JOURNAL OF MODERN SCIENCE

2/66/2026

www.jomswsge.com

DOI: 10.13166/jms/224805

Małgorzata Such-Pyrgiel
WSGE University of Applied Sciences in Józefów, Poland
ORCID iD: 0000-0001-5435-1154

Dariusz Prokopowicz
Cardinal Stefan Wyszyński University in Warsaw, Poland
ORCID iD: 0000-0001-6383-916X

Anna Mazurkiewicz-Pizło
Józef Piłsudski University of Physical Education in Warsaw, Poland
ORCID iD: 0000-0001-8273-2229

Anna Gołębiowska
Fire Academy in Warsaw, Poland
ORCID iD: 0000-0003-0478-5047

Ewa Listopadzka
Kozminski University, Poland
ORCID iD: 0000-0002-4581-2163

THE GROWING IMPORTANCE OF CYBERSECURITY FOR MOBILE BANKING SYSTEMS AND THE USE OF ARTIFICIAL INTELLIGENCE IN IDENTIFYING CYBER THREATS

Abstract

The main objective of the article was to highlight the growing importance of cybersecurity in mobile banking systems in the context of accelerated digitalization of the economy, intensified during the COVID-19 pandemic, and the dynamic development of artificial intelligence applications in the identification of cyber threats. The pandemic has significantly contributed to the growth of remote communication, e-commerce, and mobile banking, which has increased the exposure of financial systems to new forms of cybercrime. In response to these processes, the importance of improving cyber threat risk management using artificial intelligence-based tools such as machine learning, big data analysis, and automatic anomaly detection is growing. Analyses confirm that the integration of cybersecurity and AI solutions is becoming a key factor in increasing the resilience of mobile banking and the stability of financial activities in the digital economy.

Keywords: *internetization, digitization, cybersecurity, cybercrime, mobile banking, pandemic, Covid-19, economic activity, new media, Internet, information technologies, artificial intelligence*

Extended abstract

Objectives: The aim of this article is to analyze the growing importance of cybersecurity in mobile banking systems in the context of accelerated digitalization of the economy, especially after the Covid-19 pandemic. The study focuses on identifying key cyber threats accompanying the dynamic development of mobile banking and payments made using mobile devices. Another important research objective is to assess the role of artificial intelligence in the processes of detecting, analyzing, and neutralizing cyber threats in the financial sector. The article aims to show the relationship between the development of digital technologies and the need to improve cybercrime risk management systems. Furthermore, the aim is to highlight the importance of integrating AI tools with cybersecurity systems as a factor in the stability and competitiveness of mobile banking.

Material and methods: The article uses an analysis of scientific literature on cybersecurity, mobile banking, and the applications of artificial intelligence in the financial sector. A comparative analysis and desk research method was used, including industry reports, studies by financial institutions, and scientific publications. Logical and systemic analysis was also used to identify links between digitization processes and the development of cyber threats. The

research was qualitative and synthetic in nature, focusing on trends observed after 2020. The research methods allowed for an interdisciplinary approach to the issue, combining economic, technological, and organizational perspectives.

Results: The analyses showed a significant increase in the level of cyber threats with the development of mobile banking and the growth in the number of electronic transactions. It was found that the Covid-19 pandemic significantly accelerated digitization processes, which increased the scale of potential cyberattacks.

The results of the study indicate that traditional data protection methods are proving insufficient in the face of the complexity of modern threats. The use of artificial intelligence tools, including machine learning and big data analysis, significantly improves the effectiveness of fraud and transaction anomaly detection. It has also been shown that AI-based systems enable predictive threat modeling and faster response to security incidents.

Conclusions: The article confirms that cybersecurity has become one of the key challenges for the development of mobile banking in a digital economy. The integration of security systems with AI-based solutions is essential for effective cybercrime risk management. The results of the study indicate that AI significantly increases the resilience of banking systems to dynamically changing threats. The development of mobile banking requires continuous improvement of data protection technologies and security procedures. It is concluded that the effective implementation of AI tools in cybersecurity is one of the key determinants of the stability and trust in financial systems in the long term.

Introduction – Cybercrime has been on the rise in recent years

During the Covid-19 pandemic, the scale of digitization and internetization of remote communication processes, various aspects of economic activity, and people's daily lives has increased (Gołębiowska, Prokopowicz, pp. 307-344, 2021). In order to slow down the transmission of the SARS-CoV-2 coronavirus, governments in some countries introduced national quarantines and imposed temporary lockdowns on selected, mainly service sectors of the economy. Due to the introduction of quarantines and lockdowns as key anti-pandemic instruments, both citizens and many economic entities were

forced to switch to remote communication, which was conducted using new ICT and internet technologies. As part of remote communication via the Internet, citizens exchanged messages and companies and enterprises sent documents to business partners and public institutions. Many shops and service providers were only able to sell their products and/or provide their services via the Internet. As a result, the scale of online sales increased many times over for many product and service ranges. Due to the strong growth in online sales of products and services, the scale of online payments and settlements also increased.

The development of online and mobile banking accelerated. In addition, during the Covid-19 pandemic, there was also an increase in the development of e-logistics, e-government, the scale of remote work, e-learning, e-services, and the scale of remote contact with healthcare institutions, i.e., e-health. Some museums digitized their collections and made them available online. Some libraries have also launched their online counterparts containing digitized books and other publications. Some theaters, operas, cinemas, and concert halls have also offered citizens the opportunity to watch recorded performances, operettas, films, etc. on their websites. In view of the above, many sectors and industries of the economy have seen an acceleration in the processes of digitization and internetization. The scale of electronic data and information transfer via the Internet has increased many times over. This has led to an increase in the scale of the digital and online environment in which cybercriminals can operate. Consequently, it is possible that during the Covid-19 pandemic, the scale of cybercrime has increased, as has the importance of cybersecurity for data transfer (Grzywak, Widenka, pp. 56-57, 2015), online transactions and payments, etc. The need to improve cybersecurity instruments and systems has also increased. The above-mentioned processes have been implemented on a large scale at the national, regional, and global levels, and in recent years have become an important factor in globalization (Komorowski, Prokopowicz, pp. 157-180, 2022).

Based on online analytics conducted using Google's Google Trends tool, it appears that in recent years, Internet users have become increasingly interested in the issue of ransomware viruses. Unlike cybercriminal techniques based on phishing, which have been known since the 1990s, Internet users' interest in ransomware viruses has only grown significantly since 2010. The results

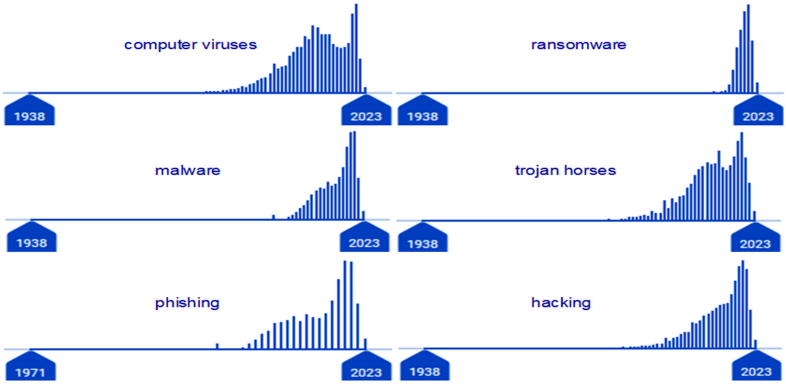
of the aforementioned analysis of Internet users' interest in cybercrime and cybersecurity, conducted on the basis of selected keywords entered into the Google search engine between January 1, 2004, and July 28, 2023, on a global scale, are presented in the chart below. The chart shows the increase in Internet users' interest in cybercrime and cybersecurity in recent years. In May 2017, one of the largest cyberattacks using ransomware viruses took place.

Chart 1. *Analysis of Internet users' interest in cybercrime and cybersecurity based on selected keywords entered into Google search engine between January 1, 2004, and July 28, 2023 (globally)*

Source: Opracowanie własne na podstawie analityki Google Trends.

The growing importance of cybercrime and cybersecurity issues in recent years is also illustrated by the charts below, based on Big Data analytics carried out for scientific publications collected in the Academia.edu online scientific portal database. These charts confirm the significant increase in the importance of cybercrime issues as a topic addressed in scientific publications in recent years. The following Big Data analysis was prepared on the basis of the full texts of many thousands of scientific publications archived on the Academia.edu online portal on topics such as computer viruses, ransomware malware, Trojan horses, phishing, and hacking. The charts present the results of this analysis for the period from 1938 to July 28, 2023. Most of the publications on these topics found on the aforementioned scientific website were published in 2020, i.e., the year of the first and second waves of the Covid-19 pandemic.

