SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 240

COOPETITION IN THE BANKING SECTOR IN RESONSE TO CYBERTHREATS

Paweł SZLĘZAK

Silesian University of Technology; pawel_szlezak@o2.pl, ORCID: 0009-0003-0685-1404

Purpose: The purposes are the analysis of coopetition in the Polish banking sector as a response to cyber threats and legal regulations. Identification of the causes of coopetition in the Polish banking sector in terms of increasing cyber resilience. Identification and analysis of key forms of coopetition in the area of cybersecurity.
Design/methodology/approach: The paper addresses a contemporary and critical challenge faced by the Polish banking sector: the need to collaborate on cybersecurity despite being direct competitors. This approach is not purely theoretical. It seeks to provide actionable insights for industry practitioners and regulators.
Findings: The research creates a detailed map by identifying the most dangerous cyber threats, the most valued benefit, and the most critical barriers. This tripartite analysis offers a comprehensive and practical view of the coopetition landscape.
Research limitations/implications: The study's primary limitations include its focus on the Polish banking sector, which may limit the generalizability of the findings to other countries with different regulatory environments and market structures. Longitudinal case studies tracking existing coopetition initiatives over time would provide invaluable insights into their long-term effectiveness and evolution.
Practical implications: The primary practical implication is that Polish banks should strategically develop formalized coopetition structures, such as information-sharing system, to enhance collective cybersecurity. This cooperation will directly impact the business by reducing financial losses and regulatory fines, while strengthening customer trust.
Social implications: The findings can inform both industry policy by encouraging the creation of formal threat-sharing platforms and public policy by shaping regulations, that incentivize secure collaboration over pure competition.
Originality/value: It is one of the first empirical investigations into the drivers, benefits, and barriers of cybersecurity coopetition specifically within the Polish banking sector. The value is for banking executives, cybersecurity professionals and policymakers.
Keywords: Banking sector, cybersecurity, coopetition, cyberattacks, legal regulations.
Category of the paper: Cybersecurity research within the banking sector coopetition as a response of syber threats and legal regulations.

1. Introduction

The banking sector, which is of key importance to the economy, is a prime target for cybercriminals. The rapid growth of digitalization, the processing of sensitive data, and the potential for financial and reputational losses make banking institutions an attractive target. Traditional, isolated security models, relying solely on internal investments in technology and personnel, are proving insufficient in the face of organized, transnational criminal groups using advanced techniques such as Advanced Persistent Threats (APT) and ransomware attacks. In response to the increasing sophistication of cyber threats and the resulting legal regulations, a strategy has been developed for cooperation between competing banking entities in selected specialist areas where the synergistic benefits outweigh the costs of competition. In the context of cybersecurity, coopetition manifests itself in the sharing of threat intelligence, the development of standards, joint training, and investment in advanced detection and response systems. Banks increasingly need to embrace coopetition system between them and collaborate even as competitors to strengthen collective defenses against escalating cyber threats. Such joint efforts enable faster threat detection, shared intelligence, and more resilient financial systems.

The main objective of this article is to analyze the phenomenon of coopetition in the Polish banking sector as a response to cyber threats and legal regulations. The specific objectives are:

- To identify the causes of the coopetition phenomenon in the Polish banking sector in increasing the level of cyber resilience.
- To identify and analyze key forms of coopetition in the area of cybersecurity.
- To determine the barriers and benefits resulting from coopetition in the banking sector.

The research hypothesis is: Cyber incidents and associated legal regulations have contributed to the undertaking of coopetitive activities in the banking sector. The research questions are:

- What types of cyberattacks may cause the undertaking of coopetition in the banking sector in response to cyber threats?
- Which legal regulations (EU and national) stimulate and which hinder the development of coopetition in the cybersecurity of the banking sector?
- What could be the benefits of coopetition in the banking sector in the context of cybersecurity?
- What could be the barriers to implementing coopetition in the banking sector in the area of cybersecurity?

The phenomenon of coopetition in banking is becoming increasingly important, especially in the context of growing cyber risk and regulatory requirements. It is a strategy, that allows banks to operate beyond the boundaries of competition for the common good of the system.

The banking sector, as the foundation of the economy, remains one of the main targets of cybercrime. The growing digitization of services, the processing of sensitive customer data, and the high potential financial and reputational losses make financial institutions particularly vulnerable to attacks such as ransomware or advanced, long-term APT operations. Traditional, isolated protection models based solely on internal technology and human resource investments are becoming insufficient in the face of the scale and complexity of today's threats (Santos et al., 2025; Prasad et al., 2025).

In response to this situation and regulatory pressure (including EU frameworks such as NIS2 and DORA), a model of coopetition (cooperation between competitors) is developing, which in the area of cybersecurity is materializing, among other things, through the sharing of threat intelligence (CTI), the creation of technical standards and procedures, joint exercises/training, and investments in advanced detection and response systems. Such partnerships enable faster threat detection, consolidated responses, and increased resilience of the entire financial system. At the same time, coopetition requires balancing the benefits of synergy against the costs associated with losing competitive advantage and the risk of disclosing sensitive information (Chang, Huang, 2023; Harasim, 2021).

In addition, EU regulations aimed at harmonizing digital resilience requirements, primarily the Digital Operational Resilience Act (DORA) and the updated NIS2 directive, strengthen incentives for cooperation between banks and between banks and supervisory authorities. These regulations not only impose obligations related to ICT risk management and incident reporting, but also encourage the creation of information sharing mechanisms and common supervisory standards. However, the implementation of these regulations also involves practical barriers: supervisory divergences, compliance costs, and legal uncertainties regarding data protection and competition (Buttigieg, Zimmermann, 2024; Singh, 2023).

From an empirical and theoretical perspective, the literature provides evidence that the coopetition model can increase the cyber resilience of the sector by accelerating the exchange of threat intelligence and pooling resources for rapid response. However, research also points to significant barriers: insufficient standardization of CTI formats, lack of trust between entities, and difficulties in determining incident reporting thresholds, which hinder effective cooperation. These problems also point to areas for further research and practical intervention (Santos et al., 2025; Schmitz-Berndt, 2023).

In light of the above, the main objective of the article, to analyze the phenomenon of coopetition in the Polish banking sector as a response to cyber threats and regulations, is justified and necessary. The study aims to determine the causes of this phenomenon, identify key forms of cooperation in the area of cybersecurity, and recognize the barriers and benefits of such cooperation, particularly in the context of legal requirements in force in the EU and Poland (Fuszder et al., 2025; Waizel, 2023).

2. Methods

The methodological approach of this study is based on a qualitative analysis of existing sources and empirical data collected through a survey. The research procedure consisted of two main stages. First, a comprehensive analysis of the subject literature, case studies of cyber incidents in the banking sector, and the applicable legal framework at both the EU and Polish national levels was conducted. This included regulations such as the GDPR, NIS2 Directive, DORA Regulation, the Act on the National Cybersecurity System, the Banking Law, and the Act on Competition and Consumer Protection. This stage allowed for the identification of the theoretical and legal context of coopetition. Subsequently, empirical research was carried out. Initially, interviews were conducted with representatives of seven banks operating in Poland to establish research criteria. Following this, research surveys were distributed to employees of these banks. The study involved 107 respondents working in departments dealing with fraud prevention, cybersecurity, compliance, and IT security engineering.

