Journal of Intercultural Management
Vol. **17** | No. **3** | **2025**
pp. **5–30**
DOI **10.2478/joim-2025-0009**

Barbara Kożuch
SAN University, Poland
bkożuch@san.edu.pl
ORCID ID: 0000-0002-6594-3662

Justyna Fijałkowska
SAN University, Poland
jfijalkowska@san.edu.pl
ORCID ID: 0000-0002-4236-149

Understanding Digital Organizational Trust: A Socio-Technical Approach to Human-Technology Collaboration

ABSTRACT

Objective: The aim of this article is to conceptualize organizational digital trust in the context of emerging technological paradigms such as Industry 5.0, Society 5.0, and Actor–Network Theory (ANT). The study seeks to identify the key dimensions, mechanisms, and implications of digital trust in contemporary organizations, highlighting its socio-technical character and strategic relevance.

Methodology: The article adopts a conceptual and theoretical approach based on an extensive literature review, including foundational models of trust (e.g., Mayer et al., 1995) and recent contributions in digital transformation research. Actor–Network Theory (Latour, 1996; Cressman, 2009) is employed as a lens for analyzing trust as a relational outcome among heterogeneous actants – technologies, users, and organizational environments.

Findings: The study reveals that digital trust is a multi-dimensional construct shaped by both human and technological factors. It encompasses ethical organizational values, compliance with digital standards, and the interplay between user and technology trustworthiness. Three proposed models illustrate different levels of digital trust formation, including trust between actants and human--technology collaboration. Digital trust is shown to function as both a precondition and a product of organizational cooperation, with direct implications for performance and innovation.

Value Added: This article contributes to the growing discourse on digital trust by offering an integrative framework rooted in both classical trust theory and ANT. It underscores the need to consider digital trust as a dynamic organizational asset, shaped by interactions between people, technologies, and institutional environments. The study also highlights areas for future empirical validation, addressing the current gap between theoretical elaboration and practical assessment.

Key words: organizational digital trust, Actor–Network Theory, Industry 5.0, Society 5.0, human-technology collaboration, socio-technical systems, trustworthiness, digital transformation

JEL codes: 033, L86, D83, M15

Introduction

The ongoing digital transformation of society and industry has profoundly altered how organizations operate, communicate, and build relationships. Concepts such as Society 5.0 and Industry 5.0 reflect a shift toward human-centered, sustainable, and interconnected systems in which advanced technologies – particularly artificial intelligence, robotics, and automation – are embedded in everyday structures and processes. In this new landscape, digital trust has emerged as a critical organizational resource and strategic asset. No longer limited to interpersonal relationships, trust now extends to technical and technological systems, shaping how individuals interact with platforms, algorithms, and autonomous processes. Despite its growing importance, digital trust remains conceptually underdeveloped in organizational studies.

Most existing research on trust in organizations has centered on traditional interpersonal frameworks or technology acceptance models, often neglecting the hybrid nature of trust in digitally mediated environments. There is a lack of integrative theoretical approaches that would account for the increasingly complex interactions between human and non-human actors in organizations. This article addresses that research gap by drawing on Actor–Network Theory (ANT) – a sociotechnical framework that views reality as a network of interdependent human and non-human actants – to explore the foundations, dimensions, and processes of organizational digital trust. While ANT has gained traction in management and technology studies, its application to trust – particularly in digital organizational contexts – remains limited and fragmented.

The aim of this article is to conceptualize organizational digital trust as a multi-dimensional, relational phenomenon that emerges through dynamic interactions among technologies, users, and organizational environments. Anchored in the foundational model of trust proposed by Mayer et al. (1995), and reinterpreted through the lens of ANT (Latour, 1996; Cressman, 2009), the article offers a novel theoretical framework for understanding how digital trust functions both as a precondition for collaboration and as a result of interaction and cooperation, particularly in complex digital ecosystems. The study introduces three original conceptual models that reflect varying degrees of complexity: a simplified model of digital trust formation, a socio-technical model inspired by ANT, and a model focusing on decision-making and cooperation between key actants, especially humans and intelligent systems. Together, these models highlight the relational, ethical, and strategic dimensions of digital trust in organizational settings.

This article contributes to the literature by offering a new conceptual foundation that integrates classical trust theory with sociotechnical perspectives. It emphasizes the need to approach digital trust as a dynamic process involving cognitive, technological, and institutional components. The article also underscores the importance of further empirical validation, especially regarding the interaction between internal and external forms of trust, and the conditions under which trust in digital systems is formed, maintained, or eroded.

The article begins by outlining the theoretical underpinnings of digital trust in the context of Society 5.0, Industry 5.0, and ANT. It then explores the distinct characteristics and dimensions of trust in digital organizational relationships. This is followed by the presentation of three conceptual models that illustrate the structure and formation of digital trust. The final section discusses research limitations and proposes future directions, particularly the need to translate theoretical insights into empirical research designs. By situating digital trust within a broader sociotechnical framework, this article offers scholars and practitioners a deeper understanding of how trust operates – and can be cultivated – in the digitally transformed organization.

