AI development and application of AI-based solutions in the area of information and data management in Poland

Grzegorz Chmielarz
Faculty of Management
Czestochowa University of Technology
Czestochowa, Poland
grzegorz.chmielarz@pcz.pl

Arnold Pabian
Faculty of Management
Czestochowa University of Technology
Czestochowa, Poland
arnold.p@wp.pl

***Abstract*—The intensity of cyberattacks aimed at information resources of Polish organisations is growing. Polish entrepreneurs are concerned about hacking attacks and cybercrime prevalent in the contemporary digital world. Tools traditionally applied in the cybersecurity area are becoming insufficient in ensuring protection against ever more sophisticated types of cyberattacks. Therefore, it seems reasonable to search for new solutions that can support organisations in combating cyberthreats. One of them can be application of Artificial Intelligence (AI) in the domain of information and data management in Polish organisations. These solutions offer new capacities that can be successfully utilised for the benefit of organisations that wish to secure themselves against growing occurrences of cyberattacks. Yet, the knowledge of Polish organisations pertaining to possibility of applying AI in the cybersecurity area is relatively low. This needs to be changed as the application of AI in this domain is no longer an option but a necessity.**

Keywords*—*AI, cybercrime, cybersecurity, security management

I. Introduction

The ever-growing amount of information and data being currently processed by organisations worldwide has translated into a growing intensity of cyberattacks aimed at their information resources. This is becoming a serious problem for Polish organisations. Today's cybercriminals tend to incorporate in their attacks latest advances of Artificial Intelligence (AI). So, it seems reasonable for those being attacked to cease relying on tools and solutions previously implemented in the cybersecurity area and apply AI-based solutions in their IT systems as well. Nowadays, AI and Machine Learning (ML) can offer organisations advantages of real-time threat analysis and prediction as well as making autonomous decisions and adapting to constantly updated types of cyberattacks.

978-3-903176-31-7 © 2020 IFIP

The AI is already beyond its stage of infancy and is being increasingly adopted by organisations on global scale and across various industries. Still, its uptake level differs depending on the particular region of the world. Therefore, analyses pertaining to its implementation need to be conducted not only with global reference. They should provide a clear and detailed picture of its advancement at regional levels as well. This pertains also to AI-based solutions that are becoming more frequently applied for cybersecurity purposes.

The underlying objective of the paper is to analyse the present level of AI development in Poland and possibility of implementing it in the cybersecurity area. The results of the conducted in the paper analyses may prove to be a valuable source of information about the Polish AI market, cybersecurity threats reported by Polish businesses and intelligent means of eliminating them through utilisation of AI-based tools. With this in view the authors have formulated the objective of the present paper – an attempt to answer the following research question:

RQ – "Can AI at present effectively support Polish organisations in protecting their resources against cybercrime?".

In the research process the authors have conducted extensive literature studies and analyses of latest reports pertaining to the issues of cyberthreats and AI implementation level in Poland. These included also market availability of AI-based tools supporting the security of information and data management in organisations. As Poland is the country located in the heart of Europe, trends that can be observed in the area of AI application in this country may as well reflect the condition in the discussed domain represented by other Central and Eastern countries of Europe. This can be not only of theoretical but also practical value for both the organisations that search for and provide AI solutions. However, it needs to be stressed that the paper focuses primarily on the managerial aspect of AI-based solutions implementation in the domain of data and information protection. The authors intend to highlight the fact that such solutions are already available on the market and their efficiency in protecting information resources of organisations should be communicated to those who make decisions regarding their implementation – managers, especially top-level ones. For this reason, the paper focuses not so much on scientific issues pertaining to utilisation of AI for cyberdefence purposes, but instead addresses the issue of its practical use in organisations.

II. Literature Review

The issue of implementing AI-based solutions in the area of information and data management has been gaining in importance in the scientific literature on the subject. This is to a large extent driven by recent advances in the area of Artificial Intelligence development. It comprises a wide range of topics that pertain to various aspects of the role that AI can play in supporting organisations of all types in the domain of information and data protection. They are not limited to the technical aspects of using Machine Learning (ML), Deep Learning (DL) and Neural Networks (NN) for cybersecurity purposes. The authors also point out the problems of ethics, values and rights of individuals to protect their privacy in the information and data driven contemporary world.