The survey utilized a 5-point Likert scale for responses. For assessing causes, benefits, and barriers, the scale was: 1 – Completely Insignificant (CI), 2 – Slightly Insignificant (SI), 3 – Neutral (N), 4 – Significant (S), 5 – Very Significant (VS). For assessing the severity of cyberattacks and their consequences, the scale was: 1 – Very Low (VL), 2 – Low (L), 3 – Medium (M), 4 – High (H), 5 – Very High (VH). For assessing the benefits of coopetition, the scale was: 1 – No Benefit (NB), 2 – Slight Benefit (SB), 3 – Moderate Benefit (MB), 4 – Major Benefit (MB), 5 – Very Major Benefit (VMB).

The collected data were analyzed using descriptive statistics, including the calculation of mathematical average (MA) and standard deviations (SD), and the distribution of responses was presented in percentage terms.

3. Literature review

In recent years, the digital transformation of the banking sector has significantly increased the convenience and efficiency of financial transactions. However, this transformation has also contributed to a significant increase in cybersecurity threats that jeopardize the integrity, confidentiality, and availability of banking systems and customer data (Ovewole et al., 2024). Technology plays a key role in various areas of life, especially in the banking sector. The dynamic development of technology has effectively streamlined the functioning of the banking sector and financial services institutions, causing a fundamental change in the way the banking sector operates, which has provided banking institutions with many opportunities to raise and improve the level of services provided to customers (Shehab et al., 2024).

3.1. Cybersecurity in the banking sector

Business objectives related to cybersecurity in banks focus on marketing and sales, as well as services, to ensure secure and trustworthy operations. In terms of marketing and sales, banks strive to update customer information programs with new threats (Tran, 2025). Cybersecurity is a process aimed at protecting computers, servers, networks, and digital data from unauthorized access, destruction, or attack in cyberspace. The goal of businesses and governments in ensuring an adequate level of cybersecurity is not only to protect confidential data, but also to ensure its availability while maintaining its integrity (Al-Alavi, Al-Bassam, 2020). The banking and finance sector faces a triple challenge in cybersecurity, aptly named the cybersecurity triangle. This triangle encompasses three interrelated aspects: high-value targets, complex IT infrastructure, and stringent regulatory requirements. Each of these issues exacerbates the others, creating an exceptionally difficult environment for cybersecurity professionals in the financial sector (Reddem, 2024). Ensuring cyber resilience in banks is one of the greatest challenges of our time due to the continuous development of technologies that create cyber threats. Cybersecurity can be systemic in nature in certain cases. An attack on one institution can have a domino effect and undermine confidence in the entire banking sector. For this reason, banks work together to prevent attacks from spreading, respond quickly to threats, and strengthen the stability of the financial system as a whole. The main reasons for this cooperation are increasingly complex cyber threats and legal regulations.

3.2. Causes of coopetition in the banking sector – cyberattackes

Cyberattacks on the banking sector are currently characterized by a high degree of specialization and continuous evolution. Increasing the level of security requires a comprehensive, multi-layered approach that combines advanced technologies, regular training, cooperation within the sector, and cooperation with law enforcement agencies. Attacks on the banking sector are evolving from simple fraud to sophisticated, advanced persistent threats (APTs) that exploit gaps in technology, processes, and human error.

Advanced persistent threats (APTs) are one of the main cybersecurity issues that have emerged this decade. They can be defined as long-term, sophisticated activities that are covert and remain undetectable for a long time (Hasan et al., 2023). ATP attacks are typically organized by well-funded and organized cybercriminal groups or state actors to gain unauthorized access to sensitive systems. ATP cyberattacks steal sensitive data, maintain a long-term covert presence on the target network, or destroy the system they infect (Nelles et al., 2024). When using APT, attackers employ a variety of tools to ensure that cyberattacks remain undetected within the target network for months or even years (Mat et al., 2024). Attackers search for security vulnerabilities in order to bypass detection systems, and continuously modify their malware to circumvent intrusion detection systems (Krishnapriya, Singh, 2024).

DDoS (Distributed Denial of Service) attacks involve preventing users from accessing an online service, most often through temporary disruptions or suspension of the hosting service. These attacks may be aimed at disrupting the operation of a critical system or interrupting connectivity, resulting in denial of access to services for users of the targeted resources (Tripathi et al., 2020). DDoS attacks are a common form of cyber aggression aimed at disrupting the normal functioning of targeted online services (Merkebaiuly, 2024). The main components of DDoS attack architecture typically include command and control infrastructure, a network of compromised devices (botnets), a traffic generation mechanism, and techniques to amplify the impact on the attacker's resources (Khaund, 2025).

Ransomware is a type of malware that locks down a system, preventing users from accessing the system or specific files. The attacker then demands a ransom in exchange for restoring access. If the victim does not pay the ransom within a specified time frame and amount, the data will be lost (Aggarwal, 2023). The most common vectors for ransomware attacks are phishing, exploiting vulnerabilities in outdated services, or inadequately secured remote access (KNF CSIRT, 2024).

Ransomware-crypto encrypts files and data on the victim's computer or mobile phone. Once installed on the system, this type of software invisibly searches for files and data. Ransomware-locker attacks end-user systems or mobile devices. It can lock the input interface, such as the keyboard and mouse, preventing the user from accessing the device. Master boot record-ransomware encrypts the MBR table, which contains information about the organization of logical partitions containing file systems. Encrypting the MBR table makes it impossible to find files on the hard drive (Hoseini, 2020). With ransomware attacks, perpetrators can affect not only large organizations, but also small and medium-sized entities (Sudheer, 2024).

Living-Off-The-Land (LOTL) – cybercriminals devote a lot of time to trying to deceive and circumvent advanced malware detection algorithms. A particularly interesting method is the use of binary files and tools that are often part of the basic distribution of the operating system (OS). Because this technique uses elements already present in the system, it is called “living off the land” (Boros et al., 2022). Despite the widespread availability of heuristic rule-based detection methods, these systems often fail to detect new or hidden threats, especially those using LOTL techniques. These threats use legitimate software to perform malicious actions, blending in with harmless system behavior (Trizna et al., 2024).

Man-in-the-Browser (MitB) attack aims to intercept data transmitted as part of secure communication between the user and a web application. The Trojan embeds itself in the user's browser and can be programmed to activate when the user accesses specific websites, such as online banking sites. Once activated, the MitB Trojan can intercept and manipulate information sent by the user in real time (Ayyagari, 2017). Man-in-the-Browser malware is based on browser extensions, which are a target for attack because browser extensions have access to sensitive data such as usernames and passwords (Tong, Nwokeji, 2023).

An attack on SWIFT refers to deliberate, malicious activities aimed at stealing money or disrupting operations by compromising the SWIFT (Society for Worldwide Interbank Financial Telecommunication) system. Criminals have carried out a series of successful cyberattacks on the global banking system through this system. One of the most notorious attacks was a fake transfer of $81 million from the central bank of Bangladesh in February 2016. The hackers introduced malware into the bank's server to steal login details for the SWIFT communication system. They then successfully covered up the traces of their infiltration by removing evidence from printed SWIFT messages in real time (Liu, 2021).

Digital skimming is a type of cyberattack in which criminals install malicious code (usually a so-called skimmer) on a store's website or other platform in order to steal users' payment or personal data. Europol defines digital skimming as "the act of stealing credit card or payment card information from online store customers. Transaction data is intercepted during the online purchase process, and customers do not notice anything unusual. Digital skimming attacks are also known as internet skimming, online card skimming, e-skimming, formjacking, or magecart" (EUROPOL, 2024). Skimming is not limited to physical, man-made devices. This crime can also be software-based. Silent skimmers are threats, that infiltrate payment systems and steal payment information using Python (Ciaccio, Onat, 2025).

