DOI: 10.55643/ser.2.60.2026.676

Serhiy Podosynnikov
PhD Student, SEO, SENCI LCC, Sumy, Ukraine;
ORCID: 0009-0006-3786-5907

Dmytro Halynskyi
PhD Student, SEO, WELLNES-KARPATIA Ltd, Shaian, Ukraine;
e-mail: halynskiy.d@ukr.net
ORCID: 0009-0004-9035-188X
(Corresponding author)

Received: 23/01/2026
Accepted: 11/04/2026
Published: 27/05/2026

CYBER RESILIENCE AS A NEW REQUIREMENT FOR GREEN STARTUPS

ABSTRACT

The article addresses the growing importance of cyber resilience for green startups operating at the intersection of digital technologies and the energy sector. The purpose of the research is to theoretically substantiate cyber resilience as a key requirement for green startups and to reveal its content in the context of their functioning and development in a digitalised energy environment. The study relies on a systems approach, logical-structural analysis, abstraction, generalisation, and interpretation to conceptualise cyber resilience not only as a technical property of digital infrastructure but also as a systemic characteristic of entrepreneurial activity.

The principal results show that cyber resilience is a distinct condition for the viability of green startups, as disruptions to digital platforms, monitoring systems, and data processing simultaneously affect economic performance, ecological impacts, and stakeholders' trust. Second, the paper proposes treating cyber resilience as a multidimensional construct encompassing technological, organisational, human, institutional, ecosystem, financial, reputational, and strategic dimensions, each with its own tasks, actors, and specific challenges for green startups. Third, it is demonstrated that cyber resilience acts as a transversal dimension of the business model, influencing value proposition, key resources and partnerships, channels and customer relations, cost structure and revenue streams. Furthermore, the analysis shows how the requirements of regulators, energy companies, investors, cybersecurity clusters, and end-users shape the conditions for integrating startups into energy systems and innovation ecosystems.

The main conclusions are that cyber resilience should be regarded as an integral requirement complementing traditional criteria of ecological and economic performance in green entrepreneurship, and that the proposed conceptual framework can serve as a basis for future empirical assessments of green startups and for designing policies and support programmes that jointly promote green transition, digitalisation, and resilience in the energy sector.

Keywords: green startups, cyber resilience, digitalisation, energy entrepreneurship, business models, sustainable energy, critical infrastructure, stakeholders, entrepreneurial ecosystems

JEL Classification: L26, O33, Q40

INTRODUCTION

The development of green startups is accompanied by a growing reliance on digital technologies, data, and connectivity to energy infrastructure. Digital platforms, the Internet of Things, cloud services, and data analytics are becoming integral components of solutions across renewable energy, energy efficiency, and demand management. Under such conditions, disruptions in the operation of digital systems directly affect not only financial performance but also the ability to fulfil declared environmental objectives, ensure the continuity of "green" services, and maintain consumer and partner trust.

At the same time, the intensity and complexity of cyber threats targeting energy and infrastructure facilities, as well as digital platforms and services, are increasing. Startups operating at the intersection of green energy and digital technologies find themselves in a situation where any disruptions in cyberspace can lead to the failure of energy services, deterioration of environmental indicators, and loss of access to markets or

partnerships. Under these circumstances, the ability to maintain operations, adapt, and recover in the face of cyber incidents becomes an inherent characteristic of the viability of green startups.

Cyber resilience, understood in this way, acts not only as a technical property of digital infrastructure but also as a systemic characteristic of entrepreneurial activity that influences the design of business models, the organisation of processes, the choice of partners, and the modes of interaction with the energy system. For green startups, this means the need to combine an environmental orientation with requirements for the reliability and security of digital solutions, thereby forming a comprehensive vision of resilience. Consequently, the study of cyber resilience as a new requirement for green startups is important for understanding the conditions for the functioning and development of entrepreneurship in the modern green and digitalised energy environment.

LITERATURE REVIEW

Green entrepreneurship is currently regarded as one of the key mechanisms for the transition to a circular and low-carbon economy, in which business models combine economic performance with reduced environmental impact, particularly in waste management and energy efficiency (Mondal et al., 2023; OECD, n.d.). In this context, digitalisation emerges not as an auxiliary tool but as a factor shaping new formats of 'green' solutions: the use of data, digital platforms and services is changing how value is created, delivered and captured in the energy sector and related industries (Ren & Xia, 2024; Hogan et al., 2019; Moeve, n.d.; European Commission, 2025).

The development of digital energy entrepreneurship is accompanied by the emergence of new ecosystems in which startups interact with energy companies, investors, and innovation programmes, offering solutions based on platforms, data, and demand-side management services (Hogan et al., 2019; EIT, 2025; Ren & Xia, 2024). At the policy level, this is combined with the EU's orientation towards a synchronous 'green' and digital energy transition, where investments in digital infrastructure and innovative business models are considered as part of the implementation of climate goals and the strengthening of energy security (European Commission, 2020; European Commission, 2025).

In the field of cybersecurity and cyber resilience, an understanding is emerging that protecting energy systems and related digital services is a component of energy security and the overall resilience of infrastructure. Regulatory and analytical documents outline requirements for protecting critical infrastructure, incident management, and maintaining the continuity of energy supply, emphasising the role of technical, organisational, and managerial measures (Lazari, 2025; World Economic Forum, 2025; ENISA, n.d.). Various cyber resilience assessment frameworks have been proposed, and analyses of threat scenarios and possible approaches to their neutralisation have been conducted in the context of energy, renewable sources, virtual power plants, energy management systems, and IoT infrastructure (Sepúlveda Estay et al., 2020; Safitra et al., 2023; Halgamuge, 2024; Korukonda et al., 2025; Mehmood et al., 2023; Haque et al., 2019; Zhao et al., 2021; Shabanian-Poodeh et al., 2025; Eze et al., 2024).

At the same time, in studies on small and medium-sized enterprises, the emphasis is placed on resource constraints, insufficient formalisation of cyber risk management processes, and the need for adapted tools to assess and enhance the cyber resilience of entrepreneurial structures. Approaches to assessing security maturity in digital SMEs, models for operationalising cyber resilience, as well as organisational factors related to leadership, security culture, and personnel awareness are described (Alahmari & Duncan, 2020; Yigit Ozkan & Spruit, 2023; Carías et al., 2020; Hausken, 2020; Mmango & Gundu, 2023; Al-Momani et al., 2024; Abu Al-Haija & Hammad, 2025; Taherdoost, 2026). Within the domain of energy entrepreneurship, attention is drawn to the link between the development of electrical and renewable energy businesses, self-employment, and the need to counter cybercrime, as well as the resilience of small enterprises to crises in the energy environment (Odika, 2025; Apostolopoulos et al., 2024). In parallel, a direction focused on small and medium-sized enterprises and the entrepreneurial environment is developing.

The totality of these developments forms a basis for combining three analytical directions – green entrepreneurship, the digital transformation of energy and the cyber resilience of entrepreneurial structures – which opens up the possibility for a targeted study of the cyber resilience of green startups specifically as participants in the energy and digital transition (Mondal et al., 2023; Hogan et al., 2019; Ren & Xia, 2024; Lazari, 2025; World Economic Forum, 2025). Thus, existing studies provide an important foundation for analyzing digital green entrepreneurship, the cyber resilience of energy systems, and the cyber resilience of entrepreneurial structures. Still, they require further development in integrating these approaches to green startups, which are simultaneously participants in the energy transition and digital innovation ecosystems (Mondal et al., 2023; Hogan et al., 2019; Ren & Xia, 2024; Lazari, 2025; World Economic Forum, 2025). In particular, several important questions remain unresolved, among which are: the absence of a holistic conceptual vision of cyber resilience specifically for green startups that are simultaneously involved in the energy transition and digital

DOI: 10.55643/ser.2.60.2026.676

innovation ecosystems; the nature of the impact of cyber resilience requirements on the logic of green startup business models; the lack of research into the mechanisms by which cyber resilience requirements are formed through the interaction of various stakeholder groups and their influence on the conditions of entry and operation of startups in energy markets; the study of the relationship between the level of cyber resilience of green startups and the long-term results of their activities, in particular the ability to scale the business, ensure the stability of environmental effects and maintain stakeholder trust in the face of growing cyber threats.