Chart 2. *The results of Big Data analytics compiled on the Akademia.edu scientific portal website on selected issues related to cybercrime, addressed in scientific publications archived on this portal. Analytics for the period from 1938 to July 28, 2023 (globally)*



Source: Own study based on Big Data analytics compiled on the Academia.edu scientific portal. For the term *phishing,* the research period was set from 1971.

Over the past few years, there has been an increase in cyberattacks on the IT systems of various institutions, including government institutions, social media databases, banks' ICT systems, and electronic banking systems. Cybercriminals are increasingly attacking mobile internet banking systems available to internet users and bank customers via mobile devices, mainly smartphones. Research shows that the scale of cyberattacks on the IT systems of banks, institutions, etc. is growing. using social engineering techniques combined with malicious software such as ransomware, i.e., software that encrypts access to data on disks or redirects users to fake websites of banks and institutions on the Internet in order to obtain personal data, passwords to electronic banking accounts, and ultimately steal money. For several years now, many email users have been receiving strange emails of unknown origin, which are sent as spam from other private email accounts or other accounts with false information. Many of these suspicious emails, usually sent by cybercriminals and hackers, contain attachments with false information. The attachments are usually WORD documents (*.doc/*.docx), Acrobat Reader files (*.pdf), image files, or other formats, and often contain ransomware viruses. These are very dangerous viruses that encrypt access to your computer's hard drive. In addition, cybercriminals are

increasingly using email accounts set up on email portals to send infected emails to other Internet users, generating fake emails to make it look as if a specific email account user is sending emails crafted by cybercriminals to their friends. Such cybercriminal techniques are becoming increasingly common.

In recent years, the scale of hacker data theft from social media portals has also grown rapidly (Such-Pyrgiel, Prokopowicz, Gołębiowska, *pp.* 10-43, 2022). The security of data posted on social media is a complex, multifaceted, and ambiguous topic. Sometimes it is difficult to draw a clear line between hacking data theft from social media portals and reading information from the profiles of many social media users in order to analyze the sentiments and opinions of Internet users and to prepare analytical reports based on them, presenting changes in the trends of Internet users' opinions on specific topics. There are many programs, applications, and internet worms that are used to read data and information from comments, entries, posts, etc. written by users of social media portals. (*Social media is the main source of misinformation on the internet,* 2018). The data collected in this way is stored in Big Data Analytics database and analytical systems (Dahl, Prokopowicz, Gwoździewicz, Grzegorek, pp. 43-56, 2018) is used to analyze the sentiment of Internet users' opinions on various topics, including the analysis of brand recognition, evaluation of products and services, forecasting trends in consumer preferences for specific types of products and services, etc.

On the other hand, there have been many cases of cybercriminals stealing data about users of specific social media portals, including certain categories of sensitive personal information posted on these portals. Therefore, Internet technology companies that provide specific information services to Internet users are constantly improving their security systems, procedures for protecting the data of website users, and improving their systems for managing the risks of cybercrime and the transfer and sharing of data on the Internet. Due to the fact that technological progress is constantly being made in the field of information services available on the Internet, the process of improving the security systems for data collected on social media portals will continue and will probably continue for many years to come. For example, on the one hand, Industry 4.0 technologies are being used to improve security systems, user data protection procedures on websites, and cybercrime risk management systems.

However, cybercriminals can also take advantage of current technological advances, so this rivalry between IT specialists on both sides of the fence continues and is likely to continue for many years to come. In addition, the issue of data security, including information posted by users of social media portals on these portals, does not only concern the specific cybersecurity systems of the portals themselves. In recent years, other applications installed on smartphones or emails sent with links to specific other websites through which cybercriminals gain access to the profiles of specific social media users have become one of the targets of cyberattacks.

In view of the above, the importance of cybersecurity for sensitive data posted on websites by Internet users, including social media users, has also been growing in recent years (Górka, 2014). One of the key features of the use of data by various institutions and technology companies offering specific information services available on new Internet media is that citizens do not have full knowledge or awareness of the extent to which data about them that can be found on the Internet is used. Citizens are usually not even fully aware of how much information about them can be obtained from the Internet (Kępiński, Kordowski, Sałkowski, Sztubacki, 2015). If citizens were fully aware of these issues, they would not post a significant amount of information about themselves on these websites, and some users of the aforementioned social media (i.e., Facebook, Twitter, LinkedIn, Instagram, TikTok, etc.) would significantly limit the amount of information they publish about themselves. Perhaps some users would significantly reduce their activity on these websites. Such situations concerning the level of engagement in the use of online social media are becoming an important factor in the daily functioning of citizens and an important element of their lifestyle (Pizło, Mazurkiewicz-Pizło, pp. 111-112, 2017). In that case, the companies operating these platforms could see a decline in the availability of the advertising market in which they operate, and their business objectives would no longer be fully realized. Similarly, central institutions and public security institutions also do not publicly disclose the full scope of possibilities for using data available on the Internet about citizens who are users of specific Internet portals (Szybowski, Prokopowicz, Wołowiec, pp. 237-238, 2019).

Central public security institutions, state security institutions, including cyber security, government crisis management institutions (Domańska-Szaruga,

Prokopowicz, pp. 39-40, 2015), institutions detecting and combating cybercrime, and anti-pandemic security institutions perform very important work and fulfill particularly important functions ensuring the effective development of the Internet in accordance with the principles of social security. Due to the high level of importance of this issue in the context of the growing scale of cybercrime threats, the aforementioned security aspects should be included in key legal norms, including the Basic Law, i.e., the Constitution of the Republic of Poland (Pogódek, Maksymiuk, pp. 28-29, 2016). In order for these functions to be performed effectively, unfortunately, there will most likely always be a significant asymmetry of information between citizens, Internet portal users, and state institutions and key providers of specific Internet information services. On the other hand, every Internet user should be aware of the limited security of personal data that they enter anywhere on the Internet, should be cautious when providing data about themselves, and should also be guided by the principles of social responsibility and ethics.

Key types of fraud and crime committed in the financial industry, apart from cybercrime, which may cause a decline in customer confidence in commercial banks

The most prevalent forms of fraud and crime committed in the context of the development of online and mobile banking include extortion and cyberattacks. The increase in the scale of crime committed using new information technologies is due to a number of factors that have grown in importance in recent years. The development of ICT (Grzegorek, Prokopowicz, Gwoździewicz, pp. pp. 125-126, 2021) and Industry 4.0, on the one hand, has led to technological advances in the development of remote internet communication, e-commerce, internet and mobile banking, e-logistics, e-learning, internet videoconferencing, internet payments and settlements, and internet marketing (Mazurkiewicz-Pizło, Pizło, pp. 37-38, 2016) carried out on social media portals, etc. (Such-Pyrgiel, Prokopowicz, Gołębiowska, pp. 17-18, 2022). As a result, the environment of online applications and information services

is growing, within which cybercrime is developing. On the other hand, the development of ICT and Industry 4.0, including blockchain technology, is generating new solutions that are being applied to improve cybersecurity techniques and the process of managing the risk of cybercrime. The above-mentioned processes accelerated during the Covid-19 pandemic.

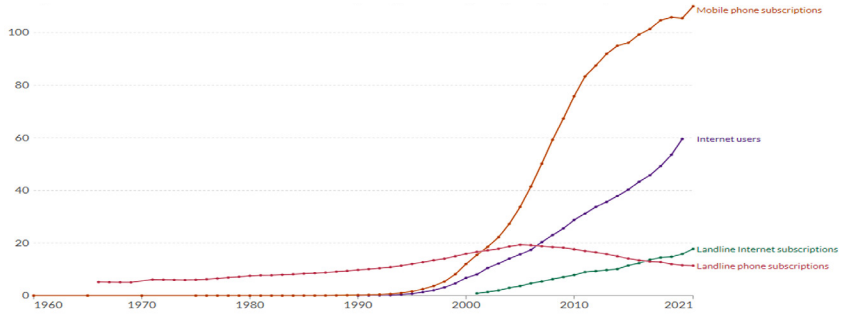
During the Covid-19 pandemic, the scale of purchases of products and services made via the Internet increased (Kos-Łabędowicz, 2015). The development of e-commerce, e-logistics, e-banking (Ali, Ali, Surendran, Thomas, pp. 70-77, 2016), e-marketing, etc. Due to the acceleration of the development of online and mobile banking, the importance of cybersecurity for financial transactions carried out within mobile banking is growing (Gwoździewicz, Prokopowicz, pp. 127-128, 2017). More and more citizens are making payments with their smartphones and have an electronic payment card in their smartphones. The importance of improving cybercrime risk management is growing. Due to the increase in the scale of cybercrime and the growing importance of improving cybersecurity systems in financial institutions, including commercial banks, in recent years, the issue of improving cybercrime risk management systems in online and mobile banking has gained a similar status to the improvement of credit risk management systems, which has been carried out in banks operating in Poland since the 1990s (Wereda, Prokopowicz, Domańska-Szaruga, pp. 257-293, 2018).