A key threat to banks, though not necessarily technical, is phishing attempts that aim to obtain usernames, passwords, and credit card details in the banking sector. Phishing involves impersonating a credible website and making official-sounding statements. Phishing attacks take various forms that deceive victims: emails, phone calls, website impersonation, and social media posts (Yuspin et al., 2024). Phishing and social engineering are the two most popular attack vectors. Phishing attacks targeting specific customers account for the largest share of these attacks. In most cases, customers themselves are contacted by hackers to verify information about their bank accounts. Bank employees have also become targets of these attacks, especially after the increase in remote working during the pandemic (Khemka, 2024).

Cyberattacks are currently one of the most serious challenges facing the financial sector. Although their direct effects (such as financial losses or data loss) are obvious, they have a profound and multidimensional impact on the very nature of competition between banks. Instead of supporting innovative competition, cyber threats can stifle and distort it. Attacks in cyberspace can therefore influence cooperation between banks despite their simultaneous competition in the sector.

3.3. Causes of coopetition in the banking sector – UE regulations

The GDPR (Regulation 2016/679) imposes an obligation to ensure the security of personal data processing (Article 32). This encourages banks to cooperate on best practices. At the same time, provisions on consent, confidentiality, and the legitimacy of processing can complicate the free exchange of information about incidents, especially if they contain personal data. In many cases, personal data is a vector for cybercriminals, as it can be used at a later time to

prepare/commit further/other crimes (Official Journal of the UE, 2016). The NIS2 Directive, transposed in Poland in 2024 (Official Journal of the UE, 2022), includes financial sector participants in the scope of "important" and "key" entities. It obliges them to implement risk management measures and report significant incidents to the competent authorities (CSIRT MON, CSIRT NASK). This directly creates an environment for coopetition between the sector and the regulator. It is worth adding here, in the context of key cyber threats, that Article 21(3) of the NIS2 Directive defines a serious computer security incident as an incident, that (Kapica, Rosiak, 2024):

- has caused or may cause severe operational disruption of services or financial losses for the entity concerned,
- has affected or is capable of affecting other natural or legal persons, causing significant material and non-material damage.

The DORA, Digital Operational Resilience Act (EU, 2022), regulation, as a key act in considering the implementation of a coopetition model in the banking sector, encourages the creation and participation in the sharing of information on cyber threats. It establishes a legal framework for such activities, aimed at overcoming legal concerns related to competition and data protection regulations. It also mandates regular resilience testing, which naturally evolves into joint interbank training.

3.4. Causes of coopetition in the banking sector – national legal regulations

The Act of July 5, 2018 (Act of a National Cybersecurity System, 2018), on the national cybersecurity system is a key piece of legislation implementing the EU NIS Directive into Polish law. Its main objective is to increase the level of digital security in the country, and the banking sector, as part of critical infrastructure, is subject to its particular rigor. Banks are required to implement technical and organizational security measures adequate to the identified risks. These measures must ensure the security of the data processed and the services offered. The purpose of the Polish Financial Supervision Authority's supervision of the financial market is to ensure the proper functioning of this market, its stability, security, and transparency, trust in the financial market, as well as to protect the interests of market participants, including through the provision of reliable information on the functioning of the market (Financial Supervision Authority, 2006). The Financial Market Supervision determined the organization, scope, and purpose of the KNF's activities. The Polish Financial Supervision Authority (KNF) plays a key role in the area of cybersecurity for banks operating in Poland, acting as a regulator, supervisor, and coordinator.

It is worth mentioning that, in addition to national regulations, the National Bank of Poland plays an important role as the central bank (bank of banks), which "performs regulatory functions in relation to banks, aimed at ensuring the security of deposits held in banks and the stability of the banking sector. It organizes the cash settlement system, conducts ongoing interbank settlements, and actively participates in the interbank money market. The National

Bank of Poland is responsible for the stability and security of the entire banking system, acts as the bank of banks, and supervises payment systems in Poland" (National Bank of Poland). The central bank is responsible, among other things, for macroprudential supervision to ensure the stability of the financial system or its key elements. This supervision is related to the activities of the Financial Stability Committee, which is a body operated by the National Bank of Poland and an office serving the Minister of Finance (Dmowska, 2022).

3.5. Legal regulations that may constitute barriers to the coopetition development

GDPR Regulation (EU) 2016/679: While Article 32 imposes an obligation to ensure data security, the principles of data minimization and purpose limitation can be interpreted as a barrier to the free sharing of incident details that may contain personal data. This requires the use of anonymization and aggregation techniques. With regard to the increasingly common use of ZTA (Zero Trust Architecture) in financial institutions, which is guided by the principle of "never trust, always verify" (Ramakrishna, 2025) and requires continuous verification of every user, device, and transaction, this type of approach may constitute a limitation in the context of cooperation with other banks.

Articles 104-105 of the Banking Law Act of August 29, 1997 refer to aspects related to banking secrecy. Violating it during the process of sharing information about an attack (which could reveal customer data) may result in criminal liability. This is the most serious legal barrier, which is overcome by strictly defining the scope of the information shared (only attack metadata, without sensitive data). Banking secrecy is not an obstacle to cooperation with supervisory/law enforcement authorities (KNF, KAS, Prosecutor's Office, Police) or in the context of reporting obligations. However, voluntary exchange with other commercial banks (i.e., competitors) requires a very cautious approach and often relies on general clauses of "statutory authorization" or "customer consent," which are difficult to apply in practice.

With reference to the Act on Competition and Consumer Protection of February 16, 2007, uncontrolled cooperation between competitors, including banks, may raise concerns about bid rigging or the exchange of commercial information. Therefore, coopetition should be limited solely to security issues. The Act prohibits agreements that restrict competition. Close cooperation between competing banks, even in the area of cybersecurity, may raise suspicions on the part of the antitrust authority (UOKiK) that it is a front for illegal agreements in other areas (e.g., pricing, market). The exchange of overly detailed information on the costs of implemented security measures, planned investments, or internal procedures may be considered an exchange of sensitive information from a competition perspective.

3.6. Coopetition in the Polish banking sector in the context of cybersecurity

The concept of coopetition represents the dichotomy between competition and cooperation. Cooperative and competitive forces are fundamental components of business in this regard. The challenge associated with implementing coopetition is the exchange of information and

sharing of knowledge, which allows a company to assimilate its competitor's know-how (Kobiyh et al., 2025). Coopetition can be considered a key strategy in developing economies. Innovative activities related to research and development involve many risks and costs, and the coopetition strategy is one of the key factors that can be used in this situation (Salamzadeh et al., 2024).

In turn, coopetition in the banking sector in the context of cybersecurity consists of voluntary, formalized cooperation between banks to exchange information about threats (Threat Intelligence), best practices (implementation of data anonymization requirements), and anomalies detected on the basis of network traffic. Banks operating in Poland cooperate through the Polish Bank Association (ZBP), using joint response and coordination centers, through the Cybersecurity Threat Information Exchange Forum coordinated by the ZBP, or within the framework of international cooperation in European and global initiatives.

The Polish Bank Association is the main platform for cooperation within the Polish banking sector. In response to cybersecurity threats and incidents, as well as the needs of banks, on November 29, 2016, the Council of the Polish Bank Association, together with banks, established the ZBP Banking Cybersecurity Committee. FinCERT.pl operates within the Committee as an operational unit that collects, analyzes and transmits information on identified threats and criminal incidents within the banking sector, among others (The Polish Bank Association). Cooperation through the ZBP may include:

- threat intelligence sharing,
- developing standards and recommendations for electronic banking,
- organizing joint training courses on cyberattack simulation,
- representing the sector's interests before the regulator (KNF) and legislators.