Below, the authors have included a brief review of research matters that have been undertaken in this area in recent years.

Some part of research concerns deficiencies of AI.

For example, in their interdisciplinary approach Dwivedi et al. discuss the inability of AI systems to understand the situations that humans experience and formulate proper conclusions. They draw attention to the fact that such a flaw in current AI systems generates vulnerabilities in many areas of data management [1].

Salah et al., turn attention to the fact that the centralised nature of AI may result in the possibility of data tampering, being the consequence of managing and storing data in a centralised manner, which makes them vulnerable to hacking and manipulation. This in turn may lead to AI decision outcomes that can be highly erroneous, risky, and dangerous [9].

There is also a significant scientific interest in the defensive capabilities of AI.

Lee et al., address the issue of intrusion detection using machine learning and artificial intelligence techniques for detecting attacks. Intelligent network attacks are difficult to recognise and detect due to their high false alerts and the huge amount of security data. Advancements in AI fields can support the investigation of network intrusions by security analysts in a timely and automated manner [5].

T. Kurpjuhn emphasises the ability of defensive AI that can evolve employing machine learning to develop ever more precise responses to threats as well as anticipate new attacks. In his opinion supplementing traditional cybersecurity approaches with an intelligent, machine-based layer can improve the manner in which companies secure their networks [3].

Qiu et al., advocate implementation of AI-based authentication to protect data and information security in wireless networks. They analyse the limitation of traditional security solutions in these networks, such as a conflict between costs and security, which may result in a failure of secure legitimate communications. They introduce a new AI-based solution to assist lightweight authentication. This increases security in a wireless multimedia environment [7].

According to Gupta et al., data mining techniques can be applied in security to analyse threats to infrastructure services, power grids, auditing, and intrusion detection in data storage. Techniques and algorithms such as classification, clustering, prediction, fuzzy logic, artificial neural networks, support vector machine and genetic algorithms can be utilised to find out malicious users and unusual patterns [10].

Zhou et al., propose that Deep learning technology is used in Mobile Crowd Sensing Computing (MCSC) in order to verify and guarantee information security avoiding in this way insignificant messages or malicious fraudulent data transmission. They introduce the architecture of Robust Mobile Crowd Sensing to meet the challenges of MCSC such as Lack of Incentive-Compatible Mechanism, Quality of Sensory Data and High Traffic Load and Latency [12].

Some of the approaches pertain to the issues of AI in categorising and creating new models of data protection.

Larriva-Novo et al., compared multilayer and recurrent neural networks, with particular interest in data of a temporary nature. They demonstrated the behaviour of different configurations of neural networks (multilayer and recurrent) to categorise cybersecurity dataset and determine

978-3-903176-31-7 © 2020 IFIP

which neural network configuration offers the best results, in terms of accuracy, for each category of data [4].

Alessandro Mantelero addressed the issue of adopting a broader view of data protection impact assessment resulting from an extensive use of Artificial Intelligence in modern data processing techniques, as well as data-intensive technological trends. Questioning a technology-specific approach the author presents a rights-based and values-oriented model of data protection [6].

However, the issue of applying AI-based solutions in the cybersecurity area by Polish organisations has not been covered in the global literature. Therefore, this paper can contribute to the scientific literature on the subject, constituting a valuable source of information as to the present scale and perspectives of utilising AI in this domain.

III. Current uptake and forecasts of AI development in Polish organisations

Global investments in AI systems are driven by a wide range of factors. Three of them are the prevailing ones: automated customer service agents, automated threat intelligence and prevention systems, and sales process recommendation and automation. It is estimated that in 2019 these constituted a share of 25% of all the spendings in this area [www 14].

