of smart technologies aimed at increasing resilience, inclusion and security. This study proposes a comprehensive framework for promoting smart cities and smart villages, with particular emphasis on cybersecurity as a fundamental pillar of socio-technical resilience. The study focuses on strengthening regional cybersecurity in the Republic of Moldova within the framework of Interreg programs, emphasizing their relevance for building secure digital ecosystems. The study examines European experiences, best practices and case studies related to digital transformation in rural areas, focusing on innovative ways to implement cybersecurity. Special attention is given to the integration of secure digital solutions into smart village initiatives to reduce cyber risks and enhance cyber defense capabilities, particularly in the agro-industrial sector of the regional economy of Moldova. A strategic roadmap for developing secure, interconnected and adaptive socio-technical systems for urban and rural areas is outlined, highlighting the growing importance of cybersecurity in protecting critical sectors such as agriculture, energy and utilities. Key strategies include infrastructure modernization, alignment with EU standards (e.g. NIS2) and enhancing digital literacy. Additionally, the transformative role of AI, the agricultural Internet of Things (AIoT) and data-driven automation in boosting agricultural productivity and rural development, while underscoring the need for secure-by-design digital ecosystems. The study examines the cross-sectoral potential of digital innovation, provides some recommendations for sustainable development and demonstrates, for example, how integrated digital solutions such as agrovoltaics, smart energy and AI can improve resilience, cybersecurity and economic sustainability in rural areas, supporting the Republic of Moldova's strategic transition to a safe, green and digital future.

Keywords: agricultural internet of things; renewable energy; triple transition; generative AI.

1. Introduction
In the context of an accelerating digital transition and the modernization of agriculture, cybersecurity emerges as a critical pillar of sustainable rural development - particularly in emerging economies such as the Republic of Moldova. The challenges facing rural communities in this transformation demand a multidimensional and integrated approach, particularly as digital technologies become deeply embedded in agricultural production, public administration, and infrastructure systems. A core dimension of this transformation involves the development of spatial data infrastructures and the coordination of cross-border information systems. These systems are increasingly exposed to cybersecurity risks, especially given the rapid digitization of services that rely on geospatial information. While digitalization offers numerous benefits - such as improved accessibility and efficiency - it

also introduces vulnerabilities, particularly to cyberattacks that have intensified across Europe in recent years. In response, national cybersecurity policies, aligned with European directives such as the NIS2 framework, are becoming essential for rural resilience and data protection. Despite notable progress in ICT adoption, Moldova's rural areas continue to face substantial digital exclusion. According to the National Regulatory Agency for Electronic Communications and Information Technology (ANRCETI), over 370 rural settlements remain without internet access due to a lack of commercial incentive for infrastructure deployment. This digital divide not only limits access to e-services but also reduces awareness of cyber threats, increasing vulnerability to cybercrime. In 2024, more than 1,000 cyber-related offenses were reported nationwide, with common schemes including fake investments, cryptocurrency scams, and social engineering via messaging platforms - threats that disproportionately affect underserved communities.

The digitalization of the European agricultural sector is accelerating the adoption of IoT-based precision farming systems, which can reduce crop losses by 20–30% and enhance resource efficiency by up to 20%. As noted by the European Commission (2025a) [1], such technologies are instrumental in driving sustainability and productivity across EU farms. However, the implementation of smart agriculture remains uneven due to high entry costs - typically ranging from €5,000 to €20,000 per farm - where cybersecurity measures account for 10–20% of the total investment. Despite their importance, cybersecurity risks are still underprioritized, leaving digital farming systems vulnerable to disruptions. Unlocking the full potential of these technologies requires coordinated EU action, increased funding, and tailored support to farmers, particularly in rural areas, as emphasized in CORDIS (2025) [2]. To ensure Moldova's rural areas can participate meaningfully in the digital and green transition, significant investment is required across four key domains: digital infrastructure, broadband connectivity, sustainable energy, and IoT integration. Estimates suggest that total investment needs may range from €300 million to €800 million, depending on regional disparities, technological choices, and institutional capacity. The implications of the digital transformation of rural areas in Moldova on cybersecurity are examined below, assessing current vulnerabilities, investment needs, and policy recommendations to support a secure and inclusive transition to smart villages.

2. Digital transformation in agriculture

2.1. The role of EU data space for sustainable rural areas development

The digital transformation of agriculture is exerting a transformative influence on both the agricultural economy of EU regions as well as on candidate countries, with significant ramifications for rural development. The integration of information and digital technologies is facilitating a dual transition in the field of agriculture, encompassing both green and digital aspects. This evolution aims to enhance farmers' efficiency and sustainability in their operations. Rural natural resources [3] are critical assets in the pursuit of sustainable and prosperous future prospects. When managed effectively, rural landscapes, encompassing forests and natural areas, have the capacity to regulate water flows, sequester carbon and pollutants from the atmosphere, prevent soil erosion, and provide ecosystem services. Sustainable management of agriculture and forestry, encompassing environmental, economic, and social dimensions, contributes to decent work and livelihoods, ecosystem conservation, biodiversity preservation, and increasing

resilience to climate change and risks. It is necessary to recognise the key role of improving product quality and providing comprehensive support to farmers, foresters and rural entrepreneurs, who play an important role in advancing the transition to a greener economy.

A greater focus on climate change mitigation, including through the promotion of renewable energy production, presents rural regions with a significant opportunity to address energy poverty. This potential is contingent upon the proper valuation of ecosystem services and the development of business models that are designed to benefit local communities. The bioeconomy constitutes a sizable segment of the EU's economy, encompassing agriculture, forestry, fisheries, aquaculture, and the production of food, feed, bioenergy, and bioproducts. It is further anticipated that the aforementioned measures will facilitate a transition of rural areas within the Republic of Moldova to a circular and low-carbon economy, in addition to modernizing and fortifying the food sector and industrial base in these regions. The establishment of a sustainable bio- and circular economy has been demonstrated to engender novel, more diverse value chains and processes that are ecologically sustainable. In 2017, the EU bioeconomy yielded €614 billion in value-added output and supported approximately 17.5 million individuals, thereby substantiating its significance in underpinning rural economic activity [4].

Digital technologies in agriculture can significantly improve farm productivity by improving the sustainability and efficiency of agricultural processes. This applies in particular to technologies such as the IoT, sensors, data analytics (including AI) and decision support systems, which enable more precise and individualized agricultural operations. There are successful examples of digitalization in agriculture in the EU. The European Commission supports various research and innovation projects [5] such as ATLAS and DEMETER, as well as initiatives to establish a Common European Agricultural Data Space (CEADS) [6] aimed at improving data exchange between farmers, equipment manufacturers and public authorities. These efforts are based on a step-by-step approach, starting with the preparation of the AgridataSpace project [7] funded under the Digital Europe Program. Important EU policies and legislation define the rules for the use and reuse of data related to the agricultural sector. The evolution of agricultural practices in the future is being influenced by ongoing research endeavors, technological innovations, and capacity-building initiatives within the agri-food sector supported by diverse financial frameworks [8] (Fig. 1).