AIMS AND OBJECTIVES

To provide a theoretical substantiation of cyber resilience as an important requirement for green startups and to reveal its content in the context of the functioning and development of entrepreneurship in a digitalised energy environment.

Research objectives:

1. To reveal the essence of cyber resilience as a characteristic of entrepreneurial activity related to the maintenance of operations under cyber incident conditions.
2. To explain why cyber resilience is a distinct requirement for green startups that combine environmental orientation and digital infrastructure.
3. To outline the main dimensions of cyber resilience of green startups (technological, organisational, human, institutional, ecosystem) in connection with the specifics of their activities.
4. To demonstrate how the requirement of cyber resilience influences the design and implementation of business models of green startups, as well as their interaction with the energy environment and stakeholders.

METHODS

The study is of a theoretical-conceptual nature and relies on a combination of general scientific and specialised methods of inquiry. The foundation is the systems approach, which enables consideration of green startups as elements of an entrepreneurial and energy system that combine an environmental orientation, digital infrastructure, and resilience requirements. Logical-structural analysis is used to sequentially disclose the content of key concepts and identify links between digitalisation, cyber resilience, and the specificities of green startups' functioning.

The method of abstraction is applied to isolate cyber resilience as a separate analytical category, to distinguish it from the totality of cybersecurity technical aspects, and to shift the emphasis to the entrepreneurial dimension. Generalisation and interpretation are used to develop a holistic understanding of the cyber resilience requirements of green startups for their business models and interactions with the energy environment. By combining the aforementioned methods, a conceptual framework of the main dimensions of cyber resilience for green startups and their place within the structure of modern green entrepreneurship is developed.

RESULTS

The development of green entrepreneurship is associated with the search for business models that simultaneously ensure economic performance and reduce the negative impact on the environment, supporting the transition to a circular and low-carbon economy (Mondal, 2023; OECD, n.d.). This type of entrepreneurship encompasses the creation and scaling of solutions in the fields of renewable energy, energy efficiency, waste management, and the decarbonisation of production and consumption (Mondal, 2023; OECD, n.d.). Within this approach, startups are viewed as important actors capable of experimenting with new technologies and organisational forms that accelerate the green transition of the energy sector and other industries (Mondal, 2023; Ren, 2024).

Modern green startups increasingly build their solutions on digital technologies – from the Internet of Things and sensor networks to digital platforms, cloud services, and big data analytics (Hogan et al., 2019; Ren, 2024; Mondal, 2023). In the energy sector, this manifests as the development of digital energy, where software, optimisation algorithms, new energy data streams, and demand-supply management platforms play a central role in value creation (Hogan et al., 2019; Ren, 2024). Digitalisation makes it possible to increase resource efficiency, optimise operational processes, and support more flexible integration of renewable energy sources into the energy system (Ren, 2024; Moeve, n.d.).

For green startups, the digital components of business models become not merely an auxiliary tool but also a key source of differentiation and scalability. Access to data on energy production and consumption, the ability for remote monitoring, the use of optimisation algorithms and digital platforms for interaction with consumers create conditions for the emergence of new service formats, including virtual power plants, flexible demand management services, and digital solutions for energy efficiency in buildings and industry (Hogan et al., 2019; Ren, 2024; European Commission, 2025). At the same time, such digital 'saturation' means that the resilience of green startups depends on the reliability and security of the digital infrastructure through which energy and related services are delivered (Hogan et al., 2019; Ren, 2024; European Commission, 2020).

The digitalisation of the energy sector does not occur in isolation but in the context of broader shifts in entrepreneurial ecosystems emerging around digital and energy innovations. Studies of digital energy entrepreneurship show that the combination of energy technologies and digital solutions stimulates the emergence of new participants, forms of partnership, and support mechanisms – such as accelerators, incubators, and specialised investment programmes (Hogan et al., 2019; EIT, 2025). In such ecosystems, green startups act as carriers of innovation but at the same time depend on the conditions under which the digital and energy transition takes place, including requirements for the protection of critical infrastructure and the reliability of digital services (Hogan et al., 2019; European Commission, 2020; World Economic Forum, 2025).

As a result, the digital dimension of green startups' activities becomes an important prerequisite for their contribution to the green transition and, at the same time, a source of specific challenges. On the one hand, digital technologies support the 'greening' of the energy sector by increasing the efficiency, flexibility and transparency of energy services (Ren, 2024; Moeve, n.d.; European Commission, 2025); on the other hand, dependence on digital platforms, networks and data makes green startups sensitive to disruptions in cyberspace, which raises the question of what resilience requirements should be taken into account in the design of their business models and interaction with the energy environment (Hogan et al., 2019; European Union Agency for Cybersecurity, 2023; World Economic Forum, 2025).

The increasing reliance of energy systems on information and communication infrastructure and network services is accompanied by the spread of digital technologies in the energy sector. This means that breaches of the confidentiality, integrity, or availability of data and digital resources can have direct consequences for the continuity of energy supply, the reliability of energy services, and consumer safety (European Commission, 2020). In response, European energy policy is developing an approach in which cyber protection is viewed as a component of overall energy security and the resilience of energy systems, in particular through regulation focused on critical infrastructure and digital energy networks (European Commission, 2020; Lazari, 2025).

Under these conditions, the concept of cyber resilience extends the traditional understanding of cybersecurity. Whereas cybersecurity primarily focuses on preventing unauthorised access and reducing the likelihood of incidents, cyber resilience emphasises a system's ability to maintain critical functions, adapt to disruptions, and recover after attacks or failures (Lazari, 2025; World Economic Forum, 2025). In studies on the energy sector, cyber resilience is understood as a combination of technical, organisational, and managerial measures that ensure the continuity of energy services even under targeted cyberattacks or complex crises (Lazari, 2025; ENISA, n.d.).

In the entrepreneurial context, cyber resilience extends beyond the purely technical characteristic of IT infrastructure. It also concerns the construction of risk management processes, decision-making, organisational culture, and stakeholder interactions. For companies operating in digital and innovative ecosystems, the ability to ensure service stability, incident management transparency, and data reliability becomes an important factor in building trust with clients, partners, and investors (World Economic Forum, 2025). In this understanding, cyber resilience can be viewed as an element of broader organisational resilience that combines technological solutions, managerial approaches, and the human factor.

In the energy sector, the issue of cyber resilience has an additional dimension: energy networks and facilities are classified as critical infrastructure. European approaches emphasise that the digitalisation of the energy sector – in particular, the development of smart grids, smart metering, decentralised management systems and integrated digital platforms – reinforces the need for modes of operation that allow the system to remain functional even under conditions of partial failures or disruptions (European Commission, 2020; Lazari, 2025). Cyber resilience in this case involves not only preventing attacks but also developing response scenarios, redundancy, recovery procedures, and coordinating among various participants in the energy system (Lazari, 2025; ENISA, n.d.).