According to the report by PricewaterhouseCoopers (PWC) being in the vanguard of the countries that will adopt AI in their economies can prove beneficial. The estimates show that AI could contribute up to $15.7 trillion to the global economy in 2030, which is more than the current output of China and India combined. The economic impact of AI is supposed to be driven primarily by productivity gains. They result from business processes automation, businesses augmenting their existing labour force with AI technologies and increased consumer demand. These in turn are caused by the emergence of personalised and higher-quality AI-enhanced products and services on the markets [www 6]. In Fig. 1 the authors present the forecasts regarding the influence of AI adoption on the boost of economies in particular regions of the world and growth of their Gross Domestic Product in 2030.

Fig. 1. Fig. 1. Impact of AI adoption on GDP in particular regions of the world in 2030

Fig. 2. Source: own elaboration based on: [www 8]

As Fig. 1 demonstrates the country which is estimated to benefit most from the adoption of AI in the forecast period is China, where the expected growth in GDP amounts to 26.1%. The second region of the world likely to record a significant impact of AI adoption on its economy is North America with an expected GDP growth at the level of 14.5%. Southern and Northern Europe's GDP is supposed to growth respectively by 11.5% and 9.90%, being separated by the Developed Asia with its GDP growth at the level of 10.4%. The uptake of AI in Africa, Oceania and other Asian countries is expected to be lower and so will be the gains for their economies that are supposed to amount respectively 5.6% and 5.4%. Poland, as a representative of Central and Eastern Europe can be expected to benefit from AI uptake at the level similar to those of Southern and Northern Europe, with a 10% growth in its GDP. These forecasts seem to be confirmed by the findings of the report by McKinsey&Company Poland, according to which this country can become a regional centre for the development of AI. This is possible largely due to the fact that Poland can boast a large number of graduates in science and technology and features a dynamic startup ecosystem allowing for the formation of future AI specialists. Also, the scale of investments required for the development of AI technology is relatively small compared to the industrial sector where major investments are necessary in plants and machinery. As recently AI has been successfully adopted in specific applications and uses, this may as well facilitate the development of smaller companies in Poland [www 3]. This seems to be confirmed by the latest research conducted by A. Wodecki, which shows that currently there are 3 270 companies in Poland that declare works on Artificial Intelligence. The largest number of them specialise in Big Data technology and over 1 720 conduct works in the area of machine learning. Other companies investigated in the research included the areas of Internet – 682, natural language processing – 375, application of AI in marketing – 238, finances – 208 and health – 199. Few companies operate in the area of predictive analytics. Good news is that Polish companies that are active in the AI area can expect financial support that comes, among other, from investments. Most substantial funds were provided to companies that specialise in Big Data technology (USD 16.5 billion) as well as the ones that utilise AI on the Internet (USD 5.1 billion). Companies active in the area of software development received USD 4.2 to continue the AI development and those operating in the security area were provided USD 3.9 billion of funds. Also enterprises that specialise in image recognition and robotics obtained funds for AI technologies development, which amounted to, respectively USD 2.9 billion and USD 2.4 billion [www 1].

However, not all data in this respect are so optimistic. According to the findings of the report Map of the Polish AI by Digital Poland (research conducted on a representative sample) there are also obstacles that need to be overcome before the uptake of AI in Polish companies can accelerate its pace. The authors have presented such main obstacles in Fig. 2.

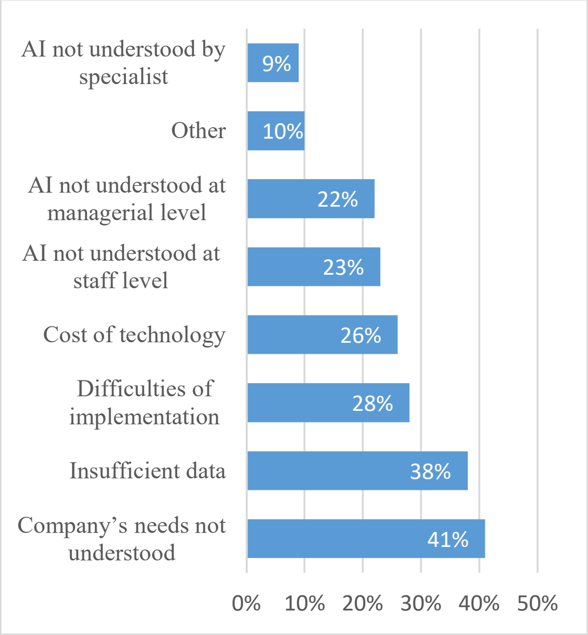

Fig. 3. Fig. 2. Main obstacles to AI implementation in Poland

Fig. 4. Source: own analysis based on: [www 6]