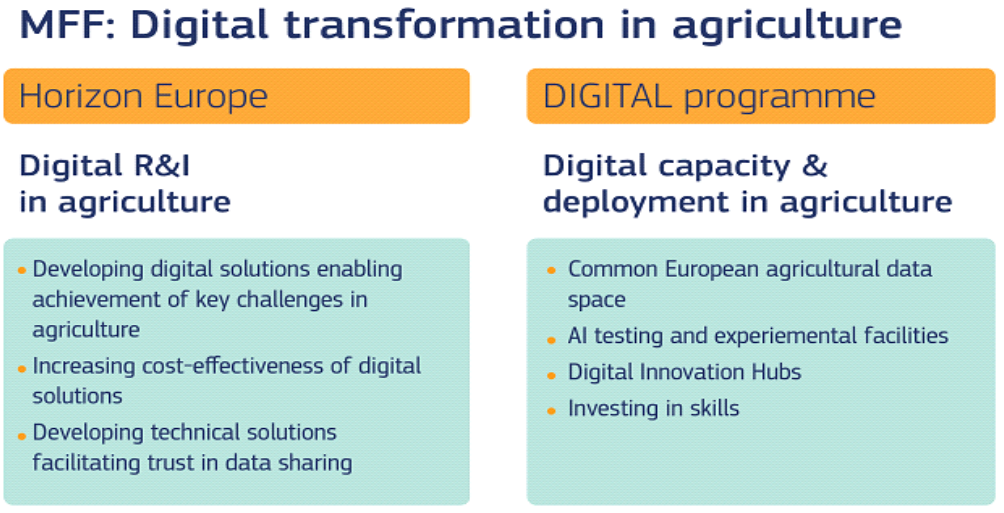

Fig. 1. Multi-Financial Framework: Digital transformation in agriculture. [8]

The agricultural value chain includes producers, agrochemical suppliers, processors, retailers and consumers. Digitalization provides all actors in the chain with greater transparency and streamlined processes, improving communication and automated data transfer. Technologies, such as blockchain, enable traceability of products and increased efficiency across the value chain, reducing costs and emissions. Innovative small and medium enterprises (SMEs) and start-ups can grow, providing new solutions and ideas for the agri-food ecosystem. Despite the obvious benefits of digitalization, it also creates digital divides – for example, between farmers who have access to modern technology and those who do not. These divides can arise due to distance, differences in business models, investment opportunities and the skill level of farmers.

The increased use of digital applications in the agricultural sector is resulting in increasing volumes of data of a diverse nature. Agricultural data collection includes information on land, crops, livestock, agronomic and climate data, machinery data, financial data and compliance information. Some data may be considered personal or sensitive to farmers, such as tractor routes or factors that contribute to successful production. Other data may be important to agribusiness and are needed for market forecasting, product development and insurance. Farmers often express concerns about the use of their data by third parties without consent. Protecting trade secrets is becoming increasingly important, so it is necessary to provide strong guarantees for data sharing, data sovereignty and data security to build trust and not compromise the development of smart agriculture. To promote fair data sharing across sectors, the EU has adopted a Data Act [9] that will come into force in 2025. An EU Code of Conduct on the Exchange of Agricultural Data [10] has also been created, which provides guidance on accessing and using this data. Data related to agricultural production include farm data and all types of data generated within the farming processes are presented on Figure 2.

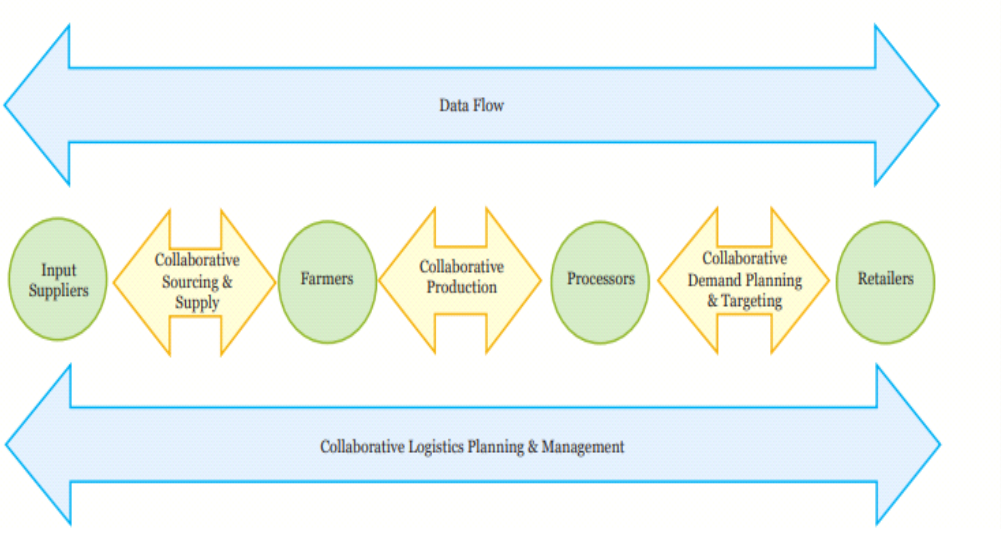

Fig. 2. Data generated within the farming processes.
Source: Irish Farmers' Association, February 2018

However, unlocking the potential of data technologies to improve agricultural productivity and support policy monitoring and evaluation is a complex task. EU practice shows that the main bottlenecks are:

- Moderate use of digital technologies by end users due to unclear costs and benefits, insufficient clarity of data and lack of skills to interpret them;
- Digital divide between farms due to differences in business models and investment opportunities;
- Low availability of data for effective monitoring and evaluation of policies;
- Lack of homogeneous reference data sets to capitalize on Earth and environmental observations;
- Lack of solutions for processing big data in agriculture;
- Difficulties for farmers in gaining control over their data;
- Insufficient data compatibility and lack of modern cybersecurity and privacy protection mechanisms.

Thus, special attention is required to data protection and cybersecurity issues, given the increased needs associated with the application of new technologies in the agri-food sector, including industrial biotechnology, robotics, big data and the Internet of Things.

2.2. The triple transition: integrating social, green, and digital dimensions in agriculture

The European Green Deal [11] has paved the way for a new understanding of economic development: the digital and green transitions should not be tackled separately, but simultaneously, to reinforce each other for greater and faster benefits. This is the essence of the concept of a dual - digital and green - transition [12] . However, the dual transition cannot be successful without addressing the social dimension of the transformation. This transition aspires to incorporate all societal actors into the process of transforming the

economy into one that is more sustainable and competitive. A fundamental aspect of a just and prosperous society is the equitable distribution of opportunities and challenges during major societal transitions.

