Artificial intelligence in business models as a tool for managing digital risks in international markets

Luka Buntić[1*], *Mate* Damić[1], *and Ines* Dužević[1]

[1]University of Zagreb, Faculty of Economics and Business, Department of Trade and International Business, Trg J. F. Kennedyja 6, 10000 Zagreb, Croatia

Abstract.

Research background: Through the ongoing trend of digitalization, organizations competing in international markets are getting more exposed to different technology related risks. Globalization and technology support enabled small tech-based companies to scale and expand their business. On the other hand, this has also led to a significant rise of different types of threats. Companies engaged in the process of internalization are more exposed to digital risks than companies competing on the local market. In order to help their companies to manage digital risks, governments use relevant institutions and resources. However, many organizations still largely depend on their own capabilities. A growing number of organizations uses artificial intelligence in business models as a new type of response to digital risks. Artificial intelligence could be the missing link that will help connect organizational and government resources for successful management of digital risks.
Purpose of the article: To shed more light on this understudied issue, we conducted a literature review on the use of artificial intelligence in business models as a tool for managing digital risks on the global market.
Methods: Literature review.
Findings & Value added: We analysed the key determinants of artificial intelligence, their use in business models, and the way it can help organizations manage digital risks. Literature review summarizes the most important research on the topic and proposes new avenues for future research.

Keywords: *artificial intelligence; business model; digital risks; globalization*

JEL Classification: *M10; M16; F23*

[*] Corresponding author : lbuntic@efzg.hr

1 Introduction

The process of digital transformation has made a significant impact on how companies build a strategy to enter international markets. When creating an internalization strategy, companies need to consider the (de)regulation of international markets, and the potential digital risks that may occur on that market as well. These digital risks could be initiated by competitors, individuals or even foreign governments. Formerly they were characterized as industrial espionage, but nowadays they are more sophisticated, and are classified as security breaches. Companies struggle to find a way of achieving a competitive advantage on the global market against these risks. Accordingly, some companies have started to innovate their business models by implementing artificial intelligence (AI) solutions.

2 Methods

To shed more light on this understudied research area, we have written this exploratory paper. The aim of this study is to identify digital risks companies are facing on international markets, and the possibilities of AI technology that help manage these risks. The scope of the study is limited to summarising key steps in the development of AI implementation in business models as well as discussing related risks and potential future trends in the research field.

3 Digital risks in international markets

Organizations competing on the global market are handling large data sets related to different categories of stakeholders. This data usually contains very sensitive information. Therefore, security seems to be one of the most important segments of organizational capabilities which dictates the tempo of digital transformation [1]. The key digital risk today comes in the form of cyber-attacks. Any attempt to change, disable, destroy, steal or gain unauthorized access to a company's computer network and data can be classified as a cyber – attack. These attacks are usually launched by competitors, individuals or governments that try to gain unauthorized data access in order to gain leverage against an organization. To prevent these attacks from occurring, organizations usually create a digital security strategy. One of the key elements necessary for digital security strategy is employee education. Through education, employees of an organisation can be made aware of the kinds of attacks that can occur and what they could do about them. These strategies focus on learning proper operating procedures, the key attack targets, and the classic attack methods. Other countermeasures regarding cyber-attacks could include [2]:

- Legal Responses - Laws can however be effective against repeat offenders.
- Patches - fix flaws or bugs in software as soon as they are discovered.
- Backups - making copies of digital information is essential to recovery from attack.
- Access Controls - generally managed by passwords.
- Encryption - Any attempts to modify encrypted data will result in indecipherability.
- Intrusion Detection and Computer Forensics - Forensics includes a wide variety of techniques and requires an intelligent investigator.
- Honeypots - systems with no legitimate purpose other than to receive attackers, so everyone using them other than their system administrator is inherently suspicious.
- Intrusion Prevention Systems - active network defence.
- Back Tracing - find where an external attack is coming from so as to stop it more easily.
- Counterattacking
- Deception - mislead attackers to prevent them from achieving their goals.