As it can be observed in Fig. 2 the biggest obstacle in Poland that hinders implementation of AI solutions on a large scale is the lack of understanding of the company's own needs and inability to see the potential benefits arising from AI adoption. This is the opinion of 41% of the survey respondents. The overall lack of understanding of AI is seen as more crucial at the staff and managerial level, respectively 23% and 22%, than in case specialists (9%). This highlights the necessity to increase the awareness of both managers and staff as to the potential benefits that AI adoption would bring their companies. Another indicated obstacle in this area is the lack of necessary structured data that would allow to implement AI solutions – 38% of the surveyed companies indicated this as an obstacle. It is worth pointing out that cost of technology was ranked fourth in the survey (26%), which indicates that the adoption of AI in Polish enterprises is to a larger extent associated with lack of proper knowledge on its potential advantages and lack of data rather than by purely financial aspects [www 6].

IV. AI-BASED TOOLS IN THE CYBERSECURITY AREA IN POLISH ORGANISATIONS

Security of information management in Polish organisations is becoming an issue of outmost importance. This is largely driven by the fact the contemporary organisations rely to a large extent on IT tools and networking, which they utilise in their operations. The requirements for networks and services operation include continuous and error-free availability, flexibility to satisfy the needs of users, prompt and precise accounting, minimal use of resource (i.e. operating efficiency), and secure, fraud-free operation [2]. Additionally, the traditional constraints to performing business or administrative tasks, that is time and space, do not apply to the contemporary model of work, where the Internet has eliminated these barriers. Also, wireless communication is being used presently on a large scale. The open communications environment causes that wireless transmissions are much more vulnerable than wired communications to malicious attacks, including both the passive eavesdropping for data interception and the active jamming for disrupting legitimate transmissions [13]. This means that it is easier for cybercriminals to access computer systems of enterprises and public administration units regardless of their geographical location and time. The problem of cybercrime is of particular importance to the industrial sector as well. This sector has been more widely using the solutions based on the Internet of Things (IoT). However, in industry the margin of accepted risk is very narrow. This may lead to security issues and safety risk may also be involved. The heterogeneous structure of IoT produces a large number of possible vulnerabilities that still need to be fully understood [11].

As cybercrime is on the increase there is a particular need for AI-based solutions that can relieve employees of their tasks in the area of information and data security management. Given the amount of information that needs to be processed on a daily basis and the growing traffic that IT staff members have to analyse so as to prevent their systems against cyberattacks, it is not an option but a necessity to utilise the power offered by AI solutions in the cybersecurity domain. For example, phishing attacks still constitute a major threat to Polish organisations. AI and Machine Learning can significantly reduce the impact of such attacks. AI-ML is able to detect and track more than 10,000 active phishing sources and can react much quicker than humans can. In addition, AI-ML is capable of scanning phishing threats from all over the world without being limited to a particular geographical area [8]. Unfortunately, the number of organisations in Poland that have already implemented AI solutions to protect themselves against cybercrime occurrences is unknown. Yet, the limited amount of data pertaining to this issue allows to assume that this number is relatively low.

Therefore, in this part of the paper the authors have attempted to identify the AI-based solutions that could support Polish entrepreneurs in combating and preventing cyberthreats. Also, a brief analysis of current threats and fears of the Polish business sector related to cybercrime has been included in it. This is meant to present potential solutions that could reduce or eliminate the problem efficiently.

Generally, the primary objective of this part of the paper is to provide an answer to the research question "Can AI at present effectively support Polish organisations in protecting their resources against cybercrime?"

