

HOW DIGITAL TRANSFORMATION AND CYBERSECURITY AFFECT COMPANIES' PERFORMANCE?

Oana Alexandra SARCEA (MANEA)

National University of Political Studies and Public Administration

30A Expozitiei Blvd, Sector 1, 012104 Bucharest, RO

oana.manea.22@drd.snsa.ro

doi: 10.25019/STR/2023.039

Abstract

This research paper delves into the complex interplay between digital transformation and cybersecurity, elucidating their combined impact on organizational performance. The ever-evolving landscape of technology has led to a symbiotic relationship between these two domains, shaping the strategies and outcomes of modern businesses. A thorough examination of the existing scientific literature reveals the multifaceted nature of digital transformation and its integral role in contemporary business performance. The literature underscores the significance of cybersecurity as a critical digitalization enabler, emphasizing its role in safeguarding sensitive information, mitigating risks, and enhancing overall resilience. Furthermore, a bibliometric analysis conducted using VoS Viewer complements the literature review, offering a quantitative perspective on the evolution and trends within these domains.

Keywords

change management; cybersecurity; digital transformation; organizational performance; strategies.

Introduction

In an era of relentless technological advancements, the synergy between digital transformation and cybersecurity has emerged as a pivotal frontier, reshaping the contemporary business landscape. This study ventures into this intricate nexus, unraveling its profound implications for organizational performance across a spectrum of companies. The main argument underpinning this exploration centers on the novel intersections between digital transformation, cybersecurity, and their collective influence on businesses.

Digitalization, an omnipresent force, has permeated every facet of modern enterprises. It is no longer a matter of technological adaptation but a transformative journey that revolutionizes how organizations deliver value and engage with their clientele (Hinings et al., 2018). This metamorphosis transcends mere technical shifts, delving into the realms of strategic orientation and the quest for sustainable competitive advantages. In essence, digitalization has become the linchpin of contemporary business strategies, reshaping operational paradigms and consumer interactions.

Concurrently, the global discourse on internet governance has witnessed a pronounced shift towards cybersecurity. It has been identified as one of the most pivotal domains in this broader context (De Nardis, 2014). Mueller's astute observation (2017) accentuates the conflation of cybersecurity with state responsibility and national

security, potentially leading to a transformation in global internet policy-making. This phenomenon underscores the escalating importance of cybersecurity in the face of the relentless march of digital transformation.

The rapid digital transformation, technological leaps, and the burgeoning expertise of cybercriminals have fueled a sharp upsurge in cyberattacks targeting organizations. The financial ramifications of these attacks, estimated to cost between \$375 and \$575 billion annually, are staggering (Carcary, Doherty, & Conway, 2019). Moreover, the expanding interconnectedness of devices, systems, and collaborations amplifies the potential points of vulnerability within organizations. In response, organizations have adopted diverse approaches to address these threats, leading to varying degrees of cybersecurity readiness and resilience.

In light of these evolving challenges, traditional cybersecurity paradigms anchored in access controls and perimeter defenses are proving inadequate. Even organizations with a propensity for risk recognize robust cybersecurity's indispensability. A paradigm shift is imperative, encompassing holistic, proactive approaches capable of adapting to emerging threats. Consequently, assessing cybersecurity effectiveness becomes paramount, and herein lies the significance of the conceptual framework presented in this study. Organizations can fortify their cybersecurity strategies and adeptly counteract evolving threats by meticulously scrutinizing critical factors and management themes.

One compelling avenue for addressing cyber threats lies in integrating artificial intelligence (AI) within cybersecurity protocols. AI empowers organizations to automate threat detection and mitigation, ensuring swift and precise responses across a spectrum of attacks. AI's capacity to discern real-time behavioral patterns and anomalies, coupled with its adaptive learning from previous incidents, endows organizations with a formidable arsenal against evolving threats. It is a powerful ally in the battle to secure digital landscapes against increasingly sophisticated adversaries.