These countermeasures can be considered as traditional tools. Artificial intelligence, on the other hand is the future of digital risk management [3]. There are several key elements that define artificial intelligence. Reim et al. state that "AI can be categorized as a capital–labour hybrid with the ability to self-learn, continuously improve and quickly scale-up" [1]. Also, AI could be defined as: "any artificial system that performs tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance. AI could solve tasks requiring human-like perception, cognition, planning, learning, communication, or physical action" [4]. Moreover, AI can continuously gather behavioural biometrics data and learn as input data changes through time to act appropriate [5]. Based on traits described above AI is an ideal tool for digital risk management. However, there are two major risks related to the use of AI in companies facing digital risk on the global market [6].

The first one is the risk of not implementing the AI on time. AI will inevitably impact the labour market. It is estimated that AI will replace almost 50% of all jobs by 2030. Accordingly, companies face the risk of becoming irrelevant on the global market without implementing the AI in their businesses. Furman and Seamans state that artificial intelligence and robotics have the potential of raising productivity, but their further development could continue or aggravate trends in declining labour force participation and increased inequality [7]. Another risk related to implementation of AI is that without AI, it is almost impossible to create a good security strategy and detect AI on the other side of the competition. There are unsophisticated programmers who are not skilled enough to develop their own cyber-attack programs but can effectively mix, match, and execute code developed by others. This category of narrow AI lowers the bar for attacks by individuals and non-state groups while increasing the scale of potential attacks for all actors and the capabilities of unsophisticated programmers.

With the development of automated decision-making systems, transparency became crucial topic due to the fact that decisions are delegated to a machine or a system [8]. Machine learning with other AI technologies is embedded in everyday communication services [9]. Machine learning algorithms are programmed to detect content and to remove it, block it, or filter it out before it is uploaded on some platforms [10].

4 Rapid development of AI and security concerns

Although research of AI began in the 1950s, more significant growth occurred in 2010s with the availability of "big data" sources, improvements to machine learning approaches, and increase in computer processing power. This growth strengthened Narrow AI (algorithms that address specific problem sets like game playing, image recognition, and self-driving vehicles). Usual approach to Narrow AI is machine learning, which involves statistical algorithms that replicate human cognitive tasks by deriving their own procedures through analysis of large training data sets. During the training process, the computer system creates its own statistical model to accomplish the specified task in various situations [4]. In the past, machines have been used for automated routine tasks, but what makes AI special is the growing capacity for automated non-routine tasks or knowledge-based work [11].

Fountain et al. estimate that AI will add $13 trillion to the global economy over the next decade as companies see rapid advancements and affordability in development platforms, vast processing power and data storage [12]. The development of AI can be seen as a disruptive innovation that has the potential to change the rules of competition in many industries. Implementation of AI can be a catalyst for business model innovation and enabler for disruption in industries [1]. The growing importance of AI is supported by globalization and redefinition of professional standards as well as deregulation of professional monopolies [11].

AI has radical, massive and widespread impact on the society [13]. Therefore, companies and governments often invest heavily in automated systems in order to achieve benefits for society [14] and the best examples are China and the USA [15]. Many countries have started to invest in AI to gain competitive advantage and to help domestic companies face the global competition. According to [16] companies that lead in specific uses of AI could create significant economic advantages for countries in which they operate. This is particularly true for heavy compute algorithms and other first mover advantages that are difficult to replicate. This type of AI intellectual property can ensure future economic leadership for pioneer countries. Chinese government believes AI is crucial for the future of global military and economic power [17]. India seems to be a major player in the future of AI development as well, evidenced by a growing number of AI start-ups, where private sector investments are projected to increase to $500 million [16].

Although there are many positive effects that can be expected from AI application in the future, it could also be misused to manipulate financial markets and destabilize currencies. Financial records present an important source of data for investigations and intelligence work. While daily communication is being encrypted, tools to use financial data have not evolved on the same level. This gap could be filled by AI in the future [6]. [18] argues AI has the potential to be the key part of transformative economic technology and dramatically accelerate the pace of innovation and productivity growth with the key roles in automation of scientific experiments, synthesizing findings in thousands of scientific papers and automatically generating and optimizing engineering designs.

The application of AI in everyday business routines will not only influence digital risk management, but also likely lead to large-scale shifts in the global economy as well as social and political impact. Horowitz eta al. state countries could face different AI related scenarios [6]:

- Bounty – AI increased productivity and prosperity for all citizens.
- Rising inequality –in a labour-light economy where the wealthy get wealthier.
- Resource curse – economic paradox in countries abundant in natural resources.
- Luddite's revenge – where scenarios of the 19th century Luddites come true and machinery eliminates jobs that are not replaced by new ones.
- Generational dislocation – social and political disruption lasting a generation because of the mismatch of skills between the people.
- Fall behind – Due to resistance of economic and political disruption, but maintain stability.