According to the findings of the report by KPMG International regarding threats perceived by the Polish business sector in the area of cybersecurity the most commonly indicated issue in this domain was cybercrime. In 2019 most of the investigated enterprises feared single hackers – 84% of indications (up by 23% yoy), while organised groups of cybercriminals ranked second – 58% of indications (down by 4% yoy). Polish entrepreneurs also felt threatened by cyberterrorists – 54% of indications (up by 7% yoy), script kiddies – 34% of indications (up by 4% yoy) and hacktivists – 27% of indications compared to 20% in the previous year [www 7].

Polish companies also express specific fears pertaining to the potential negative outcomes that activities of cybercriminal can exert on their operations. The findings of the report by the IT consultancy company VECTO provide valuable insights as to which of the areas of the conducted business activity Polish entrepreneurs consider as particularly important to protect against cyberattacks. The survey respondents evaluated the significance of particular threats on Likert scale where 5 meant the most significant threat and 1 the least significant one. The most feared outcome of a hacking attack in their opinion would constitute a loss of client and contact databases (4 points). The second most feared consequence would be a loss of unique know-how and infringement to intellectual property (3.9 points). Almost equally harmful result of a cyberattack would be the perspective of losing customers (3.82 points) as well as image and trust of the business environment (3.38 points). A possibility of sustaining financial losses was given 3.24 points and a potential closure of the company 2.9 points [www 12].

With regard to the abovementioned concerns of Polish entrepreneurs it can be assumed that application of AI-based tools in Polish organisations, offers tremendous advantages compared with the traditional ones. They can significantly reduce time and workload of IT teams responsible for ensuring security to organisations' information resources. The process of ensuring cybersecurity includes the following stages: prediction, prevention, detection and reaction. According to experts not many new AI-based solutions can be introduced in the two first stages as the options are to a large extent limited. Not all the threats can be predicted and thus, prevented in time. Prediction and prevention algorithms are based on the analysis of data gathered following a detection and then reaction. However, the two remaining stages – detection and reaction require a particular attention as quick detection of threats is of key importance while defining the ways of reacting to them. This is particularly significant for Polish organisations where the average time of detecting a breach to data security is 200 days [www 2]. Analysing data and seeking for anomalies in them that can signal threats is a mundane and time-consuming work when done by network security analysts. However, AI can be successfully utilised to perform such tasks. In particular, AI can be applied by Polish organisations to detect threats and eliminate them at the pre-execution stage. Such technologies as machine learning and deep learning are characterised by unique capabilities that allow for constant improvement of detection parameters. Behavioural analysis is applied to identify anomalies. One of the examples in this area can constitute an AI-based solution which prevents industrial organisations against threats introduced while using USB devices. Also, cybercrime prevention is the area where AI can be applied to a large extent by Polish organisations to help them protect their IT systems against cyber threats. AI is capable of scanning huge amounts of data and based on the pre-defined patterns it can make predictions regarding potential malicious contents. This allows for creating a special non-intrusive operational technology platform which automatically identifies organisational assets and network topology, is able to identify critical vulnerabilities and in a continuous mode monitor their networks for any potential cyberattacks. Response stage seems not to be fully utilised when reacting to cyberthreats. Yet, Polish companies can also apply AI to create a virtual path for a detected threat or develop new protection mechanisms for evolving technologies, which can result in considerable time-savings. Response platforms can generate broader output as a reaction towards a single attack and in response block the attacker on all similarly situated machines [www 4].

Thus, the authors of the paper have conducted analyses aimed at identifying the knowledge of Polish organisations pertaining to availability of such solutions. For this reason they studied the reports that investigate the application of AI tools for cybersecurity purposes in Polish organisations. The analysis demonstrates that the level of applying AI-based solutions in this domain in Polish organisations is low. With this end in view, the authors have attempted to conduct a brief review of the AI-based solutions. This was meant to provide Polish organisations with information about measures that could be successfully implemented to improve their cybersecurity. In Table 1 the authors have summarised briefly characteristics of selected AI-based tools that can be utilised by them.