Cyber Threat Intelligence (CTI) involves gathering and analyzing threat intelligence to support decision-making and help organizations respond effectively (Fieblinger, 2024). CTI is an integral part of the cybersecurity assurance process. Development in this area means responding to the ever-increasing sophistication of adversaries and helping to include new elements of cyber threats in the analysis process (Baraniuk, Marszałek, 2024). In the banking sector, CTI in the coopetition model is a strategic collaboration in which, instead of acting in isolation, banks strengthen their common defense against evolving cyber threats.

In the Polish banking sector, banks compete with each other for customers and market share, but at the same time they cooperate in the area of cybersecurity, because a common threat (cyberattacks) poses a systemic risk to the entire sector. The success of one bank in defense depends on the security of the entire ecosystem. The KNF CSIRT team, performing the tasks of the Sectoral Cybersecurity Team, in cooperation with entities of the national cybersecurity system, in particular national CSIRT teams, supports Key Service Operators in handling serious incidents and conducts activities aimed at analyzing other incidents (Financial Supervision Authority, 2006), blocking fraudulent domains of a fraudulent nature, and analyzing malware in the context of financial security (Mroczka, Groniewski, 2025).

The Banking Security Centers of the Polish Bank Association are specialized units whose purpose is to strengthen the resilience of the Polish banking sector to cyber threats through coordination, analysis, and response to incidents. In a report by ENISA (European Union Agency for Cybersecurity) dated February 14, 2018, FinCERT.pl, the Banking Cybersecurity Center of the Polish Bank Association, was recognized as the ISAC (Information Sharing and Analysis Center) of the Polish banking sector (Polish Bank Association).

The European Financial Information Sharing and Analysis Centre (EU-FI-ISAC) functions as a platform for the exchange of information between financial institutions operating within the European Union. European FI-ISAC is an independent organization supported by ENISA (European Union Agency for Cybersecurity). FI-ISAC's mission is to exchange information on electronic and mobile channels, cards, central systems, and all ICT-related issues, including (European FI-ISAC):

- cybercrime affecting the financial community,
- vulnerabilities, technology trends, and threats,
- incidents, and case studies.

The European Cybercrime Center (EC3) was established by Europol to strengthen law enforcement efforts in combating cybercrime, thereby protecting European citizens, businesses, and governments from online crime. Since its establishment in 2013, EC3 has contributed significantly to the fight against cybercrime and has participated in numerous high-profile operations (EUROPOL Cybercrime Centre).

The Basel Committee on Banking Supervision (BCBS) is the body that sets global standards for prudential regulation of the banking sector and provides a forum for regular cooperation on supervisory matters. Its 45 members are central banks and banking supervisory authorities from 28 jurisdictions. The BCBS's main objective is to enhance the stability and resilience of the global financial system and to ensure that no bank can escape supervision by operating solely within the borders of a single country (The Basel Committee).

The European Union Agency for Cybersecurity (ENISA) is responsible for ensuring a high and effective level of security in networks and information systems in the European Union. ENISA's task is to ensure a uniform level of cybersecurity across Europe. ENISA participates in the implementation of EU policy in the field of cybersecurity. It builds trust in digital products and services by designing cybersecurity certification systems (Enisa).

Cooperation between banks in the Polish banking sector manifests itself in various types/forms of coopetition, examples of which are as follows:

- Network-based.
- Formal.
- Informal.
- Indirect.
- Direct.

The sectoral threat information sharing centers (FS-ISAC) that have been established can be regarded as a model of formal network coopetition. Banks that are members of FS-ISAC anonymously share data on incidents, indicators of compromise (IOCs), and best practices in near real time. Another example is joint cyberattack simulation platforms, where teams from competing banks jointly train to respond to a coordinated attack on critical infrastructure. Informal coopetition can be ad hoc and based on telephone/email alerts about a newly observed threat, or meetings where valuable insights are exchanged.

In indirect coopetition, the regulator (e.g., the Financial Supervision Authority, the European Banking Authority, or national authorities) acts as a catalyst and oversees cooperation. The regulator not only imposes legal obligations on banks in the area of cybersecurity (NIS2 directive, EBA standards), but also often creates platforms for the exchange of information. Direct coopetition is a grassroots initiative by banks themselves, undertaken without direct regulatory coercion. It stems from purely business-based risk calculations. Banks themselves decide on bilateral or multilateral data exchange, joint purchases of security services from external providers, or the creation of common industry standards that go beyond minimum legal requirements. No single model of coopetition is optimal in all situations. An effective defense ecosystem requires their parallel use. Regulator-supervised coopetition is essential to ensure a basic, uniform level of security across the sector. Direct and informal coopetition is the driving force behind advanced, innovative forms of cooperation, allowing for immediate response once a threat has been identified.

4. Results

In order to obtain answers to the research questions, interviews were first conducted with representatives of seven banks operating in Poland to establish the research criteria, and then responses to previously prepared research questionnaires were obtained from the employees of these banks. The respondents were 107 people working in departments dealing with fraud prevention, cybersecurity, compliance, and IT security engineering. The survey used a 5-point Likert scale with the following options: 1 – Completely irrelevant (CR), 2 – Not very relevant (NR), 3 – Neutral (N), 4 – Relevant (R), 5 – Very relevant (VR). Table 1 presents the reasons for banks to cooperate in the area of cybersecurity.

Cyber threats are perceived as the most important drivers of coopetition, while regulatory pressure is also very important, but to a slightly lesser extent. During the interviews, it was established that respondents perceived the following issues, among others, as other reasons: reduction of operating costs, joint investments in technology development, and response to changing customer expectations.

Table 1.
Causes for cooperation in the Polish banking sector

Causes	AM	SD	CR	NR	N	R	VR
Cyberattacks on the banking sector	4.63	0.59	0%	2%	3%	29%	67%
EU legal regulations	4.53	0.80	2%	2%	3%	28%	65%
Overall growth in cyberattacks	4.46	0.91	3%	3%	4%	27%	63%
National legal regulations	3.84	1.21	4%	13%	20%	22%	41%
Pressure from fintech companies	3.71	1.24	8%	8%	22%	28%	34%
Other	3.17	1.09	10%	23%	26%	36%	5%

AM – Arithmetic Mean, SD – Standard deviation, CR – Completely irrelevant, NR – Not very relevant, N – Neutral, R – Relevant, VR – Very relevant.

Source: Own work based on a survey questionnaire.

Undoubtedly, the most important reasons for cooperation between banks are cyber threats, especially those directed specifically at the banking sector. Average ratings indicate a very high, shared perception of risk. EU regulations are seen as a significantly stronger incentive than national regulations. Directives such as PSD2, which enforce data sharing, themselves create the groundwork for coopetition. Pressure from fintechs is proving to be a significant, though not the most important, factor influencing the adoption of coopetition.

Table 2 presents the survey results in the context of answering the question of which cyberattacks pose the greatest threat to the banking sector. The survey used a 5-point Likert scale with the following options: 1 – Very low (VL), 2 – Low (L), 3 – Medium (M), 4 – High (H), 5 – Very high (VH). Phishing, APT, and ransomware are the most serious threats, as evidenced by the highest averages (above 4.4). The low standard deviation for phishing and APT indicates that respondents agree on the severity of these attacks. Attacks on SWIFT are also rated as very high risk, reflecting the strategic importance of this system.