Barbara Kożuch, Justyna Fijałkowska

Signs of the Transition into the Digital Era

The digital era began to unfold even before the industrial era had fully realized its potential. According to Growiec (2018), humanity has entered a new technological revolution – the digital revolution – which began around the year 2000, when the Internet connected computers into a truly global network. Its defining features include personal computers, the Internet, mobile phones, and industrial robots, as well as advanced socio-technological systems such as business ecosystems. A significant acceleration and advancement of the digital revolution occurred at the beginning of the third decade of the 21st century. Two concepts were key in this process: Japan's Society 5.0 (Society 5.0, 2020) and the European vision of Industry 5.0 (Tlili et al., 2023; Huang et al., 2022; Carayannis & Morawska-Jancelewicz, 2022; Deguchi et al., 2020).

A concise definition of Society 5.0 emphasizes its distinctive integration of cyberspace with physical space, enabling the simultaneous pursuit of economic progress and the resolution of social challenges. This is achieved through the provision of goods and services that precisely meet diverse and latent human needs, regardless of location, age, gender, or language. Moreover, instead of each system operating within a limited scope – such as maintaining indoor comfort, supplying energy, or ensuring the punctuality of trains – Society 5.0 envisions systems that function across the entirety of society in an integrated manner. The goal is to enhance comfort in all areas of life, including energy, transportation, healthcare, shopping, education, work, and leisure. Achieving this requires the collection of diverse and extensive data sets. These data are processed by advanced information systems, such as artificial intelligence, which alone are capable of handling such a broad range of data. The insights derived from this processing are applied in the physical world to make life more convenient and fulfilling. However, in Society 5.0, the information obtained does not merely control an air conditioner, a generator, or a railway system – it also directly influences human actions and behavior. Contemporary societies rely on a wide range of services, including those related to energy, transportation, water, healthcare, public safety, logistics, retail, education, and entertainment.

While each service may appear to function independently, in reality, they are interconnected. Building a better society requires an understanding of how these services interact and how to design appropriate integrated solutions. In the context of Society 5.0, a key challenge lies in optimally balancing societal needs with those of the individual. Progress depends on addressing this issue effectively. There is a pressing need for coordination between political actors and the high-tech sector to ensure a shared understanding of how policy proposals and technological developments contribute to the realization of Society 5.0. Without such coordination, actors may pursue their own technologies or policies in isolation, lacking awareness of how these efforts align with the broader vision of a super-smart Society 5.0 (Deguchi et al., 2020).

As highlighted in the Industry 5.0 report, this concept presents a coherent vision for the future of the European industry, serving as a continuation of the Industry 4.0 paradigm. Notably, the proposed vision uniquely acknowledges the capacity of industry to contribute to societal goals – an aspect that was largely absent from previous frameworks. These new concepts clearly extend beyond the boundaries of individual organizations and sectors, and beyond the objectives of job creation and economic growth. The aim is for societies to become resilient providers of prosperity, by respecting the planet and placing the well-being of industrial workers at the heart of production processes.

At the core of this vision lies the belief that research and innovation drive the transition toward a more sustainable, human-centric, and resilient European industry. This approach shifts the focus away from shareholder value alone and toward value for all stakeholders. The goal is to increase productivity without displacing workers from the manufacturing sector, while upholding the principles of justice, inclusiveness, and sustainable development.

Industry 5.0 emphasizes enhanced collaboration between humans and intelligent systems. The precision of industrial automation is combined with human cognitive and critical thinking skills, while monotonous and repetitive tasks are left to machines – thereby unlocking the creative potential of human workers (Atwell, 2017). This fosters greater responsibility and oversight among personnel over modern systems, ultimately contributing to improved production quality across all sectors.

This concept refers to examples such as advanced production lines based on human–robot collaboration, increased productivity, sustainability, and operational efficiency. It also emphasizes the creation of collaborative robotics potential for an economy and society that uphold European values. The Industry 5.0 framework envisions an industrial transformation that is faster, more scalable, and fundamentally more human-centric, leveraging cutting-edge technologies not only to optimize processes but also to align production systems with broader societal and environmental goals. A key component of this transformation is the shift toward upcycling – the process of creating products with higher value than the raw materials used in their production. Unlike traditional recycling, which often results in downcycling (the degradation of material quality over time), upcycling aims to preserve and even enhance material utility, thereby contributing to a circular economy. In this context, Industry 5.0 promotes design and manufacturing approaches that minimize waste and environmental harm by rethinking resource use from the outset. Upcycling becomes not just a technical practice, but an ethical and strategic principle that integrates sustainability with innovation and economic competitiveness. By embedding such practices into the fabric of industrial production, Industry 5.0 seeks to build resilient, future-oriented systems that are both technologically advanced and socially responsible.

Environmental awareness and responsibility are increasingly perceived not only as ethical imperatives but also as strategic assets that provide both competitive and cooperative advantages. Companies that adopt environmentally friendly business models gain market differentiation and long-term trust from stakeholders, particularly in light of growing consumer support for sustainable and regenerative practices. Government policies, international frameworks, and global sustainability agendas – such as the European Green Deal or the UN Sustainable Development Goals – further reinforce this shift by incentivizing green innovation, resource efficiency, and corporate transparency.

As a result, ecological responsibility becomes a lever for strategic positioning within value networks, enabling firms to participate in collaborative ecosystems where shared environmental values translate into stronger partnerships, access to funding, and preferential treatment in procurement or investment processes.

In this context, the emergence of regenerative organizations – entities that not only minimize harm but actively restore and enhance natural and social systems – reflects a profound transformation in how economic value is conceived and pursued.

Some of the current analyses focus on the skills requirements associated with the new stage of development in the European industry. The sector is already experiencing a shortage of skills, while educational and training institutions have yet to effectively respond to this demand – both in terms of advanced expertise and general digital competencies.