The dynamic development of mobile banking and the growing importance of cybersecurity in the use of smartphones and other mobile devices is related, among other things, to the dynamic development of mobile telephony and the spread of smartphones. The issue of the rapidly growing number of Internet and smartphone users on a global scale is presented in the chart below.

The chart shows a significant increase in the types of devices used by Internet users to access online information services. Part of the population uses the Internet on laptops, smart TVs, and desktop computers, but the number of mobile users who access the Internet mainly via smartphones is growing rapidly (The Internet of Everything, The age of Internet ubiquity has arrived, 2014). Recently, the development of Internet technologies has been determined, among other things, by the use of technologies such as machine learning, deep learning, artificial intelligence, the Internet of Things, Big Data

database systems (Sun, pp. 2-3, 2022) and other advanced information processing technologies typical of the current fourth technological revolution known as Industry 4.0 (The Internet of Everything, The age of Internet ubiquity has arrived, 2014). These new technologies are also used to improve cybersecurity instruments and systems (Mohammed, pp. 173–174, 2020).

Chart 3. *Adoption of communication technologies per 100 people (World)*
Landline Internet subscriptions are defined as a fixed access to the public Internet with a download speed of at least 256 kbit/s. Internet users are people who have accessed the Internet fromany location in the last three months



Source: *Technological change*, Internet portal *OurWorldinData*, 29.05.2023, (in:) H. Ritchie, M. Roser (2017) *Technology Adoption*, Published online at OurWorldInData.org (https://ourworldindata.org/technological-change), for: Science and Technology – World Bank, 2021, International Telecommunication Union, World Telecommunication/ICT Development Report and database, Variable time span 1960-2021 (https://datacatalog.worldbank.org/search/dataset/0037712/World-Development-Indicators).

In view of the above, the pandemic, through the development of mobile banking, has increased the importance of improving cybercrime risk management. The report *Abuses in the financial sector. 2022 Edition,* prepared by the Association of Financial Companies and EY Poland, shows that financial product fraud and cyberattacks are currently the most significant challenges in the context of fraud in the financial industry (Fraud in the financial industry. The main problems are fraud and cyberattacks, 2022). Other prevalent types of fraud in the financial industry include falsifying financial statements, conducting unauthorized transactions, money laundering, evading sanctions imposed for specific reasons, internal fraud, and crimes committed using credit cards. In addition, for commercial banks and other financial institutions

operating in Poland, the main types of threats also include credit and loan fraud. On the other hand, there has been an increase in the percentage of entities that believe that financial institutions offer a high level of security for financial transactions carried out by customers (Komorowski, Filip, pp. 145-146, 2019), are doing well in limiting the scale of financial crime and cybercrime, and are developing risk management systems for these types of threats (Kosiński, 2015). In 2022, the percentage of respondents who are convinced of the high level of security of financial transactions carried out in financial institutions is 88%, while in 2021 it was 77%. In addition, the results of the report show that most financial institutions are prepared for the challenges associated with the new economic sanctions imposed on Russia and related to the war in Ukraine (Cieślak, Maj, Pająk, Prokopowicz, Radomyski, Soroka, Śledź, 2023). Furthermore, in connection with the war in Ukraine, there is also an increased risk of cybercrime (Scott, 2022), hacking, and disinformation activities carried out in many countries in Europe and around the world, including Poland (Prokopowicz, pp. 291-292, 2023a). The scale of fraud and crime in the financial industry is an important determinant of customer confidence in banking, including online and mobile banking, which is the basis for the effective development of banking. The last time confidence in the banking system declined was during the global financial crisis of 2008-2009.

Currently, however, the key factor in customer confidence in online and mobile banking is the improvement of cybercrime risk management and the development of cybersecurity systems for transactions carried out by customers as part of the aforementioned remote electronic banking. In Poland, customer confidence in commercial banks has fallen significantly in recent years since the global financial crisis of 2008-2009, mainly due to unreliable provisions in mortgage agreements granted in the foreign currency CHF. On the other hand, due to the increase in the digitization and internetization of economic processes since the Covid-19 pandemic, the development of internet banking, including mobile banking, has accelerated since 2020. The importance of improving cybersecurity systems and instruments for banking operations, financial transactions, payments, and settlements carried out online from the bank's electronic branch has also increased (Komorowski, Filip, pp. 145-146, 2019).

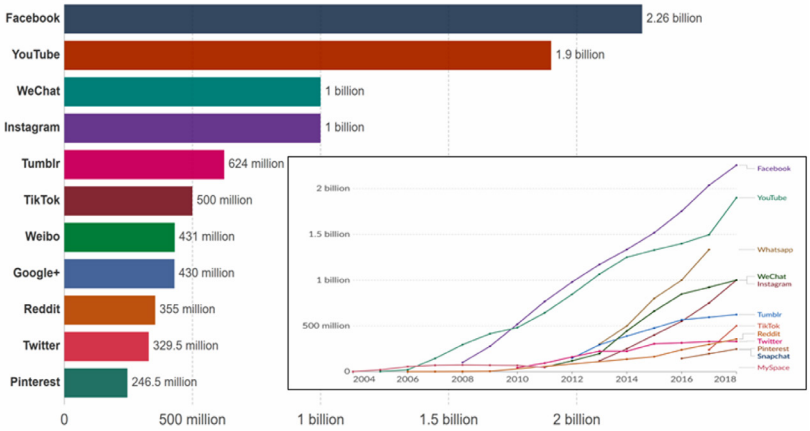
Changes in mobile customer behavior over the past few years and current trends in this area

In recent years, much may have changed in terms of customer mobile behavior. The Covid-19 pandemic may have changed and increased the scale of customer mobile behavior, which is related to the growth of digitization and internetization of economic processes, business activities, companies, and financial and public institutions. During the pandemic, the scale of online purchases of various types of products and services by consumers has increased. Due to government-imposed quarantines and lockdowns, some citizens who had not previously made purchases online began to do so. Many SMEs also created websites for their businesses and online platforms for selling products and/or services whose traditional sales were hampered or blocked by the lockdowns imposed by the government on selected sectors of the economy during the pandemic. Sales of certain product and service ranges have increased several times over thanks to the Internet. This has accelerated the development of e-commerce, e-logistics, e-banking (Grzywacz, 2016), and online payments and settlements. The development of online and mobile banking has accelerated.

Many companies have increased their investments in the implementation of new information technologies and Industry 4.0 (Reinhard, Jesper, Stefan, 2016) in their business activities in order to increase their efficiency and adapt to current trends in business. The scale of purchases and use of various information services by citizens via smartphones has increased. Public offices and institutions have also increased the scale of online services for citizens in terms of remote communication, electronic document transmission, and remote handling of official matters. As a result, there has been an increase in the digitization and internetization of public institutions, where citizens can now carry out all or almost all of their official business via the Internet. There has also been an increase in the creation of smartphone applications that allow citizens to use various online information services. There may also have been an increase in the use of social media available on smartphones by citizens, including young people and children. Unfortunately, there have also been negative effects, such as a significant increase in the amount of time children and young people spend

using social media and playing computer games on smartphones and laptops. This may also be related to the increase in the scale of remote education during the pandemic through online video conferencing platforms. A negative aspect may be the decline in the necessary social interaction of children and young people, playing with peers, teamwork at school, cooperation and collaboration in peer groups, i.e., factors that are key to proper social development, the development of teamwork skills, and social skills in children and young people during their development and education (Matosek, Prokopowicz, Grzegorek, pp. 53-54, 2022). In view of the above, the issue of changing the behavior of mobile customers is a multifaceted one. The growing importance of social networking sites as a significant information medium is illustrated in the chart below, which shows the number of users of leading social media.

Chart 4. *Number of people Rusing social media platforms in 2018. Estimates correspond to monthly active users (MAUs). Facebbok, for example, measures MAUs as users that have logged in during the past 30 days*



Source: *Monthly active users*, Internet portal *OurWorldinData*, 25.06.2021, (in:) M. Roser, H. Ritchie (2019) *Technology Progress*, Published online at OurWorldInData.org (https://ourworldindata.org/technological-progress), for: Statista and The Next Web 2019. (Statista: https://www.statista.com; and TNW: https://thenextweb.com/tech/2019/06/11/most-popular-social-media-networks-year-animated).