In this dynamic landscape, the fusion of cybersecurity measures (Khursheed et al., 2016) with digital transformation initiatives emerges as the catalyst for enhancing organizational performance. This convergence safeguards sensitive data and operations, streamlines processes, optimize resource utilization, and fosters innovation. It creates a resilient digital foundation that empowers companies to leverage the full potential of digital transformation, thereby augmenting overall efficiency and competitiveness within the dynamic modern business arena.

This study explores the intricate relationship between digital transformation and cybersecurity and their impact on organizational performance in today's rapidly advancing technological landscape. The central argument revolves around the intersections of these two areas and their collective influence on businesses. Given the increasing importance of digital transformation and cybersecurity and their effects on companies and societies, this paper provides an overview of the current state of these two constructs in the literature. An analysis of co-occurrence, based on selected keywords, was conducted to achieve this.

Literature review

The "digital transformation" concept has garnered substantial attention in contemporary discourse, yet it remains a multifaceted and evolving phenomenon with no universally accepted definition. Scholars have approached the subject from diverse angles, shedding light on its intricate dimensions. At its core, digital transformation represents a paradigm shift driven by technology, reshaping fundamental aspects of organizational existence (Westerman et al., 2014). However, it transcends technological upgrades, encapsulating profound alterations across products, processes, organizational structures, and management paradigms (Cheng et al., 2016). The transformative nature of digitalization extends beyond technology, exerting its influence on people, society, communication, and the broader business landscape (Brynjolfsson & McAfee, 2014).

Digital transformation is a globally significant and widely discussed subject of immense importance for companies across all industries. It fundamentally reshapes customer interactions, internal operations, and organizational value creation. One of the primary challenges stakeholders face in this transformative process is formulating a clear vision and a strategic roadmap that guides the path forward (Zaoui & Souissi, 2020). While many technologies underpinning digital transformation are not novel innovations, the innovation lies in their integration into a seamless tapestry of capabilities (Hirsch-Kreinsen & ten Hompel 2017). These technologies, often referred to as "general-purpose technologies," encompass cyber-physical systems (CPS), the industrial internet of things (I/loT), cloud computing (CC), big data (BD), artificial intelligence, and augmented and virtual reality (Cheng et al., 2016).

Embracing digital transformation often necessitates radical changes within organizations. This transition can be daunting, and many organizations grapple with the profound shifts required (Brynjolfsson & McAfee, 2014). Nonetheless, researchers and practitioners alike acknowledge its transformative potential. Digitalization engenders manifold benefits, enhancing sales and productivity through innovative value creation and novel interactions with customers and suppliers (Parviainen et al., 2017). For instance, the interconnectivity of digital machines fosters flexible, small-scale production, revolutionizing the value-creation process. Digital communication channels and virtual networks reshape business practices, bestowing competitive advantages (Parviainen et al., 2017). Moreover, digital transformation spurs job growth, particularly in service sectors and robot development (Brynjolfsson & McAfee, 2014).

In today's business landscape, competitive differentiation is increasingly rooted in superior digital capabilities and technological elements that enable agile product/service delivery. Leading organizations, whether originally digital or traditional enterprises have made substantial investments in new business models and digital strategies (Cozza et al., 2020). These companies have entered the digital age with robust technology foundations, positioning them as leaders within their respective industries. In the coming years, the survival of the fittest in this context implies that some companies will successfully harness the advantages of digital technologies, while others may face challenges and potentially fail to adapt.

Digital transformation is characterized by an intricate amalgamation of technologies, including the Internet of Things (IoT), Additive Manufacturing, Big Data, Artificial Intelligence, Cloud Computing, Augmented and Virtual Reality, and Blockchain, among others (Rindfleisch et al., 2017). However, the primary challenge lies in understanding the organizational metamorphosis catalyzed by these technologies. While each technology bears transformative potential in isolation, their combined impact is unparalleled and disruptively transformative (Teece, 2018; Nelson, 2018).