In combination with entrepreneurial activity oriented towards 'green' solutions, cyber resilience acquires a meaning that goes beyond the technical function of information security. For businesses offering digital energy services, consumption management platforms, solutions for decentralised generation or digital support for renewable energy sources, the loss of

DOI: 10.55643/ser.2.60.2026.676

service availability or the corruption of data may signify not only financial losses but also the undermining of environmental outcomes and the impact on the energy transition (Hogan, Wittenberg, & O'Neill, 2019; World Economic Forum, 2025). Therefore, the requirement to maintain the ability to function under cyber incident conditions becomes an inherent characteristic of business models that aspire to serve as elements of a resilient and low-carbon energy system (Hogan et al., 2019; Lazari, 2025).

This approach to cyber resilience lays the foundation for its analysis as an important requirement not only for large energy companies and network operators but also for small entrepreneurial structures, particularly startups, that integrate into the energy ecosystem through digital solutions. It makes it possible to view the cyber resilience of green startups as a characteristic that combines the technological state of their digital components, the organization of risk management, team competencies, and interaction with the regulatory environment and partners (Hogan et al., 2019; ENISA, n.d.; World Economic Forum, 2025).

The distinctive feature of green startups is that they combine an environmental orientation with the active use of digital technologies and integration into energy infrastructure. It means that their products and services simultaneously influence environmental outcomes and depend on the stability of the digital environment through which these outcomes are achieved. Under such conditions, any disruptions in the operation of digital components – platforms, sensor networks, control systems, analytical services – are reflected not only in economic indicators but also in the startup's actual contribution to the energy transition and the fulfillment of 'green' objectives.

It gives rise to a transition from viewing security as an auxiliary technical function to viewing cyber resilience as a fundamental requirement for how a green business is organized. For startups working with renewable energy sources, intelligent metering systems, flexible demand management, and digital energy efficiency services, the ability to maintain service delivery under cyber incident conditions is a requirement for participation in the energy market and for interacting with partners. In other words, the environmental orientation loses its practical meaning if the startup's solution cannot ensure reliability, predictability, and operational continuity in the digital environment.

At the business model level, this means that cyber resilience must be taken into account from the outset in designing the value proposition, determining key resources and partners, and defining the architecture of consumer interaction channels. For a green startup offering a digital energy service, the ability to maintain platform operations, protect and correctly process data, anticipate failure scenarios, and have recovery mechanisms is not an external add-on but an integral part of the quality of the core product. Therefore, the requirement for cyber resilience effectively becomes one of the characteristics of competitiveness – it influences perceptions of the solution's reliability, the readiness of energy system participants to integrate it into their own processes, and the startup's ability to scale.

The systemic inclusion of cyber resilience in the field of attention of green startups is also related to the fact that they operate in an environment where the expectations of other participants – regulators, investors, energy companies, consumers – are gradually changing. When digitalization becomes a fundamental condition for the energy sector's functioning, the requirement for the reliability and resilience of digital services ceases to be selective: it becomes a criterion for admission to cooperation, financing, and participation in innovation programmes. For green startups, this means that their perception as responsible, 'future-oriented' participants in the energy transition depends on the extent to which their solutions can remain operational amid cyber threats and digital disruptions.

In summary, cyber resilience can be seen as a new requirement for green startups, complementing the traditional criteria of environmental performance and economic efficiency. It establishes that in a digitalized energy environment, the resilience of entrepreneurial activity is determined not only by the ability to offer environmentally oriented innovations but also by the capacity to ensure their reliable implementation through digital infrastructure. This approach lays the foundation for further identification of the key dimensions of cyber resilience for green startups and for analyzing how these dimensions are integrated into their business models and their interactions with the energy ecosystem.

The cyber resilience of green startups should also be viewed as a multidimensional characteristic that encompasses not only the technical design of digital infrastructure but also the organisation of processes, team competencies, interactions with the institutional environment, and the startup's place in the entrepreneurial and energy ecosystem. This approach is consistent with the interpretation of cyber resilience in the energy sector as a combination of technical and managerial solutions necessary to maintain the continuity of critical functions (European Commission, 2020; Lazari, 2025; ENISA, n.d.).

Given that the cyber resilience of green startups is not a separate technical function but a set of interrelated dimensions that form the ability to maintain critically important functions in a digitalized energy environment, the further analysis

should focus on revealing the content of these dimensions, beginning with the technological dimension as the foundational level of constructing the digital infrastructure of a green startup.

The technological dimension concerns the startup's digital infrastructure: the architecture of software solutions, the use of cloud services, network connections, sensor devices, and data storage and processing systems. In the energy context, this encompasses digital platforms for energy consumption management, monitoring systems for renewable energy sources, and interfaces for interaction with networks and other participants in the energy system (Hogan et al., 2019; European Commission, 2020). To ensure cyber resilience, the principles of secure design, vulnerability management, network segmentation, redundancy of critical components, and the availability of recovery mechanisms after failures are important (Lazari, 2025; ENISA, n.d.).

In green startups, the technological dimension has a dual significance: on the one hand, digital infrastructure is an instrument for achieving environmental outcomes; on the other hand, its vulnerability to cyberattacks can negate these outcomes. Therefore, the question of the level of protection of platforms, the reliability of sensor networks, the integrity of data, and the ability of the system to recover after incidents is an integral part of constructing the technological foundation of 'green' business models (Hogan et al., 2019; European Commission, 2020; Lazari, 2025).

The organisational dimension concerns how risk management, planning processes, monitoring, incident response, and recovery are structured within the startup. In studies of the cyber resilience of energy companies, it is emphasised that, even with technical solutions in place, the absence of established procedures, roles, and responsibilities significantly reduces the organisation's ability to withstand cyberattacks (Lazari, 2025; ENISA, n.d.). For startups, this is particularly relevant given limited resources and small teams, where technical, managerial, and entrepreneurial functions are often combined.

Organisational cyber resilience includes designating those responsible for the security and resilience of digital services, establishing basic backup procedures, conducting recovery testing, and documenting key processes and incident response scenarios. For green startups operating in the energy sector, this may also mean aligning their procedures with the requirements of partners – network operators, energy companies, and support programmes (European Commission, 2020; Lazari, 2025).

The human dimension of cyber resilience concerns the competencies, behaviour, and motivation of team members, as well as how perceptions of the role of security and resilience in digital solutions are formed within the startup. In small entrepreneurial structures, where a single specialist may combine several roles, the risk of errors or procedural neglect is particularly high.

For green startups, the human dimension of cyber resilience requires basic team training on cyber threats, password management, handling critical data, and detecting suspicious activity. At the same time, it is important to adopt a security mindset not as an external constraint but as a condition for the reliability of the 'green' product, which supports the value proposition for clients and partners (World Economic Forum, 2025). In this sense, cyber resilience acquires a component of organisational culture that influences everyday practices of working with digital tools.

The institutional dimension encompasses normative requirements, industry standards, contractual obligations, and policies that define the framework for the startup's operations in the energy and digital environments. In the European context, the cyber resilience of the energy sector is viewed through the lens of critical infrastructure regulation, incident-reporting requirements, and network and information-system protection standards (European Commission, 2020; CERRE, 2025). For startups that integrate their solutions into energy networks or work with consumer data, this means the need to take relevant norms into account from the outset of service design.

The institutional dimension also includes the requirements imposed by investors, donors, accelerators, and corporate partners regarding risk management, data protection, and service continuity (World Economic Forum, 2025). For green startups aspiring to participate in programmes supporting the 'green' and digital transition, compliance with such requirements may be a condition for access to financing and markets. Thus, cyber resilience acquires significance not only as an internal characteristic of the startup's activity but also as an element of the startup's institutional legitimacy in the eyes of external stakeholders (European Commission, 2020; Lazari, 2025).