TABLE I. SELECTED AI-BASED SOLUTIONS FOR CYBERSECURITY PROTECTION

AI- based tool	Functionality
Darktrace Antigena	Based on an intelligent decision-making engine, without human intervention or previous knowledge of attacks reacts to in-progress cyber-threats, protecting organisations from any damage they could cause,
Senseon's AI Triangulation	Based on technology which emulates the behaviour of a human security analyst, automates the process of threat detection, investigation and response. Analyses the behaviours of users and devices from multiple perspectives, and learns from experience,
Vectra's Cogito	Based on deep learning and neural networks this solution combines human expertise with data science and advanced machine learning techniques. Using behavioural analysis this model offers continuous real-time protection against threats,
Deep Instinct	Solution based on deep learning, uses two-phase approach imitating human brain learning and instinctive reactions. In the training phase a prediction model is elaborated. In the prediction phase it autonomously predicts real-time threats and prevents them at a pre-execution level,
Intercept X	Created by Sophos, based on deep learning solution that detects both known and unknown malware without relying on signatures. Endpoint Detection and Response automatically detects and prioritises potential threats,
Targeted Attack Analytics	Symantec's solution based on machine learning. Utilising the Integrated Cyber Defence Platform, the tool learns across all local and global data, across all control points, all at once. The high precision analytics developed by the company analyses suspicious and mundane data to detect new attack activity before attackers can get a chance to exfiltrate data.

Source: own elaboration based on: [www 5], [www 9], [www 13], [www 14], [www 11], [www 10]

The data aggregated in Table 1 regarding selected already available AI-based solutions that can be applied by Polish organisations in the cybersecurity area demonstrate that AI-powered functionality largely exceeds the capacities of traditional tools utilised in this domain. Yet, Polish organisations seem reluctant to use them for their benefit. It can be concluded that their limited application largely results from the obstacles to AI implementation, which have been presented in Fig. 2. It seems that the lack of knowledge on AI advantages in the cybersecurity area at both the managerial and staff level are largely to blame for this state of affairs. Also, as Polish organisations are frequently unable to determine their own needs with reference to AI utilisation, they do not perceive the role of AI in managing information security as a crucial one. However, this is an issue that will have to be addressed by them soon as cybercriminals also take interest in the potential of AI to leverage in their attacks directed at organisations of all types.

Another reason for the limited AI application in the cybersecurity area in Poland may result from the fact that AI's algorithms function properly as long as proper input data feed them from databases. However, it means that these algorithms need to be incorporated into a broader picture of the whole information infrastructure of an organisation. This can only be done by experts who know which links of the organisation's security chain may constitute possible targets of cybercriminals and train AI to be able to react to threats in these areas. Not surprisingly, it is not easy and without them, a successful application of AI solutions in the cybersecurity area in Poland will still be troublesome.

Therefore, it can be concluded that AI can effectively support Polish organisations in protecting their resources against cybercrime, which is an answer to the research question set by the authors of the paper. However, we believe that Polish organisations, and their decision-makers in particular, need to understand that not catching up with the accelerating adoption of AI technologies in the cybersecurity area puts them in a disadvantageous position in the battle against constantly evolving cybercrime. Also, there is a demand for AI experts in the cybersecurity area. This has to be satisfied in order to enable the diffusion of such solutions in Poland on a larger scale.

V. CONCLUSIONS AND DISCUSSION

Cyberattacks which are currently on the increase worldwide are also a great concern for Polish organisations. Tools and solutions traditionally applied in the cybersecurity area cannot keep up with the ever-growing number of evolving new threats. Therefore, organisations need to search for new ways to protect the security of stored and processed data. AI application has been increasing across various industries, it can also offer organisations advantages in the area of cybersecurity. Yet, AI uptake level varies significantly in the geographical dimension. To obtain a clear picture of its implementation it is necessary to look for patterns that can account for the similarities and differences.

These countries where adoption of AI will be the fastest are also expected to record largest contribution of this sector to their economies. Poland, as a representative of Central and Eastern Europe is also expected to benefit from AI uptake. Poland also stands a chance to be the centre for AI development for the whole region. This in turn creates a good environment for AI diffusion to other European countries.