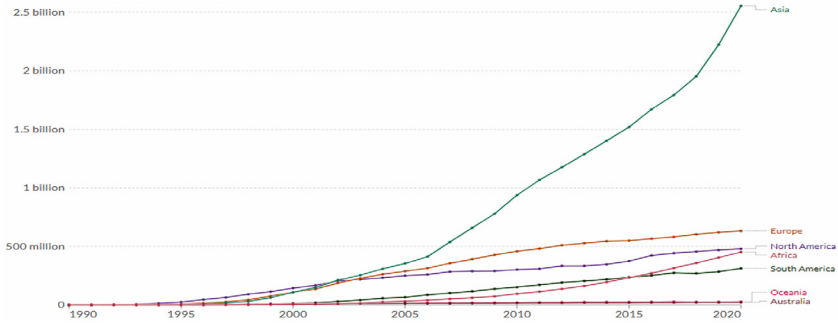
According to futurologists' predictions, virtual cities will be created in the future in the metaverse model or in online computer games with shopping

malls and stores where it will be possible to make online purchases. Some online computer games feature virtual cities or city districts that are digital equivalents of real cities. In addition to online and mobile banking, some commercial banks are already developing virtual banking on the Internet, e.g., by creating a specific game or online banking application in virtual reality for digital bank branches, which are virtual counterparts of real, physically existing bank branches operating in specific city districts. Some shopping malls are creating virtual, spatial guides to the space of a specific mall on the Internet, with marked shops, restaurants, and other services. Google also includes specific shops, hotels, gas stations, restaurants, and various other services on its online maps and in its Street View system. Maps used for navigation to facilitate movement in the field are also increasingly equipped with additional information about The combination of all the above solutions and technologies may enable the creation of virtual cities in the metaverse model or in online computer games with shopping malls, with shops where it will be possible to make online purchases and perhaps also use or order specific services via the Internet. The rapid growth in the number of Internet users is shown in the chart below.

The development of online and mobile banking may now be entering a new phase. Following the dynamic growth of electronic banking in the form of home banking solutions, then the development of electronic banking on the Internet, and then the development of mobile banking as the next stage in the development of online banking, a new stage in this development may now be beginning. This next stage in the development of online and mobile banking may be the development of virtual banking, which will develop in virtual worlds created for this purpose, built on websites or in online computer games created specifically for this purpose by banks. Links or gateways to these virtual worlds and computer games containing built-in virtual branches of commercial banks may be posted on social media used by Internet users representing specific segments of potential customers of banks and/or offers of other types of business entities. Virtual bank branches created in these virtual worlds may offer the full range of products and services of a specific commercial bank and the possibility of performing online banking operations. A virtual world built in the metaverse formula, in which shops, shopping centers, city districts, and bank branches can be embedded, can be accessed, for example, from various

mobile devices other than smartphones, such as glasses equipped with Internet access, virtual reality systems, Google Street View, virtual maps, etc. In this way, online banking could also use augmented reality technology.

Chart 5. *Number of people using the Internet*



Number of people who used the Internet in the last three months.

Source: *Number of Internet Users*, Internet portal *OurWorldinData*, 2.06.2022, in: H. Ritchie, M. Roser (2022) *Internet*, Published online at OurWorldInData.org (https://ourworldindata.org/grapher/number-of-internet-users), based on International Telecommunication Union (via World Bank) and UN (2022), Variable time span 1990-2020 (https://datacatalog.worldbank.org/search/dataset/0037712/World-Development-Indicators). The number of internet users is calculated by Our World in Data based on internet access figures as a share of the total population, published in the World Bank, World Development Indicators and total population figures from the UN World Population Prospects, Gapminder and HYDE.

Development of artificial intelligence-based systems in mobile banking cybersecurity

Recent years have seen rapid development of artificial intelligence-based IT systems, which are increasingly used in business activities, including in the financial sector and electronic banking. This process is closely linked to the ongoing digitization of the economy, the growing importance of mobile banking, and the increasing complexity of cyber threats. In particular, commercial banks and financial institutions are implementing AI solutions to increase the resilience of IT systems, improve the quality of risk management, and more

effectively identify cybercrime. Artificial intelligence is thus becoming a key element of modern cybersecurity strategies.

Machine learning systems, which enable the analysis of very large transaction data sets in real time, play an important role in this process. This makes it possible to detect anomalies and patterns of behavior that deviate from the norm, which may indicate attempts at fraud or unauthorized access to banking systems. Compared to traditional rule-based methods, AI-based solutions are more flexible and adaptable in a rapidly changing threat environment (BIS, 2020).

The development of mobile banking, where the primary interface between the customer and the bank is an application installed on a smartphone, generates new challenges in terms of information security. The use of AI agents allows for continuous monitoring of user activity, transaction risk assessment, and contextual analysis of customer behavior. This approach enables early detection of phishing attacks, account takeovers, and attempts to use malicious mobile software. These systems are increasingly operating autonomously, making decisions to block transactions or activate additional authentication mechanisms (Listopadzka, Prokopowicz, pp. 358-359, 2024).

AI agents are also used to improve operational and cyber risk management systems in banks and other financial institutions. By integrating historical data, security incident information, and current threat signals, predictive risk modeling becomes possible. This approach allows not only to respond to incidents, but also to prevent them by identifying weaknesses in the IT infrastructure. Research shows that the use of artificial intelligence significantly increases the effectiveness of early warning systems against cyberattacks (ENISA, 2021).

In the context of the business activities of companies and financial institutions, AI systems that support identity and access management (IAM) are also becoming increasingly important. Machine learning algorithms enable dynamic assessment of user trust levels based on a number of variables, such as location, device type, login history, and how the user interacts with the application. These solutions increase the security of mobile banking by reducing the risk of unauthorized access to sensitive data and financial resources (Prokopowicz, pp. 101-102, 2023b).

Artificial intelligence is also used in threat analysis at the level of banks' ICT infrastructure. AI-based systems support the identification of malicious

network traffic, DDoS attacks, and attempts to penetrate backend systems supporting mobile banking. Automating log and security event analysis (AI-supported SIEM) significantly reduces incident response times and lightens the load on IT security teams (Goodfellow et al., 2016).

It should be emphasized that the development and implementation of AI agents in cybersecurity is not without its challenges. One of the key issues remains ensuring the transparency and explainability of decision-making models, which is particularly important in the highly regulated banking sector. Financial institutions must balance the benefits of automating security processes with the need to comply with regulatory requirements and protect customer rights.

The literature on the subject also emphasizes the importance of integrating AI systems with existing risk management procedures and the organizational culture of financial institutions. The effectiveness of AI-based solutions depends not only on technological advancement, but also on data quality, staff competence, and the consistency of cybersecurity strategies (OECD, 2021).

With the growing scale of cybercrime and the further development of mobile banking, the use of artificial intelligence is becoming an indispensable element in ensuring the security of financial transactions. AI agents support both the ongoing protection of systems and the long-term improvement of information security strategies. Consequently, it can be concluded that the dynamic development of AI technology in recent years is significantly changing the cybersecurity paradigm in banking, shifting the emphasis from reactive incident response to a predictive and adaptive approach.

From the perspective of the further development of the financial sector, the integration of artificial intelligence with cybersecurity systems will be crucial for maintaining customer confidence in mobile banking. The implementation of advanced AI solutions helps to increase the resilience of financial institutions to digital threats and is an important factor in competitiveness (Hryniewicka, Trzaskowska-Dmoch, pp. 315-316, 2013) in a data – and digital-technology-based economy.

Below is a summary of key cybersecurity techniques in which artificial intelligence agent applications are increasingly used in the business activities of companies, enterprises, and financial institutions (including commercial banks). The table includes both the technique/area of application, examples

of IT solutions with AI, and their main functionalities. The technologies presented reflect a multifaceted approach to real threats in the context of the growing scale of mobile banking and electronic communications.

Table 1. *Key Cybersecurity Techniques Supported by AI Agents in Business Activity and the Financial Sector*

Cybersecurity Technique / Area	Examples of AI-Based Solutions / AI Agents	Core Functionalities and Applications
Transaction Fraud and Anomaly Detection	Machine learning - based transaction monitoring systems (e.g. anomaly detection models, supervised fraud classifiers)	Real-time identification of unusual transaction patterns, automatic blocking of suspicious operations, reduction of false positives, enhanced fraud detection in mobile banking
Predictive Threat Intelligence and Risk Modeling	AI-driven big data analytics platforms, AI-enhanced SIEM systems	Identification of emerging cyberthreat trends, early warning of phishing and malware campaigns, predictive modeling of cyberattacks based on historical and real-time data
Identity and Access Management (AI-driven IAM)	Adaptive authentication systems, biometric and behavioral profiling agents	Dynamic risk-based authentication, continuous assessment of user behavior, detection of account takeover attempts, strengthening access control in mobile banking
Network and Infrastructure Protection (AI-based NDR)	AI-enabled network traffic analysis tools, neural network - based intrusion detection agents	Detection of malicious network behavior, identification of botnets and DDoS attacks, automated response to network-level cyberthreats
Incident Response and Security Automation (SOAR + AI)	SOAR platforms enhanced with AI decision-support agents	Automated incident classification, orchestration of response playbooks, faster reaction to security incidents, reduced workload of SOC teams
Data Protection and Data Loss Prevention (DLP + AI)	AI-powered DLP systems using content and context analysis	Automatic classification of sensitive data, detection of data leakage risks, enforcement of security policies, protection of confidential financial and personal data

Source: Author's own elaboration.