This is why experts and politicians have started talking about the triple transition, which brings together the digital, green and social aspects of the EU's vision of the future - the European Growth Model [13]. The triple transition is a concept that brings together three key aspects of sustainable development: social, green and digital. In the context of agriculture, these three aspects can be interlinked and serve as the basis for a more sustainable and efficient agricultural system. The following discussion will proceed in an exhaustive fashion, with each component of the topic undergoing rigorous scrutiny.

The social aspect of the triple transition includes:

- Improving working conditions: The introduction of modern technologies and automation of processes can improve safety and convenience for farmers and workers.
- Education and training of personnel: Need to train agronomists and workers in modern agricultural methods, including digital tools and sustainable farming practices.
- Social justice: Supporting local communities and smallholder farmers to improve their situation and reduce inequalities.

The green aspect transition includes:

- Sustainable agricultural practices: Reducing the use of chemical fertilizers and pesticides, switching to organic farming and agroforestry.
- Conservation of biodiversity: Supporting ecosystems and natural resources, which is important for the long-term sustainability of agriculture.
- Efficient use of resources: Implementing technologies to optimize the use of water, land and energy, such as drip irrigation or solar panels on farms.

The digital aspect transition covers:

- Digitalization of processes: Implementation of IoT (Internet of Things), Big Data and Analytics to optimize agricultural production and resource management.
- Information exchange platforms: Creating digital platforms for farmers to share knowledge, resources and experiences.
- Precision farming technologies: Using drones, sensors and GPS to monitor crop health, increasing yields and reducing costs.

The combination of social, green and digital aspects can lead to the creation of new cross-sectoral initiatives such as:

- Agroecology systems: Integration of traditional knowledge and modern technologies to create sustainable agricultural systems.
- Smart farms: Using digital technologies to monitor and manage agricultural processes, thereby reducing the negative impact on the environment.

- Crowdfunding and cooperatives: Creating platforms to support local farmers where society can invest in sustainable projects.

Thus, the triple transition in agriculture can contribute to the creation of more sustainable, equitable and technologically advanced agricultural systems that will improve the quality of life of the population and protect the environment.

2.3. The use of the Internet of Things and artificial intelligence

To feed a growing global population and offset the loss of arable land, the agricultural sector needs to improve efficiency, productivity, and food quality while reducing labor costs and environmental impact. It should be noted that according to some projections, climate change will reduce agricultural production by 18% by 2050.

Current approaches focus on deploying more powerful machines in the field that become semi- or fully autonomous. These machines plan precise fertilization, irrigation, pest control, and harvesting schedules based on detailed environmental data. The race for solutions has begun: fields, crops, and livestock are equipped with numerous sensors that monitor the environment. Machines are equipped with intelligent algorithms, allowing them to perform their daily work with high accuracy and provide extensive information on the status of the work, ensuring 24/7 availability. The infrastructure of the agricultural system, consisting of many networked digital devices, is called the Agricultural Internet of Things [14].

The resulting data sets contribute to more accurate decision-making in agricultural operations and support the development of improved products by equipment manufacturers. However, large-scale data collection also increases exposure to cyber threats, including data theft, manipulation, and misuse.

Within the scope of the AFarCloud project [15] a consortium of European collaborators is undertaking the advancement of the implementation of the Agricultural Internet of Things (AIoT) concept. The present study proposes the conceptualisation of an abstraction layer for AIoT-based architectures. The purpose of this layer is to define key software components and procedures. This middleware functions as an interface between the field layer, comprising sensors, actuators, and on-site devices, and the cloud-based data processing layer, which hosts various farm management services (see Figure 3). The ELD layer incorporates sensors, actuators, outdoor devices, vehicles, and livestock.

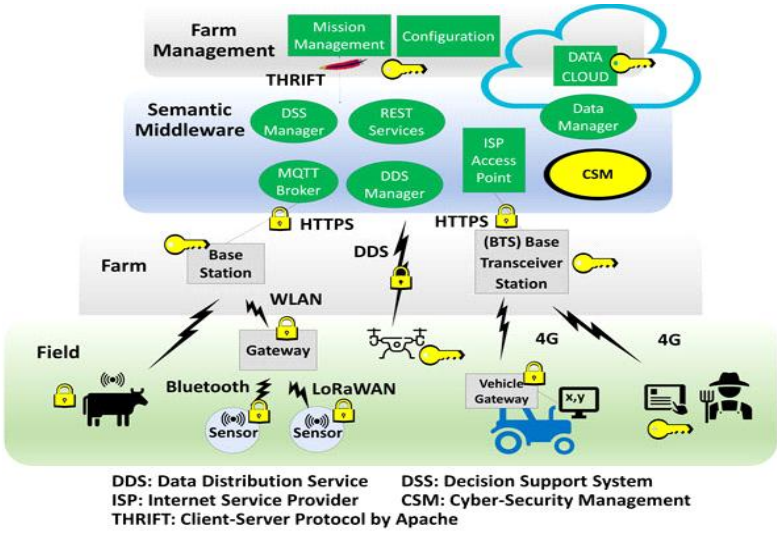

Fig. 3. System architecture with middleware as an interface between the field level and cloud farm management Source: [15]

A key element of the middleware under discussion is the cross-layer Cybersecurity Management (CSM) service, which is designed to oversee the security maintenance process through the provision of a security process definition, facilitating periodic assessment and the generation of recommendations for enhancement. This approach is intended to facilitate seamless and secure operations within the manufacturing facility by protecting it from potential cyber-attacks. During the initial period of automation implementation, it was observed that the cybersecurity challenges were confined exclusively to the information technology sector, particularly within the domains of farm management and middleware.

Modern sensors are not just data sources that send information to a data gateway: they are small, complex systems with microcontrollers, flash and RAM memory, containing an operating system and firmware for pre-processing the data. They need to be able to update their firmware, which, given the growing number of sensors in the field, must be done wirelessly, such as over-the-air (OTA). Unfortunately, this significantly increases security risks. Cybersecurity risks are generally not addressed by European agricultural standards, which focus on food and nutrition safety, preventing harm to workers from agricultural work or exposure to pesticides, minimizing the use of heavy machinery and ensuring the humane treatment of livestock.

In the contemporary, digitally connected world, the significance of robust cybersecurity extends far beyond the scope of major technological hubs to encompass extensive, frequently disregarded rural areas. These rural communities play an essential role within the agricultural and economic framework of the country as a whole. However, they are confronted with distinctive cybersecurity issues as a result of their distinct demographics, infrastructure constraints and resource limitations.

Rural communities are the lifeblood of traditional industries such as agriculture, mining and forestry. These sectors, while critical, often lag behind in digital transformation, leaving them exposed to cyber vulnerabilities that are not typically seen in more urbanized areas. For example, imagine a small community where the local water utility relies on automated systems that become the target of a cyberattack, disrupting the water supply for days or even weeks. The impact of such an attack extends beyond the immediate water shortage, potentially compromising sanitation and agriculture, thereby impacting the health and economic stability of the entire community. Furthermore, the sparse population distribution in rural areas often results in diminished investment in local cyberinfrastructure and a paucity of cybersecurity experts, leading to a reduction in the speed of detection and response to cyber incidents. This scenario has the potential to exacerbate the duration of outages, as well as the financial and logistical expenses associated with recovery.

