Cybersecurity Governance as an Enabler for Responsible AI Adoption and Digital Transformation

ISBN: 978-1-943295-26-5

Adriana Nitescu
Polytechnic University of Bucharest
(office@octo-go-n.com)

Amid the transition toward an immersive digital economy (2025–2050), the adoption of emerging technologies including AI, IoT, blockchain, quantum and edge computing, together with 6G–10G networks is driving a profound redefinition of organizational governance and security paradigms. This paper examines an evolutionary conceptual model that progresses from Governance to TechGovernance and ultimately to Augmented Governance, forming the foundation of a new hybrid system of technology-driven leadership. In this context, cyber security emerges as a strategic pillar balancing innovation and control, while also acting as a catalyst for economic competitiveness and sustainability. According to recent studies (WEF, 2023; EU Cyber Resilience Act, 2024), organizations with mature cyber governance structures significantly accelerate the adoption of intelligent technologies. Therefore, the introduction of a Cyber Compliance Index (CCI), integrated into a maturity assessment framework — the Cyber Governance Maturity Framework — constitutes a strategic priority for enhancing global digital resilience.

Keywords: Digital Economy; Artificial Intelligence (AI); TechGovernance; Augmented Governance; Cybersecurity; Cyber Governance Maturity Framework; Digital Resilience; Emerging Technologies

1. Introduction

The transition from the digital economy to the virtual economy represents one of the most profound transformations in contemporary economic history. Beginning in the 1990s, with Don Tapscott's seminal work The Digital Economy: Promise and Peril in the Age of Networked Intelligence (1995), the world entered a new era of value creation based on information, connectivity, and networks. The year 1995 is conventionally regarded as the starting point of the digital economy — not only due to the publication of Tapscott's work but also because of the emergence of the commercial Internet and the first e-commerce platforms (Amazon, eBay) (Tapscott, 1995; Brynjolfsson & McAfee, 2014). This phase marked the substitution of physical capital with informational capital, as competitive advantage became dependent on the ability of organizations to transform data into knowledge and knowledge into decision-making.

According to the definitions of international organizations (OECD, 1998), the digital economy represents the initial stage of economic transformation driven by information technologies and the Internet. Its main characteristics include the digitalization of processes and services, the exponential growth of data flows and information-based value creation, as well as the expansion of digital platforms, e-commerce, and cloud computing. More precisely, it is the period when data became a central economic asset, and digital infrastructures became essential to competitiveness (Leahovcenco, 2021; Dede et al., 2024).

Starting from the 2020s, academic literature highlights the emergence of a new evolutionary stage — the virtual economy — considered an immersive extension of the digital economy. This new paradigm unfolds within virtual and augmented environments (VR/AR), built on blockchain, artificial intelligence, and met averse technologies, where digital goods (such as NFTs, avatars, or virtual spaces) acquire real economic value (Castronova, 2002; Schwab, 2022). The virtual economy is characterized by the increasing mediation of economic interactions and value creation through immersive and extended reality (AR/VR/Metaverse); the dominance of digital assets as primary units of value (NFTs, tokenization, digital property); and the conduct of transactions and production within fully virtualized environments. Its sustainability depends on interoperability, digital standards, and advanced cybersecurity frameworks.

While the digital economy redefined economic processes through digitalization and interconnectivity, the virtual economy amplifies them through immersiveness and interactivity, laying the foundation for a decentralized and algorithmic economy. In this perspective, current literature positions the digital economy between 1995 and 2035, followed by the virtual economy (2020–2050), which in turn prepares the transition toward the cognitive economy, based on artificial intelligence and algorithmic autonomy (Schwab, 2016; Harari, 2021).

Where Are We Today? The Era of Digital Transformation

At present, we are in a stage of accelerated digital transformation marking the transition from the digital economy toward the virtual economy. This intermediate period is increasingly defined in academic literature as the integrated economy, driven by emerging technologies and the Internet of Things (IoT). It is characterized by the extensive integration of technologies such

as IoT, artificial intelligence, blockchain, and edge computing; the automation of industrial processes and expansion of smart infrastructures (smart industry, smart cities); as well as the real-time valorization of data generated by interconnected systems (Joshi, 2022; Weinberg & Cohen, 2024).

In this phase, the economy is no longer merely digital but profoundly interconnected, self-optimizing, and algorithmically adaptive. Cybersecurity thus becomes a critical enabler of sustainable economic ecosystems, ensuring data integrity, continuity of information flows, and protection of smart infrastructures — making it a fundamental pillar of contemporary economic competitiveness.