The ecosystem dimension reflects the connections of the green startup with other participants in the energy and entrepreneurial ecosystem – energy companies, network operators, innovation clusters, entrepreneurship support centres, and cybersecurity structures. The experience of forming digital and energy innovation ecosystems demonstrates that the ability of individual participants to withstand cyber threats depends to a significant extent on access to shared resources, infrastructures, knowledge, and practices (Hogan et al., 2019; World Economic Forum, 2025).

DOI: 10.55643/ser.2.60.2026.676

For green startups, participation in ecosystems offers the opportunity to rely on shared security standards, leverage partners' experience, engage external cybersecurity solution providers, and participate in training and consultancy programmes. At the same time, this implies responsibility for compliance with agreed rules for the protection of data and infrastructure, since the vulnerability of one participant can affect the resilience of the entire system (European Commission, 2020; ENISA, n.d.). Thus, the ecosystem dimension underscores that the cyber resilience of a green startup is formed not only within the organisation but also through its embeddedness in networks of interaction where norms and practices for responding to cyber threats are jointly produced.

The financial dimension of cyber resilience concerns how the costs of ensuring resilience against cyber threats are incorporated into the green startup's financial model. It concerns not only the acquisition of technical solutions but also the costs of team training, the engagement of external expertise, the implementation of backup and recovery procedures, and the time the team devotes to security and resilience issues. For a startup operating in the field of green energy and digital services, these costs are an integral part of service delivery, even if they do not have a 'visible' effect on the end user.

A distinctive feature of green startups is that they often operate under conditions of limited budgets and high competition for resources between the development of product functionality, environmental innovations, and 'invisible' investments in resilience. Under such conditions, founders must decide how to prioritise expenditures, arguing that financing cyber resilience is a prerequisite for the reliability and long-term viability of the business model. The financial dimension thus reflects the extent to which the startup systematically takes into account resilience to cyber threats in budget planning, risk assessment, and communication with investors and donors.

The reputational and communication dimension of cyber resilience concerns how the green startup forms and maintains stakeholder trust in the context of handling cyber threats and incidents. For startups operating in green energy and digital services, reputation is inextricably linked to perceptions of responsibility, reliability, and transparency. How a company informs clients and partners about potential disruptions, how it responds to incidents, and how honestly and promptly it communicates about consequences and recovery steps influence consumers' readiness to trust its services and continue cooperating.

In this context, cyber resilience manifests itself not only in the technical ability to restore operations but also in communication practices: the availability of clear messages about the status of services, the readiness to explain to users what happened and what measures have been taken to prevent the recurrence of incidents. For green startups, mismanagement of the reputational aspects of cyber incidents can undermine their positive image of environmental responsibility, creating the impression of a discrepancy between declared values and actual practice in their interactions with clients and partners.

The strategic dimension of cyber resilience concerns the role of resilience against cyber threats in the long-term vision for the development of the green startup. It concerns the extent to which cyber resilience issues are taken into account when choosing target markets, technological platforms, scaling models, forms of partnership, and participation in energy and digital ecosystems. For startups operating in regulated domains such as the energy sector and critical infrastructure, strategic underestimation of resilience requirements can limit their ability to enter promising markets or participate in projects with large energy companies.

In the strategic dimension, cyber resilience ceases to be a reactive response to existing threats and becomes a decision-making criterion. Founders must assess whether the chosen technological solutions and architecture provide the necessary level of resilience during scaling, whether the partnership model meets expectations for security and reliability, and whether short-term compromises in cyber resilience create barriers to future development. For green startups, this means the necessity of including cyber resilience in strategic discussions on a par with environmental objectives and market opportunities, viewing it as a key factor in competitiveness in a digitalised energy environment.

The proposed dimensions of cyber resilience for green startups can be viewed as interrelated elements of a holistic conceptual framework that combines the technological, organizational, human, institutional, ecosystem, financial, reputational, and strategic aspects of activity (Table 1). This approach enables avoiding reducing cyber resilience to a purely technical characteristic of digital infrastructure and interpreting it as a multidimensional property of the entrepreneurial system that determines the startup's ability to maintain its operations and fulfil its 'green' mission under conditions of cyber threats and digital disruptions.

ISSN: 2786-5800 | eISSN: 2786-5819 | Том 2 (60), 2026

Table 1. Dimensions of cyber resilience of green startups.

Dimension	Essence	Tasks	Involved Participants	Specificities for Green Startups
Technological	Architecture and state of digital infrastructure: software, platforms, networks, sensors, data storage, communication channels	Ensure secure design of solutions, resilience to failures and attacks, and the ability to recover critical functions	Development team, IT specialists, cloud service providers, equipment suppliers, energy system integrators	High dependence on IoT and platforms in RES; vulnerability of the technical component can disrupt both the digital service and the 'green' effect of the solution
Organisational	System of processes, rules, and areas of responsibility for managing cyber risks, incidents, and business recovery	Form a clear structure of roles and procedures for the timely detection, localisation, and overcoming of the consequences of incidents	Founders, operational management, those responsible for risks and security, and partners imposing organisational requirements	Small teams and limited resources; 'minimalist' yet realistically executable procedures are needed
Human	Competencies, behaviour, and attitudes of team members regarding security and working with digital systems	Increase awareness of threats, reduce the probability of errors, and form a culture of responsible attitudes towards data and access	Founders, developers, analysts, product managers, and users of internal and external tools	Absence of specialised security roles; security knowledge must be 'embedded' in the core competencies of the entire team
Institutional	Norms, regulations, standards, policies, and contractual requirements in the field of energy and digital services	Ensure compliance with requirements for the protection of critical infrastructure, data, incident reporting, and service resilience	Regulators, energy regulatory bodies, support programmes, investors, donors, corporate partners, network operators	Access to markets and support programmes depends on compliance with requirements; these need to be taken into account at the stage of product and business model design
Ecosystem	Embeddedness in energy and innovation ecosystems, clusters, and cybersecurity communities	Utilise shared resources, knowledge, and infrastructure to enhance resilience and coordinate security practices in joint projects.	Energy companies, distribution and transmission system operators, other startups, accelerators, hubs, cybersecurity clusters, platform providers	The vulnerability of one participant can affect the entire ecosystem; participation enhances resilience but imposes requirements for the alignment of practices
Financial	Reflection of cyber resilience costs in the financial model and budgeting of the startup	Integrate resilience costs (infrastructure, expertise, training) into the cost of services.	Founders, financial managers, investors, donors, grant providers, and partners assessing risks	Limited budgets and competition between 'visible' green product functions and 'invisible' resilience costs; justification of such expenditures is required
Reputational / Communication	How the startup communicates resilience issues and incident response to external stakeholders	Maintain trust through transparency, timely communication, and responsible behaviour during disruptions.	Clients, partners, investors, media, user communities, regulators, and monitoring public communications	For 'green' startups, reputation is tied to the image of responsibility; poor incident response can negate the environmental image
Strategic	The place of cyber resilience in the long-term vision for the development of the startup and the choice of growth directions	Embed resilience requirements into decisions regarding markets, scaling, technological platforms, and partnerships.	Founders, strategic investors, boards of directors/advisors, key partners.	Entry into regulated and demanding markets (energy, critical infrastructure) is impossible without strategic consideration of cyber resilience; ignoring it limits scaling potential

The use of a table to describe the dimensions of cyber resilience allows a structured demonstration of how the tasks, the range of involved stakeholders, and the specific challenges for green startups change across each dimension. It facilitates further theoretical analysis and lays the foundation for the development of indicators for empirical studies to assess the level of cyber resilience of startups operating at the intersection of digital technologies and green energy. In this context, it is important to consider how cyber resilience is concretised in the key elements of a green startup's business model and what changes these elements require in light of the resilience requirements for digital solutions.