However, there are also several obstacles that hinder AI adoption in Polish organisations. The most significant one is the inability to perceive the advantages of AI implementation as Polish organisations are uncertain as to what their needs are. Also, a general lack of understanding as to the growing in importance role of AI in activities of contemporary organisations is demonstrated by both their personnel as well as managerial staff. Polish companies also struggle with lack of cyber-security experts skilled in AI area, which negatively influences AI adoption in the cybersecurity domain.

AI-based solutions for cybersecurity are already available. This seems to be good news for Polish organisations which are becoming increasingly targeted by cybercriminals. Polish entrepreneurs are concerned about hacking attacks, cybercrime is the most frequently indicated fear with relation to cybersecurity.

Polish companies are also very specific with regard to what would impede their operation most in case of a hacker attack. The loss of client and customer database is considered to be the most damaging outcome as well as infringement to intellectual property and perspective of losing customers as well as good image and trust in the business environment.

Several issues need further discussion and analyses within the confines of the undertaken research problem. One of them regards limited utilisation of AI-based solutions in the cybersecurity area in Polish organisations. Is it a result of distrust in AI? Or maybe Polish organisations do not believe in the defensive capacities of AI?

The functionality of AI-powered solutions outperforms the capacities of tools traditionally applied in this domain. Solutions based on intelligent decision-making algorithms, deep learning and neural networks can without human intervention monitor IT systems of organisations, detect potential threats and neutralise them prior to their execution. This is what traditional cybersecurity approaches lack and supplementing them with intelligent features would certainly boost their performance. Why do Polish organisations largely depend on traditional security measures then?

Applying AI-based solutions in Polish organisations would certainly increase their ability to defend themselves against cyberthreats. Is their poor knowledge regarding the availability of such solutions to blame for not opting for them?

As the issues of AI application for security purposes in Poland are relatively new and have not been studied extensively the need for future research in the analysed domain definitely exists. It could provide valuable information on the changing level of adopting AI-based solutions, its efficiency in reducing and eliminating cyberthreats and also the changes in the attitudes of Polish decision-makers towards AI utilisation in the cybersecurity area.

References

[1] Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., Medaglia, R., Le Meunier-FitzHugh, K., Le Meunier-FitzHugh, L. C., Misra, S., Mogaji, E., Sharma, S. K., Singh, J. B., Raghavan, V., Raman, R., Rana, N. P., Samothrakis, S., Spencer, J., Tamilmani, K., Tubadji, A., Walton, P., and Williams, M. D. 2019. “Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy,” International Journal of Information Management, p. 101994. (https://doi.org/10.1016/j.ijinfomgt.2019.08.002).

[2] Gyires-Tóth, B., Varga, P., & Tóthfalusi, T. (2019). Utilizing Deep Learning for Mobile Telecommunications Network Management. 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 575–580.

[3] Kurpjuhn, T. 2019. “Demystifying the Role of AI for Better Network Security,” Network Security (2019:8), pp. 14–17. (https://doi.org/10.1016/S1353-4858(19)30097-2).

[4] Larriva-Novo, X. A., Vega-Barbas, M., Villagra, V. A., and Sanz Rodrigo, M. 2020. “Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies,” IEEE Access (8), pp. 9005–9014. (https://doi.org/10.1109/ACCESS.2019.2963407)

[5] Lee, J., Kim, J., Kim, I., and Han, K. 2019. “Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles,” IEEE Access (7), pp. 165607–165626. (https://doi.org/10.1109/ACCESS.2019.2953095).

[6] Mantelero, A. 2018. “AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment,” Computer Law & Security Review (34:4), pp. 754–772. (https://doi.org/10.1016/j.clsr.2018.05.017).

[7] Qiu, X., Du, Z., and Sun, X. 2019. “Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks,” IEEE Access (7), pp. 172004–172011. (https://doi.org/10.1109/ACCESS.2019.2956480).

[8] Ramachandran, R. 2019. “How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks,” Entrepreneur, September 14. (https://www.entrepreneur.com/article/339509, accessed February 17, 2020).

[9] Salah, K., Rehman, M. H. U., Nizamuddin, N., and Al-Fuqaha, A. 2019. “Blockchain for AI: Review and Open Research Challenges,”

IEEE Access (7), pp. 10127–10149. (https://doi.org/10.1109/ACCESS.2018.2890507).