Recent studies such as Machina Economicus: A New Paradigm for Prosumers in the Energy Internet of Smart Cities (Hou et al., 2024), All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda (Lee et al., 2021), and The Role of Cybersecurity in the System of Economic Security: Bibliometric Analysis (Koibichuk, 2023), emphasize that the effective transition from the digital to the virtual economy depends on three major systemic factors: **Energy + Next-generation Internet** (6G–10G) + **Cybersecurity**

2. Theoretical foundations

Digital transformation has become one of the most significant processes of economic and organizational reconfiguration in the 21st century, generating new business paradigms, managerial models, and forms of corporate governance. It does not represent merely a technological adaptation, but rather a structural redefinition of the way organizations create, capture, and distribute value (Hess, 2022; Iansiti & Lakhani, 2020). Thus, we can identify several dimensions of this transformation:

1. New Business Paradigms

In the context of digital transformation, traditional business models based on linear value chains are being replaced by interconnected digital ecosystems and collaborative platforms (Parker, Van Alstyne & Choudary, 2016). These operate by orchestrating interactions between producers and consumers through data infrastructures and intelligent networks. Business models are becoming data-centric, and economic value increasingly derives from organizations' ability to process, interpret, and monetize data (Brynjolfsson & McAfee, 2017).

At the same time, the emergence of blockchain technologies has fostered the paradigm of algorithmic trust and decentralized organizations (Tapscott & Tapscott, 2016). In a broader sense, digital transformation supports the transition toward forms of conscious capitalism, oriented toward sustainability, ethics, and socio-ecological impact (Mackey & Sisodia, 2013), as well as toward immersive models based on experience and virtual value (Dwivedi et al., 2022).

2. New Management Models

Contemporary management is being redefined through digital augmentation, agility, and data-driven decision-making. In Competing in the Age of AI, Iansiti and Lakhani (2020) argue that algorithms have become direct actors in the decision-making process, transforming management into a hybrid human–algorithmic system. According to Hess (2022), digital leadership requires not only technological competence but also the ability to orchestrate organizational change in dynamic and uncertain environments.

Westerman, Bonnet, and McAfee (2014) introduce the concept of leading digital transformation, in which managers act as agents of cultural change rather than mere drivers of operational performance. In this context, Daugherty and Wilson (2018) define the Human + Machine model, through which human–AI collaboration optimizes decisions and processes, shifting leaders' roles toward the strategic and ethical dimensions of the organization.

Thus, digital management becomes adaptive, collaborative, and grounded in collective intelligence. Decision-making processes unfold within a continuous learning and self-regulating framework, amid the diversification of risk factors and the emergence of new, still-forming risk management processes.

3. New Governance Models

Digital transformation profoundly reconfigures corporate governance, shifting the focus from hierarchical control to transparency, accountability, and cyber resilience (Sun & Guo, 2024). In this framework, boards of directors integrate digital competencies, and IT committees emerge as strategic components of corporate leadership (Kapustina, 2025).

Catarino (2024) proposes a model of Digital Transformation Governance based on three pillars: digital strategy, organizational culture, and transdisciplinary leadership.

Given the complexity and the discrete specific differences, our study highlights a series of terms related to the new governance paradigm—transitioning from traditional corporate governance to the governance of emerging technologies within the company, and ultimately toward the management of the company through emerging technologies.

Gouvernance	Leadership through governance
The set of principles, processes, rules and mechanisms through which an organization is led, controlled and held accountable, so that it achieves its objectives ethically, transparently and efficiently.	Leading an organization through the principles, mechanisms, and values of governance, not through the direct authority of the manager. It is a form of leadership based on rules, ethics, fairness, and transparency.

Technological governance	Governance through technology	Technological Leadership
The branch of organizational governance that deals with establishing the decision-making framework, responsibility, and control over the use of technologies (IT, digital infrastructures, emerging technologies, biotechnologies, etc.) to support the organization's strategic objectives.	Using technology as a tool for implementing and enforcing governance principles. Companies not only govern technology, but use technology as a means of governance (control automation, traceability, technology audit, AI for decisions, etc.).	The way leaders and organizations use technology (machines, equipment, hardware, software, etc.) to streamline, coordinate and motivate human activities. The focus is on management and leadership facilitated by technological tools (robots, automation, devices, data analysis, digital communication).