The conceptual frameworks of Society 5.0 and Industry 5.0, alongside the less frequently cited Actor–Network Theory (ANT), provide valuable perspectives for understanding the defining features of the digital era. ANT, although conceptually distinct from traditional notions of networks commonly explored in management and quality sciences, has been applied in these disciplines (Świątowiec-Szczepańska & Kawa, 2018). It offers a lens through which to examine the complex interplay between human and non-human actors in socio-technical systems, thereby enriching the theoretical understanding of digital transformation.

The observed conceptual differences warrant a closer examination of the foundations of Actor–Network Theory (ANT) (Latour, 1996; 2010; Cressman, 2009). Many contemporary technologies inherently take the form of networks – computer networks being a prime example. Nothing appears to be more interconnected, more distant, and more strategically organized than this type of network. However, this is not the central metaphor of actor–networks. A technical network in the engineering sense is merely one of the possible final and stabilized states of an actor–network.

An actor–network may lack the defining features of a technical network: it may be local, devoid of obligatory paths, and lacking strategically distributed nodes, yet it exhibits other characteristics, as outlined below. Another key distinction lies in the purpose of ANT, which seeks to describe the very nature of societies. This is achieved not by limiting the concept of actors to individual humans, but by extending it to include "non-human" and "non-individual" entities, referred to as actants. In this framework, a social network is not simply a map of human relationships, but a relational space between human and non-human actors in both the social and natural world.

Importantly, ANT does not analyze social networks in the conventional sense; rather, it aims to reconstruct the foundations of social theory itself. While social networks are encompassed within the scope of ANT, they are not granted any epistemological privilege or prominence. According to ANT, modern societies cannot be adequately described without recognizing their fibrous, thread-like, sinewy, and capillary nature – an ontological texture that resists capture by traditional conceptual categories such as levels, layers, territories, spheres, categories, structures, or systems.

Moreover, it is entirely impossible to understand what holds society together without reintegrating into its fabric the facts produced by the natural and social sciences, as well as the artifacts designed by engineers. Several key considerations must therefore be taken into account:

1. The networks envisioned by Actor–Network Theory (ANT) constitute the evolving tissue of life itself.
2. These networks create space, challenging the traditional notion of space as a domain defined by local proximity, distance, or scale – whether local or global. Offices and computers in distant cities may, in practice, be more closely connected than adjacent neighborhoods within impoverished urban areas.
3. All elements within a network are actors (actants), endowed with agency or the capacity to act. The identities and properties of these actors are not innate but relational – they emerge from the networks in which they are embedded.
4. Power must be understood as distributed throughout the network, rather than concentrated solely in central or dominant nodes.

According to the notion of the heterogeneous – or socio-technical – network, such networks can be used to describe virtually anything, as all phenomena – people, organizations, technologies, nature, politics, and social order – are the result or effect of the functioning of heterogeneous networks. The social world is neither entirely "social" nor must it be perceived in traditional sociological terms. Every type or form of social order – such as work, economy, or education – is an outcome of relational dynamics within a heterogeneous network. Even human beings themselves are products of such networks.

In this sense, Actor–Network Theory (ANT) does not focus on causes but on effects. It rejects essentialist explanations, positing instead that what exists is a consequence of the networked interplay of diverse actors. For example, if we begin by asserting that Organization X is a powerful and influential actor, we separate it from other networks and implicitly assume a core, static property. Yet, from an ANT perspective, power, influence, and scale are not intrinsic attributes but effects produced through the relationships and interactions of the actors within the network.

Actor–Network Theory (ANT) makes visible the extent to which everyday processes in the contemporary world involve a multitude of interacting actants – including ideas, texts, chemicals, machines, organisms, processes, finances, organizations, and more. The study of any form of organization, social order, technological innovation, or scientific discovery is, in essence, the study of connections among heterogeneous actors embedded within networks.

However, the current lack of a clear explanation regarding how the size and strength of actor–networks emerge – and what contributes to their stabilization – implies a gap in understanding how the socio-technical world inhabited by humanity actually operates. Without this clarification, any analysis remains incomplete.

In conclusion, identifying the manifestations of digital structures and relationships would benefit not only from referencing the conceptual frameworks of Society 5.0 and Industry 5.0, but also from drawing upon Actor–Network Theory. ANT conceptualizes our reality as a fabric composed of facts produced by the natural and social sciences, as well as artifacts engineered by humans – offering a valuable theoretical lens through which to interpret the dynamics of the digital era.

In light of the accelerating digital transformation and the emergence of frameworks such as Society 5.0 and Industry 5.0, it becomes increasingly important to adopt interdisciplinary and relational perspectives when analyzing contemporary socio-technical realities.

Barbara Kożuch, Justyna Fijałkowska

Digital Trust in Organizational Relationships

Among the defining issues of the digital age, digital trust stands out as a key concern and at the same time challenges for both technological development and organizational integrity. The literature reveals that trust in the digital era has proven difficult to conceptualize, raising important questions about its characteristics, benefits, and the conditions under which it can be effectively leveraged in organizational management. It is increasingly evident that interactions now take place predominantly through digital means, influencing numerous aspects of human life. As a result, digital trust continues to grow in significance (Digital, 2017).

