STUDIA NAD BEZPIECZEŃSTWEM

Nr 10 s. 181–191 2025

ISSN 2543–7321

© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku

DOI: 10.34858/SNB.10.2025.010

Joanna Grubicka
Chair of the organising committee

REPORT OF THE 10TH NATIONAL SCIENTIFIC CONFERENCE – 'MODERN MAN FACING THE CHALLENGES AND THREATS OF CYBERSPACE'

Introduction

On 20–21 May 2026, the 10th anniversary edition of the National Scientific Conference entitled 'Contemporary Society Facing the Challenges and Threats of Cyberspace' took place at the MORZE Hotel in Ustka. The event was organised by the University of Pomerania in Słupsk, the Institute of Security and Sociology and the Department of Cyberspace Security, in collaboration with numerous academic partners, including the Rzeszów University of Technology, as well as leaders from the technology and finance sectors (Samsung, mBank, Allegro, NASK and PIIT). It marked an important milestone in the ten-year cycle of interdisciplinary academic meetings dedicated to the issue of human interaction within the digital environment. Since its inception, the conference has developed as a forum for the exchange of knowledge, experience and best practice in the fields of cybersecurity, personal security, digital education, combating cybercrime, information protection, new technologies and the social consequences of digitalisation. This anniversary edition confirmed that the initiative has become a recognised meeting place for academia, public administration, the uniformed services, the technology sector, business, education and young researchers. The 10th edition of the conference was held under the theme: 'Ten years of interdisciplinary debate on cyberspace – from threats to solutions.' This theme succinctly captured both the anniversary nature of the event and the evolution of the entire conference series. Over the course of ten years the conference has served as a forum for systematic reflection on the transformations of

cyberspace, initially viewed primarily as an area posing new threats to individuals, young people, institutions and the state, and subsequently analysed with increasing clarity as an environment for seeking effective organisational, educational, legal and technological solutions. The theme of the anniversary edition emphasised the shift from identifying problems to designing practical mechanisms to counter cyber threats. In the early years, particular focus was placed on issues such as prevention, the online safety of the younger generation, cyberpathology, digital addiction, privacy protection and user education. Over time, the scope of the debate expanded to include cybercrime, institutional security, information warfare, disinformation, the digital economy, artificial intelligence, data protection, IT support for law enforcement agencies and the resilience of the state and society to digital threats. The phrase 'from threats to solutions' indicated that the aim of the conference was not merely to describe the threats accompanying technological development. Equally important was the search for answers to the question of how to build a secure digital environment, develop users' skills, strengthen information resilience, design effective incident response procedures and integrate the efforts of academia, public administration, the security services, the business sector and education. In this sense, the anniversary edition was not only a review but also set out a programme for the future – it charted the course for further cooperation and research. The conference theme also reflected its interdisciplinary nature. Cyberspace was analysed from the perspectives of security studies, law, education, sociology, psychology, computer science, social communication, management and the practices of law enforcement agencies and the technology sector. This made it possible to demonstrate that contemporary cyber threats are not one-dimensional in nature. They are simultaneously a technical, social, educational, legal, organisational and strategic problem. This anniversary edition confirmed that the ten-year debate on cyberspace has led to the development of an important environment for academic and practical collaboration. The conference served as a meeting place for researchers, experts, law enforcement officers, representatives of government, technology companies, public institutions, teachers, students and early-career researchers. Joint reflection on cyberspace enabled participants not only to identify new threats, but also to propose concrete solutions: educational, preventative, technological, regulatory and organisational. In this context, the slogan 'Ten years of interdisciplinary debate on cyberspace – from threats to solutions' should be seen as a summary of the achievements of the entire conference series. Ten editions have created a lasting platform for the exchange of knowledge and experience, whilst also demonstrating that cybersecurity requires constant dialogue, the updating of knowledge and collaboration across many sectors.

The conference was not limited to the role of an academic event, but became a forum for building a culture of digital security, founded on knowledge, responsibility, cooperation and the ability to respond to the rapidly changing challenges of the modern world.