Digital Gouvernnce	Governance through digital	Digital Leadership
Digital governance (or IT governance) is a sub-branch of technological governance and represents the set of structures, processes, and decision-making mechanisms through which an organization ensures the alignment of investments and use of information technology with its strategic objectives, organizational values, and compliance standards.	The concept expresses the approach in which information technology supports, streamlines, monitors, coordinates, automates tasks related to governance, policies, structures, regulations, reporting, etc.	Digital leadership represents the leadership model oriented towards innovation and transformation, in which the leader uses information technology and data as tools and strategies for generating added value, competitive differentiators, new sources of revenue, etc., not just as technical tools for operations.

AI Gouvernance	Governance through AI	AI Leadership
It is a sub-branch of technological governance and consists of the set of principles, policies, mechanisms and institutional frameworks that ensure that systems based on artificial intelligence are developed, implemented and used ethically, safely, transparently and responsibly, in accordance with organizational objectives and legal regulations.	It refers to the use of artificial intelligence technologies as governance and decision-making tools, that is, when AI is integrated into administrative, managerial or public processes to support policy formulation, risk analysis or resource allocation.	It is an emerging model of augmented leadership, in which leaders use artificial intelligence not just as a technological tool, but as a cognitive partner for decision-making, innovation, team management and building digital trust.

Cybersecurity Gouvernance	Governance through cybersecurity	Cybersecurity Leadership
It represents the set of policies, structures, processes and control mechanisms through which organizations ensure the alignment of cybersecurity with strategic objectives, legal requirements and risk tolerance. It is the way in which an organization leads and controls its cybersecurity strategy, to protect its own information and digital assets and those of the entire supply chain.	It is a strategic leadership model in which cybersecurity principles and values (transparency, trust, responsibility, resilience) become governance and organizational decision-making mechanisms. We are no longer talking about security as protection, but about security as a vector of governance and competitive advantage.	It is a new concept, in the area of digital trust leadership, resilience management and cyber by design. It is the primary structure (technical + regulatory) on which the rest of the technological, digital, emerging architectures are built. And the structure that distributes access, integrations, collaborations, etc.

Types of companies related to Emerging Governance and Leadership

Companies' differentiation depends on their digital maturity and the degree of integration of emerging technologies.

	Corporate Governance	Technological / digital / AI / cyber governance	Leadership through technology / digital / AI / cyber
Company type	traditional companies / with incipient digitalization	companies in the digital transformation stage	emerging companies led by visionary leaders
Area	most companies, including many in Europe and Asia	companies in IT, finance-banking, telecom, energy and digital administration	companies that develop emerging technologies and leadership (IoT, AI, blockchain quantum computing, metaverse, etc.)
Priorities	compliance, financial reporting, internal control and organizational	governance becomes technological, data-centric and algorithmic	technology is no longer governed, but becomes the main tool of leadership

	ethics		
Digital &AI	they are treated as IT&C support tools, not as governance mechanisms.	companies no longer separate technology from management. Decision-making processes are augmented by data, analytics and algorithms; Cybersecurity and AI are integrated into the governance model, not added later	1. AI-augmented leadership = strategic decisions assisted by transparent algorithms. 2. Cyber leadership = security becomes the foundation of trust and brand value. 3. Digital ethics leadership = technology is guided by principles, not just profit.
Compliance	companies that implement minimum regulations (ISO 27001, ESG, data) only for compliance reporting	**Annex 1**	not yet regulated
Board	have Boards in which the role of Chief Digital Officer / Chief Information Security Officer is secondary.	companies have - AI ethics boards - Digital risk committees - Data governance frameworks	1. Executive decisions are partially AI-augmented (e.g. Deep Mind-Google, Tesla, OpenAI.) 2. public leadership through AI governance frameworks operative (Dubai, Singapore)
Gouvernance	governance is present, but technology is not strategically integrated	governance becomes technological – data-driven, interoperability, resilience	it is a meta-governance: technology becomes the very infrastructure of decision. Security, data and AI are no longer tools, but guiding values.
Leadership style	leadership is reactive, not anticipatory	anticipatory driving	leadership becomes symbiotic: man + technology = intelligent decision system.

At present, most companies and organizations are undergoing an evolutionary process that reflects the transition from classical governance to technological governance, and subsequently to technology-driven leadership.

In the **first stage**, governance has a normative and structural character, focused on control, compliance, and reporting (Tricker, 2019; OECD, 2023), while technology is treated as operational support.

The **second stage**, corresponding to technological/digital/AI/cyber governance, marks a substantive transformation: technology becomes a decision-making and governance infrastructure, and traditional control principles are replaced by processes based on data, algorithms, and cyber resilience (Floridi, 2022; Weill & Woerner, 2021).