For instance, many scholars and practitioners argue that trust and credibility have become even more critical in e-commerce, due to the less verifiable and less controllable nature of digital business environments (Gefen, 2002). While digital trust also pertains to various other forms of digital interaction in modern societies, these broader dimensions fall outside the scope of the present discussion. Understanding the situations in which trust is needed makes it easier to build through direct connections. In contrast, trust based on indirect ties is significantly more difficult to establish. Consequently, thinking about trust in the digital era must take into account both the nature of traditional trust and the specific features of digital trust, which is layered upon the former.

The current and anticipated radical transformations in the functioning of societies heighten uncertainty and create a growing demand for trust as a resource for confronting the challenges of the modern world. This, in turn, stimulates the development of trust-related concepts and theories, including conditions for trust-building and strategies to counteract associated risks and negative phenomena. A focus on the general dimensions of digital trust allows both researchers and practitioners to better grasp the specificity of trust and its strategic relevance in the management of organizations in the digital era (Guo, 2022; Mubarak & Petraite, 2020, p. 3).

Trust in the digital era is often inaccurately equated with digital trust. The former refers to trust in contexts where individuals remain in direct interaction, yet the growing prevalence of advanced technologies necessitates a broader conceptualization of the term. Trust in the digital era thus encompasses not only interpersonal trust and the understanding of abstract systems but also includes trust in technical and technological systems.

Digital trust, on the other hand, may be described as an expanded form of traditional trust – a form specifically adapted to the realities of the digital age. According to one definition, digital trust represents an evolution of traditional trust models, aimed at meeting the additional demands of digital business through the attainment of measurable levels of trust necessary for making risk-based decisions (Gaehtgens & Allan, 2017). Another definition emphasizes the belief that a digital platform will protect stored information and provide a secure environment for content creation and engagement (Digital, 2020). A third perspective identifies key components of digital trust, such as security, legality, trustworthiness, and user experience with advertising (Business Insider Intelligence, 2020).

As evidenced, the core of these definitions lies in the increasing proximity to and reliance on technical and technological systems. The dimensions of digital trust are either fully or partially embedded within digital contexts, which influence, among other aspects:

- **Assurance** – the ability to demonstrate that a service has been designed, developed, and is maintained in accordance with formalized and rigorous controls and compliance with established standards;
- **Accountability** – the construction and management of traceability systems that help users identify the entities with whom they interact and determine legal, operational, and technical responsibility within that context;
- **Benevolence** – understood as the willingness and motivation of providers and manufacturers to add value in response to user needs, without the expectation of immediate compensation;
- **Competence** – defined as the level of knowledge and skills that enables users to distinguish between high- and low-value digital services;
- **Integrity** – the assurance that all assets, including hardware, software, and data, are accessible or modifiable only by authorized parties;

- **Predictability** – the consistency of actions and outcomes that reduces uncertainty and mitigates risk.
- **Privacy** – understood as the assurance that unauthorized entities are prevented from accessing and using sensitive or personally significant information;
- **Reputation** – defined as the perceived value attributed by end users based on their direct observations, past experiences, and partners' expectations of future behavior;
- **Security** – the guarantee of protection and control over an organization's most valuable assets (White Paper, 2017).

The conducted studies also highlight distinguishing features of digital trust such as security, reliability, privacy, and data ethics (Marcial & Launer, 2019), as well as environment, experience, attitudes, and behaviors (Digital, 2017).

Given the multitude of factors that generate uncertainty and risk, more specific types of digital trust have been identified (Siau & Wang, 2018):

- **Trust in virtual teams**: Trust is defined as the willingness of one party to be vulnerable to the actions of another, regardless of the ability to monitor or control that party. Trust is built upon trustee attributes such as perceived ability, benevolence, and integrity. The key attribute on the trustor's side is the propensity to trust.
- **Trust in e-commerce**: This refers to the belief that another party is benevolent, competent, honest, or predictable in a given situation, and includes the willingness to rely on that party. Perceived trustworthiness includes consistent reliance on others, a sense of safety fostered by impersonal structures (e.g., policies and guarantees), first-hand knowledge, and evaluations of advantages, disadvantages, costs, and benefits.
- **Trust in information systems**: The willingness of a party to be vulnerable to the functioning of an information system with the expectation that it will fulfill actions critical to the trustor, regardless of the ability to monitor or control it. Trustworthiness is grounded in faith in humanity,

cognitive cues, assessments of strengths and weaknesses, perceived risk and benefit, and a general sense of security.

- **Trust in automation**: Positive beliefs, attitudes, intentions, behaviors, and orientations toward automation. Its attributes include user experience, personality traits, cultural background, and beliefs about the reliability, predictability, and capabilities of the technology.
- **Trust in human–robot interaction**: The willingness of humans to accept information provided by robots, follow their suggestions, share tasks, exchange information, and offer support to the robot. Trust is influenced by the abilities and personality traits of the human, the attributes of the robot, and the nature of the tasks involved.
- **Trust in artificial intelligence**: The belief that machines are capable of mimicking human intelligence. Relevant attributes include cognitive compatibility, usability, testability, operational safety, data security, and privacy protection.

General and specific typologies of trust dimensions exhibit certain similarities in how sets of trust-related aspects are constructed and analyzed. In many cases – similar to other forms of trust – different terms are used to describe the same or highly similar characteristics.

The reviewed material and related findings reveal three main approaches to understanding trust in the digital era. The first focuses on traditional trust, although this form does not fully account for the specificity of digital interactions (Sztompka, 2007). The second approach conceptualizes digital trust entirely within a digital context, emphasizing exclusively digital business relationships built on trust (Digital, 2017). The third, more integrative approach takes into consideration both digital and pre-digital (i.e., traditional) forms of trust (Gaehtgens & Allan, 2017).