Companies that seek to excel in this digital landscape must reevaluate traditional strategic approaches. By blending classic strategies with innovative tactics, organizations can craft a strategy capable of thriving in an era of digital disruption (Gauger, Bachtal, & Pfnür, 2022). In the coming years, the pace of technological change is expected to accelerate, further deepening its influence on the business landscape. Consequently, surviving in this context implies that companies will need to embrace digital transformation and adapt successfully, much like in an evolutionary process. (Pînzaru, Zbucea, & Vițelar, 2019, p. 643)

The synergy between digitalization and innovation represents an emerging paradigm with unique challenges and opportunities. Innovation management in the context of digital transformation lacks predefined roadmaps and often involves intricate temporal sequences of events (Nybakk & Jenssen, 2012). The management of conflicts within this innovation process is integral to its successful navigation. In contemporary business landscapes, organizations are keenly aware of the competitive differentiation offered by digitalization (Blackburn et al., 2021). Beyond innovations in business models, digitalization influences cost-effectiveness, productivity, efficiency, and various other organizational goals. Notably, investments in digitalization commenced even before the pandemic, signaling a growing trend.

Leao and daSilva (2021) emphasize the significant influence of digital transformation on firms' competitiveness. This impact extends to various facets, including innovation, efficiency, and cost reduction. Furthermore, digital transformation has profound implications for global value chains, affecting specialization, geographic scope, governance, and upgrading factors. Although digital transformation introduces transformative shifts, it generally yields predominantly positive impacts for firms that embark on this journey.

Pînzaru et al. (2022) underline that digital transformation, much like sustainability, is not merely an end in itself but rather an integral aspect of modern business strategies, and it serves as a catalyst for sustainability in various contexts, generating innovative tools, leading to indirect benefits, and fostering new managerial approaches. This transformation also influences the development of novel digital business models driven by technological advancements and geared towards implementing sustainable, service-oriented practices for long-term business viability (Pînzaru, Zbucea, & Vereș, 2022, p. 30).

In the digital age, businesses face critical decisions regarding outsourcing (Wooding, 2022). While outsourcing can optimize resource utilization by freeing up time and resources through delegating tasks like bookkeeping, admin services, or IT support, core elements of a business should not be outsourced. Functions integral to a

company's identity, such as sales, remain closely tied to the founder's vision and personality, making them unsuitable for outsourcing.

Continuous technology innovation is reshaping labor markets globally and introducing significant changes (KU Leuven and Utrecht University, commissioned by Randstad, 2016). Routine tasks are increasingly at risk of automation, leading to a shift in the labor market's composition. The emergence of high-tech, well-paid jobs contrasts with the decline in low-skilled production roles. Employers seek candidates with interpersonal, communication, and analytical skills to meet the demands of growing sectors like education and healthcare. This changing landscape necessitates reevaluating skills acquisition and education systems to align with the requirements of the digital economy.


In the rapidly expanding cyberspace context, there is a significant concern about safeguarding this environment from cyberattacks (Hopkins and Dehghantanha, 2016). It's crucial to emphasize that these cyberattacks substantially threaten companies' digital transformation initiatives. For instance, over 4,000 ransomware attacks are reported daily in the United States, and over 330,000 malware programs are generated annually (Hasani et al., 2023). Furthermore, it is anticipated that these numbers will worsen as cyberattacks continue to evolve in terms of their scale and complexity.

Hasan et al. (2021) underline in their study that the increase in cyber-attacks in recent years has had a negative impact on organizations globally. Organizations are facing the challenge of enhancing their cybersecurity to combat these attacks. Cybersecurity readiness positively impacts security performance, which, in turn, affects financial and non-financial performance, and organizations can better prepare themselves to minimize the occurrence and impact of cyber-attacks (Hasan et al., 2021).