The integration of cyber resilience into the business models of green startups means taking into account the requirements for the resilience of digital solutions not only at the level of technical implementation but also in the design of the value proposition, the determination of key resources, partnerships, channels of interaction with consumers, and the structure of costs and revenues. In digitalised energy, it is precisely the combination of environmental orientation and the ability to ensure the reliability of digital services that determines whether solutions are perceived as making a real contribution to a sustainable energy transition.

At the level of the value proposition, cyber resilience manifests itself in the promise of not only a 'green' effect (emissions reduction, increased energy efficiency, support for renewable sources) but also the stability, predictability, and security of the digital services through which this effect is achieved. For clients and partners, it is important that monitoring services, consumption management, and platform solutions for integrating distributed generation or flexible demand are available

DOI: 10.55643/ser.2.60.2026.676

and function correctly even in the event of cyber incidents or partial failures. In this sense, cyber resilience becomes a component of product quality: it increases trust in digital energy services and reduces the perception of risk associated with their use.

Key resources in the business model of a green startup include not only technological components (software, sensor infrastructure, cloud services, data) but also organisational and human resources that ensure cyber resilience. These may include team members' competencies in cyber risk management, the availability of basic backup and recovery procedures, the use of external security support services, and access to expertise in the field of cyber protection. From this perspective, investments in cyber resilience are viewed not as 'additional costs' but as expenditures to support key resources without which it is impossible to guarantee the fulfilment of the value proposition.

Partnerships play a special role, as green startups rarely function in isolation from the broader energy and entrepreneurial ecosystem. Interaction with energy companies, network operators, digital platform providers, cloud service providers, cybersecurity clusters, accelerators, and support programmes forms the context in which the business model is implemented. In many cases, cyber resilience requirements are enshrined in contractual relationships, technical specifications, and integration standards: these include, for example, service availability levels, incident notification procedures, and data protection policies. For the startup, this means aligning its internal approaches to cyber resilience with partners' expectations to ensure compatibility and mutual trust.

Channels of interaction with consumers for digital 'green' solutions are also linked to cyber resilience, as it is through these channels that access to services, data transmission and visualization, and communication regarding system operation are provided. The reliability of these channels, the security of user accounts, and the transparency of messages about possible disruptions or incidents influence the perception of the startup as a responsible service provider. When client interaction is conducted entirely through a digital interface, maintaining operability under challenging conditions becomes part of the customer experience and can determine users' readiness to continue cooperating.

The cost and revenue structure of green startups, taking cyber resilience into account, reflects the extent to which founders systematically incorporate resilience issues into the economic logic of their business model. The costs of developing and maintaining a secure architecture, redundancy of critical systems, team training, and engaging external cybersecurity experts can be viewed as components of the cost of delivering resilient digital energy services. On the other hand, the ability to demonstrate a high level of cyber resilience can create additional revenue opportunities through access to more demanding market segments, participation in pilot projects with large energy companies, and attraction of investments oriented towards the combination of 'green' and digital solutions.

In summary, integrating cyber resilience into green startups' business models means that resilience against cyber threats ceases to be a peripheral technical issue and becomes a structural element of entrepreneurial design. It influences how value is created for clients, which resources and partnerships are considered critical, how processes are organised within the startup, and how costs and risks are assessed. This approach makes it possible to view green startups as entities capable not only of generating environmental innovations but also of sustaining their implementation amid instability in the digital environment, a necessary characteristic of modern green entrepreneurship. Accordingly, a generalised vision of integrating cyber resilience into the business model of a green startup is presented in Figure 1, which illustrates how the corresponding resilience dimensions 'permeate' the model's key elements and define the conditions for its implementation in a digitalised energy environment.

The interaction of green startups with the energy environment occurs in a context where the digital infrastructure of the energy system is considered part of critical infrastructure, and ensuring its resilience to cyber threats is an element of energy security (European Commission, 2020; CERRE, 2025). For startups whose solutions are integrated into metering systems, network management, demand-supply balancing platforms or consumer services, this means that the requirement of cyber resilience is formed not only 'from within' the business model but also 'from outside' – through rules of access to infrastructure, technical conditions for connection, data exchange standards and the expectations of other participants in the energy system (European Commission, 2020; ENISA, n.d.).

In interaction with energy companies and network operators, cyber resilience becomes a condition for the technical and organisational integration of the startup's solutions. Requirements for the level of communication channel protection, authentication, event logging, and incident response procedures are often enshrined in contracts, technical specifications, and partner security policies (Lazari, 2025; ENISA, n.d.). For a green startup, this means that the lack of sufficient cyber resilience can not only create risks of disruption but also effectively preclude access to joint projects, pilots, or commercial operations in the energy environment. Thus, the requirement for cyber resilience shapes the configuration of partnerships and the roles the startup can play in the energy ecosystem.