This latter approach appears the most promising, as narrower perspectives overlook the fact that digital connections extend into individuals' private lives, including areas such as learning and education (Paliszkiewicz & Koohang, 2016).

The discussion of trust dimensions highlights the conceptual challenges involved in researching digital trust and underlines the need for further in-depth scientific inquiry.

Selected Models of Organizational Digital Trust

The analyses conducted in this study demonstrate that the concept of organizational digital trust builds upon the framework of integrative organizational trust (Mayer et al., 1995), which remains dominant in the literature. Thanks to its ongoing development by subsequent scholars, the concept continues to evolve, refine its dimensions, and incorporate new contextual factors. These changes remain within the scope of the original model, as many researchers propose constructs closely aligned with ability, benevolence, and integrity. The development of an integrative model of digital trust has also been grounded in these key components of perceived trustworthiness (Kożuch, 2021a).

The foundations of trustworthiness encompass both human actors and technical or technological systems. Reliability, accountability, confidence, security, predictability, and privacy are achieved through individual or organizational competencies. These include creating an environment in which individuals can speak and act without fear of negative repercussions; managing in a predictable and intentional manner; operating with transparency; trusting colleagues, staff, and clients; giving others appropriate recognition; fulfilling agreed-upon actions; and appropriately handling sensitive or confidential information. Enhancing technological awareness is also essential in this context.

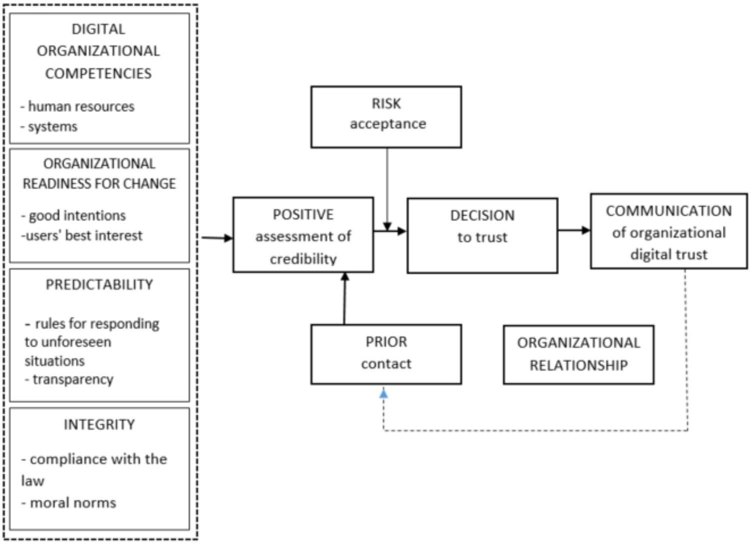
Good intentions, understood as a positive orientation toward others and perceived by the trusted party – typically an online user – are reflected in behaviors such as (Hardin, 2009; Gefen, 2002): the willingness and motivation to assist digitally connected individuals; demonstrating goodwill toward them; prioritizing client interests over personal gains; being aware of cultural differences between people, understanding other cultures, and actively engaging with and integrating cultural awareness, knowledge, and sensitivity in every digital interaction (Rice & Mathews, 2012).

Propensity to trust is also crucial, as positive orientation, selflessness, and inherited trust (passed down through social or familial systems) represent three core foundations of trust. However, as several scholars have noted, propensity to trust significantly influences the other three dimensions.

Another key element of the model is integrity, understood as adherence to sound moral and ethical principles (Colquitt et al., 2007). In general, it refers to loyalty, openness, and support (Mayer et al., 1995). This dimension is built on ethics in digital interactions – such as signaling honesty, keeping promises, offering justified evaluations, and demonstrating sincerity and fairness (Gefen, 2000).

The proposed integrated model of digital organizational trust (Figure 1) represents an attempt to combine features of both organizational trust and digital trust. The mechanism of digital organizational trust formation begins with an evaluation of the potential trustee's strengths and limitations in the context of digital interaction. When the perceived trustworthiness of the other party is assessed positively – which is more likely in cases of continued cooperation or return to the same trustee – the trustor accepts the associated risk and decides to trust. This decision marks the moment of initiating a trust-based relationship. Subsequently, trust is communicated through appropriate organizational behaviors. In the proposed model, effective communication is viewed as the result of emerging or reinforced trust.

Figure 1. Simplified Model of Digital Trust


DIGITAL ORGANIZATIONAL COMPETENCIES
- human resources
- systems
ORGANIZATIONAL READINESS FOR CHANGE
- good intentions
-users' best interest
PREDICTABILITY
- rules for responding to unforeseen situations
- transparency
INTEGRITY
- compliance with the law
- moral norms
RISK acceptance
POSITIVE assessment of credibility
DECISION to trust
COMMUNICATION of organizational digital trust
PRIOR contact
ORGANIZATIONAL RELATIONSHIP

Source: based on Kożuch (2021a).

This model represents a simplified version that highlights the interdependence between trust, risk-taking, and performance outcomes. Similar to its original version (Mayer et al., 1995), the model incorporates interpersonal organizational trust.