Methodology

In this section, we elucidate the research approach and methodology employed to explore the keywords' co-occurrence within the realm of "Digital Transformation," "Cybersecurity," and "Performance." Our primary aim is to discern overarching research trends and patterns in this multifaceted domain. To accomplish our research objectives, we extensively searched for relevant academic papers in Scopus and Web of Science, two reputable bibliographic databases known for their comprehensive coverage of peer-reviewed, high-quality publications. The search spanned the publication years from 2019 to 2023 without imposing date filters, underscoring the novelty and timeliness of the subject matter. This broad timeframe allowed us to capture the most recent developments and trends in the field. A total of 45 documents focused on this particular research area were found in Scopus, and 25 papers were found in the Web of Science database. After combining the files and removing duplicates using Zotero software, 52 publications remained for VosViewer analysis.

Regarding the keywords in terms of co-occurrence, 7 keywords met the threshold of 5 minimum number of occurrences; the terms "cyber security" and "cybersecurity" were merged using a thesaurus file, as in the first instance, they appeared as separate keywords. The full counting method was used. Figure 3 shows the most frequently used keywords, their number of occurrences and their total link strength with the other keywords.

 **Verify selected keywords**

Selected	Keyword	Occurrences	Total link strength
<input checked="" type="checkbox"/>	cybersecurity	20	36
<input checked="" type="checkbox"/>	digital transformation	20	29
<input checked="" type="checkbox"/>	industry 4.0	8	15
<input checked="" type="checkbox"/>	risk assessment	5	13
<input checked="" type="checkbox"/>	risk management	5	13
<input checked="" type="checkbox"/>	internet of things	5	12
<input checked="" type="checkbox"/>	network security	6	12

Figure 1. Keywords in terms of co-occurrence (>5)
 (Source: Authors' own research results)

Figure 4 represents the co-occurrence of keywords network in VosViewer, their interconnections, and their link strength. The analysis yielded two separate clusters of keywords, represented in the figure in two distinct colors, red and yellow. There are 18 links between these keywords, with a total link strength of 65, suggesting meaningful relationships between the terms identified in the clusters and significant interconnections between them. The strongest link is the one between digital transformation and cybersecurity. It shows their inherent interdependency and implies that digital transformation in organizations relies heavily on robust cybersecurity systems and practices to protect all digital assets and data. The overall landscape suggests that research is focused on exploring the potential risks of implementing digital transformation processes and applications and developing strategies to mitigate them. The current study is also anchored in the context of the fourth industrial revolution, or Industry 4.0, characterized by interconnectivity, automation, and high technology advancements bringing digital developments into the physical world. It appears that research is being conducted on innovative technologies that could enhance security in digital systems and networks.

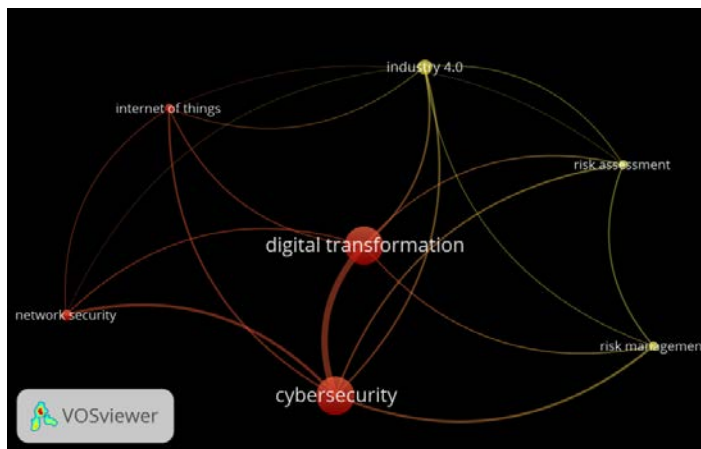


Figure 2. Co-occurrence map of keywords in Vosviewer
 (Source: Authors' own research results)

Table 1 shows the terms in the red cluster and their definitions.