Table 2.
The degree of threat posed by the indicated types of cyberattacks to the banking sector

Cyberattacks types	AM	SD	VL	L	M	H	VH
Phishing	4.65	0.69	0%	2%	6%	16%	76%
Advanced Persistent Threats (APTs)	4.52	0.78	0%	3%	9%	21%	67%
Ransomware	4.43	0.86	0%	4%	13%	20%	63%
Attacks on SWIFT	4.15	1.11	2%	10%	13%	21%	54%
DDoS	3.92	1.29	5%	14%	17%	14%	54%
Attacks on cloud computing	3.75	1.17	7%	12%	8%	46%	27%
Man in the Browser	3.64	1.22	5%	20%	11%	35%	29%
Digital skimming	3.22	1.26	9%	22%	27%	21%	21%
Living off the Land (LOTL)	3.05	1.17	7%	29%	29%	21%	14%
Other	2.45	1.07	21%	32%	30%	14%	3%

AM – Arithmetic Mean, SD – Standard deviation, VL – Very low, L – Low, M – Medium, H – High, VH – Very High.

Source: Own work based on a survey questionnaire.

Figure 1 shows the distribution of responses regarding the threat of phishing (average = 4.65). Banks and financial institutions store vast amounts of customer personal data (social security numbers, account numbers, identification data) and manage large financial flows. This makes them a very attractive target for criminals. Phishing is primarily an attack on

people, through emails, text messages, and impersonating a trusted institution. As bank employees or their customers can be a vector of entry, phishing poses a very high threat, as illustrated by the chart.

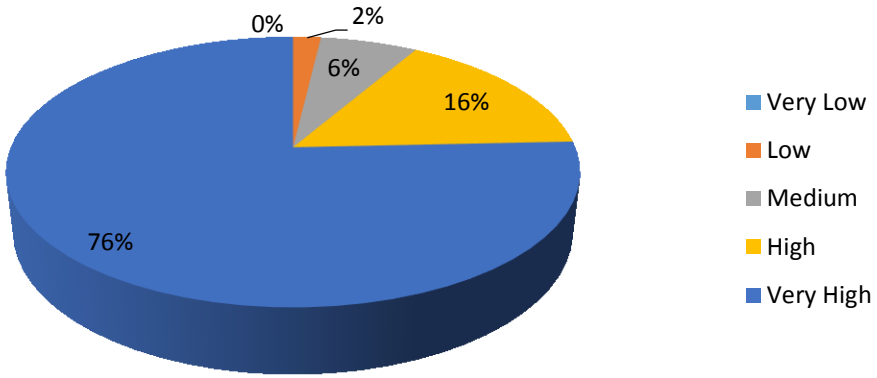

Figure 1. Distribution of responses to a phishing cyberattack.

Source: Own work based on a survey questionnaire.

Table 3 presents the survey results in the context of answers to the question of which effects of cyberattacks are most serious for banks/the banking sector. The survey used a 5-point Likert scale with the following options: 1 – Very low (VL), 2 – Low (L), 3 – Medium (M), 4 – Serious (S), 5 – Critical (C). The most serious threats in the respondents' perception are those that destroy the bank's intangible assets, i.e., customer trust (average 4.74) and reputation, and lead to direct financial and legal consequences (losses, penalties). The results show that modern banks fear not only cyberattacks themselves, but above all their cascading business, legal, and reputational consequences.

Table 3.

The degree of significance of the effects of cyberattacks on the banking sector

Type of cyberattacks impact	AM	SD	VL	L	M	S	C
Loss of customer trust	4.74	0.56	0%	0%	6%	15%	79%
Data leaks	4.62	0.61	0%	0%	7%	25%	68%
Regulatory penalties and fines	4.52	0.78	0%	2%	12%	18%	68%
Financial losses	4.41	0.93	0%	7%	8%	20%	64%
System disruptions	4.34	0.99	0%	9%	9%	20%	62%
Loss of trust in the banking sector	4.10	0.88	0%	7%	14%	42%	37%
Discrediting of trading platforms	4.01	0.79	0%	6%	14%	54%	26%
Bank employee involvement in cyberattacks	3.57	0.74	1%	6%	36%	51%	7%
Acquisition of know-how by perpetrators	3.48	0.71	3%	2%	42%	51%	2%
Other	2.68	0.69	3%	36%	50%	10%	0%

AM – Arithmetic Mean, SD – Standard deviation, VL – Very low, L – Low, M – Medium, S - Serious, C – Critical.

Source: Own work based on a survey questionnaire.

Table 4 presents the results of the survey in the context of answering the question of what benefits may result from co-opetition between banks in response to cyberattacks. The survey used a 5-point Likert scale, with the following options: 1 – No benefit (NB), 2 – Minor benefit (MnB), 3 – Moderate benefit (MdB), 4 – Major benefit (MjB), 5 – Very major benefit (VMB). By sharing data on new attack vectors or detected incidents, banks can respond much more

quickly to emerging risks. This prevents a single attack from escalating into a mass attack affecting multiple institutions simultaneously. Cooperation enables the creation of consistent and up-to-date standards for technical solutions, security policies, identity management, and incident response processes. Standardization raises the average level of protection in the industry. When every institution has access to the most up-to-date threat data and applies best practices, consumers gain a truly safer environment for using financial services. The risk of identity theft or loss of funds is also reduced. Shared analytical systems and the exchange of warning signals allow for faster identification of unusual events and counteraction to their effects.

Table 4.
The benefits of coopetition among banks in the context of cybersecurity

Benefits	AM	SD	NB	MnB	MdB	MjB	VMB
Faster exchange of information about threats	4.61	0.79	0%	4%	7%	13%	76%
Joint development of standards	4.44	0.87	0%	5%	11%	20%	64%
Increased customer protection	4.33	0.93	0%	5%	18%	18%	60%
More efficient detection of anomalies	4.21	0.95	0%	11%	3%	40%	46%
Limiting the impact of cyberattacks	4.12	1.00	0%	11%	10%	34%	45%
Reducing serious incidents	4.02	1.04	0%	13%	13%	33%	41%
Joint incident simulations	3.85	1.07	2%	16%	7%	47%	29%
Increasing operational resilience	3.70	1.06	3%	10%	27%	34%	26%
Technological improvement	3.53	1.01	3%	12%	32%	36%	18%
Cost reduction	3.47	0.96	5%	8%	34%	42%	11%
Increasing the costs for cybercriminals	3.43	0.93	5%	9%	32%	47%	7%
Regulatory lobbying	3.37	0.86	4%	11%	32%	50%	3%
Other	3.04	0.78	7%	8%	60%	25%	0%

AM – Arithmetic Mean, SD – Standard deviation, NB – No benefit, MnB – Minor benefit, MdB – Moderate benefit, MjB – Major benefit, VMB – Very major benefit.

Source: Own work based on a survey questionnaire.

The survey clearly shows that the banking sector sees very specific, tactical benefits from coopetition in the area of cybersecurity. The most highly valued activities are those that directly translate into rapid response times and common standards. Cost and political (lobbying) aspects are considered important, but less crucial for direct defense against cyberattacks. Figure 2 illustrates the distribution of responses for the most highly rated benefit (average = 4.61) resulting from bank coopetition. While joint initiatives obviously allow for cost reductions through economies of scale, and a coordinated industry voice has greater leverage with regulators, operational effectiveness remains the priority in the context of immediate threats. In the face of increasingly sophisticated cybercriminals, a common line of defense is proving to be a necessity, not just an option.

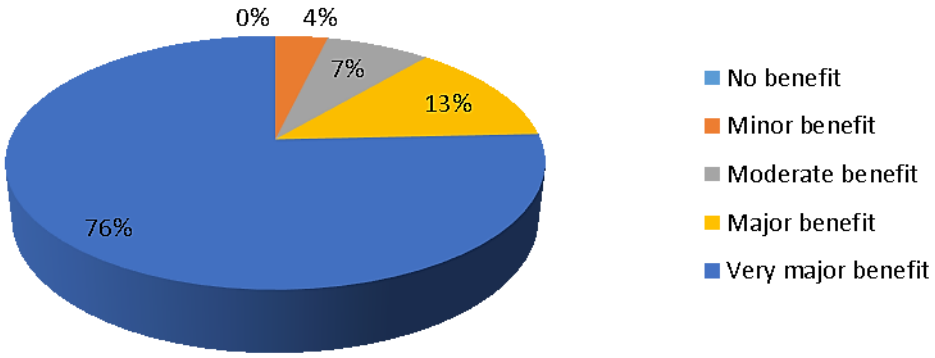

Figure 2. Distribution of responses for the benefit of faster information exchange.