The second presented model (Fig. 2) is the organizational digital trust model from the perspective of Actor–Network Theory, incorporating insights from the works of Latour (1996), Cressman (2009), and Ejdys (2018). This model (Figure 2) integrates the key components of organizational digital trust across three dimensions: technology, environment, and users, and is grounded in the assumptions of Actor–Network Theory (ANT). According to this theory (Latour, 1996), trust is not merely an interpersonal relation but emerges from dynamic interactions among heterogeneous actants – including humans, technologies, institutions, and social practices. Therefore, this model represents an attempt to conceptualize organizational digital trust as the outcome of dynamic interactions among three primary groups of actants. It is based on the assumptions of Actor–Network Theory (ANT), which posits that social relations – including trust – are not exclusively the domain of human actors, but are co-constructed by diverse, heterogeneous elements – both human and non-human (Latour, 1996; Cressman, 2009).

Figure 2. A Model of Organizational Digital Trust from the Perspective of Actor–Network Theory

Key Components of Organizational Digital Trust		
Technological Features	**Environment – Features**	**Users – Features**
technology usefulness	**Internal**	interpersonal trust
technology functionality	institutional trust privacy policy interdependence among employees organizational community organizational culture	general propensity to trust
perceived ease of use		trust in technology
level of security		level of satisfaction
privacy guarantee		prior experience in technology
system quality		familiarity with technology
quality of products and services	**External**	knowledge about technology
information quality	reputation of the institution/organization in the community trust in the institution/organization perceived privacy protection by the public perceived security protection by the public social acceptance of technology legal requirements for ensuring security and privacy	education

Source: own elaboration based on Latour (1996), Cressman (2009), and Ejdys (2018).

This model consists of three main dimensions: technology, environment, and users, described below.

1. Technology

This dimension includes technical attributes that influence trust, such as:

- the usefulness, functionality, and ease of use of technology,
- privacy guarantees and security level,
- the quality of systems, products, and services,
- and the quality of information, which is central to trust in the digital era.

In line with the ANT perspective, technologies are considered actants that not only enable action but actively co-construct trust relationships through their properties and constraints (Cressman, 2009). Technologies are active participants as carriers of trust through their usability, security, functionality, and the quality of systems and information. Their attributes can either strengthen or weaken trust relationships.

2. Environment

This component refers to the institutional and organizational context in which technologies and their users operate. Trust is shaped by:

- the internal environment of institutions (e.g., privacy policies, organizational culture),
- the organizational community and relationships among employees,
- and the external perception of the institution – how the organization and its practices related to security and privacy are socially interpreted (Ejdys, 2018).

The environment serves as a space for actor interaction in which behaviors, norms, and expectations influence the stabilization or destabilization of trust. The organizational environment provides the context for building trust – both internally (e.g., organizational culture, privacy policies, employee relations) and externally (e.g., the organization's image and reputation in the broader environment). The environment influences how technological and human actions within the organization are interpreted.

3. Users

The third dimension encompasses cognitive and social characteristics of users, such as:

- interpersonal trust,
- propensity to trust technology,

- satisfaction, experience with technology, technical knowledge, and educational background.

As Latour (1996) emphasizes, users are not passive recipients of technology but actors who shape the network through their decisions, habits, competencies, and expectations. Their willingness to trust, digital competence, experience, educational background, and level of satisfaction all affect how both the technology and the organization are perceived in terms of trustworthiness.

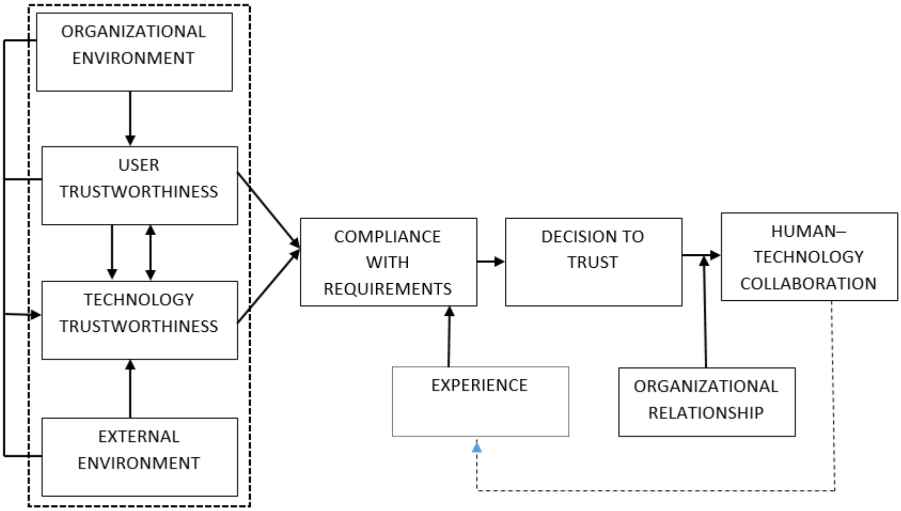
This model illustrates how digital trust emerges from interactions among diverse actants: technology, the environment, and the user. In the spirit of Actor–Network Theory, trust is not assigned to a single side but arises within relationships, which are strengthened (or weakened) by experience, cultural context, institutional frameworks, and technological attributes.

The model thus captures the multidimensional nature of organizational digital trust, which cannot be adequately analyzed without considering the interplay of infrastructure, human agency, and the socio-institutional environment.

The third proposed model (Fig. 3) focuses on the trustworthiness of technologies and the trustworthiness of their users. In addition, both the internal (organizational) and external environments are treated as actants. The internal organizational environment (e.g., structures, culture, policies) and the external environment (e.g., legal, social, and cultural context), which create conditions that either facilitate or constrain digital trust. The internal organizational environment exerts a direct influence on both primary actants, while the external environment influences the internal one.