Term	Definition
Cybersecurity (Kuzior et al., 2022)	The practice and measures taken for protecting computer systems, networks, devices, and data from unauthorized access, theft, damage, or criminal use.
Digital Transformation (Kraus et al., 2021)	Remodeling and reimagining business processes by implementing digital technologies into various aspects of an organization.
Internet of Things (IoT) (Kumar et al., 2019)	The use of the internet for connecting devices, services, and automated systems embedded with sensors creates a network of objects working in sync, from which data can be extracted.
Network Security (Amarudin et al., 2020)	Network protection measures, including firewalls and encryption, in place to prevent unauthorized access, misuse, and cyber-attacks.

Table 1. Red cluster concepts definition (Source: Authors' own research results)

The red cluster indicates a growing emphasis on securing digital systems during the process of digital transformation. The focus is ensuring the safety of interconnected IoT devices and networks that generate vast amounts of data. Issues with one component can quickly spread, potentially causing major problems. This cluster highlights the strong link between digital transformation and cybersecurity, suggesting a holistic approach that includes technology, processes, policies, and human factors to ensure the security of digital systems throughout their lifecycle. This cluster signifies an understanding that the protection of digital assets goes beyond mere technological measures, and the researchers are working on finding holistic approaches for digital transformation at a system level, which encloses the human factor, technology, operational processes, etc.

Table 2 exhibits the concepts in the yellow cluster and their short definitions.

Term	Definition
Industry 4.0 (Ghobakhloo, 2020)	The 4th industrial revolution wave, characterized by the integration of digital technologies (CPS, IoT, AI cloud computing, etc.), data exchange, and automation into manufacturing and production processes.
Risk Assessment (Rodríguez-Espíndola et al., 2022)	Assessing the probability and potential consequences of different risks (including intrinsic vulnerabilities and external threats) for an organization, company, system, process, etc.
Risk Management (Rodríguez-Espíndola et al., 2022)	The strategies, methods, and techniques used to evaluate, rank, and mitigate risks to prevent any unfavorable outcomes or possible repercussions.

Table 2. Yellow cluster concepts definition (Source: Authors' own research results)

The topic of the yellow cluster is the integration of digital technologies into industrial and organizational processes, along with the potential risks that come with it. This includes risk management in the context of the fourth industrial revolution. The study

focuses on the risks associated with implementing Industry 4.0 applications, such as robotics, machine learning, artificial intelligence, predictive maintenance, and 3D printing. Therefore, these technologies can have significant ethical and practical implications and are thoroughly examined. The yellow cluster centers on exploring ways to enhance organizational operations in the digital era while mitigating potential risks. The elements of this cluster stress the importance of approaching digitalization with caution so as not to disrupt existing processes. Additionally, the yellow cluster highlights the critical role of risk assessment and management in the ever-changing landscape of the fourth industrial revolution.

Results and discussion

Concluding, the clusters demonstrate the current research landscape that recognizes cybersecurity and risk management as essential components in digital transformation processes for organizations. These systems' accuracy and sustainable performance are directly linked to their efficiency. The environment will force most companies to rethink their strategy and approach the actual era of investing in new tools, elements, and machineries for a sustainable and going concern business (Grigorescu & Sarcea, 2022).

Cloud computing has allowed companies to be able to give up some or all of their IT investments since the 2000s, in favor of online services (storage, software, computing power, etc.). One in four companies in the European Union with 10 or more than 10 employees uses cloud-based paid services, compared to one in five in 2018 in France - mainly the difference is due to companies that have fewer than 250 employees. It varies depending on the size of the companies the services paid for the cloud. There are more chances to buy accounting software for smaller companies, and the focus on managing customer relationships remains on the side of larger companies. The computing power in the cloud and its acquisition can be easily reduced or increased, this phenomenon being advantageous to a new practice on the market: the analysis of large volumes of data. 16% of French enterprises with 10 or more employees perform extensive data analyses, compared to 12% in the European Union. The companies that provide services for analyzing large volumes of data in France use more data from the geolocation of mobile devices than, on average, at the level of the European Union (Cloud Computing and Big Data: Dematerialization at the Service of European Companies).