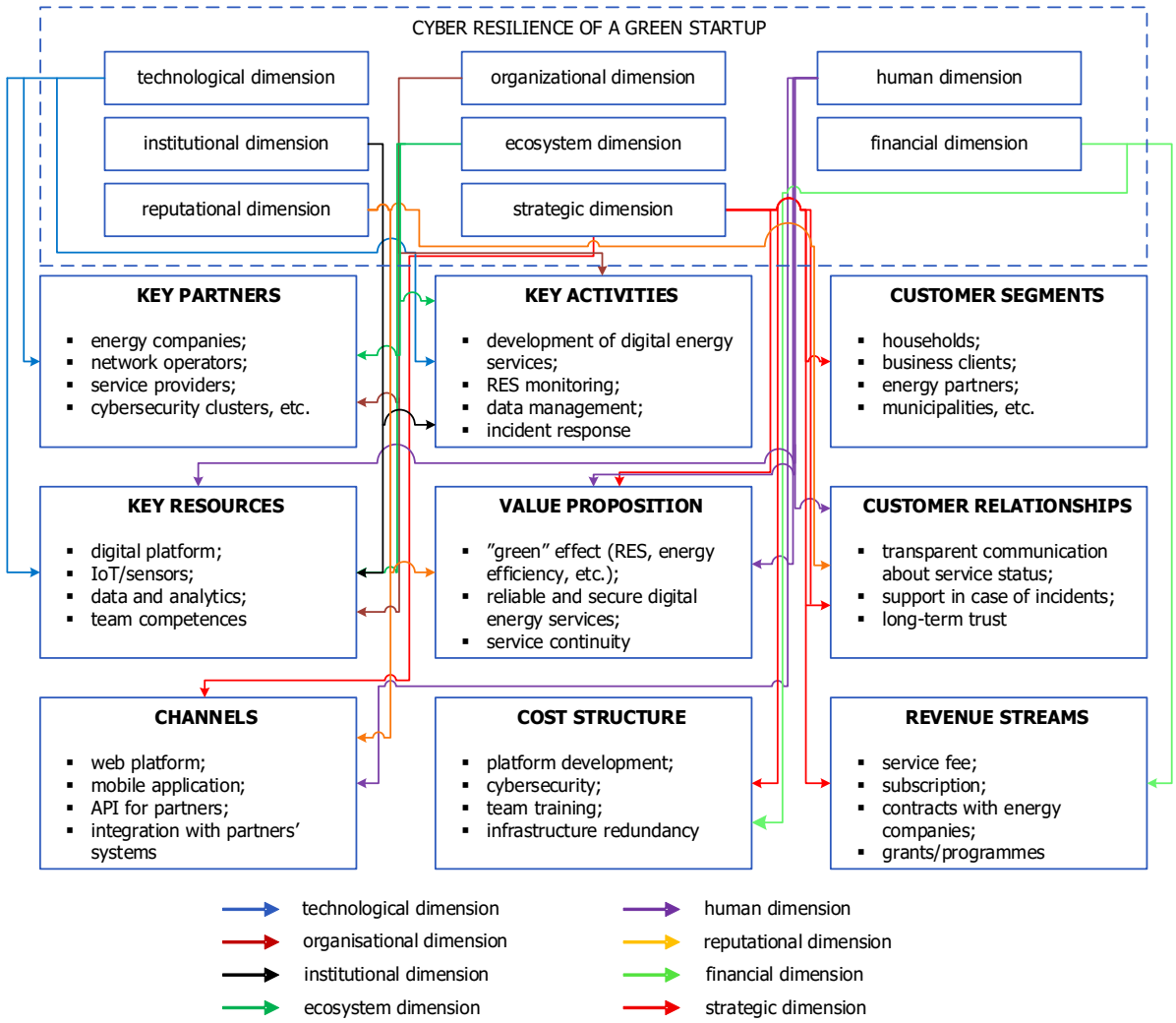

Figure 1. Cyber resilience as a transversal dimension of the business model of a green startup in a digitalised energy environment.

On the part of regulators and support programmes oriented towards the 'green' and digital transition, cyber resilience is gradually being included in the criteria used to determine the eligibility of projects for financing or participation in innovation initiatives (European Commission, 2020; World Economic Forum, 2025). It influences the interaction of green startups with the political and institutional environment: to meet expectations regarding the security of critical infrastructure and data protection, startups are compelled to consider cyber resilience requirements from the outset of product development and business model formation. As a result, new development trajectories are formed: projects capable of demonstrating incorporated cyber resilience have a better chance of accessing support programmes and partnerships with major energy players.

A separate dimension of interaction concerns end consumers and users of energy services. For households, business clients, or municipalities, the question of the security and resilience of digital solutions manifests itself in trust in services, readiness to rely on them in everyday practices, and the perception of the 'green' product as a reliable alternative to traditional solutions (World Economic Forum, 2025). When clients become aware of the risks associated with failures of digital platforms or data breaches, the startup's ability to ensure transparent communication, prompt response, and service recovery becomes an important part of interaction with stakeholders. Thus, cyber resilience influences trust, loyalty, and users' readiness to support the scaling of 'green' digital solutions.

Finally, within broader innovation and industry ecosystems, the requirement for cyber resilience shapes the nature of interactions among startups, cybersecurity clusters, research institutions, accelerators, and other support institutions. Participation in such structures enables green startups to gain access to shared knowledge, tools, and practices for preparing for cyberattacks, but it also presupposes compliance with agreed rules and standards (Hogan et al., 2019; ENISA, n.d.). In this sense, the requirement for cyber resilience influences not only the internal organisation of the business model but

DOI: 10.55643/ser.2.60.2026.676

also how the startup embeds itself in networks of interaction that shape the conditions for its functioning and development in the energy environment.

Figure 2 summarises how the requirement for cyber resilience is formed through the interactions of a green startup with key stakeholder groups in the digitalised energy environment.

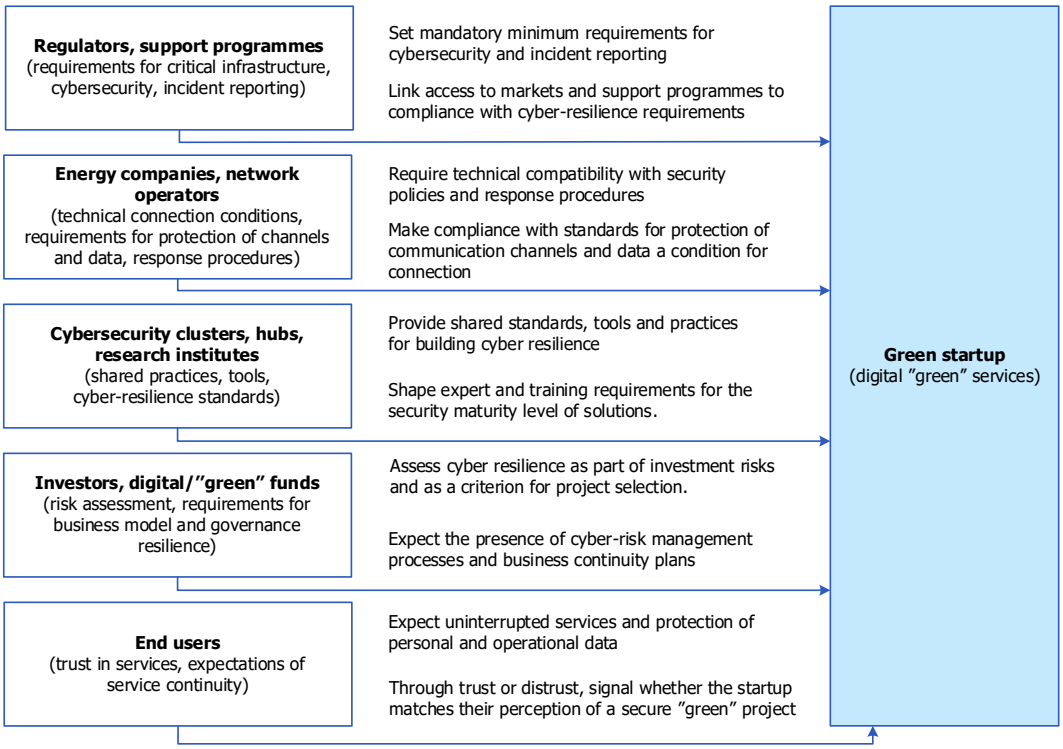

Figure 2. Cyber resilience as a requirement formed in the interaction of a green startup with the energy environment and key stakeholder groups.

At the centre of the scheme is the green startup as a provider of digital 'green' services, and around it are the key actors that set the frameworks and expectations regarding resilience to cyber threats: energy companies and network operators, regulators and support programmes, investors, cybersecurity clusters and innovation hubs, and end consumers. Each of these groups transmits specific requirements – from technical conditions for connection and regulatory norms to investment attractiveness criteria and user trust – that influence how the business models of green startups are designed and implemented amid the growing cyber threat landscape in the energy sector.

DISCUSSION

The results considered allow for a new interpretation of cyber resilience in the context of green entrepreneurship. The theoretical generalisation obtained confirms that for green startups, the digital component of business models is not a secondary element but a key condition for creating and delivering 'green' value, which is consistent with approaches where digitalisation is viewed as a factor in the transformation of value creation models in the green economy (Mondal et al., 2023; Ren & Xia, 2024; Hogan et al., 2019; European Commission, 2025). At the same time, previous studies focus predominantly on the digital or 'green' aspects of business models without systematically taking into account the dimensions of cyber resilience (Mondal et al., 2023; Ren & Xia, 2024; Hogan et al., 2019), whereas in this work, resilience to cyber threats is viewed as a necessary condition for the implementation of environmentally oriented digital solutions.