Rural areas often struggle to access modern technology and high-speed internet. This digital divide can severely limit the ability of rural businesses and government agencies to protect their operations from cyber threats. For example, a small clinic may be using outdated computers that are vulnerable to malware, putting patient data at risk and disrupting health services. Without access to modern cybersecurity tools and expertise, these clinics become easy prey for cybercriminals.

In education, rural schools may lack the resources to teach proper online security, leaving the next generation unprepared for the digital challenges they will inevitably face. Improving digital literacy across all age groups is critical to protecting personal and professional data from increasingly sophisticated cyberattacks.

It is evident that the economic and social repercussions of cyber incidents in rural areas are often especially pronounced. To illustrate this point, consider the potential consequences of a successful attack on a major agricultural processor. Such an attack has the capacity to halt production, disrupt the supply chain, and cause financial damage that will resonate throughout the community. The repercussions of this phenomenon extend beyond the immediate victims, encompassing the local business community that is dependent on them, encompassing suppliers and retailers. The impact on society can be equally significant. The repercussions of cyberattacks on rural communities include the erosion of trust in digital systems, the deterrence of investment, and the retardation of the adoption of beneficial technologies. This phenomenon can engender further social isolation for these communities, as they become marginalised in comparison to urban areas that are benefiting from digital advancements.

The European Union has committed to positioning its Member States as global centers of excellence in artificial intelligence (AI) through the development of dedicated Testing and Experimentation Facilities (TEFs) [16, 17]. In cooperation with national governments, the European Commission is co-financing these infrastructures to support AI developers in bringing trustworthy, high-impact technologies to market, ensuring their effective and responsible deployment across the continent. The TEF model signifies large-scale, purpose-built environments – encompassing both physical and virtual domains – that

enable technology providers to evaluate, authenticate and showcase state-of-the-art AI systems in authentic, real-world scenarios.

These facilities are open to all European developers and support the integration of both software and hardware innovations, including robotics, into operational settings. The TEFs also serve as hubs for cross-sector experimentation, offering infrastructure for solving complex societal and industrial challenges in energy, mobility, and public services.

Importantly, TEFs will play a central role in supporting the implementation of the forthcoming AI Act, particularly through the development of regulatory sandboxes [18] in collaboration with national authorities. These controlled environments enable safe testing of AI applications, aligning with the EU's ambition to foster both technological excellence and regulatory compliance.

Within this framework, the Digital Europe Programme has introduced Coordination and Support Actions (CSAs) to ensure the cross-sector integration of AI testbeds, particularly in domains such as smart cities and communities. One flagship initiative is the Citcom.AI project [19, 20], a pan-European TEF network focused on the sustainable digital transformation of urban ecosystems.

Citcom.AI is structured around three strategic pillars:

- POWER – transformation of energy systems and optimization of energy consumption;
- MOVE – development of sustainable, intelligent mobility and logistics solutions;
- CONNECT – enhancement of citizen-centric services through local digital infrastructure.

Each pillar targets specific AI-enabled applications, such as predictive load balancing in heating networks, adaptive lighting systems, pedestrian traffic forecasting, smart intersections, air pollution monitoring, and water resource management. The initiative fosters innovation in AI and robotics by offering robust testing environments that simulate real-life urban scenarios. The project is organized into three regional "supernodes" - North, Central, and South Europe - comprising satellite centers and subnodes in 11 EU countries, including Denmark, Sweden, Finland, the Netherlands, Belgium, Luxembourg, France, Germany, Spain, Poland, and Italy. This initiative is overseen by imec, a renowned European R&D institute specialising in nanoelectronics and digital technologies. The Digital Europe Programme has allocated a budget totalling €40 million to Citcom.AI, the project being implemented by the organisation, since its launch in January. The ambition of Citcom.AI is to ensure its long-term financial sustainability.

In parallel, the AgrifoodTEF [21] represents another strategic facility under the TEF initiative, aimed specifically at the agri-food sector. It offers services for evaluating and validating AI and robotics-based innovations, supporting sustainable food production, operational efficiency, and market readiness of emerging technologies.

Collectively, these initiatives form a critical component of the EU's strategy to accelerate digital innovation while ensuring cybersecurity, ethical alignment, and societal benefit in both urban and rural environments.

The project includes five impact sectors:

- Agriculture - increasing the productivity of unmanned vehicles;
- Wood species - optimization of natural resources;
- Gardening - nutrient balance and crop quality;
- Livestock farming - increasing sustainability in breeding;
- Food processing - supply chain traceability.

Use cases cover a wide range of topics, including quality crops, agronomy, AI conformity assessment and sustainable farming.

These examples show the prospect of planning the interaction of two advanced technologies Artificial Intelligence (AI) and the Internet of Things (IoT), which are actively developing and mutually reinforcing each other, creating new opportunities for business, everyday life and technology in rural areas and small towns in the regions of the Republic of Moldova. Smart Specialization Communities of Practice are professional associations created to share experience, knowledge and best practices among specialists working within the framework of the Smart Specialization concept. This concept implies the targeted development of innovative and competitive areas of the economy of a region or country, taking into accounts its unique features and potential. The results of 'Smart Specialization' studies in Finnish regions related to the issues of establishing test sites [22] in Moldovan development regions may suggest farms to consider some innovative solutions. The interconnection of Nokia's Artificial Intelligence (AI) and Internet of Things (IoT) solutions in agriculture is an important area of modern technology development to improve the efficiency and sustainability of the agricultural sector. The key aspects of this relationship are summarized below.

1. Smart sensors and IoT devices:
    - Utilizing sensors to monitor soil, moisture levels, temperature and plant health;
    - Real-time data transfer to cloud-based systems for analysis and decision making.
2. Analytics and AI:
    - Big data processing using AI algorithms to determine optimal sowing, watering and fertilization timing;
    - Predictive analytics to prevent plant diseases and pests.
3. Smart control systems:
    - Automation of irrigation, fertilizer and pesticide delivery systems based on AI data and recommendations;
    - Use of unmanned aerial vehicles (drones) for monitoring large areas and spot intervention.
4. Communication and infrastructure:
    - Development of communication networks (e.g. NB-IoT, LTE-M) to provide reliable data transmission in rural areas;

- Integration of Nokia solutions into a single platform for centralized management and analysis.

5. Benefits for agriculture:
   - Improved crop yields and product quality;
   - Reduced input and chemical costs;
   - Improved sustainability and reduced environmental impact.
6. Implementation examples:
   - Smart farms using IoT and AI to automate processes;
   - Crop forecasting and risk management programmes;
   - Analytics-driven decision support for farmers and agribusinesses.