The modern cyber threat environment, particularly in the mobile banking sector, is forcing a shift in the cybersecurity paradigm – from reactive incident response to predictive and adaptive detection and response. Traditional rules based on rigid threat signatures are becoming less effective in the face of complex attacks and the enormous volumes of data generated by electronic transactions (BIS, 2020). In response to this challenge, AI technologies – in particular, machine learning and big data analytics – are becoming a natural component of modern security systems, offering multidimensional behavioral analysis, anomaly detection, and automated response.

The first area where AI demonstrates high added value is transaction analysis and fraud detection. Deep learning models are able to learn non-obvious patterns of user behavior and identify subtle deviations from the norm, which surpasses the capabilities of classic rules (Goodfellow, Bengio & Courville, 2016). In the context of mobile banking, where the number of transactions is enormous and

often performed under conditions of low user attention, real-time anomaly detection is critical to minimizing financial losses and building customer trust.

The second important area is predictive threat modeling and threat intelligence management, which uses algorithms to analyze cybercrime trends using historical incident data and real-time signal monitoring. These solutions enable financial institutions to predict the next steps of attackers and prepare appropriate defense strategies (ENISA, 2021). Integrating these tools with the SOC (Security Operations Center) reduces the time from detection to response, which is the foundation of organizational resilience.

In the third area – identity and access management (IAM) – AI agents are assigned a role in dynamic authentication risk assessment. By analyzing user behavior (behavioral biometrics), IAM systems can flexibly select the level of security, for example, by using more rigorous authentication methods in the case of suspicious behavior. This approach significantly increases the security of mobile banking and reduces the risk of account takeover.

Another important aspect is incident automation and attack response (SOAR). In an era of IT security specialist shortages, process automation, AI playbook support, and rapid incident escalation are essential for SOC teams to operate effectively. The use of AI in SOAR tools not only promotes more efficient incident handling, but also enables organizations to continuously learn from subsequent attacks.

In view of the above, the following recommendations for the future have been formulated:

1. Integrating AI into risk management processes should be a priority for financial institutions, as only adaptive systems can keep pace with changes in the nature of threats (OECD, 2021). A holistic approach is recommended, combining AI with classic security systems as well as corporate risk management processes.
2. Transparency and explainability of AI models is one of the biggest challenges, especially in a regulated sector such as banking. It is necessary to develop interpretable AI models in cybersecurity so that automated decisions can be audited (Goodfellow et al., 2016).
3. Investing in the competence of security teams is just as important as implementing technology. AI cannot replace experts, but it can

significantly increase their effectiveness. Training programs, cyberattack simulations, and cooperation with research units should become the norm.

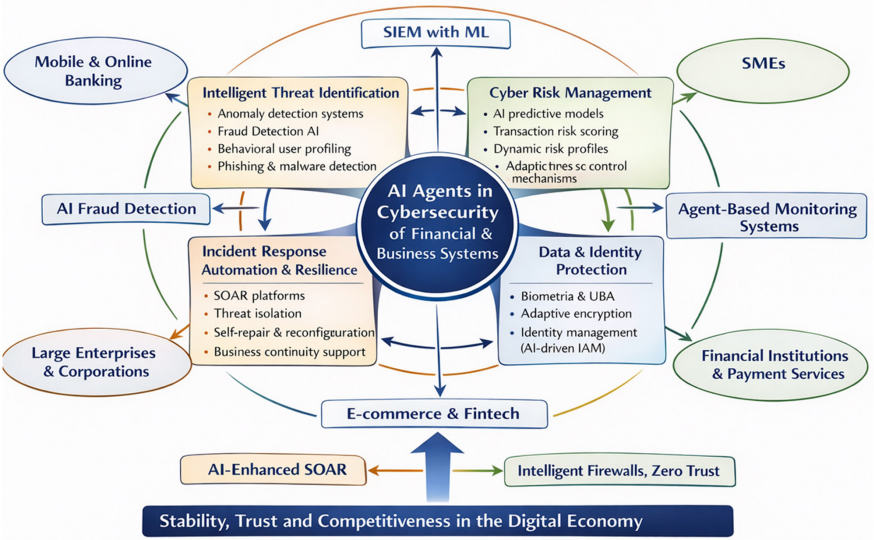
4. Standardization and cooperation between entities (banks, network operators, supervisory institutions) is crucial for the effective exchange of threat intelligence and building the resilience of the entire sector. Participation in consortia and the use of open platforms for the exchange of threat data is recommended.
5. Monitoring the impact of AI on user rights and regulatory compliance (e.g., GDPR) must be an integral part of the implementation strategy for AI systems in cybersecurity.

A graphical overview of key cybersecurity techniques using AI agents in the operations of businesses and financial institutions

The diagram below shows a systemic model of the use of artificial intelligence agents in key cybersecurity techniques in the activities of enterprises, corporations, and financial institutions. The central location of AI agents reflects their role as integrators of threat detection, risk management, incident response automation, and data and digital identity protection processes. The diagram is interdisciplinary in nature, combining technological (machine learning, SIEM, SOAR, IAM), economic (operational efficiency, loss reduction), organizational (risk management, business continuity), and social (trust and stability of the digital economy) perspectives.

The diagram illustrates the transition from a traditional, reactive cybersecurity model to a predictive-adaptive model based on autonomous or semi-autonomous AI agents. Key techniques, such as intelligent threat identification and cyber risk management, use machine learning algorithms to analyze transaction and behavioral patterns in real time. The literature emphasizes that AI's ability to process large volumes of data and detect subtle anomalies represents a qualitative change compared to traditional rule-based systems (Russell, Norvig, 2021).

Figure 1. *Key Cybersecurity Techniques Supported by AI Agents in Business Activity and the Financial Sector*



Source: Author's own elaboration.

On the other hand, the development of AI agents in cybersecurity generates new systemic challenges. The automation of incident response processes (e.g., within SOAR) increases operational efficiency but can lead to risks associated with excessive decision autonomy and limited algorithm explainability. The European approach to *trustworthy AI* points to the need for transparency, accountability, and human oversight in decision-making processes (European Commission, 2020). The diagram therefore suggests that the relationship between the technological layer and the institutional-regulatory layer is crucial for the stability of the entire system.

From a macroeconomic perspective, the use of AI agents in cybersecurity strengthens the resilience of businesses and financial institutions, reducing incident costs and limiting systemic risk. The OECD (2019) emphasizes that the responsible use of AI can support innovation (Chrzanowski, Zawada, p. 32, 2018) and the competitiveness of economies, provided that ethical and social aspects are taken into account at the same time (Karaś, pp. 82-83, 2017). The diagram

highlights this relationship by linking security techniques to the end result in the form of stability, trust, and competitiveness in the digital economy.

The analysis and the diagram presented indicate that the role of AI agents in the cybersecurity of enterprises and financial institutions is systemic and strategic, rather than merely instrumental. The conclusions drawn from the presented model emphasize the need to treat artificial intelligence as an element of the critical infrastructure of the digital economy, requiring an integrated technological, organizational, and regulatory approach.

Given the complexity of the interrelationships between technology, cyber risk, legal regulations, and public trust, recommendations for the future should focus on the long-term, sustainable, and responsible development of AI systems in cybersecurity. Key strategic actions should include both technological development and the strengthening of institutional competencies and oversight and transparency mechanisms to ensure the sustainable resilience of organizations in the context of dynamic digital transformation. In view of the above, the following recommendations for the future have been formulated:

1. The strategic implementation of AI agents in cybersecurity should be based on an integrated model in which technical solutions (SIEM with ML, AI Fraud Detection, adaptive IAM) are complementary to regulatory frameworks and risk management mechanisms.
2. It is necessary to develop explainable and auditable AI models to reduce the risk of losing stakeholder trust and to ensure compliance with legal regulations. Interdisciplinary education programs and cooperation between the scientific sector and business can play a key role in minimizing the skills gap in the area of AI and cybersecurity.
3. It is recommended to implement a *human-in-the-loop* approach in high-risk systems and to conduct periodic assessments of the impact of AI technologies on economic and social security. The diagram shows that only when there is a balance between automation and institutional control is it possible to achieve lasting stability in the digital economy.