In the **third stage**, emerging in 2025–2035, companies adopt models of technology-driven leadership, in which AI, cybersecurity, and digital ethics become vectors of strategic leadership and organizational trust (Schwab, 2022; Davenport & Mittal, 2023). Thus, governance is no longer merely a control framework but an intelligent, adaptive, and ethical ecosystem capable of guiding decision-making and performance in the extended digital economy.

Cybersecurity Compliance – A Fundamental Factor in the Adoption of AI and Emerging Technologies

In the last decade, we have witnessed a phenomenon of cybersecurity overregulation, driven by the growing global interdependence and the risks brought by new technologies (AI, IoT, quantum computing, blockchain, metaverse). As Joshi (2022) points out, the international legislative framework has expanded significantly to address cross-border challenges and prevent systemic risks. According to OECD standards (2023), cybersecurity is considered a fundamental condition for digital competitiveness and for the sustainable absorption of emerging technologies.

Contemporary models such as the Zero Trust architecture, described by Weinberg & Cohen (2024), and Cyber by Design (EU – Cyber Resilience Act 2024) replace traditional perimeter defense paradigms with continuous risk-based verification mechanisms, increasingly applied in financial institutions, smart industrial networks, and virtual environments.

This trend of overregulation, particularly visible at the European Union level (see Annex 1), seeks to create a secure integration environment for emerging technologies through:

- standardized international procedures and frameworks
- predictive governance based on risk analysis
- transparency in data chains and supply chains
- ethical audits for algorithms

Thus, regulation becomes a tool for risk anticipation rather than mere reaction, marking a maturation of the security approach at the economic level.

The Fundamental Role of Cybersecurity in New Economic Paradigms

Within digital and virtual economies, cybersecurity has emerged as a fundamental factor of functionality, trust, and resilience. As Leahovcenco (2021) observes, the development of the digital economy is inextricably linked to the level of cyber

protection, since data- and connectivity-based economic flows depend on the safety of digital infrastructures. Without robust security mechanisms, digital platforms, IoT networks, or virtual ecosystems risk systemic collapse through attacks, data loss, or algorithmic dysfunctions. Recent studies (Dede et al., 2024) demonstrate a direct correlation between the national cyber readiness index and the share of the digital economy in GDP, suggesting that security is a strategic economic variable rather than an operational cost. In this sense, in emerging virtual economies, cybersecurity becomes a mechanism of value creation, building trust in transactions and ensuring the sustainability of digital ecosystems.

The Current and Future Relationship Between Cybersecurity and Artificial Intelligence

The relationship between cybersecurity and artificial intelligence (AI) is both symbiotic and paradoxical. On one hand, AI is used to strengthen security through anomaly detection, predictive attack analysis, and automated incident response. Egbuna (2024) highlights the effectiveness of machine learning algorithms in the early identification of vulnerabilities and abnormal behaviors within complex networks. On the other hand, AI also becomes a vector of risk, as it is used by attackers to generate adaptive attacks, deep fakes, advanced phishing schemes, or data manipulation. Femi et al. (2025) emphasize that this "algorithmic duel" redefines the dynamics of security, requiring new models of trust, transparency, and ethics in AI development. Ge and Zhu (2024) propose a theoretical approach based on dynamic game theory, suggesting that the efficiency of security depends not only on technical capacity but also on trust in the AI models employed for defense. Looking to the future, cybersecurity and AI are expected to form an integrated ecosystem capable of operating in real time, preventing threats, and supporting the safe transition toward virtual economies and, ultimately, toward economies of consciousness.

3. Methodology

The research was based on a mixed quantitative–qualitative methodology, including documentary analysis from open sources (laws, policies, standards, corporate and sustainability reports), as well as mini-interviews with IT managers, executive directors, board members, and entrepreneurs from key industries such as energy, finance, IT&C, and audit.

Microsoft, Apple, IBM, Google, Cisco, SAP, Siemens, Bitdefender, UiPath, Orange, and Vodafone are among the IT&C companies cited in the study, along with companies from other industries such as BP (British Petroleum), Walmart, Ford Motor, Nestlé, AIG, HSBC, Accenture, Deloitte, and several Romanian companies (eMag, Banca Transilvania, BRD, BCR, Romgaz, OMV Petrom, PPC România, Hidroelectrica, Nuclearelectrica, Transelectrica, etc.).