Source: Own work based on a survey questionnaire.

Table 5 presents the results of the survey in the context of answering the question of what barriers may arise from co-opetition between banks in response to cyberattacks. The survey used a 5-point Likert scale, with the following options: 1 – Completely irrelevant (CR), 2 – Not very relevant (NR), 3 – Neutral (N), 4 – Relevant (R), 5 – Very relevant (VR).

Table 5.
Barriers to cooperation in the Polish banking sector

Barriers	AM	SD	CR	NR	N	R	VR
Risk of confidential data leaks	4.67	0.79	0%	4%	7%	13%	76%
Lack of trust in other banks	4.54	0.87	0%	5%	11%	20%	64%
Fear of losing competitive advantage	4.25	0.93	0%	5%	18%	18%	60%
Legal and compliance issues (GDPR)	4.12	0.95	0%	11%	3%	40%	46%
Different levels of security maturity	4.07	1.00	0%	11%	10%	34%	45%
Risk of intellectual property theft	3.91	1.04	0%	13%	13%	33%	41%
Coordination costs	3.44	1.07	2%	16%	7%	47%	29%
Technical complexity of integration	3.22	1.06	3%	10%	27%	34%	26%
Culture of competition between banks	3.11	1.01	3%	12%	32%	36%	18%
Other	2.88	0.96	5%	8%	34%	42%	11%

AM – Arithmetic Mean, SD – Standard deviation, CR – Completely irrelevant, NR – Not very relevant, N – Neutral, R – Relevant, VR – Very relevant.

Source: Own work based on a survey questionnaire.

The two key barriers are the risk of confidential data leaks (average = 4.67) and lack of trust in other banks (average = 4.54). These are clearly more important than the others. For coopetition to be possible, it is necessary to develop extraordinary mechanisms for data protection and confidentiality, and to build trust. Another set of barriers is related to competitiveness: fear of losing advantage and the risk of intellectual property being taken over, which are linked to limited trust in competitors. Legal issues (GDPR) and varying levels of security maturity are seen as important, but not as crippling as issues of mutual trust. This points to areas where the development of standards and models of cooperation could bring quick benefits. Respondents also pointed to the technical complexity of integration and the culture of competition as significant obstacles. This confirms the assumption that, apart from technology, the human and cultural aspects may prove to be the greatest challenge in relation to the coopetition of banks.

5. Discussion

The present study provides empirical and theoretical evidence that coopetition among banks is not only a viable but increasingly necessary strategy in responding to the growing cyber-risk landscape. The findings corroborate and extend prior scholarship on financial-sector cooperation, regulatory influence, and cyber resilience.

5.1. The strategic role of coopetition in cyber-resilience

The survey reveals, that cyberattacks, particularly phishing, APTs, and ransomware, are perceived by banking-sector professionals as the most significant drivers of coopetitive behavior (Tables 1-2). This aligns with the conceptualization of cyber risk as a systemic threat: not merely an operational issue, but one that can cascade across institutions. Recent work has framed cyber risk in banks as a form of systemic risk, due to interconnections and shared infrastructures (Birindelli, Iannuzzi, 2024). By cooperating, especially via threat-intelligence sharing, banks effectively internalize some of the externalities associated with cyber risk, benefiting from collective vigilance.

Moreover, the finding, that threat intelligence exchange is the top-rated benefit (mean = 4.61) underscores the strategic value of Information Sharing and Analysis Centers (ISACs). This is consistent with literature on CTI (cyber threat intelligence) ecosystems: sharing platforms foster knowledge advantages by improving detection and response capabilities across participants (Abraham et al., 2025). For instance, Sayeed et al. (2024) argue, that resource sharing, underpinned by institutional and protection motivation theories, strengthens long-term security outcomes in the financial sector.

5.2. Regulatory drivers and contraints

Regulatory incentives emerged strongly in our data: EU regulation (e.g., DORA, NIS2) scores nearly as high as cyber-risk itself. The importance of regulation in fostering coopetition echoes findings from the U.S. financial sector: Atkins and Lawson (2021) show that regulatory pressure and trust networks have been key in enabling public–private cyber collaboration. However, legal and compliance barriers, particularly concerns about GDPR and banking secrecy, remain major obstacles (Table 5). This tension between cooperation and confidentiality reflects broader challenges in coopetition theory: competing firms must balance mutual dependence with competitive safeguards. The literature on coopetition management highlights precisely these relational tensions (asymmetry, trust, paradoxicality) as critical features to operationalize (Tagscherer, Carbon, 2024). In the context, the design of intelligence-sharing frameworks must therefore emphasize strict data governance (e.g., anonymization, metadata-only sharing) and legal safeguards to maintain confidentiality while enabling collaboration.

5.3. Trust, culture and institutional maturity

Respondents identified lack of trust and the risk of confidential data leaks as among the most significant barriers, more so than technical integration or coordination costs. This underscores, that coopetition is not merely a technological problem, but fundamentally a social and organizational one. The success of CTI ecosystems therefore depends on trust-building mechanisms, reputation, and institutional maturity.

This finding echoes broader financial-sector coopetition scholarship: Marecki and Wójcik-Czerniawska (2023) discuss, how coopetition among banks and non-bank entities is shaped by mutual dependence and regulatory architecture. To build trust, banks may need to formalize coopetitive structures (e.g., via sectoral ISACs or joint simulation exercises) rather than rely solely on informal ad hoc arrangements.

6. Summary

This article aimed to analyze the phenomenon of coopetition in the Polish banking sector as a response to cyber threats and legal regulations. The research confirmed the research hypothesis, indicating that cyberattacks and related legal regulations are key catalysts for coopetitive activities among banks. In response to the research questions, it was determined that the most serious types of cyberattacks prompting coopetition include phishing, advanced persistent threats (APTs), ransomware, attacks on the SWIFT system, and DDoS attacks. An analysis of the effects of these attacks showed that the sector's greatest concerns are loss of customer trust, data leaks, and regulatory penalties, which directly motivate joint action.

When it comes to legal regulations, research shows that EU legislation (average: 4.53) is primarily perceived as the main driver of coopetition. At the same time, at the national level, problems with the interpretation and application of the GDPR have been identified as a significant legal barrier hindering the free exchange of information on threats. Clear benefits and barriers to coopetition have also been identified. The most important benefits include faster exchange of information on threats, joint development of security standards, and increased customer protection. The main barriers, on the other hand, are the fear of confidential data leaks, lack of trust between banks, and fear of losing competitive advantage.

In summary, the Polish banking sector recognizes both the urgent need for and the tangible benefits of cooperation in the area of cybersecurity. Nevertheless, the success of coopetitive initiatives depends on overcoming deeply rooted barriers of trust and competition, while adapting the legal framework to support rather than hinder such cooperation. In light of the results obtained, further research in this area could focus on the following areas:

- Research as part of a comparative analysis of the effectiveness of existing coopetitive structures in the banking sectors of other countries in order to develop best practices for Poland.
- Detailed analysis of the impact of individual legal acts (e.g., NIS2, DORA directives) on the dynamics of competitive cooperation, taking into account implementation costs and long-term effects.
- Monitoring how the emergence of new types of cyber threats (e.g., related to artificial intelligence or quantum technology) affects banks' readiness for deeper cooperation.