However, [16] emphasize that key power players in AI up to this point were private sector companies, not governments. Combining resources of big tech companies such as Google, Facebook or Twitter with government agencies could be the key for application of AI that will be beneficial for all parties included.

5 Implementation of AI in business models

The implementation of AI tools in the business model may help companies to prevent digital risks on the global market. Besides preventing the digital risks of a company, AI systems that rely on anomaly detection can help companies find new opportunities and AI algorithms can manage the innovation process [19].

Wirtz and Daiser state that if implemented successfully, the business model can present a source of competitive advantage [20]. On the global market, multinational corporations often buy IT companies with proven record in AI development. This can be seen as a strategic move due to the fact that the development of these tools requires specific employee skills that are hard to come by and expensive. Companies like Airbus, BP, Infosys, Wells Fargo, and Ping An Insurance solved their important business problems in a quick and efficient way

using AI [3]. Armour and Sako state that the key point of AI implementation is how tasks, and not jobs, are automated which can be related to business models [11].

Business models describe a firm's logic of value creation, delivery, and capture. Main differences between the traditional business models and AI enabled business models are the delivery of scaled services, using output-based pricing models, combining non-human with human capital and creating a multidisciplinary mix [11]. As business models present how companies create and deliver value for their customers and partners, the design of AI solutions needs to be aligned with the development of new business models which need to transform technological possibilities into the business value [21].

Technologies related to AI are transforming the way value is created and captured in professional services. AI has been successfully applied in human resource management, customer relationship management, supply chain management, medicine and healthcare [11]. Fountain et al. state that AI has the largest impact if it is developed by cross - functional teams with a mix of skills and perspectives, instead of siloed work to create interdisciplinary collaboration [12]. Using AI in business models can generate prolific outcomes for an organization, but it also comes with a risk if competitors manage to implement it sooner. Therefore, top management still sees AI as a strategic risk, especially in the case competitors and new entrants on international markets already use AI in their business models [3].

Significant challenges related to AI implementation remain due to many failures occurring in AI initiatives according to [3]. Their findings suggest that seven out of ten companies reported minimal or no impact from AI so far and among companies with significant investments in AI, 40 % of them do not report business gains from AI. Traditional methods of regulation like product licensing, R&D oversight and tort liability seem to be inadequate to manage the risks of AI in business models. AI autonomy leads to potential problems of control. Loss of control can occur due to a malfunction (corrupted file or physical damage to input equipment), security breach or flawed programming [22].

A number of scholars have tackled the issue of AI implementation in business models as a tool for managing digital risks. However, there still does not exist a dominant model for successful use of AI as a tool for managing digital risks. Every form of organizational change requires adaptations to be made in the socio-technological system of the organization, i.e. organizational culture and business processes. When implementing AI in the business models, organizations should consider user engagement and openness to enable technological development. Accordingly, organizations should develop strategies and back them up with technology data and security capabilities. These strategies should be adapted to scaling capabilities and scaling opportunities. Also, business models need to be constantly adapted to the environment they operate in due to the gap between technological advancements and operationalization of the value of business models [1]. In most organizations, AI transformation takes 18 to 36 months to complete. Many executives see AI as a plug-and-play technology with immediate return, which seems to be the most pronounced problem with AI use today. Investing in data infrastructure, AI software tools, data expertise, and model development is not enough, and organizations should focus more on employee education in these fields [12].

6 Results

Digital risks are becoming increasingly important issue for organizations competing in the global market. Traditional risk strategies can help manage these risks to a certain point. However, AI as an emerging technology with the ability to replicate human cognitive tasks through analysis of large data sets and growing capacity for automated non-routine tasks offers new possibilities to manage digital risks. AI will likely influence not only the digital risk management but many other organizational procedures as well as business in general.

Organizations that postpone AI implementation in their business models face different risks. One of the risks is not gaining first mover advantages on the market due to application of superior technology, especially related to digital risks. The second significant risk is losing competitive position to competition that has implemented AI sooner. The process of AI implementation is not straightforward as it requires significant resource base reconfiguration and development of new capabilities within an organization. Moreover, the benefits of AI implementation are not visible straight away.