The COVID-19 pandemic as a catalyst for internetization, digitization, and cybercrime developing in the context of the economic activities of companies, enterprises, financial institutions, and public institutions

The increase in the internetization and digitization of economic processes and the improvement of the management of public institutions and commercial entities greatly helped to survive the economic crisis caused by the Covid-19 pandemic in 2020 (*COVID-19 to plunge global economy into worst recession since World War,* 2020). During the pandemic, there was an acceleration in the digitization and internetization of both economic processes carried out by commercial enterprises and companies, as well as the organization of remote communication between public sector offices and institutions and citizens.

The development of ICT and Industry 4.0 (Zhou, Liu, Zhou, 2015) has, on the one hand, led to technological advances in the development of remote internet communication, e-commerce, internet and mobile banking, e-logistics, e-learning, internet videoconferencing, internet payments and settlements, internet marketing on social media portals, etc. (Such-Pyrgiel, Prokopowicz, Gołębiowska, pp. 17-18, 2022). As a result, the environment of online applications and information services is growing, within which cybercrime is developing. On the other hand, the development of ICT and Industry 4.0, including blockchain technology, is generating new solutions that are being applied to improve cybersecurity techniques and the process of managing the risk of cybercrime. The above-mentioned processes accelerated during the Covid-19 pandemic.

During the Covid-19 pandemic, many industries and sectors saw an increase in the number of businesses developing their activities via the Internet, providing their services remotely and selling their products through e-commerce (Sadłowski, Lewandowska-Gwarda, Pisarek-Bartoszewska, pp. 173-174, 2021). Many companies that had not previously done so switched to remote operations conducted electronically via the Internet during the pandemic. The importance of Internet marketing, including viral marketing, public relations, video conferencing, etc., conducted via the Internet increased.

The development of electronic banking, including Internet and mobile banking, also increased. The share of electronic, cashless payments made via the Internet and using electronic bank cards increased. The percentage of citizens who did not use cash when paying in stores but made contactless payments grew. As a result, the Covid-19 pandemic caused a significant increase in the share of electronic payments in the context of total payments made in national economies. The importance of financial transactions carried out remotely, via the Internet, grew. Commercial banks recorded an increase in electronic payments and an increase in the number of transfers made via online banking, including mobile banking. As a result, the importance of improving cybercrime risk management processes and the management of the risk of data loss transferred via the Internet in the context of electronic online banking, including mobile banking, has also increased, as has the importance of improving cybersecurity systems and instruments.

However, referring to the cited research results on the detection of malware by cybersecurity applications running on laptops, smartphones, and other devices with Internet access, several important issues related to this problem were pointed out. On the one hand, in recent years, the importance of improving cybersecurity instruments and systems has been growing, which is related to the increasing scale of Internet users making online payments and settlements and using online and mobile banking services. On the other hand, providers of online information and financial services are required by law to comply with and ensure certain minimum cybersecurity standards for the services they offer to customers via the Internet. Providers of these services, including social media companies and online banks, are also required to ensure a certain level of cybersecurity for systems that enable online payments, settlements, transfers, and various financial transactions carried out by customers on their laptops and smartphones (Windasari, Kusumawati, Larasati, Amelia, 2022).

Providers of these services should monitor potential cyber threats on an ongoing basis, detect them as early as possible, neutralize them, and improve cybersecurity instruments both in the internal IT systems of a given organization and at the level of applications used by Internet users of specific services. However, the ability of providers of specific online information and financial services to improve cybersecurity on the client side is limited. Therefore,

technology companies and online banks are developing a set of recommendations and advice on the safe use of their services, which is regularly updated and communicated to customers, i.e., to minimize the scale of effective cyberattacks on the applications and operating systems they support. In the context of the research conducted and for the purposes of this article, the following main research thesis was formulated: The Covid-19 pandemic has caused a multifaceted increase in the scale of cybercrime and the importance of improving the cybersecurity of online and mobile banking systems. In view of the above, the main research thesis mentioned above has been confirmed on the basis of the research conducted.

Emerging threats and future directions in mobile banking cybersecurity: the role of quantum computing, deepfakes, and regulatory evolution

The dynamic transformation of the cybersecurity landscape in mobile banking is driven not only by the continued evolution of known threat categories, but increasingly by the emergence of qualitatively new risks that challenge the effectiveness of existing protective mechanisms. Among the most significant of these is the growing application of generative artificial intelligence by cybercriminals, particularly in the creation of highly convincing deepfakes and synthetic voice or video materials. These technologies enable attackers to impersonate bank employees, senior managers, or customers themselves during telephone or video verification procedures, rendering traditional multi-factor authentication methods based on voice or image recognition substantially less reliable. Financial institutions must therefore urgently expand their threat models to account for synthetic media attacks, integrating dedicated deepfake detection algorithms into identity verification pipelines (ENISA, 2023).

A further dimension of the evolving threat environment is the proliferation of mobile malware specifically designed to target banking applications. Modern banking trojans, such as variants of the Anatsa and Teabot families documented in recent years, are capable of overlaying legitimate

banking application interfaces with convincing fraudulent screens, intercepting one-time passwords transmitted via SMS, and exfiltrating credentials stored in device memory. The increasing sophistication of these attacks, combined with the widespread distribution of malicious applications through unofficial channels and, in documented cases, through official application stores, places significant pressure on both mobile operating system developers and commercial banks to implement more robust application integrity verification and runtime protection mechanisms. The adoption of mobile threat defense (MTD) solutions, which leverage AI-powered behavioral analysis to detect anomalous application activity in real time, is becoming a recognized standard practice in the financial sector (Zhang, Xiong, Xiao, 2020).

The long-term strategic horizon of cybersecurity in mobile banking is also shaped by the anticipated advent of practically useful quantum computers. While large-scale quantum computing remains a medium-term prospect, the so-called *harvest now, decrypt later* strategy is already a present-day concern: adversaries with sufficient resources may currently be collecting encrypted banking communications with the intention of decrypting them once sufficiently powerful quantum systems become available. This scenario necessitates a proactive migration toward post-quantum cryptographic standards, a process that the National Institute of Standards and Technology (NIST) has been leading through the formal standardization of post-quantum algorithms, including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures. Commercial banks and payment infrastructure operators face the complex challenge of conducting a comprehensive cryptographic inventory of their systems and planning a phased transition that maintains backward compatibility and operational continuity (NIST, 2022).

The regulatory environment governing cybersecurity in mobile banking has also undergone significant transformation in recent years, particularly within the European Union. The Digital Operational Resilience Act (DORA), which entered into application in January 2025, establishes binding requirements for ICT risk management, incident reporting, digital operational resilience testing, and the oversight of critical third-party ICT service providers across the financial sector. For commercial banks operating mobile banking platforms, DORA represents a substantial compliance challenge, requiring not only technical

adaptation but also organizational restructuring of governance processes related to ICT risk. Particularly significant is the requirement for threat-led penetration testing (TLPT), which mandates that significant financial entities periodically subject their critical systems, including mobile banking applications and associated backend infrastructure, to simulated cyberattacks conducted by qualified external red teams. The implementation of DORA thus functions as a systemic driver of cybersecurity maturity improvement across the European financial sector (European Commission, 2022).

Complementing the regulatory dimension is the growing recognition of cybersecurity as an element of broader digital trust infrastructure. Customer willingness to adopt and consistently use mobile banking services is closely correlated with their perception of security and privacy protection. Research consistently indicates that a single high-profile security incident, particularly one involving the public disclosure of customer financial data or funds, can cause lasting damage to an institution's reputation and customer retention rates that may persist for years beyond the original event. In this context, the investment in advanced AI-driven cybersecurity systems should be understood not merely as a compliance cost or operational necessity, but as a strategic component of value creation, directly contributing to customer loyalty, brand equity, and sustainable competitive advantage. The development of transparent communication strategies regarding security practices, combined with user-friendly tools that empower customers to actively manage their own digital security settings, represents an important frontier in the human dimension of mobile banking cybersecurity (Windasari, Kusumawati, Larasati, Amelia, 2022).

Looking at future directions in the field, a key area of development is the convergence of cybersecurity and privacy-preserving technologies. Federated learning frameworks, which allow AI models to be trained across distributed datasets held by multiple institutions without centralizing sensitive customer data, offer a promising pathway for collaborative threat intelligence without compromising data protection requirements under the General Data Protection Regulation (GDPR). Similarly, confidential computing environments, which leverage hardware-based trusted execution environments (TEEs) to protect data even during processing, are increasingly being explored by financial institutions as a means of enabling secure AI inference on sensitive

transaction data without exposing raw inputs to cloud infrastructure operators. The intersection of these technologies with mobile banking cybersecurity represents one of the most technically advanced frontiers in the field and is likely to attract growing research and investment attention in the coming years (BIS, 2020). Ultimately, the resilience of mobile banking cybersecurity will depend not on any single technological solution, but on the effective integration of AI-driven detection and response capabilities, robust regulatory frameworks, human-centered security design, and proactive adaptation to the evolving threat landscape shaped by quantum computing, synthetic media, and the continuous ingenuity of adversarial actors.