Once alignment with trustworthiness criteria for both users and technologies is confirmed, a decision to trust is made, leading to the formation of an organizational relationship, expressed through human–machine collaboration. This assessment and initiation of trust-based interaction is facilitated when positive prior experience with similar or identical cooperation is present.

Figure 3. Model of Trust Between Key Actants


ORGANIZATIONAL ENVIRONMENT
USER TRUSTWORTHINESS
TECHNOLOGY TRUSTWORTHINESS
EXTERNAL ENVIRONMENT
COMPLIANCE WITH REQUIREMENTS
DECISION TO TRUST
HUMAN–TECHNOLOGY COLLABORATION
EXPERIENCE
ORGANIZATIONAL RELATIONSHIP

Source: based on Kożuch (2021b).

This model may serve as a framework for analyzing digital trust in organizations and designing strategies for building trust in human–technology interactions.

The proposed model of trust between actants incorporates the main stages of establishing trust-based collaboration between humans and trust in the technologies used in organizational functioning.

An effort to systematize other factors shaping digital trust was undertaken by Siau and Wang (2018). Among their findings, they observed that visualization plays an important role in building trust, which explains the growing popularity of humanoid robots. The more human-like a robot appears, the easier it is for people to form an emotional bond with it. A robotic dog is another example of visualization (a representation of AI) that people are more likely to trust, as dogs symbolize loyalty and diligence.

The current perception of artificial intelligence has largely been shaped by science fiction books and films, which often portray AI as a force that escapes human control and becomes dangerous. This framing serves as a key factor influencing people's initial trust in artificial intelligence. Moreover, peer reviews and user opinions shared online also significantly affect the initial level of trust.

Transparency, along with explainability, is another critical factor. Trust in artificial intelligence applications requires an understanding of how they are programmed and what functions they are expected to perform under specific conditions. Therefore, transparency alone is insufficient – AI systems should also be capable of explaining and justifying their behaviors, including their decision-making processes.

Testability is equally important. It refers to the ability of users to access and try out an AI application before accepting or adopting it, which promotes a higher level of initial trust. Developing and maintaining ongoing trust in artificial intelligence requires performance to remain at an expected level. This is supported by usability and reliability: AI applications should operate in a simple and intuitive manner, without unexpected downtime or failures.

Collaboration and communication are among the most frequently cited organizational behaviors associated with trust. Trust typically precedes collaboration, while continued collaboration reinforces and deepens trust. Social bonds also contribute positively to the development of trust. For instance, a robotic dog that recognizes its owner and displays affection can be perceived as a household pet, thereby fostering emotional connection and trust.

The list of cited factors concludes with security and privacy protection. Operational security and data security exert the strongest influence on trust in technology. People tend not to trust technologies that are perceived as too risky or difficult to operate. In the digital world, the generation of vast volumes of data makes privacy a pressing concern.

Conclusions

This article has conceptualized organizational digital trust as a dynamic, multi-dimensional phenomenon shaped by interactions between users, technologies, and organizational environments. Drawing on Actor–Network Theory and classical trust models, the study proposes that digital trust functions both as a prerequisite and as an outcome of collaboration in digitally enabled contexts.

In summary, it can be concluded that a better understanding of the ongoing changes – along with how individuals respond to everyday problem-solving, work, business operations, communication, and relationship-building – leads to the recognition that digital communication enables interactions across social media, e-commerce, digital business, as well as in public and social e-services. Understanding the digitization of trust increases readiness for change and the ability to address challenges associated with the emerging paradigms of Industry 5.0, Society 5.0, and Actor–Network Theory, as well as the evolving applications of advanced technologies, especially artificial intelligence.

The proposed models demonstrate that trust in the digital era extends beyond interpersonal relationships to include socio-technical systems, institutional frameworks, and the evolving role of artificial intelligence. Understanding how digital trust is formed and sustained is essential for organizational effectiveness, innovation, and long-term resilience.

The conducted analyses indicate that the essence of organizational digital trust is primarily shaped by the following elements:

- ethical organizational values,
- recognizing digital trust as both an organizational resource and a strategic asset,
- understanding it as both a precondition for cooperation and a result of collaboration, though on a higher level,
- acknowledging that it constitutes a relationship connecting people, as well as people and both material and abstract organizational systems,
- its positive influence on organizational effectiveness, particularly in achieving intended outcomes,
- and its role in reinforcing the capacity for collaboration, both within organizations and between organizations.

While these findings provide a meaningful conceptual foundation, it is important to acknowledge certain limitations of the current study and identify future directions for research. One of the key limitations lies in the predominance of theoretical inquiry over empirical validation. The empirical verification of the proposed theoretical considerations remains a challenge and an important task for future scholarly inquiry.

Given the complexity of interpersonal digital trust within organizational contexts, which poses methodological challenges, further efforts should be directed toward:

- advancing the systematization of knowledge concerning the development of organizational digital trust, and
- broadening the scope of empirical research to include perspectives on internal and external types of trust, as well as exploring the interdependencies between intra-organizational and inter-organizational digital trust.

As demonstrated in this article, digital trust is deeply embedded in the relationships between people, technologies, and institutional environments; therefore, as digital infrastructures continue to evolve, our theoretical and practical approaches to fostering trustworthy and inclusive organizational systems must evolve with them.