7 Discussion and conclusion

In the paper we analysed the development of AI, its traits that help manage digital risks and ways organizations can implement it in their existing business models. However, the use of AI in business models is still an emerging research field and we can expect it to develop in the years to come. Future research should focus on more detail analysis in organizations that have implemented AI in their business models vs. organizations that have not. Since this is still an emerging topic, case studies and longitudinal studies seem like appropriate methods for researchers entering the field.

References

1. Reim, W., Åström, J., Eriksson, O. (2020). Implementation of Artificial Intelligence (AI): A Roadmap for Business Model Innovation. *AI*, 1(2), 180-191.
2. Jahankhani, H. (2020). *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*. Cambridge: Springer.
3. Ransbotham, S., Kiron, D., Gerbert, P., Reeves, M. (2017). Reshaping business with artificial intelligence: Closing the gap between ambition and action. *MIT Sloan Management Review*, 59(1), 1-17.
4. Hoadley, D. S., Lucas, N. J. (2018, April). *Artificial intelligence and national security. Congressional Research Service*. Retrieved from : https://crsreports.congress.gov/product/pdf/R/R45178/3
5. Purgason, B., Hibler, D. (2012). Security through behavioral biometrics and artificial intelligence. *Procedia Computer Science*, 12, 398-403.
6. Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., Scharre, P. (2018, July). *Artificial intelligence and international security. Center for a New American Security*. Retrieved from : https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-AI-and-International-Security-July-2018_Final.pdf?mtime=20180709122303&focal=none
7. Furman, J., Seamans, R. (2019). AI and the Economy. *Innovation Policy and the Economy*, 19(1), 161-191.
8. Felzmann, H., Villaronga, E. F., Lutz, C., Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*, 6(1), 1-14.
9. Kerr, A., Barry, M., Kelleher, J. D. (2020). Expectations of artificial intelligence and the performativity of ethics: Implications for communication governance. *Big Data & Society*, 7(1), 1-12.
10. Elkin-Koren, N. (2020). Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence. *Big Data & Society*, 7(2), 1-13.

11. Armour, J., Sako, M. (2020). AI-enabled business models in legal services: from traditional law firms to next-generation law companies?. *Journal of Professions and Organization*, *7*(1), 27-46.
12. Fountain, T., McCarthy, B., Saleh, T. (2019). Building the AI-Powered Organization. Technology isn't the biggest challenge, Culture is. *Harvard Business Review*, *97*(4), 62.
13. Rességuier, A., Rodrigues, R. (2020). AI ethics should not remain toothless! A call to bring back the teeth of ethics. *Big Data & Society*, *7*(2), 1-5.
14. Gorwa, R., Binns, R., Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, *7*(1), 1-15.
15. Micheli, M., Ponti, M., Craglia, M., Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2), 1-15.
16. Horowitz, M. C., Allen, G. C., Kania, E. B., Scharre, P. (2018, July). *Strategic competition in an era of artificial intelligence*. *Center for a New American Security*. Retrieved from : https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Strategic-Competition-in-an-Era-of-AI-July-2018_v2.pdf?mtime=20180716122000&focal=none
17. Allen, G. C. (2019, February). *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*. Retrieved from : https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf?mtime=20190215104041&focal=none
18. Allen, G., Chan, T. (2017, July). *Artificial intelligence and national security*. *Belfer Center for Science and International Affairs (Harvard Kennedy School)*. Retrieved from : https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf
19. Häfner, N., Wincent, J., Parida, V., Gassmann, O. (2020). Artificial intelligence and innovation management: A review, framework, and research agenda. *Technological Forecasting and Social Change*, *162*, 1-10.
20. Wirtz, B., Daiser, P. (2018). Business model innovation processes: A systematic literature review. *Journal of Business Models*, 6(1), 40-58
21. Metelskaia, I., Ignatyeva, O., Denef, S., Samsonowa, T. (2018). A business model template for AI solutions. In L. Moutinho & X. She Yang (Eds.), *Proceedings of the International Conference on Intelligent Science and Technology* (pp. 35-41). London: United Kingdom.
22. Scherer, M. U. (2015). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, 29, 353-400.