In summary, Nokia solutions that combine AI and IoT are creating new opportunities to transform agriculture, making it smarter, more sustainable and profitable. Nokia also offers a new approach that combines the best of smart farming with an innovative business model built on a managed IoT connectivity service. Nokia Worldwide IoT Network (WING) [23] is a managed IoT 'one-stop-shop' IoT service that includes a pre-integrated global IoT core network, connectivity management as well as dedicated IoT operations, billing, security and data analytics, and an ecosystem of applications. Smart Agriculture as a Service offers four packages to help farmers understand how their crops are produced and identify potential threats from disease, weather and pests (Figure 4).

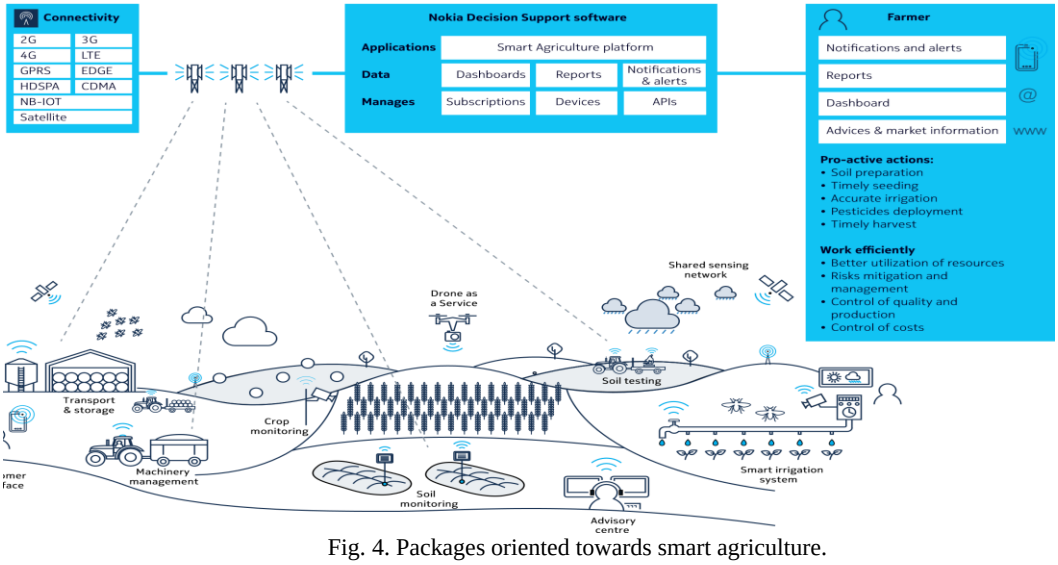

Fig. 4. Packages oriented towards smart agriculture.
Source: [24]

Nokia's Smart Agriculture as a Service introduces a scalable, IoT-based digital agriculture solution built on its global WING platform, offering managed connectivity, data analytics, and cybersecurity. The system is structured around four core modules - environmental monitoring, crop and soil management, and an advisory center - designed to enhance precision farming. This integrated approach enables real-time decision-making, optimizes resource use, and supports sustainable food production. The model provides economic

value for both farmers and telecom operators by aligning technological innovation with a service-based business framework.

2.4. Integrating renewable energy, smart agriculture, and generative AI: A cyber-resilient framework for sustainable rural transformation

Food systems consume about 70% of the world's water resources [25] while the energy sector uses 15% of these resources. Thus, the interlinkages between water, energy and food systems are critical for sustainable development. Climate change is disrupting water cycles, threatening both food production and human health. In the context of increasing resource scarcity, there is a need to harness the potential of rural areas to generate renewable energy, including solar, wind and biogas, which can significantly improve the sustainability of the agribusiness sector.

With the growing global demand for energy efficiency and the need to reduce greenhouse gas emissions from agriculture, the topic is becoming increasingly important. Since 2005, emissions from agriculture have remained at the same level, requiring urgent action to reduce them in order to meet the EU climate targets. Forecasts show that by 2030 the EU is expected to see only a modest reduction of 4% compared to 2005 levels. The introduction of decentralized generation from renewable energy sources (RES) on agricultural land may be one way to address this problem.

The necessary investments in infrastructure create opportunities for cross-sectoral use of resources [26], which is key to achieving sustainable development. An example of such solutions is bidirectional charging of electric vehicles, which connects the energy and transport sectors. Below are some examples of cross-sectoral approaches that contribute to a sustainable transition:

- Energy and mobility: Bidirectional charging of electric vehicles not only reduces emissions from internal combustion engine vehicles, but also uses stored electricity to improve grid resilience and optimize the use of renewable energy sources.
- Energy and industry: Energy efficiency and demand response strategies help reduce energy consumption and improve flexibility, which reduces costs for industrial customers and improves the carbon footprint.
- Energy and construction: Energy-efficient building design, including intelligent heating and cooling systems, helps reduce energy consumption and improve the adaptability of buildings to fluctuations in renewable energy production.
- Energy and agriculture: The concept of agrovoltaics allows solar panels to be installed on agricultural land, which makes it possible to simultaneously produce energy and agricultural products without increasing the area used.

These examples highlight the importance of implementing cross-sector solutions to overcome the challenges of modern sustainable energy systems. However, the implementation of such approaches faces a number of challenges, including the lack of necessary infrastructure, a lack of bidirectional charging, and insufficient consumer engagement. Administrative barriers may also slow down the implementation of innovative solutions.

The rapid rise in energy prices and increasing threats to energy security require the Government and academic community of the Republic of Moldova to take decisive action toward radically improving the energy resilience of its development regions. This can be achieved by promoting sustainability and establishing innovative regulatory sandboxes in the energy sector focused on long-term pricing in rural areas.

The European Green Deal and the REPower EU plan call for a deep transformation of Moldova's energy system, which must become more interactive and intelligent to enable consumers to benefit from the green transition. In this action plan, the European Commission highlights how emerging technologies can enhance the efficiency of energy resource use, facilitate the integration of renewable energy into the grid, and reduce costs for both consumers and energy companies across the EU.

A valuable innovation for end users may lie in the UK's "Data Sharing Infrastructure" concept - comprising the Digital Spine and Data Exchange Scheme - which, alongside the European approach to decentralized cybersecurity services, could position Moldova's regions as pioneers in Southeast Europe and the Eastern Partnership. This would offer the potential for a scalable plan to unlock data value and promote digitalization [27] beyond the energy sector.The Digital Spine [28] concept is a paradigm aimed at addressing infrastructure investment disparities through the utilization of advanced digital technologies. This approach, founded on the principle of decentralized intelligence across sectors (including agriculture), has the potential to enhance the efficiency and resilience of existing rural infrastructure in Moldova's development regions.
s Moldova expands renewable energy systems in rural communities, the adoption of the "Data Sharing Infrastructure" - the Digital Spine - could enable:
1. Significant reduction in the costs of launching regulatory energy innovation sandboxes by minimizing data collection requirements.
2. Lower client-side expenses through more efficient systems with reduced grid expansion.
3. Decreased uncertainty around potential energy and flexibility resources from consumers, networks, and generation, thereby reducing cybersecurity risks.
4. Support for interdisciplinary research and innovation, improved transparency, and easier integration of scientific research into agri-industrial development and policy-making.