References

Atwell, C. (2017). Yes, Industry 5.0 is already on the horizon. *Machine Design*. Retrieved from https://www.proquest.com/trade-journals/yes-industry-5-0-is-already-horizon/docview/1938056866/se-2. Access: 29.05.2024.

Business Insider Intelligence (2020). The 2020 Digital Trust Report Preview. Retrieved from https://www.emarketer.com/topics/category/business%20insider%20intelligence. Access: 6.06.2024.

Carayannis, E. G., & Morawska-Jancelewicz, J. (2022). The futures of Europe: Society 5.0 and Industry 5.0 as driving forces of future universities. *Journal of the Knowledge Economy*, *13*(4), 3445–3471. https://doi.org/10.1007/s13132-021-00854-2.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, *92*(4), 909–927. https://psycnet.apa.org/doi/10.1037/0021-9010.92.4.909.

Cressman, D. (2009). A brief overview of Actor–Network Theory. University of British Columbia.

Deguchi, A., Hirai, C., Matsuoka, H., Nakano, T., Oshima, K., Tai, M., & Tani, S. (2020). What is Society 5.0? In: *Society 5.0: A people-centric super-smart society* (pp. 1–23). Springer.

DIGITAL (2017). The Digital Evolution Index 2017. Retrieved from https://www.dosdoce.com/wp-content/uploads/2017/07/The-Digital-Evolution-Index-2017.pdf. Access: 16.01.2026.

Business Insider (2020). The 2020 Digital Trust Report Preview. Business Insider. Retrieved from https://www.businessinsider.com/intelligence/digital-trust-enterprise--report-preview?IR=T. Access: 09.01.2025.

Ejdys, J. (2018). Building technology trust in ICT application at a university. *International Journal of Emerging Markets*, *13*(5), 980–997. https://doi.org/10.1108/IJoEM-07-2017-0234.

Gaehtgens, F., & Allan, A. (2017). Digital trust – redefining trust for the digital era. Gartner Trend Insight Report. Retrieved from https://www.gartner.com/en/documents/3727718. Access: 09.01.2025.

Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega*, *28*(6), 725–737. https://doi.org/10.1016/S0305-0483(00)00021-9.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM SIGMIS Database*, *33*(3), 38–53. https://doi.org/10.1145/569905.569910.

Growiec, J. (2018). The digital era, viewed from a perspective of millennia of economic growth. SGH KAE Working Papers Series.

Guo, Y. (2022). Digital trust and the reconstruction of trust in the digital society. *Digital Government: Research and Practice*, *3*(4), 1–19. https://doi.org/10.1145/3543860.

Hardin, R. (2009). *Trust*. Polity Press.

Huang, S., Wang, B., Li, X., Zheng, P., Mourtzis, D., & Wang, L. (2022). Industry 5.0 and Society 5.0 – Comparison, complementation and co-evolution. *Journal of Manufacturing Systems*, *64*, 424–428. https://doi.org/10.1016/j.jmsy.2022.07.010.

Kożuch, B. (2021a). *Anatomia zaufania organizacyjnego*. CeDeWu.

Kożuch, B. (2021b). The dimensions of trust in the digital era. In: J. Paliszkiewicz & K. Chen (Eds.), *Trust, organizations and the digital economy* (pp. 15–26). Routledge.

Latour, B. (1996). Social theory and the study of computerized work sites. In: W. Orlikowski et al. (Eds.), *Information technology and changes in organizational work* (pp. 295–307). Springer.

Latour, B. (2010). *The making of law: An ethnography of the Conseil d'État*. Polity.

Marcial, D. E., & Launer, M. A. (2019). Towards the measurement of digital trust. *International Journal of Scientific Engineering and Science*, *3*(12), 1–7. https://doi.org/10.5281/zenodo.3595295.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734.

Mubarak, M. F., & Petraite, M. (2020). Industry 4.0 technologies, digital trust and technological orientation. *Technological Forecasting and Social Change*, *161*, 120332. https://doi.org/10.1016/j.techfore.2020.120332.

Paliszkiewicz, J., & Koohang, A. (2016). *Social media and trust*. Informing Science Press.

Rice, M. F., & Mathews, A. L. (2012). A new kind of public service professional. In: K. Norman-Major & S. Gooden (Eds.), *Cultural competency for public administrators* (pp. 19–31). M.E. Sharpe.

Siau, K., & Wang, W. (2018). Building trust in AI. *Cutter Business Technology Journal*, *31*(2), 47–53.

Society 5.0. (2020). Society 5.0. Government of Japan. Retrieved from https://www8.cao.go.jp/cstp/english/society5_0/index.html. Access: 16.01.2026.

Sztompka, P. (2007). *Zaufanie. Fundament społeczeństwa*. Znak.

Światowiec-Szczepańska, J., & Kawa, A. (2018). Metafory, modele i teorie sieci w naukach o zarządzaniu. Organizacja i Kierowanie, *181*(2), 79–91.

Tlili, A., Huang, R., & Kinshuk, X. (2023). Metaverse for climbing the ladder toward Industry 5.0 and Society 5.0. *The Service Industries Journal*, *43*(3–4), 260–287.

White Paper (2017). Digital trust for smart ICT (Version 3). Retrieved from https://portail--qualite.public.lu/content/dam/qualite/publications/confiance-numerique/white-paper--digital-trust-september-2017.pdf. Access: 16.01.2026.