In these companies, we examined their policies, strategies, investment plans, and financial/non-financial reports, as well as the methods used to measure the impact of cyber indicators through standard approaches (assessment of financial and operational risks, analysis of prevention vs. remediation costs, reputational impact, cybersecurity audit) and multifactorial methods (Balanced Scorecard, Enterprise Risk Management, correlation of cybersecurity with ESG objectives, Business Continuity Planning, etc.).

The theoretical framework of the study was built upon the concepts of Corporate Governance (OECD Principles, COSO Framework), Cybersecurity Governance (NIS2/DORA, CSR, CSA, AI Act, NIST, ISO/IEC 27001), and Digital Transformation Models (MIT, Gartner).

4. Results

Cyber Profile of Companies Compatible with Emerging Technologies

Today, business continuity no longer refers only to how companies cope with crises, risks, and market changes, but to how they integrate into digital platforms where the operations of the digital and virtual economy take place. Our study identified three types of companies based on their potential for sustainable digital transformation through compliance with cybersecurity standards: vulnerable companies, secure companies, and strong companies prepared to engage in digital transformation through the absorption of emerging technologies.

To ensure a smooth transition of companies from low-level governance to emerging governance, the following recommendations were formulated:

- inclusion of a Chief Information Security Officer (CISO) on the Board of Directors;

- establishment of a cybersecurity committee within the boards of European companies, in line with new regulatory frameworks (NIS2, DORA, CRA, CSA, AI Act);
- development of a Cyber Governance Maturity Framework for assessing governance maturity, applicable to global organizations.

5. Perspectives

The study is currently being expanded through a doctoral research project, which consists of an applied study proposing a Cyber Governance Maturity Framework based on the calculation of a company's Cybersecurity Compliance Index (CCI), along with a platform that automates compliance in accordance with the European Union regulatory package.

6. Conclusions

1. Digital Transformation Redefines Corporate Governance.

The study demonstrates that the digitalization process goes beyond simple technology adoption, becoming a mechanism for strategic and cultural reconfiguration of organizations. Traditional governance, based on hierarchical control, is gradually replaced by algorithmic governance and technology-driven leadership models.

2. Compliance and Cybersecurity as Pillars of Competitiveness.

Adhering to cybersecurity standards is no longer just a legal obligation; it is an essential condition for digital competitiveness and economic sustainability. Companies that integrate security into strategic processes achieve greater resilience and enhanced stakeholder trust.

3. Cybersecurity as a Foundation for AI adoption.

Cybersecurity provides the essential foundation for responsible artificial intelligence deployment. In a secure environment, AI can be used to detect anomalies, prevent attacks, and optimize decision-making processes. Conversely, the absence of robust security limits AI adoption, as associated risks—adaptive attacks, deepfakes, and data manipulation—increase exponentially. Companies that integrate AI within an ethical and transparent cybersecurity governance framework enhance both operational safety and strategic innovation capacity.

4. Emergent Governance as a Process of Organizational Maturity.

The transition from traditional to technology-driven governance requires increased maturity in decision-making, risk management, and digital ethics. Mature companies are those that successfully transform technology from an operational tool into a strategic leadership vector.

5. Cyber Governance Maturity Framework – a Strategic Evaluation Tool.

The proposed framework for cybersecurity governance maturity and the Cybersecurity Compliance Index (CCI) provides a practical approach to measure digital performance and the integration of emerging technologies in a standardized and comparable manner.

6. The Future Of Governance is Digital, Ethical, and Predictive.

In the context of global interdependencies and virtual economies, corporate governance will evolve toward predictive models based on data, AI, and cybersecurity, where transparency, ethics, and sustainability become fundamental criteria for performance and trust.

7. ANNEX 1

Country	Regulation	Content	Results
US	Executive Order 14017 - Security America s Supply Chaines | **2021**	- supply chain security and transparency of hardware/software products - applies voluntarily in industry and mandatory for government suppliers	1. analysis and reporting in critical areas 2. safer defense industry 3. improving transport and logistics infrastructure 4. supply chain regulation
	IoT Cybersecurity Labeling Program (NIST) | **2022**	offers cybersecurity labels for IoT devices (optional)	1. basic criteria for cybersecurity 2. launch of the US Cyber Trust Mark 3. launch of the certification system 4. alignment between NIST and European standards
	CISA Cibesecurity Information Sharing Act| **2015**	facilitates the exchange of information about cyber threats between GOV and the private sector	1. Strengthening information transfer 2. Better response to cybersecurity threats
UK	Product Security and	cybersecurity regulation for connected	1. cybersecurity standards for connected