Summary and conclusions

The above considerations show that the use of artificial intelligence agents in the cybersecurity of enterprises and financial institutions is one of the key vectors of transformation in the modern digital economy. The analyses carried out and the diagrammatic model developed indicate that AI is not only a technological tool, but also an infrastructural element that influences organizational resilience, financial system stability, and the level of public trust. The literature emphasizes that the ability of AI systems to perform predictive data analysis and detect anomalies is an important factor in competitive advantage, but at the same time requires the implementation of principles of transparency and accountability (Russell, Norvig, 2021; OECD, 2019). In light of the analyses carried out, the following key conclusions can be drawn:

1. AI agents significantly increase the effectiveness of threat detection and reduce losses resulting from cyber incidents.
2. Automation of security processes improves the operational efficiency of organizations, but generates new challenges related to control and explainability of decisions.
3. The integration of AI with regulatory frameworks and trustworthy AI principles is a prerequisite for maintaining stability and trust in the digital economy.
4. A strategic approach to cybersecurity requires a balance between innovation and systemic risk management.

The development of AI agents in cybersecurity should be analyzed in the context of broader socio-economic changes, in which autonomous technologies are shaping business models, employment structures, and the architecture of institutional responsibility. Strategic documents emphasize that the long-term sustainability of AI systems requires transparency, accountability, and human oversight in high-risk processes (European Commission, 2020). This means that technological innovation must be combined with ethical reflection and an adequate regulatory framework.

In view of the above, the future of cybersecurity in business and the financial sector will increasingly depend on the quality of the integration of AI agents with risk management systems, organizational structures, and public policies. Only a model based on interdisciplinarity, responsibility, and adaptability will allow the potential of artificial intelligence to be exploited without exacerbating systemic and social risks.

References

Ali L., Ali F., Surendran P., Thomas B. (2016). *The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services* (in:) *International Journal of e-Education, e-Business, e-Management and e-Learning*, Volume 7, Number 1, March 2017, pp. 70-77.

Bank for International Settlements (2020) *Sound practices: implications of fintech developments for banks and bank supervisors*. Available at: https://www.bis.org/bcbs/publ/d431.pdf

Bank for International Settlements (BIS). (2020). Sound practices: implications of fintech developments for banks and bank supervisors. Basel: BIS. Available at: https://www.bis.org/bcbs/publ/d431.pdf

Chrzanowski M., Zawada P. (2018). *Otwarte innowacje i ich wykorzystanie w przedsiębiorstwach typu start-up*, Publishing House of the Rzeszów University of Technology, Rzeszów 2018, pp. 7-122.

Cieślak E., Maj J., Pająk K., Prokopowicz D., Radomyski A., Soroka P., Śledź P. (2023). *Wybrane aspekty rosyjskiej agresji na Ukrainę w obszarze politycznym, militarnym i gospodarczym*, (ed. P. Soroka i K. Pająk), Elipsa Publishing House, Warsaw 2023. ISBN 978-83-8017-474-0.

COVID-19 to plunge global economy into worst recession since World War, (2023). World Bank, 2020 (http://www.worldbank.org/en/news/press-release/2020/06/08/covid-19-to-plunge-global-economy-intoworst-recession-since-world-war-ii), Access: 15 July 2023.

Dahl M., Prokopowicz D., Gwoździewicz S., Grzegorek J. (2018). *Application of data base systems Big Data and Business Intelligence software in integrated risk management in organization* (in:) *International Journal of New Economics and Social Sciences*, International Institute for Innovation *Science – Education – Development* in Warsaw, No. 2 (8) 2018, Warsaw, December 2018, pp. 43-56. ISSN 2450-2146.

Domańska-Szaruga B., Prokopowicz D. (2015). *Makroekonomiczne zarządzanie antykryzysowe* (in:) 34 Zeszyty Naukowe Uniwersytetu Przyrodniczo – Humanistycznego w Siedlcach, No. 107, Seria: Administracja i Zarządzanie (34) 2015, Uniwersytet Przyrodniczo-Humanistyczny, Wydział Nauk Ekonomicznych i Prawnych, Siedlce 2015, pp. 37-48. ISSN 2082-5501.

ENISA (2021) *Artificial Intelligence cybersecurity challenges*. Available at: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

ENISA – European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Commission. (2022). Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (DORA) and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

European Commission (2020), *White Paper on Artificial Intelligence: A European approach to excellence and trust*, Brussels, https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

Goodfellow, I., Bengio, Y. and Courville, A. (2016) *Deep Learning*. MIT Press. Available at: https://www.deeplearningbook.org

Gołębiowska A., Prokopowicz D. (2021). *Increase in the Internetization of economic processes, economic, pandemic and climate crisis as well as cybersecurity as key challenges and philosophical paradigms for the development of the 21st century civilization* (in:) *Journal of Modern Science*, Issue 2/2021, volume 47, Wyższa Szkoła Gospodarki Euroregionalnej, pp. 307-344. ISSN 1734-2031. DOI: 10.13166/jms/143848.

Grzegorek J., Prokopowicz D., Gwoździewicz S. (2021). *Wykorzystanie platform analitycznych Big Data Analytics technologii informacyjnych ICT w analizie sentymentu dla wybranej problematyki związanej z Przemysłem 4.0*, (in:) P. J. Suwaj, S. Gwoździewicz, K. Samulska (ed.), *Bezpieczeństwo informacyjne jednostek organizacyjnych. Wybrane problemy*, Publishing house Naukowe Akademii im. Jakuba z Paradyża w Gorzowie Wielkopolskim, Gorzów Wielkopolski 2021, pp. 101-142. ISBN 978-83-66703-34-6.

Grzywacz, J. (2016). *Bankowość elektroniczna w przedsiębiorstwie*, Warszawa: Publishing house SGH.

Grzywak, A., Widenka, G., (2015). *Bezpieczeństwo rozproszonych systemów informatycznych – Kryptografia w zastosowaniu do podpisu cyfrowego i identyfikacji użytkownika w sieci Internet*, Publishing House of the University of Business in Dąbrowa Górnicza.

Górka, M. ed. (2014). *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Warsaw: Difin Publishing House.

Gwoździewicz, S., Prokopowicz, D. (2017). *Determinanty rozwoju cyberprzestępczych ataków na systemy informatyczne firm i klientów indywidualnych w instytucjach finansowych* (in:) S. Gwoździewicz, K. Tomaszycki (ed), *Prawne i społeczne aspekty cyberbezpieczeństwa*, Warsaw: International Institute of Innovation *Science – Education – Development* in Warsaw, pp. 127-128.

Hryniewicka M., Trzaskowska-Dmoch A. (2013). *Venture capital and banks loans as a combination of traditional and modern instruments for the financing of corporate Innovativeness* (in:) *Zarządzanie w XXI w. Menedżer innowacyjnej organizacji,* E. Gołębiowska (ed), *Przedsiębiorczość i Zarządzanie*, Tom XIV, Zeszyt 12, część I, SAN, Łódź 2013, pp. 311-321, ISSN: 1733-2486.

Karaś D. (2017). *Dylemat więźnia jako podstawowe narzędzie analizy kooperacji rynkowej*, (in:) *Zeszyty Naukowe Uniwersytetu Kardynała Stefana Wyszyńskiego Ekonomia i Zarządzanie*, No. 2(2)/2017, pp. 80-89.

Kępiński, Ł., Kordowski, M., Sałkowski, D., Sztubacki, K. (2015). *Twoja firma widoczna w internecie Marketing internetowy. Nowe możliwości, nowi klienci, nowe rynki*, Warsaw: Poltext Publishing House.

Komorowski P., Filip D. (2019). *Information and Statistical Efforts of Selected Safety Network Institutions in the Area of Financial System Stability* (in:) *Journal of Management and Financial Sciences*, 2019, Volume 10, No. 29, pp. 143-157.

Komorowski P., Prokopowicz D. (2022). *Impact of the Sars-Cov-2 coronavirus pandemic (Covid-19) on globalization processes* (in:) *International Journal of New Economics and Social Sciences*, International Institute for Innovation *Science – Education –*

Development in Warsaw, June 2022, Volume 15, No. 1, pp. 157-180. ISSN: 2450-2146. DOI: 10.5281/zenodo.7114252.

Kos-Łabędowicz, J. (2015). *Internet jako źródło informacji w decyzjach nabywczych konsumenta*, Warsaw: C.H. Beck Publishing House.

Kosiński, J. (2015). *Paradygmaty cyberprzestępczości*, Warsaw: Difin Publishing House.

E. Listopadzka, D. Prokopowicz, *The need to reduce the scale of misinformation and unethical business practices used with the help of AI use in social media as an important element of risk management of the development of artificial intelligence technology applications* (in:) *International Journal of Legal Studies*, International Institute for Innovation *Science – Education – Development* in Warsaw, December 2024, No. 2 (18) 2024, pp. 343-374. DOI: 10.5604/01.3001.0055.0959 ISSN 2543-7097.