Conclusions

This research paper explores two prominent academic directions in the field: the first direction encompasses technical aspects, including technological adaptation and cybersecurity measures, and the second direction is equally significant, emphasizing managerial effectiveness and risk management. These two directions collectively contribute to understanding how organizations strategically navigate the evolving digital transformation landscape to achieve sustainable competitive advantages and optimize consumer interactions. Digital transformation is no longer a matter of technological adaptation but a transformative journey that reshapes how organizations operate and deliver value. It transcends technology and influences strategic orientation, sustainable competitive advantages, and consumer interactions.

The global discourse on internet governance has seen a pronounced shift towards cybersecurity. The rapid digital transformation has led to increased cyberattacks, emphasizing cybersecurity's escalating importance. The financial ramifications of cyberattacks are substantial, and organizations are adopting diverse approaches to address these threats. Traditional cybersecurity paradigms based on access controls and perimeter defenses are proving insufficient in the face of evolving threats. Organizations recognize the need for robust cybersecurity strategies encompassing holistic, proactive approaches. Integrating artificial intelligence (AI) within cybersecurity protocols offers the potential to effectively automate threat detection and mitigation.

The bibliometric analysis using VoS Viewer identified significant research trends and relationships between keywords such as "digital transformation" and "cybersecurity." The study emphasized the interdependency between these terms and focused on exploring risks associated with digital transformation and strategies to mitigate them. Researchers are also exploring innovative technologies to enhance security in digital systems and networks.

In conclusion, the dynamic interplay between digital transformation and cybersecurity reshapes the business landscape. Organizations that recognize the symbiotic relationship between these domains and adopt holistic cybersecurity measures are better positioned to thrive in the digital age. The ongoing research in this field underscores the importance of staying informed and adaptive in the face of evolving technology and security challenges.

References

- Amarudin, Ferdiana, R., & Widyawan. (2020, November 10). A Systematic Literature Review of Intrusion Detection System for Network Security: Research Trends, Datasets and Methods. In *2020 4th International Conference on Informatics and Computational Sciences (ICICoS)*. <https://doi.org/10.1109/icicos51170.2020.9299068>
- Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (1st ed.). W. W. Norton & Company.
- Carcary, M., Doherty, E., & Conway, G. (2019). A Framework for Managing Cybersecurity Effectiveness in the Digital Context. In *Proceedings Paper of the 18th European Conference on Cyber warfare and Security (ECCWS 2019)* (pp. 78-86).
- Cheng, G., Liu, L., Qiang, X., & Liu, Y. (2016). Industry 4.0 development and application of intelligent manufacturing. In *2016 International Conference on Information System and Artificial Intelligence (ISAI)* (pp. 407-410).
- CIMA E1. (2019). *Managing Finance in a Digital World*.
- Cozza, M., Gherardi, S., Graziano, V., Johansson, J., Mondon-Navazo, M., Murgia, A., & Trogal, K. (2021). COVID-19 as a breakdown in the texture of social practices. *Gender, Work & Organization*, 28, 190-208. <https://doi.org/10.1111/gwao.12524>
- De Nardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

Gauger, F., Bachtal, Y., & Pfnür, A. (2022). Work experience from home: Hybrid work and the future of distributed work locations — a comparative empirical analysis between the US and Germany. *Corporate Real Estate Journal*, 11(3), 280-292.

Ghobakhloo, M. (2020). Industry 4.0, digitization, and opportunities for sustainability. *Journal of Cleaner Production*, 252, 119869. <https://doi.org/10.1016/j.jclepro.2019.119869>

Grigorescu, A., & Sarcea (Manea), O.-A. (2022). Managing Business in a Digital World – Covid-19 Impact: Innovation tools and techniques. In *8th BASIQ International Conference on New Trends in Sustainable Business and Consumption - Graz, Austria*.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, 3(5), 97. <https://doi.org/10.1007/s43546-023-00477-6>

Hinings, B., Gegenhuber, T., & Greenwood, R. (2018). Digital innovation and transformation: an institutional perspective. *Information and Organization*, 28(2), 52-61.