	Telecommunications Infrastructure Act | **2022**	devices (IoT)	products 2. obligations for manufacturers, importers and distributors 3. strengthening the role of regulators 4. modernizing telecommunications infrastructure
China	Cybersecurity Law | **2017**	- data storage exclusively within Chinese territory - access to data by Chinese governamental authorities	1. increasing price of data storage for international companies 2. exposing customer data to Chinese state control
	Data Security Law | **2021**	- regulates the collection, storage and transfer of data - imposes strict restrictions on the export/import of sensitive or important data	1. high protection of data transmitted/received across borders 2. creation of the National Data Bureau
Sin gapore	Cybersecurity ACT |**2024**	launches national security label scheme for smart devices (optional)	1. strengthening security in critical infrastructure and essential services 2. increasing operator responsibilities 3. strengthening administrative power over company security
India	IT Act | **2000** Amendment ITAct | **2008**	The main law regulating information technology and computer security;	1. regulation of digital signature 2. regulation of electronic documents 3. establishment of cyber protection obligations 4. lists cyber crimes and sanctions (e.g. hacking, computer fraud)
	IT Rules | **2011**	Reasonable Security Practices and Procedures and Sensitive Personal Data or Information	Obligations for "corporate entities" to adopt reasonable security practices for "Sensitive Personal Data or Information" (SPDI)
	IT Intermediaries Guidelines Rules | **2011**	Rules for intermediaries: online platforms, service providers	1. regulates online content 2. establishes monitoring and reporting responsibilities
	Digital Personal Data Protection Act | **2023** (DPDP Act)	Law on the protection of digital personal data	1. regulates the collection, processing and distribution of data 2. establishes the rights of individuals with regard to sensitive data 3. establishes data security obligations for operators
	National Critical Information Infrastructure Protection Centre Guidelines (NCIIPC)	Rules for the protection of critical information infrastructures (CII)	regulates sectors: energy, telecom, banking
	Indian Computer Emergency Response Team (CERT-In)	Instructions & notifications	1. regulates incident reporting 2. regulates data retention procedure 3. establishes obligations for VPN service providers, etc.
	Telecommunications Act | **2023**	Regulation of the telecommunications sector, which also has an impact on cybersecurity	
EU	GDPR | **2016**	regulates the management of private user data in companies and their transfer between companies	1. better data protection 2. educating companies and individual users to be careful with personal data 3. assuming responsibility for companies based on individual agreement 4. individual users have access and power over their own transmitted data
	NIS 1 | **2018** NIS 2 | **2024**	- ensures cybersecurity in essential and important sectors - requires cyber audit and reporting of security risks	1. databases of essential and critical companies 2. auditing and mapping vulnerabilities of companies in sensitive industries
	Dora | **2023**	requires financial and banking institutions to better manage IT&C risks	1. harmonization of cyber requirements in the financial sector and between member states 2. advanced risk management 3. oversight of critical suppliers 4. involvement of board in IT&C risk management

	AI Act | **2024**	regulates the adoption and use of AI products in business operations	1. implementing AI governance 2. conducting impact assessments to ensure that individual rights are not violated 3. introducing security auditing 4. increasing transparency and reporting for generative AI providers
	Cybe Resilience ACT | **2024**	- certifies and labels hardware /software products imported, marketed or produced in the EU. - requires reporting of cyber vulnerabilities of products sold in the EU market	Solutions and services for SMEs
	Cyber Solidarity ACT | **2025**	- regulates the European integrated cyber alert system to strengthen detection, analysis and response to cyber threats European Cybersecurity Shield = 27 interacting national centers + 3 cross-border centers	The European Cybersecurity Competence Centre (ECCC), based in Romania, coordinates 3 Cross-border Security Operations Centres (SOCs) 1. ENSOC Consortium Spain, Italy, Luxembourg, Austria, Portugal, Romania, Netherlands 2. ATHENA Consortium Bulgaria, Greece, Malta 3. -
Global	ISO 27001 | **2022**	Information security management systems	
	ISO 28000| **2022**	Supply chain security management applied to all organizations regardless of size or sector	
	ISO/IEC 27036 | **2016**	Information Security for Supplier Relationships	
		ISO/IEC 27036-1:2021 – Overview and concepts Provides a general introduction to supplier relationship management	
		ISO/IEC 27036-2:2021 – Requirements Specifies security requirements for supplier relationships.	
		ISO/IEC 27036-3:2013 – Guidelines for ICT supply chain security It directly targets the IT supply chain (hardware/software).	
		ISO/IEC 27036-4:2016 – Guidelines for security of cloud services relationships	
	ISO/IEC 28000 | **2022**	**Security Management Systems for the Supply Chain** Standard for managing the security of physical supply chains.	
	ISO/IEC 27002 | **2022**	**Code of Practice for Information Security Controls** Includes specific controls for supplier relationships It is complementary to ISO/IEC 27001	
	ISO/IEC 20243 | **2018**	**Open Trusted Technology Provider Standard (O-TTPS)** Aims at the integrity and security of the supply chain for IT technologies. Covers secure practices in the design, development and distribution of hardware/software products. Useful for suppliers in the military, government, telecom, etc.	
	ISO/SAE 21434 | **2021**	**Road Vehicles: Cybersecurity Engineering** Applies to the automotive industry. Includes security requirements for the automotive supply chain	
	ISO/IEC 62443 | **2002 - 2024**	**Industrial Automation and Control Systems Security** Standard dedicated to industrial systems (OT – operational technology). Includes security requirements for component suppliers, integrators and operators in the industrial supply chain. Important for: Energy, Oil & Gas, Manufacturing	
	ISO/IEC 27019 | **2017**	**Information security for process control systems in the energy industry** Applicable to the energy supply chain. Complementary to ISO/IEC 27001, with a focus on SCADA and ICS.	