[10] Shivangi Gupta, A. Sai Sabitha, Ritu Punhani. 2019. “Cyber Security Threat Intelligence Using Data Mining Techniques and Artificial Intelligence,” International Journal of Recent Technology and Engineering (8:3), pp. 6133–6140. (https://doi.org/10.35940/ijrte.C5675.098319).

[11] Varga, P., Plosz, S., Soos, G., & Hegedus, C. (2017). Security threats and issues in automation IoT. 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), 1–6. https://doi.org/10.1109/WFCS.2017.7991968

[12] Zhou, Z., Liao, H., Gu, B., Huq, K. M. S., Mumtaz, S., & Rodriguez, J. (2018). Robust Mobile Crowd Sensing: When Deep Learning Meets Edge Computing. IEEE Network, 32(4), 54–60. https://doi.org/10.1109/MNET.2018.1700442

[13] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Proceedings of the IEEE, 104(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521:

[14] [www 1] A. Wodecki. 2019. “Ekspert: ponad 3,2 tys. firm pracuje nad sztuczną inteligencją,” Nauka w Polsce, May 29. (http://naukawpolsce.pap.pl/aktualnosci/news%2C77280%2Cekspert-ponad-32-tys-firm-pracuje-nad-sztuczna-inteligencja.html, accessed February 17, 2020).

[15] [www 2] https://crn.pl/artykuly/rynek/ai-w-cyberbezpieczenstwie, accessed February 19, 2020.

[16] [www 3] AI Revolution - Report in English.Pdf. https://www.mckinsey.com/pl/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Polska/Raporty/Rewolucja%20AI%20Jak%20sztuczna%20inteligencja%20zmieni%20biznes%20w%20Polsce/Raport-AI_Forbes_PL.ashx

[17] [www 4] AI-in-Cybersecurity_Report_20190711_V06.Pdf. https://www.capgemini.com/pl-pl/news/ai-in-cybersecurity/

[18] [www 5] “Darktrace.” (https://www.darktrace.com/en/, accessed February 19, 2020).

[19] [www 6] Map-of-the-Polish-Ai-2019-Edition-i-Report.Pdf. https://www.digitalpoland.org/assets/reports/map-of-the-polish-ai---2019-edition-i.pdf

[20] [www 7] Pl-Raport-KPMG-Barometr-Cyberbezpieczenstwa-W-Obronie-Przed-Cyberatakami.Pdf. (https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-KPMG-Barometr-Cyberbezpieczenstwa-W-obronie-przed-cyberatakami.pdf).

[21] [www 8] Pwc-Ai-Analysis-Sizing-the-Prize-Report.Pdf. (https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf)

[22] [www 9] “Self-Driving Cyber Defence: Automated Detection, Investigation and Response.” Self-Driving Cyber Defense | Senseon | Automated Threat Detection Investigation and Response. (https://www.senseon.io, accessed February 19, 2020).

[23] [www 10] “Sophos Endpoint Protection. Advanced Security with Intercept X.” (https://www.sophos.com/products/endpoint-antivirus.aspx, accessed February 19, 2020).

[24] [www 11] “Targeted Attacks: The Game Has Changed.” (https://www.symantec.com/blogs/feature-stories/targeted-attacks-game-has-changed, accessed February 19, 2020).

[25] [www 12] https://bizmarket.pl/2019/02/06/raport-cyberbezpieczenstwo-w-polskich-firmach-2018/.

[26] [www 13] “Vectra - AI-Driven Threat Detection and Response Platform.”. (https://www.vectra.ai/, accessed February 19, 2020).

[27] [www 14] “What Is Deep Learning? Training a Deep Neural Network Algorithm | Deep Instinct AI Cybersecurity.” (https://www.deepinstinct.com/what-is-deep-learning/, accessed February 19, 2020).

[28] [www 15] “Worldwide Spending on AI Systems.” 2019. IDC: The Premier Global Market Intelligence Company, , September 4. (https://www.idc.com/getdoc.jsp?containerId=prUS45481219, accessed February 17, 2020).