Matosek M., Prokopowicz D., Grzegorek J. (2022). *The importance of activating entrepreneurship and innovation of economic agents functioning in the economy and contemporary trends in teaching entrepreneurship in higher education* (in:) *International Journal of New Economics and Social Sciences*, International Institute for Innovation *Science – Education – Development* in Warsaw, No. 16 (2) 2022, December 2022, pp. 43-81. ISSN 2450-2146. DOI: 10.5604/01.3001.0016.3406.

Mazurkiewicz-Pizło A., Pizło W. (2016). *Social marketing – a concept of marketing management*, (in:) *Marketing Science&Inspirations*, No. 1, vol. 11, pp. 35-42.

Mohammed I. A. (2020). *Artificial Intelligence for Cybersecurity: A systematic Mapping of Literature* (in:) *International Journal of Innovations in Engineering Research and Technology*, No. 7(09), pp. 172–176. Retrieved from https://repo.ijiert.org/index.php/ ijiert/article/ view/2797.

Monthly active users, Internet portal *OurWorldinData*, 25.06.2021, (in:) M. Roser, H. Ritchie (2019) *Technology Progress*, Published online at OurWorldInData.org (https://ourworldindata.org/technological-progress), for: Statista and The Next Web 2019. (Statista: https://www.statista.com; and TNW: https://thenextweb.com/tech/2019/06/11/most-popular-social-media-networks-year-animated).

Nadużycia w branży finansowej. Główne problemy to wyłudzenia i cyberataki (in:) Portal *podatki.biz*, Informacje dla Podatników Małych i Dużych, Dział: Aktualności – podatki, rachunkowość, ZUS, gospodarka, 27.10.2022, (https://www.podatki.biz/artykuly/naduzycia-w-branzy-finansowej-glowne-problemy-to-wyludzenia-i-cyberataki_16_51586.htm).

National Institute of Standards and Technology (NIST). (2022). Selected Algorithms 2022. Post-Quantum Cryptography Standardization. U.S. Department of Commerce. Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

Number of Internet Users, Internet portal *OurWorldinData*, 2.06.2022, in: H. Ritchie, M. Roser (2022) *Internet*, Published online at OurWorldInData.org (https://ourworldindata.org/grapher/number-of-internet-users), based on International Telecommunication Union (via World Bank) and UN (2022), Variable time span 1990-2020 (https://datacatalog.worldbank.org/search/dataset/0037712/World-Development-Indicators).

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, https://www.oecd.org/going-digital/ai-in-society/

OECD (2021) *Artificial intelligence, machine learning and big data in finance*. Available at: https://www.oecd.org/finance/artificial-intelligence-machine-learning-big-data-finance.htm

Pizło W., Mazurkiewicz-Pizło A. (2017). *Styl życia – jako egzemplifikacja zmian zachowań konsumpcyjnych Polaków*, (in:) *Polityki Europejskie, Finanse i Marketing Zeszyty Naukowe Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie*, No. 17 (66), pp. 104-117.

Pogódek A., Maksymiuk M. (2016). *Konstytucja jako ustawa zasadnicza*, (in:) *Prawo konstytucyjne*, ed. B. Szmulik, Warszawa: Wydawnictwo C. H. Beck, pp. 28 – 29.

Prokopowicz D. (2023a). *Gospodarcze skutki wojny w Ukrainie* (in:) E. Cieślak, J. Maj, K. Pająk, D. Prokopowicz, A. Radomyski, P. Soroka, P. Śledź, *Wybrane aspekty rosyjskiej agresji na Ukrainę w obszarze politycznym, militarnym i gospodarczym*, (ed. P. Soroka i K. Pająk), Elipsa Publishing House, Warsaw 2023, pp. 284-332. ISBN 978-83-8017-474-0.

Prokopowicz D. (2023b). *Opportunities and threats to the development of Artificial Intelligence applications and the need for normative regulation of this development* (w:) *International Journal of Legal Studies*, International Institute for Innovation *Science – Education – Development* in Warsaw, December 2023, No. 2 (14) 2023, pp. 95-129. DOI: 10.5604/01.3001.0054.2699 ISSN 2543-7097

Reinhard G., Jesper V., Stefan S. (2016). *Industry 4.0: Building the digital enterprise* (in:) *2016 Global Industry 4.0 Survey*, 2016, available at: https://doi.org/10.1080/01969722.2015. 1007734.

Russell S., Norvig P. (2021), *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson, https://aima.cs.berkeley.edu/

Sadłowski A., Lewandowska-Gwarda K., Pisarek-Bartoszewska R., Engelseth P. (2021). *A longitudinal study of e-commerce diversity in Europe* (in:) *Electronic Commerce Research*, Springer, February 2021, No. 21, pp. 169–194. DOI: 10.1007/s10660-021-09466-z.

Scott M. (2022). *How Ukraine used Russia's digital playbook against the Kremlin. From hacktivists to info wars, Kyiv is mastering digital warfare in ways previously associated with the Kremlin*. 24.08.2022. https://www.politico.eu/article/ukraine-russia-digital-playbook-war.

Such-Pyrgiel M. K., Prokopowicz D., Gołębiowska A. (2022). *The postpandemic reality and the security of information technologies ICT, Big Data, Industry 4.0, social media portals and the Internet* (in:) *Journal of Modern Science*, Issue 2/2022, Volume 49, Wyższa Szkoła Gospodarki Euroregionalnej, pp. 10-43. ISSN 1734-2031. DOI: 10.13166/jms/156912.

Sun Z. (2022). *Big Data, analytics intelligence, and Data Science*, PNG UoT BAIS, December 2022, No. 7(4), pp. 1-7, preprint. DOI: 10.13140/RG.2.2.11911.47525.

Szybowski D., Prokopowicz D., Wołowiec W. (2019). *Methods of development network analysis as a tool improving efficient organization management* (in:) *International Journal of New Economics and Social Sciences*, International Institute for Innovation *Science – Education – Development* in Warsaw, No. 1 (9) 2019, Warsaw, June 2019, pp. 229-249. ISSN 2450-2146.

Technological change, Internet portal *OurWorldinData*, 29.05.2023, (in:) H. Ritchie, M. Roser (2017) *Technology Adoption*, Published online at OurWorldInData.org (https://ourworldindata.org/technological-change), for: Science and Technology – World Bank, 2021, International Telecommunication Union, World Telecommunication/ICT Development Report and database, Variable time span 1960-2021 (https://datacatalog.worldbank.org/search/dataset/0037712/World-Development-Indicators).

The Internet of Everything, The age of Internet ubiquity has arrived, (in:) BI Intelligence Estimates, 24.10.2014, (https://www.businessinsider.com/the-internet-of-everything-2014-slide-deck-sai-2014-2?IR=T).

To media społecznościowe są głównym źródłem dezinformacji w sieci (in:) Website *Interaktywnie.com*, Dział: Raporty i badania, 20 July 2018, (https://interaktywnie.com/biznes/artykuly/raporty-i-badania/to-media-spolecznosciowe-sa-glownym-zrodlem-dezinformacji-w-sieci-257647), for: Przeprowadzony wśród Internautów Raportu IAB Polska *Dezinformacja w sieci*.

Wereda W., Prokopowicz D., Domańska-Szaruga B. (2018). *Globalizacyjne i normatywne determinanty procesu doskonalenia zarządzania bankowym ryzykiem kredytowym w Polsce, Globalizational and normative determinants of the improvement of the banking credit risk management in Poland* (in:) *International Journal of Legal Studies*, International Institute for Innovation *Science – Education – Development* in Warsaw, Warsaw, December 2018, No. 2 (4) 2018, pp. 257-293. ISSN 2543-7097.

Windasari N. A., Kusumawati N., Larasati N., Amelia R. P. (2022). *Digital-only banking experience: Insights from gen Y and gen Z* (in:) *Journal of Innovation & Knowledge*, vol. 7, No. 100170.

Windasari N. A., Kusumawati N., Larasati N., Amelia R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z (in:) *Journal of Innovation & Knowledge*, vol. 7, No. 100170.

Zhang, Y., Xiong, Y., Xiao, S. (2020). *AI-driven cyber security for financial institutions* (in:) *IEEE Security & Privacy*, No. 18(4), pp. 54–62. https://ieeexplore.ieee.org/document/9103824

Zhou K., Liu T., Zhou L. (2022). *Industry 4.0: Towards future industrial opportunities and challenges*, (in:) 12th International Conference Fuzzy Systems Knowledge Discoveries, FSKD 2015. Retrieved January 26, 2022 from https://doi.org/10.1109/FSKD.2015.7382284.