8. References

1. Academy of Management Learning & Education, 5(3), 304–313.
2. Brynjolfsson, E., & McAfee, A. (2017). Machine, Platform, Crowd: Harnessing Our Digital Future. W.W. Norton & Company.
3. Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W.W. Norton & Company.
4. Cadbury Committee. (1992). The Financial Aspects of Corporate Governance (Cadbury Report). London: Gee & Co
5. Calderón-Monge, E., & Ribeiro-Soriano, D. (2023). The role of digitalization in business and management: Asystematic literature review. Heliyon, 9(3), e14456.
6. Caldwell, C., Hayes, L. A., & Long, D. T. (2015). Leadership, trustworthiness, and ethical stewardship.
7. Castronova, E. (2002). Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier. CESifo Working Paper No. 618.

8. Catarino, J. (2024). Governance of Digital Transformation: Extended Abstract. Instituto Superior Técnico, Lisbon.
9. Daugherty, P. R., & Wilson, H. J. (2018). Human + Machine: Reimagining Work in the Age of AI. Harvard Business Review Press.
10. Debei, M. M., & Wamba, S. F. (2022). Metaverse marketing: How the metaverse will shape the future of consumer research and practice. Journal of Business Research, 153, 215–232.
11. Dede, G., Ioannidis, S., & Gkatzelis, V. (2024). Cybersecurity and Sustainable Economic Growth: Evidence from IoT and Smart Infrastructure. Information, 15(12), 798.
12. Davenport, T., & Mittal, N. (2023). All-in on AI: How Smart Companies Win Big with Artificial Intelligence. Harvard Business Review Press.
13. Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-
14. Egbuna, O. P. (2024). Artificial Intelligence and Cybersecurity: Risk and Opportunity.
15. Femi, A. G., & Asere, I. (2025). AI and Cybersecurity: Threats and Defenses in the Digital Economy. Journal of Cyber Security and Privacy, 3(1).
16. Floridi, L. (2022). Ethics, Governance, and AI. Oxford University Press.
17. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., et al. (2022). AI governance: A framework for trust and accountability. AI & Society.
18. Future Systems Journal, 5(1), 24–39.
19. Ge, Y., & Zhu, Q. (2024). Game-Theoretic Trust in AI-Driven Cyber Systems. arXiv preprint arXiv:2411.12859.
20. Government Information Quarterly, 39(4).
21. Haenlein, M., Kaplan, A., Tan, C. (2023). Artificial Intelligence and the Future of Leadership. California Management Review.
22. Harari, Y. N. (2021). Homo Deus: A Brief History of Tomorrow. Harper.
23. Hess, T. (2022). Managing the Digital Transformation: A Guide to Successful Organizational Change. Springer Gabler.
24. Hou, X., Lin, H., & Zhang, S. (2024). Machina Economicus: A New Paradigm for Prosumers in the Energy Internet of Smart Cities. arXiv preprint arXiv: 2403.14660.
25. Iansiti, M., & Lakhani, K. R. (2020). Competing in the Age of AI: Strategy and Leadership When Algorithms and Networks Run the World. Harvard Business Review Press.
26. International Journal of Innovative Economics, 5(2), 55–72.---Lucrări transversale (energie, securitate, IoT, metaverse)
27. Joshi, A. (2022). Cybersecurity Regulations and Emerging Technologies. Law and Society Journal, 4(1).
28. Joshi, A. (2022). Cybersecurity and the Digital Economy: Risk, Trust and Resilience in Smart Societies.
29. Journal of Science and Technology, 5(2).
30. Journal of Cyber Policy, 7(3), 411–428.
31. Journal of Business Ethics, 132(1), 1–13.
32. Journal of Management Studies, 58(3), 738–762.
33. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines.
34. Kane, G. C., Palmer, D., Phillips, A. N., & Kiron, D. (2019). The Technology Fallacy: How People Are the Real Key to Digital Transformation. MIT Press.
35. Kapustina, E. (2025). Corporate Governance in the Context of Business Digital Transformation.
36. Koibichuk, V. (2023). The Role of Cybersecurity in the System of Economic Security: Bibliometric Analysis.
37. Kurzweil, R. (2005). The Singularity Is Near: When Humans Transcend Biology. Viking.
38. Leahovcenco, A. (2021). Cybersecurity and the Digital Economy: Interconnections and Challenges. MEST Journal, 9(2), 10–17.
39. Lee, L.-H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A., & Hui, P. (2021). All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda. ArXiv preprint arXiv: 2110.05352.
40. Maak, T., & Pless, N. M. (2006). Responsible leadership in a stakeholder society – A relational perspective.
41. Mackey, J., & Sisodia, R. (2013). Conscious Capitalism: Liberating the Heroic Spirit of Business. Harvard Business Review Press.
42. Nature Machine Intelligence, 1(9), 389–399.
43. OECD. (2023). G20/OECD Principles of Corporate Governance. OECD Publishing.
44. OECD. (2020). Digital Government Index: 2019 results. OECD Publishing.
45. OECD. (2023). Digital Economy Outlook 2023. OECD Publishing.
46. Organisation for Economic Co-operation and Development (OECD). (2023). Digital Government Review of Latin America and the Caribbean: Building Inclusive and Responsive Public Services. OECD Publishing.
47. Organisation for Economic Co-operation and Development (OECD). (1998). The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda. OECD Publishing.
48. Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). Platform Revolution: How Networked Markets Are Transforming the Economy—and How to Make Them Work for You. W. W. Norton & Company.
49. Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox.
50. Rifkin, J. (2009). The Empathic Civilization: The Race to Global Consciousness in a World in Crisis. Penguin.