The interpretation of cyber resilience as a multidimensional characteristic that includes technological, organisational, human, institutional, ecosystem, financial, reputational, and strategic dimensions extend existing models that are predominantly oriented towards technical or organisational aspects of resilience (Sepúlveda Estay et al., 2020; Safitra et al., 2023; Hausken, 2020). Compared with works focused on the cyber resilience of energy systems, renewable energy, virtual power plants, or energy management (Halgamuge, 2024; Korukonda et al., 2025; Mehmood et al., 2023; Haque et al., 2019; Zhao et al., 2021; Shabanian-Poodeh et al., 2025; Eze et al., 2024), the proposed framework shifts the focus to the level

of the entrepreneurial unit – the startup – and captures the specificity of combining environmental objectives with requirements for the resilience of digital infrastructure. In comparison with studies of the cyber resilience of SMEs, where the emphasis is placed on resource constraints and general organisational practices (Alahmari & Duncan, 2020; Yigit Ozkan & Spruit, 2023; Carías et al., 2020; Mmango & Gundu, 2023), the green startup emerges as an entity additionally linked to critical energy infrastructure and environmental commitments.

The interpretation of cyber resilience as a transversal dimension of the business model makes it possible to integrate discussions about security with the analysis of the value proposition, key resources and partnerships, channels of interaction with consumers, and the financial structure of green startups (Hogan et al., 2019; Mondal et al., 2023). Compared with works in which business models in renewable energy or digital entrepreneurship are described without taking into account cyber threats, this approach demonstrates that resilience to cyber incidents influences not only the operational parameters of a service but also the perception of solutions as reliable elements of the energy transition and their scaling potential (European Commission, 2020; Lazari, 2025; World Economic Forum, 2025).

The analysis of the interaction of green startups with key stakeholder groups shows that the requirement for cyber resilience is shaped by regulatory, technical, financial, and reputational expectations. It aligns with European approaches, which view the cyber resilience of energy systems as a component of energy security that should ensure the continuity of critical functions through a combination of technical and managerial measures (European Commission, 2020; Lazari, 2025; ENISA, n.d.; World Economic Forum, 2025). In contrast to studies focused on large energy companies, the focus on startups highlights that the requirements of energy companies, investors, cybersecurity clusters, and end consumers simultaneously act as barriers to entry and sources of resources and knowledge for forming cyber resilience (EIT, 2025; Odika, 2025; Apostolopoulos et al., 2024; Al-Momani et al., 2024; Taherdoost, 2026).

At the same time, the study has several limitations. First, it is of a theoretical-conceptual nature and does not rely on empirical data on specific green startups, which limits the ability to verify the proposed framework and identify cause-and-effect relationships between configurations of cyber resilience dimensions and performance outcomes (Hausken, 2020). Second, the focus on general European and international approaches does not allow for fully accounting for the institutional differences between countries and markets (European Commission, 2020; OECD, n.d.). Third, the work does not consider quantitative methods for assessing cyber resilience proposed in some existing frameworks and models (Sepúlveda Estay et al., 2020; Mehmood et al., 2023; Carías et al., 2020).

Further research may be directed towards the empirical operationalisation of the proposed dimensions of cyber resilience and the development of indicators for their quantitative measurement, towards the study of configurations of business models of green startups with different levels of cyber resilience, as well as towards the analysis of policies and support programmes that combine the goals of the green transition, digitalisation and the strengthening of the resilience of entrepreneurial ecosystems in the energy sector.

CONCLUSIONS

The study has theoretically substantiated that cyber resilience is an important requirement for green startups whose activities combine an environmental orientation with the use of digital technologies and integration into energy infrastructure. Cyber resilience has been interpreted as a systemic characteristic of entrepreneurial activity, related to the ability to maintain operations, adapt, and recover under cyber incident conditions, rather than merely a set of technical cybersecurity measures.

The content of cyber resilience in the energy and entrepreneurial contexts has been revealed, and it has been shown that for green startups, it acquires the significance of a separate business requirement, since disruptions in the operation of digital platforms, sensor networks, and management systems simultaneously affect economic performance, environmental impacts, and stakeholder trust. It has been proposed to interpret the cyber resilience of green startups as a multidimensional characteristic encompassing technological, organisational, human, institutional, ecosystem, financial, reputational, and strategic dimensions, for each of which the essence, tasks, range of participants, and specific challenges for green startups have been outlined.

It has been demonstrated that the requirement for cyber resilience influences the design and implementation of green startups' business models, changing approaches to the formation of the value proposition, the determination of key resources and partnerships, the organisation of channels of interaction with consumers, and the cost structure and revenue sources. Cyber resilience is proposed to be viewed as a transversal dimension of the business model, integrated into its

DOI: 10.55643/ser.2.60.2026.676

elements and shaping the perception of digital green services as reliable, secure, and scalable in a digitalized energy environment.

It has been substantiated that cyber resilience is a requirement not only within the business model but also in the interactions of green startups with the energy environment and the main stakeholder groups – regulators and support programmes, energy companies and network operators, investors, cybersecurity clusters, and end consumers. Each of these groups transmits its own expectations regarding the level of resilience, which in turn shapes the conditions for startups' access to infrastructure, markets, financing, and innovation ecosystems.

The results obtained create a conceptual foundation for further empirical studies of the cyber resilience of green startups, in particular for the development of indicators for assessing individual dimensions, comparative analysis of different configurations of business models, and the study of the practices of interaction of startups with the energy environment and stakeholders under conditions of growing cyber threats.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Mondal, S., Singh, S., & Gupta, H. (2023). Green entrepreneurship and digitalization enabling the circular economy through sustainable waste management: An exploratory study of an emerging economy. *Journal of Cleaner Production, 422*, 138433. https://doi.org/10.1016/j.jclepro.2023.138433
2. Organisation for Economic Co-operation and Development (OECD). (n.d.). *Inclusive, green and digital transformation*. https://www.oecd.org/en/topics/inclusive-green-and-digital-transformation.html
3. Ren, Y., & Xia, Y. (2024). Research on the impact of digitalization on energy companies' green transition: New insights from China. *Frontiers in Energy Research, 12*, 1421832. https://doi.org/10.3389/fenrg.2024.1421832
4. World Economic Forum. (2025). *Powering cyber resilience in the energy sector*. https://www.weforum.org/stories/2025/05/powering-cyber-resilience-energy-sector/
5. European Commission. (2020). *Critical infrastructure and cybersecurity*. https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en
6. European Commission. (2025). *EU funding for digitalising and greening the energy system*. https://digital-strategy.ec.europa.eu/en/policies/eu-programmes-digitalisation-energy
7. European Union Agency for Cybersecurity (ENISA). (n.d.). *Preparing for cyber attacks in the energy sector*. https://www.energimyndigheten.se/499848/globalassets/energiberedskap/informations--och-cybersakerhet/preparing-for-cyber-attacks
8. European Institute of Innovation and Technology (EIT). (2025). *EIT startups rank among 2025's leading greentech innovators*. https://www.eit.europa.eu/news-events/news/eit-startups-rank-among-2025s-leading-greentech-innovators
9. Hogan, L., Wittenberg, I., & O'Neill, N. (2019). *Enabling digital energy entrepreneurship: A comparative analysis of German and Australian digital energy entrepreneurial opportunities*. Australian-German Energy Transition Hub. https://www.energy-transition-hub.org/resource/enabling-digital-energy-entrepreneurship-comparative-analysis-german-and-australian-digital
10. Moeve Global. (n.d.). *Digital transformation of our areas and business*. https://www.moeveglobal.com/en/innovation/digital-transformation
11. Lazari, A. (2025). *Cyber resilience as a pillar of European energy security*. CERRE. https://cerre.eu/wp-content/uploads/2025/12/CERRE_Cyber-Resilience-as-a-Pillar-of-European-Energy-Security.pdf
12. World Economic Forum. (2025). *Why we need to power cyber resilience in the energy sector*. https://www.weforum.org/stories/2025/05/powering-cyber-resilience-energy-sector/

13. Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–5). https://doi.org/10.1109/CyberSA49311.2020.9139638

14. Dasawat, S. S., & Sharma, S. (2023). Cyber security integration with smart new age sustainable startup business, risk management, automation and scaling system for entrepreneurs: An artificial intelligence approach. In *Proceedings of the 7th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1357–1363). https://doi.org/10.1109/ICICCS56967.2023.10142779

15. Yigit Ozkan, B., & Spruit, M. (2023). Adaptable security maturity assessment and standardization for digital SMEs. *Journal of Computer Information Systems, 63*(4), 965–987. https://doi.org/10.1080/08874417.2022.2119442

16. Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security, 97*, 101996. https://doi.org/10.1016/j.cose.2020.101996

17. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), 13369. https://doi.org/10.3390/su151813369

18. Halgamuge, M. N. (2024). Leveraging deep learning to strengthen the cyber-resilience of renewable energy supply chains: A survey. *IEEE Communications Surveys & Tutorials, 26*(3), 2146–2175. https://doi.org/10.1109/COMST.2024.3365076

19. Korukonda, M. P., Shahidehpour, M., & Xie, L. (2025). Cyber resilience in virtual power plants: A multiscale multilayer approach toward secure energy management. *IEEE Electrification Magazine, 13*(1), 54–65. https://doi.org/10.1109/MELE.2025.3535023

20. Mehmood, A., Epiphaniou, G., Maple, C., Ersotelos, N., & Wiseman, R. (2023). A hybrid methodology to assess cyber resilience of IoT in energy management and connected sites. *Sensors, 23*(21), 8720. https://doi.org/10.3390/s23218720

21. Haque, M. A., Shetty, S., & Krishnappa, B. (2019). Modeling cyber resilience for energy delivery systems using critical system functionality. In *Proceedings of Resilience Week (RWS)* (pp. 33–41). https://doi.org/10.1109/RWS47064.2019.8971974

22. Zhao, A. P., Cao, Z., Zeng, D. D., Gu, C., Wang, Z., Xiang, Y., Qadrdan, M., Chen, X., Yan, X., & Li, S. (2021). Cyber-resilient multi-energy management for complex systems. *IEEE Transactions on Industrial Informatics, 18*(3), 2144–2159. https://doi.org/10.1109/TII.2021.3097760

23. Shabanian-Poodeh, M., Hooshmand, R.-A., Shafie-Khah, M., & Siano, P. (2025). Resilience enhancement strategies for energy systems in the face of natural calamities and cyber threats: A comprehensive review. *IEEE Access, 13*, 67301–67322. https://doi.org/10.1109/ACCESS.2025.3556233

24. Mmango, N., & Gundu, T. (2023). Cyber resilience in the entrepreneurial environment: A framework for enhancing cybersecurity awareness in SMEs. In *Proceedings of the International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1–6). https://doi.org/10.1109/ICECET58911.2023.10389226

25. Odika, E. M. (2025). Electrical and renewable energy entrepreneurship as a pathway to youth self-reliance and cybercrime reduction in Rivers State. *African Journal of Management and Business Research, 21*(1), 111–128. https://doi.org/10.62154/ajmbr.2025.021.01016

26. Apostolopoulos, N., Makris, I., Apostolopoulos, S., & Dimitrakopoulos, P. (2024). Resilience of rural micro-businesses in an adverse entrepreneurial environment: Adapting to the energy crisis. *Journal of Enterprising Communities: People and Places in the Global Economy, 18*(5), 1023–1044. https://doi.org/10.1108/JEC-08-2023-0144

27. Al-Momani, A. M., Sarram, M., Zighan, S. M., Al-Majali, R. T., Al-Shanableh, N., Saatchi, S. G., Shatnawi, T. M., Alajarmeh, N. S., Al-Hawary, S. I. S., & Mohammad, A. A. S. (2024). The influence of cybersecurity leadership on the resilience of Jordanian businesses: A study on the role of cybersecurity measures in entrepreneurial success. In *Business analytical capabilities and artificial intelligence-enabled analytics: Applications and challenges in the digital era* (Vol. 2). https://doi.org/10.1007/978-3-031-57242-5_1

28. Taherdoost, H. (2026). Cybersecurity for sustainable entrepreneurship. In *Harnessing the potential of blockchain technology in smart healthcare*. https://doi.org/10.1016/B978-0-443-30192-6.00012-4

29. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things, 11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

30. Carías, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access, 8*, 174200–174221. https://doi.org/10.1109/ACCESS.2020.3026063

31. Eze, D., Simpa, P., & Ekechukwu, D. (2024). The future of cybersecurity in renewable energy systems: A review identifying challenges and proposing strategic solutions. *Computer Science & IT Research Journal, 5*(6). https://doi.org/10.51594/csitrj.v5i6.1197

Подосинніков С., Галинський Д.

КІБЕРСТІЙКІСТЬ ЯК НОВА ВИМОГА ДО ЗЕЛЕНИХ СТАРТАПІВ

У статті розглянуто зростання значення кіберстійкості для зелених стартапів, що працюють на перетині цифрових технологій та енергетичного сектора. Метою дослідження є теоретично обґрунтувати кіберстійкість як ключову

DOI: 10.55643/ser.2.60.2026.676

вимогу до зелених стартапів і розкрити її зміст у контексті функціонування та розвитку підприємництва в цифровізованому енергетичному середовищі. Методологічну основу становлять системний підхід, логіко-структурний аналіз, абстрагування, узагальнення й інтерпретація, що дозволяє розглядати кіберстійкість не лише як технічну властивість цифрової інфраструктури, а й як системну характеристику підприємницької діяльності.

Основні результати свідчать, по-перше, що кіберстійкість перетворюється на окрему умову життєздатності зелених стартапів, оскільки збої в роботі цифрових платформ, систем моніторингу та обробки даних одночасно впливають на економічні результати, екологічні ефекти й довіру стейкхолдерів. По-друге, запропоновано трактувати кіберстійкість як багатовимірну конструкцію, що включає технологічний, організаційний, людський, інституційний, екосистемний, фінансовий, репутаційний і стратегічний виміри з окресленням їхніх завдань, учасників і специфічних викликів для зелених стартапів. По-третє, показано, що кіберстійкість виконує роль поперечного виміру бізнес-моделі, впливаючи на ціннісну пропозицію, ключові ресурси й партнерства, канали та стосунки з клієнтами, структуру витрат і джерела доходів. Додатково проаналізовано, як вимоги регуляторів, енергетичних компаній, інвесторів, кластерів кібербезпеки та кінцевих споживачів формують умови інтеграції стартапів в енергетичні системи й інноваційні екосистеми.

Зроблено висновок, що кіберстійкість слід розглядати як невід'ємну вимогу, яка доповнює традиційні критерії екологічної та економічної результативності зеленого підприємництва, а запропонована концептуальна рамка може слугувати основою для подальших емпіричних оцінок зелених стартапів і розробки політик і програм підтримки, що поєднують завдання зеленого переходу, цифровізації та стійкості в енергетичному секторі.

Ключові слова: зелені стартапи, кіберстійкість, цифровізація, енергетичне підприємництво, бізнес-моделі, сталий енергетичний розвиток, критична інфраструктура, стейкхолдери, підприємницькі екосистеми

JEL Класифікація: L26, O33, Q40