When applying the phased model of coopetition implementation in the field of cybersecurity, it is worth considering three implementation stages. Phase 1: Foundational trust-building and limited information sharing (Short-Term: 0-12 months). Objective: Establish basic cooperation protocols and build initial trust through low-risk, high-impact activities. Key activities/actions:

- Structured metadata exchange: Implement a standardized format for sharing anonymized, technical Indicators of Compromise (IOCs), such as malicious IP addresses, file hashes, and domain names, through the existing ZBP FinCERT.pl platform. This minimizes legal and data privacy risks.
- Joint threat landscape analysis: Conduct regular, facilitated workshops where banks can discuss general threat trends and attack methodologies without disclosing sensitive internal data.
- Development of a common governance framework: Create a clear charter for cooperation, defining roles, responsibilities, data handling procedures, and rules of engagement to address fears of losing competitive advantage.

Phase 2: Standardization and operational collaboration (Medium-term: 12-24 months). Objective: Deepen cooperation by aligning technical and procedural standards and initiating joint operational exercises. Key activities/actions:

- Gradual standardization: Jointly develop and adopt common technical standards for security controls, incident response playbooks, and data anonymization techniques, building on the initial exchange protocols from Phase 1.
- Periodic joint table-top simulations: Organize regular, scenario-based exercises simulating coordinated cyberattacks (e.g., on the SWIFT system or critical national infrastructure). These simulations train joint response capabilities and strengthen interpersonal trust among security teams.
- Establishment of a shared knowledge base: create a centralized, secure repository for best practices, vulnerability assessments, and non-attributable incident reports, accessible to all participating banks.

Phase 3: Advanced integration and proactive defense (Long-term: 24+ months). Objective: Achieve a mature coopetition ecosystem capable of proactive, collective defense. Key activities/actions:

- Collaborative threat hunting: Form joint analyst teams to proactively hunt for threats across participating banks' ecosystems, leveraging shared intelligence and analytics.
- Joint investment in advanced technologies: Explore consortium-based purchasing or co-development of advanced cybersecurity solutions, such as shared Security Operations Center (SOC) capabilities or AI-powered threat detection platforms, to reduce costs and increase capability.
- Unified regulatory engagement: Present a coordinated, sector-wide position to regulators (KNF, UOKiK) and legislators on cybersecurity policy, leveraging the collective experience from Phases 1 and 2 to shape a more supportive legal environment.

In conclusion, the Polish banking sector recognizes both the urgent necessity and the tangible advantages of coopetition in bolstering its cyber resilience. The benefits, ranging from accelerated threat intelligence sharing and the joint development of security standards to enhanced customer protection, are clearly perceived as vital for navigating the contemporary threat landscape. Nevertheless, the full potential of this strategic approach remains contingent upon the sector's ability to overcome deeply ingrained barriers of trust and competition.

This requires not only internal cultural shifts but also an adaptive legal framework that can support secure information sharing without compromising confidentiality or compliance. For future research, a comparative analysis of coopetitive models in other national banking sectors, a detailed investigation into the implementation dynamics of specific regulations like NIS2 and DORA, and ongoing monitoring of how emerging technologies such as AI and quantum computing reshape the threat landscape and, consequently, the impetus for cooperation, are identified as promising avenues to further develop best practices and theoretical understanding.

References

1. Abraham C. et al. (2025). Promoting research on cyber threat intelligence sharing in ecosystems. *Journal of Cybersecurity, Vol. 11, Iss. 1,* pp. 1-11.
2. Act on Competition and Consumer Protection (2007). *Journal of Laws of 2025*. Retrieved from: https://isap.sejm.gov.pl/isap.nsf, 22.08.2025.
3. Act on the National Cybersecurity System (2018). *Journal of Laws of 2024*. Retrieved from: https://isap.sejm.gov.pl/isap.nsf, 22.08.2025.
4. Aggarwal, M. (2023). *Ransomware attack: an evolving targeted threat*. 14th International Conference on Computing Communication and Networking Technologies (ICCCNT).

5. Al-Alawi, A.I., Al-Bassam, S.A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University, Vol. 14, Iss. 7*, pp. 1523-1536.
6. Atkins, S., Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity, Vol. 7, Iss. 1*, pp. 1-11.
7. Ayyagari, K.S.A. (2017). *Man in a browser attack. Culminating Projects in Information Assurance.* St. Cloud University. Retrieved from: https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1054&context=msia_etds, 22.08.2025.
8. Banking Law Act (1997). *Journal of Laws of 2025.* Retrieved from: https://isap.sejm.gov.pl/isap.nsf, 07.09.2025.
9. Baraniuk, K., Marszałek, P. (2024). Możliwości wykorzystania modeli analitycznych Cyber Threat Intelligence w badaniach operacji informacyjnych i operacji wpływu. *Przegląd Bezpieczeństwa Wewnętrznego, No. 31*, pp. 13-55.
10. Birindelli, G., Iannuzzi, A.P. (2024). *The systematic importance of cyber risk in banks*. New Economic Windows, Springer, pp. 301-321.
11. Boros, T. et al. (2022). *Machine learning and feature engineering for detecting living off the land attacks.* 7th International Conference on Internet of Things, Big Data and Security. Retrieved from: https://www.scitepress.org/Papers/2022/110045/110045.pdf, 07.09.2025.
12. Buttigieg, C.P., Zimmermann, B.B. (2024). The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision. *ERA Forum, Vol. 25*, pp. 11-28.
13. Chang, K., Huang, H. (2023), Exploring the management of multi-sectoral cybersecurity information-sharing networks. *Government Information Quarterly, Vol. 40, Iss. 4*, pp. 1-14.
14. Ciaccio, J., Onat, I. (2025). An analysis of ATM and Point-of-Sale Skimming. *Orion Forum, Cybersecurity & Info Technologies*.
15. Dmowska, K. (2022), Cyberbezpieczeństwo systemu płatniczego w nadzorze systemowym Narodowego Banku Polskiego. *Bank i Kredyt, Vol. 53, Iss. 4*, pp. 357-374.
16. ENISA. Retrieved from: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_pl, 19.09.2025.
17. EU (2022). *Digital Operational Resilience Act*. Retrieved from: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng, 07.09.2025.
18. European FI-ISAC. Retrieved from: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/information-sharing-and-analysis-centers-isacs/european-fi-isac?utm_source=chatgpt.com#contentList, 19.09.2025.
19. EUROPOL (2024). *European Union Agency for Law Enforcement Cooperation*. Retrieved from: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/digital-skimming:pl, 24.09.2025.