51. Sambamurthy, V., & Zmud, R. W. (2017). Digital governance: Balancing control and innovation in digital transformation. MIS Quarterly Executive.
52. Schwarzmüller, T., Brosi, P., Duman, D., & Welpe, I. (2018). How does the digital transformation affect organizations? Key themes of change in work design and leadership. Frontiers in Psychology, 9 (1139).
53. Schwab, K. (2016). The Fourth Industrial Revolution. World Economic Forum.
54. Schwab, K. (2022). The Fourth Industrial Revolution – Updated Edition. World Economic Forum.
55. Sun, Y., & Guo, J. (2024). How does digital transformation affect corporate governance paradigms? A synthesis of the literature.
56. Tapscott, D. (1995). The Digital Economy: Promise and Peril in the Age of Networked Intelligence. McGraw-Hill.
57. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.
58. The American Journal of Management and Economics Innovation, 7(1), 15–28.
59. 59. Tricker, B. (2019). Corporate Governance: Principles, Policies, and Practices. Oxford University Press.
60. Van den Broek, T. A., et al. (2021). Digital transformation in government: A governance perspective. Government Information Quarterly.
61. Weill, P., & Woerner, S. (2021). Future Ready: The Four Pathways to Capturing Digital Value. Harvard Business Review Press
62. Weill, P., & Ross, J. W. (2004). IT Governance: How Top Performers Manage IT Decision
63. Weinberg, S., & Cohen, J. (2024). Zero Trust Implementation in Hybrid Infrastructures. arXiv preprint arXiv:2401.09575.
64. Weinberg, J., & Cohen, E. (2024). Smart Infrastructures and the Economics of Cyber Resilience. Technological Forecasting & Social Change, 198, 122–139
65. Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading Digital: Turning Technology into Business Transformation. Harvard Business Review Press.
66. Rights for Superior Results. Harvard Business School Press.
67. Yeung, K. (2021). Algorithmic regulation and governance through AI. Regulation & Governance.
68. Zhang, J., Chen, J., & Lee, C. (2022). AI-driven public governance: Opportunities and risks.