The integration of digital infrastructures and Generative AI with the energy and mobility sectors is a cornerstone of the EU's strategy to achieve climate neutrality by 2050. The Digital Spine and its constituent components offer pragmatic solutions for establishing a sustainable, interconnected, and competitive European economy. By leveraging advanced digital technologies, Europe stands to accelerate its green transition, reduce carbon emissions, and fortify its industries by establishing a more efficient and resilient energy system.

Generative AI (GenAI) [26] plays an active role here as it can optimize energy systems, predict energy production, coordinate electric vehicle charging and automate energy efficiency practices in smart buildings. It is important that energy companies adapt to the growing complexity of local markets and provide the necessary defenses against cyber

threats. Generative AI, also known as GenAI, is a branch of artificial intelligence that focuses on creating new data from existing data. Generative AI also has applications in the context of cybersecurity, from helping threat hunters extract data for ongoing investigations to providing real-time information that informs vulnerability management workflows.

The agricultural sector stands at the precipice of a technological revolution, precipitated by the advent of generative artificial intelligence. According to the analysis conducted by McKinsey, integration of Generative AI with conventional analytical AI has the potential to generate economic benefits across the entire agricultural value chain, spanning from the development of agricultural seeds to the management of agricultural enterprises and the realm of supply chain logistics. To illustrate this point, one may envision a "Smart Farm". AI as “Virtual Farmer" system not only predicts when and where to plant crops, but also generates millions of potential scenarios based on weather forecasts, soil conditions and historical pest outbreaks to determine the best strategy. GenAI is capable of performing this function, in the role of an virtual agronomist. This virtual agronomist provides customized counsel to farmers regarding the optimal planting times, the appropriate dosages of fertilizer, and the optimal crop varieties for achieving maximum yield.

In the domain of agriculture and food production, generative AI systems frequently entail intricate networks comprising interconnected devices and platforms, extending from sensors installed on-site to cloud-based data analytics platforms. Therefore, a holistic approach to security is imperative. This approach must encompass digital security in addition to the physical security of the equipment and the human elements of the system. The implementation of educational initiatives targeting farm personnel in regard to cybersecurity best practices has the potential to contribute to the mitigation of risks associated with human error or oversight. To ensure the security of the agri-food ecosystem, particularly with regard to the use of Generative AI, it is imperative to conduct regular assessments and updates of security measures. Moreover, fostering industry-wide collaboration on security standards and practices is essential.

One illustration cited in the McKinsey article pertains to AI-powered digital farm lookalikes, which are virtual models that replicate real-world conditions. These models possess the capability to execute "what-if" scenarios concerning crop cultivation, pest management, and environmental impact. This functionality empowers farmers to formulate decisions that align with both economic viability and environmental sustainability. It has been demonstrated that agricultural producers are capable of achieving greater results with a reduced expenditure of resources. This has the potential to result in financial savings amounting to $100 billion per year, due to decreased input costs and enhanced crop management.

The main flagship initiative of the “Communication on Boosting Start-ups and Innovation in Trustworthy Artificial Intelligence” [24] is "GenAI4EU", calling for the promotion of generative AI in key strategic industrial ecosystems of the Union and promoting the development of large open innovation ecosystems that will facilitate collaboration between AI start-ups and AI developers in industry and the public sector. Research and development in the areas of AI threat detection, adaptive security measures, regulatory compliance and

automated remediation tools should address the development and testing of generative AI models for threat detection and response, and the creation of tools to ensure compliance with EU and national cybersecurity regulations. Particular attention should be given to AgrofoodTEF Cmart city villages (CitcomAI) testbed projects ensuring robust and responsible AI principles, privacy and compliance with EU policies. Collaboration between academia, SMEs and industry stakeholders to maximize innovation and technological development, including the development of key performance indicators to demonstrate added value for EU regions and countries.

3. Cybersecurity and digital innovation in agriculture

The digital transformation of the agricultural sector brings forth not only considerable opportunities but also emerging cybersecurity risks. In response, international and European regulatory frameworks are evolving to address the specific challenges associated with the digitalization of agricultural systems and machinery.

A key development is the introduction of the **ISO/WD 24882** standard [29] which sets out specifications for the cybersecurity of agricultural machinery. This standard establishes a comprehensive benchmark for ensuring the security, resilience, and operational continuity of smart agricultural equipment throughout its lifecycle - from design and development to deployment, maintenance, and decommissioning. One of its fundamental principles is the implementation of systematic **risk assessments** during early design phases. These assessments allow **original equipment manufacturers (OEMs)** to detect vulnerabilities proactively and apply appropriate mitigation strategies before security threats materialize.

The standard also supports the integration of **automated penetration testing environments,** enabling OEMs to simulate cyberattacks, identify potential system weaknesses, and ensure preemptive protection of embedded technologies. As modern agricultural machinery increasingly incorporates advanced electronic systems for enhanced operational efficiency, the risk landscape evolves accordingly. Malicious cyber activities - such as unauthorized manipulation of machine controls or the exfiltration of operational data - can disrupt entire agri-food value chains.

Within the European context, the proposed **Cyber Resilience Act (CRA)** reinforces the relevance of ISO/WD 24882 as a future global standard. Early adoption will not only position agricultural technology developers for expanded access to the European Single Market but also build trust among stakeholders by demonstrating a high level of cybersecurity compliance. Additionally, the application of **ISO/IEC 27001** [30] in the agri-food domain offers several strategic benefits:

- **Enhanced data protection** through compliance with security controls;
- **Regulatory compliance** with national and EU data protection legislation, reducing exposure to legal and financial risks;
- **Improved stakeholder confidence**, as certification evidences a strong commitment to information security management.

From a broader strategic perspective, the European Union is actively supporting the integration of advanced digital technologies in agriculture through a portfolio of programs

and funding instruments. Figure 5 illustrates how **research and innovation (R&I) activities** are connected with **deployment-oriented actions**, ensuring that digital solutions are scaled efficiently and reach market actors and end users.