20. EUROPOL Cybercrime Centre. Retrieved from: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, 19.09.2025.
21. Fieblinger, R. et al. (2024). *Actionable cyber threat intelligence using knowledge graphs and large language models*. IEEE European Symposium on Security and Privacy Workshops, pp. 100-111.
22. Financial Market Supervision (2006). Journal of Laws of 2025. Retrieved from: https://isap.sejm.gov.pl/isap.nsf, 24.08.2025.
23. Financial Supervision Authority (2006). Retrieved from: https://www.knf.gov.pl/dla_konsumenta/Ochrona_klienta_na_rynku_uslug_finansowych/KNF, 24.08.2025.
24. Fuszder, Md. H.R. et al. (2025). *Cybersecurity risk and bank competition*. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5374980, 24.11.2025.
25. Harasim, J. (2021). FinTechs, BigTechs and Banks – When cooperation and when competition? *Journal of Risk and Financial Management, Vol. 14, Iss. 12*, pp. 1-16.
26. Hasan, Md. M. et al. (2023). Advanced persistent threat identification with boosting and explainable AI. *SN Computer Science, Vol. 4, Iss. 271*, pp. 1-9.
27. Hoseini, A. (2020). *Ransomware and phishing cyberattacks: analyzing the public's perception of these attacks in Sweden*. Uppsala Universitet, Department of Information Technology. Retrieved from: https://uu.diva-portal.org/smash/get/diva2:1678538/FULLTEXT01.pdf, 03.09.2025.
28. Kapica, W., Rosiak, N. (2024), Dyrektywa NIS2: nowe standardy bezpieczeństwa w erze cyfrowej. In: A. Jarmuszkiewicz (Ed.), *Wyzwania transformacji cyfrowej i cyberbezpieczeństwa. Głos Banków Spółdzielczych, No. 4*. Retrieved from: https://kzbs.pl/files/60032/GBS_04_2024_final.pdf, 07.09.2025.
29. Khaund, B. (2025). The Evolution of Denial-of-Service Attacks: From DoS to DDoS - Mechanisms, Impacts, and Defensive Strategies. *European Journal of Computer Science and Information Technology, Vol. 13, Iss. 47*, pp. 134-146.
30. Khemka, A. (2024). The impact of cyber attacks on financial institutions and the need for improved security measures, *International Journal of Novel Research and Development, Vol. 9, Iss. 10*, pp. 864-870.
31. KNF CSIRT (2024). *Best practices for preventing and responding to ransomware attacks*. Retrieved from: www.knf.gov.pl/knf/en/komponenty/img/, 04.09.2025.
32. Kobiyh, M. et al. (2025). Relational perspective of coopetition, cooperative efforts and effects on firm performance. *Business Ethics and Leadership, Vol. 9, Iss. 3,* pp. 130-144.
33. Krishnapriya, S., Singh, S. (2024). A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques. *Computers, Materials and Continua, Vol. 80, Iss. 2,* pp. 2675-2719.
34. Liu, X.M. (2021). A risk-based approach to cybersecurity: a case study of financial messaging networks data breaches. *The Coastal Business Journal, Vol. 18, Iss. 1,* pp. 21-38.

35. Marecki, Ł., Wójcik-Czerniawska, A. (2024). Coexistence, cooperation, and competition between banks and non-banking entities. *Journal of Management and Financial Sciences, Vol. 16, Iss. 48*, pp. 9-21.
36. Mat, N.I.C. et al. (2024). A systematic literature review on advanced persistent threat behaviors and its detection strategy. *Journal of Cybersecurity, Vol. 10, Iss. 1*, pp. 1-18.
37. Merkebaiuly, M. (2024). Overview of distributed denial of service (DDoS) attack types and mitigation methods. *Information and Web Technologies, No. 193*, pp. 494-508.
38. Mroczka, K., Groniewski, M. (2025), Krajobraz cyberbezpieczeństwa rynku finansowego w Polsce a poziom edukacji finansowej – perspektywa organu nadzoru nad rynkiem finansowym oraz jego interesariuszy. *Studia Politologiczne, Studia i Analizy, Vol. 77, Iss. 359,* pp. 324-359.
39. National Bank of Poland. Retreived from: https://nbp.pl/o-nbp/funkcje-banku-centralnego/, 24.08.2025.
40. Nelles, F. et al. (2024), A federated learning approach for multi-stage threat analysis in advanced persistent threat campaigns. *Computer Science, Cryptography and Security*, pp. 1-12.
41. Official Journal of the European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022, on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Retrieved from: https://eur-lex.europa.eu/legal-content, Chapter IV, 24.08.2025.
42. Official Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Retrieved from: https://eur-lex.europa.eu/legal-content, Article 32, 24.08.2025.
43. Oyewole, A.T. et al. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews, Vol. XXI, Iss. III,* pp. 625-643.
44. Polish Bank Association. Retrieved from: www.zbp.pl/Dla-Bankow/Cyberbezpieczenstwo, 16.09.2025.
45. Prasad, N. et al. (2025). A survey of cyber threat attribution: Challenges, techniques, and future directions. *Computers & Security, Vol. 157*, pp. 1-32.
46. Ramakrishna, R.G. (2025). Implementing zero trust architecture in financial institutaions. *World Journal of Advanced Engineering Technology and Sciences, Vol. 15, Iss. 1,* pp. 2125-2133.
47. Reddem, P.R. (2024). Cybersecurity in banking and finance: navigating the digital threat landscape. *Intenrational Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol. 10, Iss. 5,* pp. 852-861.

48. Salamzadeh, A. et al. (2024). The role of coopetition in fostering innovation and growth in new technology-based firms: a game theory approach. *BAR-Brazilian Administration Review, Vol. 21, Iss. 1*, pp. 1-15.
49. Santos, P. et al. (2025). A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats. *Sensors, Vol. 25, Iss. 14*, pp. 1-28.
50. Sayeed, S.A. et al. (2024). FSCsec: Collaboration in financial sector cybersecurity – exploring the impact of resource sharing on IT security. *Computer Science, Cryptography and Security.* Retrieved from: https://arxiv.org/pdf/2410.15194, 12.10.2025.
51. Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity, Vol. 9, Iss. 1,* pp. 1-11.
52. Shehab, R.T. et al. (2024). Assessment of cybersecurity risks and threats on banking and financial services. *Journal of Internet Services and Information Security, Vol. 14, Iss. 3*, pp. 167-190.
53. Singh, C. (2023). The European approach to cybersecurity in 2023: A review of the changes brought in by the network and information security 2 (NIS2) directive 2022/2555. *International Company and Commercial Law Review, Vol. 5*, pp. 251-261.
54. Sudheer, S. (2024). Ransome attacks and their evolving strategies: a systematic review of recent incidents. *Journal of Technology and Systems, Vol. 6, Iss. 7,* pp. 32-59.
55. Tagscherer, F., Carbon, C.-C. (2024). Digital servitization and leadership: A holistic view on required leadership traits and skills. *Journal of Entrepreneurship, Management and Innovation, Vol. 20, Iss. 4*, pp. 104-129.
56. *The Basel Committee*. Retrieved from: https://www.bis.org/bcbs/index.htm, 19.09.2025.
57. *The Polish Bank Association*. Retrieved from: https://www.zbp.pl/Dla-Bankow/Cyberbezpieczenstwo, 07.09.2025.
58. Tong, J., Nwokeji, J.C. (2023). An implementation of Man-in-the-Browser attack and defence method in the Google Chrome browser. *Proceedings of the Future Technologies Conference (FTC), No. 2*, pp. 590-596.
59. Tran, T.N. (2025). Systematic review of cybersecurity in banking: Evolution from pre-industry 4.0 to post-industry 4.0 in artificial intelligence, blockchain, policies and practice. *Computer Science. Cruptography and Security*, pp. 1-28.
60. Tripathi, B. et al. (2020). A study of DDoS (Distributed-denial-of-service) attacks and its preventions. *International Journal of Scientific Research in Science, Engineering and Technology, Vol. 7, Iss. 4,* pp. 176-181.
61. Trizna, D. et al. (2024). *Robust synthetic data-driven detection of living-off-the-land reverse shells*. Retrieved from: https://arxiv.org/pdf/2402.18329, 12.09.2025.

62. Waizel, G. (2023). The potential effects of recent EU cybersecurity and resilience regulations on cloud adoption and EU cyber resilience. *CES Working Papers, Vol. 15, Iss. 3,* pp. 231-253.
63. Yuspin, W. et al. (2024). Digital banking security: Internet phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Safety and Security Engineering, Vol. 14, Iss. 6*, pp. 1699-1706.