Hirsch-Kreinsen, H., & ten Hompel, M. (2017). Digitalisierung industrieller Arbeit: Entwicklungsperspektiven und Gestaltungsansätze. In *Handbuch Industrie 4.0* (vol. 3, pp. 357–376). Springer.

Khursheed, A., Kumar, M., & Sharma, M. (2016). Security against cyber-attacks in food industry. *International Journal of Control Theory and Applications*, 9(17), 8623-8628.

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital Transformation: An Overview of the Current State of the Art of Research. *SAGE Open*, 11(3). <https://doi.org/10.1177/215824402111047576>

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*, 6, 111. <https://doi.org/10.1186/s40537-019-0268-2>

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022). Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(4), 195. <https://doi.org/10.3390/joitmc8040195>

Leao, P., & DaSilva, M. M. (2021). Impacts of digital transformation on firms' competitive advantages: A systematic literature review. *Strategic Change Journal*, 30(5), 421–441. <https://doi.org/10.1002/jsc.2459>

Mueller, M. (2017). Is Cybersecurity eating internet governance? Causes and consequences of alternate framings. Paper presented at Who Governs? States or Stakeholders? Cybersecurity and Internet Governance: Third Annual Workshop Internet Governance Project, GA Tech School of Public Policy, Atlanta, 11-12 May.

- Nelson, R. R. (2018). Observations and conjectures stimulated by David Teece's "profiting from innovation in the digital economy". *Research Policy Journal*, 47(8), 1388-1390.
- Nybakk, E., & Jenssen, J. I. (2012). Innovation strategy, working climate, and financial performance in traditional manufacturing firms: An empirical analysis. *International Journal of Innovation Management*, 16(02), 1250008.
<https://doi.org/10.1142/S1363919611003374>
- Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2017). Tackling the digitalization challenge: how to benefit from digitalization in practice. *International Journal Information System Project Management*, 5, 63-77.
<https://doi.org/10.12821/ijispm050104>
- Pînzaru, F., Dima, A. M., Zbucea, A., & Vereş, Z. (2022). Adopting sustainability and digital transformation in business in Romania: A multifaceted approach in the context of the just transition. *Amfiteatru Economic*, 24(59), 27-44
- Pînzaru, F., Zbucea, A., & Vişelar, A. (2019). Digital transformation trends reshaping companies. In *Proceedings of the International Conference on Business Excellence*, 13(1), 635-646. <https://doi.org/10.2478/picbe-2019-0056>
- Rindfleisch, A., O'Hern, M., & Sachdev, V. (2017). The digital revolution, 3D printing, and innovation as data. *Journal of Product Innovation Management*, 34(5), 681-690.
<https://doi.org/10.1111/jpim.12402>
- Rodríguez-Espíndola, O., Chowdhury, S., Dey, P. K., Albores, P., & Emrouznejad, A. (2022). Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. *Technological Forecasting and Social Change*, 178, 121562. <https://doi.org/10.1016/j.techfore.2022.121562>
- Teece, D. J. (2018). Profiting from innovation in the digital economy: enabling technologies, standards, and licensing models in the wireless world. *Research Policy Journal*, 47(8), 1367-1387.
- Westerman, G., Bonnet, D., & McAfee, A. (2014). The nine elements of digital transformation. *MIT Sloan Management Review*, 55, 1-6.
- Wooding, A. (2022). Helping small businesses focus on business growth – LinkedIn Article, Business and personal Page.
- Zaoui, F., & Souissi, N. (2020). Roadmap for digital transformation: A literature review. *Procedia Computer Science*, 175, 621-628