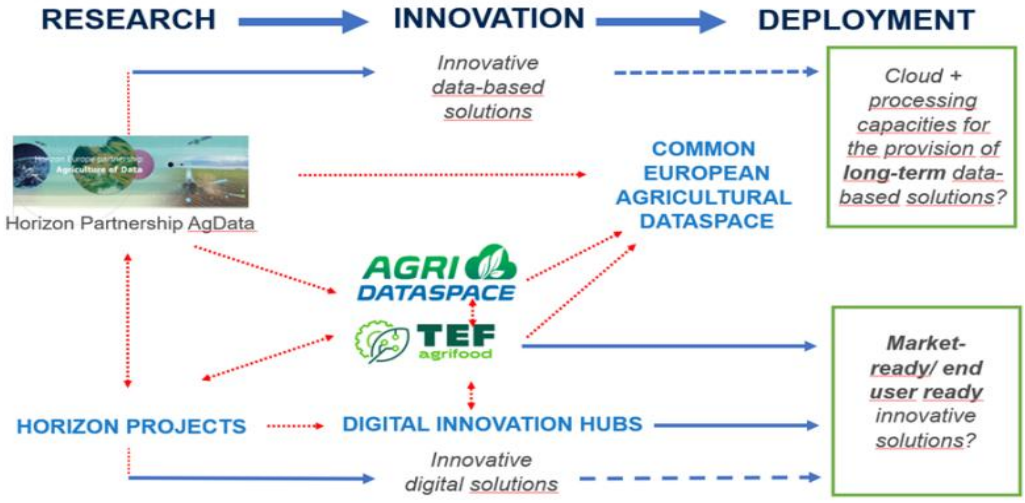

Fig. 5. A strategic approach towards bringing research and innovation to deployment stage in the field of digitalization in agri-food. Source: [31]

Key initiatives include:

- **Horizon Europe** research projects focused on smart farming and data-driven innovation [32]:
- The **Agriculture of Data partnership** under Horizon Europe [33];
- **Testing and Experimentation Facilities (TEF)** for artificial intelligence in the agri-food sector [34];
- The establishment of **European Digital Innovation Hubs (EDIHs)** [35];
- The **Pan-European Agricultural Data Space**, which supports cross-border data sharing and interoperability [36];

These initiatives are complemented by policy mechanisms under the **Common Agricultural Policy (CAP),** which aim to strengthen digital skills and infrastructure at the farm level, thus ensuring that technological innovation is inclusive, secure, and scalable across Europe's rural regions.

In the 1990s, there were several barriers to accessing and utilizing spatial data and information needed for environmental management and policy making in Europe. These included different data policies, encodings, formats and semantics, to name a few. Data were collected and applied for specific domain-specific use cases and no standards existed, affecting the reusability of such public sector data. To unlock the potential of spatial data and improve evidence-based EU environmental policy making, action was required at all levels (local, regional, national, European) to implement better data and information management for policy making and data provision for the benefit of citizens [37]. The INSPIRE Directive, Infrastructure for Spatial Information in Europe, directly addresses this

set of problems. It brings together both a legal and technical framework for EU Member States to make relevant spatial data accessible and reusable. In particular, this means that data should be discoverable and interoperable through a common set of standards, data models of development regions, localities in the Republic of Moldova and internet services. Therefore, looking at the best practices that INSPIRE offers to those interested in federated and federated approaches to cross-border and cross-regional geospatial data sharing and semantic interoperability across borders, European researchers propose a decentralized approach [38] to cybersecurity that evolves through the experience of collaborative research and the selection of interested organizations (cluster initiatives) that provide the necessary capabilities to enhance cybersecurity.

This approach enhances cybersecurity and protects spatial data, including the following:

- Data protection: Spatial data such as geographic, cartographic, cadastral and other resources are strategically important for effective territorial management and decision-making. Protecting this data from unauthorized access, loss and damage is of paramount importance.
- Maintaining confidentiality: Spatial data may contain information that may be sensitive, such as information about private property, infrastructure, ecosystems. Ensuring the confidentiality of such data is an important aspect to prevent information leakage or misuse.
- Network threats and vulnerabilities: Spatial data infrastructure often uses distributed systems and cloud technologies. This creates additional cybersecurity risks, such as the possibility of attacks on servers, hacking of data transfer protocols, etc. Measures to protect against such threats, such as data encryption, the use of multi-level authentication, threat monitoring, and the implementation of attack protection tools (e.g. DDoS), are critical to the resilience of the infrastructure.
- Regulation and compliance with standards: It is important that spatial data systems comply with international cybersecurity standards as well as national regulations and laws. This will help prevent legal risks and ensure interoperability with other countries and organizations.

Cross-border interoperability of information systems assumes:

- Unified security standards and protocols: In order to exchange spatial data efficiently and securely between countries, it is important to implement agreed protocols and security standards. This includes the use of cryptographic protection methods, compatibility with international data protection systems (e.g. GDPR for the EU).
- Cross-border data exchange [39]. Regulating data exchange between various public and private organizations from different countries requires the development of a unified cybersecurity policy. For example, in the context of the exchange of geographic and cadastral data between Moldova and neighboring countries (Romania, Ukraine, etc.) it is necessary to take into account the risks of data leaks, and in the event of incidents, have mechanisms for rapid response and coordination.
- Interoperability of information systems: To ensure smooth and secure interaction between national and international information systems, compatibility of software

and hardware that support cybersecurity is necessary, as well as the development of common standards for authentication and access authorization.

- Incident Management and Response: Cyber attacks can originate not only from within a country but also from outside its borders. In this context, it is important to establish joint systems for monitoring and quickly responding to security incidents such as cyber attacks, virus threats, and intrusion attempts. National and cross-border incident response centers Computer Security Incident Response Teams (CSIRTs) [40] can play an important role in such coordination.

4. Conclusions

Rural communities possess significant potential for sustainable development through effective digital transformation and the implementation of robust cybersecurity measures. The integration of digital technologies in agriculture and cross-sectoral coordination opens new pathways to enhance productivity, sustainability, and socio-economic resilience. However, to unlock this potential in the Republic of Moldova, it is imperative to address current systemic barriers and ensure equitable access to digital resources and knowledge.

This requires coordinated action in the following key areas:

1. Addressing Context-Specific Cybersecurity Challenges: Rural regions face distinct vulnerabilities, including limited access to modern technologies, low levels of digital literacy, and constrained financial capacity. These factors increase exposure to cyber threats and hinder overall resilience.
2. Expanding Cybersecurity Education and Awareness: Tailored educational initiatives must be developed to foster digital competence across all age groups. Promoting a culture of cyber hygiene is essential to mitigating risks and enhancing community preparedness.
3. Modernizing Digital Infrastructure: Targeted investments in critical infrastructure, such as utilities, healthcare, and agricultural facilities, are necessary to strengthen cyber-resilience and ensure uninterrupted service delivery.
4. Enhancing Policy and Regulatory Support: The establishment of supportive legislative frameworks, including financial incentives and regulatory standards for cybersecurity in rural environments, is crucial to facilitate adoption.
5. Building Local Cyber Support Networks: The formation of decentralized, community-based cyber response units can improve incident response times and provide vital recovery assistance.
6. Deploying Innovative Technologies: Advanced technologies such as blockchain and generative AI can bolster data integrity, transparency, and privacy, supporting the development of secure digital ecosystems.
7. Securing Spatial Data Infrastructure and Cross-Border Coordination: Ensuring the cybersecurity of spatial data systems is critical for protecting sensitive information and enabling effective collaboration between national and international stakeholders in areas such as territorial governance, environmental monitoring, and infrastructure planning.

In summary, a multi-dimensional strategy encompassing education, infrastructure, technology, and governance is essential for fostering a cyber-secure and digitally empowered rural development model in the Republic of Moldova.

References

[1] European Commission, "The Digitalisation of the European Agricultural Sector. Shaping Europe's digital future," 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/digitalisation-agriculture.

[2] CORDIS, "Unleashing the full potential of smart agriculture," 2025. [Online]. Available: https://www.cordis.europa.eu/article/id/413531-unleashing-the-full-potential-of-smart-agriculture .

[3] EU, "A long-term Vision for the EU's Rural Areas - Towards stronger, connected, resilient and prosperous rural areas by 2040," 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0345 .

[4] JRC EU Commission, "Developments of economic growth and employment in bioeconomy sectors across the EU," [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC120390 .

[5] EU Commission, "The Digitalisation of the European Agricultural Sector," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/digitalisation-agriculture.

[6] EU Commission, "Policy brief – Rolling out the Common European Agricultural Data Space (CEADS)," [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/policy-brief-rolling-out-common-european-agricultural-data-space.

[7] EU Commission, "AgriDataSpace project," [Online]. Available: https://agridataspace-csa.eu/.

[8] EU Commission, "The future of farming relies on research, innovation and capacity building in the agri-food sector funded through multi-financial framework initiatives," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/future-farming.

[9] EU Commission, "Data Act explained," [Online]. Available: https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained# .

[10] FAO UN, "EU Code of conduct on agricultural data sharing by contractual agreement," 2024. [Online]. Available: https://www.fao.org/family-farming/detail/en/c/1370911/.

[11] JRC EU Commission, "Food and Water Systems in the Intelligent Age," 2024. [Online]. Available: https://knowledge4policy.ec.europa.eu/publication/food-water-systems-intelligent-age_en .

[12] EU Commission, "Accelerating the green transition: The need for cross-sectoral integration," 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/accelerating-green-transition-role-digital-infrastructures-decarbonising-energy-and-mobility .

[13] EU Commission, "Accelerating the green transition: The concept of the Digital Spine," [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/accelerating-green-transition-role-digital-infrastructures-decarbonising-energy-and-mobility. [Accessed 10 07 2024].

[14] EU Commission, "GenAI4EU: Creating European Champions in Generative AI," [Online]. Available: https://eic.ec.europa.eu/eic-funding-opportunities/eic-accelerator/eic-accelerator-challenges-2025/genai4eu-creating-european-champions-generative-ai_en. [Accessed 2025].

[15] Lucia Stanham CrowdStrike, "Generative AI (GENAI) in cybersecurity," 25 11 2023. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/generative-ai/.

[16] "How Generative AI is Transforming Agriculture: From Precision Farming to Virtual Agronomists," [Online]. Available: https://www.ai4vet4ai.eu/news/how-generative-ai-is-transforming-agriculture-from-precision-farming-to-virtual-agronomists/. [Accessed 01 10 2024].

[17] S. Shahriar, M. G. Corradini , S. Sharif, M. Moussa and R. Dara, "The role of generative artificial intelligence in digital agri-food," [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666154325001589 .

[18] "European approach to artificial intelligence," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence .

[19] European Council, "European Green Deal," [Online]. Available: https://www.consilium.europa.eu/en/policies/european-green-deal/. [Accessed 17 06 2024].

[20] EU Commission, "The twin green & digital transition: How sustainable digital technologies could enable a carbon-neutral EU by 2050," [Online]. Available: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/twin-green-digital-transition-how-sustainable-digital-technologies-could-enable-carbon-neutral-eu-2022-06-29_en. [Accessed 29 06 2022].

[21] "Towards a green, digital and resilient economy: our «European Growth Mode," [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1467. [Accessed 2 03 2022].

[22] EU, "Future Cyber-security Demands in Modern Agriculture," [Online]. Available: https://ercim-news.ercim.eu/en123/r-i/future-cyber-security-demands-in-modern-agriculture.

[23] EU, "Horizon Europe project “Aggregate Farming in the Cloud”," Horizon Europe project, [Online]. Available: http://www.afarcloud.eu/about-the-project/.

[24] "IoT : unlocking the potential of precision farming," [Online]. Available: https://www.nokia.com/about-us/newsroom/articles/iot-unlocking-the-potential-of-precision-farming/.

[25] EU, "Networks of Excellence: A community of AI & Robotics researchers," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/networks-excellence-ai-robotics-researchers#. [Accessed 04 12 2024].

[26] EU, "Sectorial AI Testing and Experimentation Facilities under the Digital Europe Programme," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/testing-and-experimentation-facilities. [Accessed 21 2 2025].

[27] EU, "AI Act, Article 57: AI Regulatory Sandboxes," [Online]. Available: https://artificialintelligenceact.eu/article/57/.

[28] EU, "CitCom. AI drives public-private collaboration in Artificial Intelligence to transform cities," [Online]. Available: https://citcom.ai/. [Accessed 2025].

[29] ISO 24882, [Online]. Available: https://dissec.to/regulations/cybersecurity-in-agriculture-iso-24882/#.

[30] ISO 27001, [Online]. Available: https://www.isms.online/sectors/iso-27001-for-the-agriculture-and-farming-industry/.

[31] EU, "European Testing and Experimentation Facilities (TEF) for AI in agri-food," [Online]. Available: https://agrifoodtef.eu/?trk=public_post-text.

[32] EU, "Digital transformation in agriculture and rural areas," [Online]. Available: https://agriculture.ec.europa.eu/document/download/4a31711f-3235-4b8a-9f58-9cfa67bdba6a_en?filename=factsheet-agriresearch-digital-transformation_en.pdf.

[33] EU, "Agriculture of Data," European Partnership, [Online]. Available: https://research-and-innovation.ec.europa.eu/system/files/2023-08/AgData%20SRIA%20final_version.pdf. [Accessed 18 03 2023].

[34] EU, "European Testing and Experimentation Facilities (TEF) for AI in agri-food," [Online]. Available: https://agrifoodtef.eu/?trk=public_post-text.

[35] EU, "The Regional Digital Hub created to give industrial SMEs in the Grand Est region easier access to AI and cybersecurity technologies," [Online]. Available: https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue/edih-ge-website.

[36] EU, "Policy brief – Rolling out the Common European Agricultural Data Space," [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/policy-brief-rolling-out-common-european-agricultural-data-space. [Accessed 23 09 2024].

[37] EU, "Establishing common ground through INSPIRE: the legally-driven European Spatial Data Infrastructure," Joint Research Center EU Commission, [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC107636. [Accessed 10 07 2018].

[38] EU, "Decentralized Cyber Security Operations Centre (DCSOC) for Public Administrations," [Online]. Available: https://www.interregeurope.eu/project-ideas/decentralized-cyber-security-operations-centre-dcsoc-for-public-administrations.

[39] EU, "A new data hub for border regions within the EU," [Online]. Available: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/new-data-hub-border-regions-within-eu-2024-12-12_en. [Accessed 12 12 2024].

[40] EU Commission, "NIS2 Directive: new rules on cybersecurity of network and information systems," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.