1. Ten years of interdisciplinary debate on cyberspace

This anniversary edition provided an opportunity to look back on the entire series of conferences entitled 'Contemporary Society Facing the Challenges and Threats of Cyberspace,' held between 2016 and 2026. The first edition, held on 24 May 2016, focused primarily on the online safety of the younger generation, educational opportunities and the prevention of digital threats. It was a pioneering event, which placed particular emphasis on the need to educate young people and teachers on the safe use of the internet. In subsequent years, the conference's thematic scope has steadily expanded. In 2017, the proceedings were devoted to cyberspace security in both its structural and personal dimensions. In 2018, particular attention was paid to the social dimension of the internet, values, threats and user responsibility. The 2019 edition explored issues relating to the institutional framework for countering threats in cyberspace, cyberpathology, addiction, diagnosis and therapy. In 2020, amidst the COVID-19 pandemic, the conference was held online, which in itself served as an example of the accelerated digitalisation of academic and social life. The 2021 edition placed a stronger emphasis on technical aspects and innovative IT tools shaping social reality. In 2023, the conference addressed issues relating to society, organisations and the digital economy, whilst in 2024 the focus was on the society of tomorrow, technology, artificial intelligence and security. The 2025 edition, entitled 'Cyberspace – transcending the boundaries of reality, security and control,' delved deeper into the boundaries of protection, surveillance, regulation, artificial intelligence and institutional accountability.

The conference's ten-year history shows a clear evolution in the topics covered: from education and risk prevention among young people, through personal and social security, to issues of artificial intelligence, information warfare, cybercrime, the digital economy, digital forensics, data protection, information management and national resilience. Each edition has responded to the current challenges of its time, whilst at the same time fostering continuity in scholarly reflection on humanity in cyberspace. Of particular significance for the anniversary edition was the publication of the academic monograph The Multidimensionality of Cyberspace, edited by

J. Grubicka and A. Kamińska-Nawrot, published in 2026 by CeDeWu. This publication represents an important culmination of ten years of interdisciplinary debate conducted within the framework of the conference. It is not merely a collection of academic texts, but a comprehensive study presenting cyberspace as a complex, dynamic and multidimensional environment. The introduction to the monograph emphasises that cyberspace cannot be analysed solely as a technological space. It is simultaneously a social, cultural, informational, educational, legal, organisational and security space. This anniversary publication builds on the achievements of previous editions of the conference, drawing on issues that have recurred over the past decade in presentations, debates and expert panels. In this way, the book serves as an academic continuation of the conference and leaves a lasting mark on the academic community.

The monograph covers topics such as information ecology, disinformation, information warfare, cybercrime, artificial intelligence, deepfakes, prompt injection, the safety of children and young people, social pathologies in cyberspace, digital identity, European regulations, decision-making models and the transformation of professional competences. Its structure confirms that cybersecurity is today an interdisciplinary field, requiring collaboration between security studies, education, law, psychology, sociology, computer science, management and social communication studies. This publication can be regarded as an intellectual summary of a decade of conferences, but also as a starting point for further research into the future of humanity in cyberspace. It draws on the achievements of previous editions, organises the main areas of concern and points to new directions for reflection, particularly in the context of artificial intelligence, information resilience, cybercrime, the protection of young people and national security.

The 10th edition of the conference brought together a wide range of participants representing various academic, expert and professional communities. The event was attended by representatives from at least 28 scientific, academic, research and training centres. These included, amongst others: the University of Pomerania in Słupsk, the Rzeszów University of Technology, the University of Kalisz, the University of Łódź, the University of Gdańsk, the Nicolaus Copernicus University in Toruń, the Jagiellonian University, the University of Zielona Góra, Jan Kochanowski University in Kielce, Maria Curie-Skłodowska University in Lublin, the University of Radom, the University of the National Education Commission in Kraków, Łazarski University in Warsaw, the Police Academy in Szczytno, the Military Aviation Academy, the Vistula Academy of Finance and Business, the Pomeranian University in Starogard Gdański, the Maria Grzegorzewska Academy of Special Education, the

Angelus Silesius Academy of Applied Sciences in Wałbrzych, the Police Training Centre in Legionowo and the Information Processing Centre – State Research Institute. The programme also featured representatives from overseas institutions: Santa Ana College in the United States and OTH Regensburg in Germany. The presence of these institutions gave the conference an international dimension, particularly during the online session devoted to cybersecurity, artificial intelligence and qualitative analysis. In addition to the academic community, the conference was attended by representatives from the Ministry of National Defence, NASK-PIB, the Central Bureau for Combating Cybercrime, the Police, the banking sector, e-commerce, logistics and technology companies. Partners and practical participants included representatives from organisations such as Samsung, Allegro, OLX, mBank, DHL eCommerce, Comdrev.pl, Microsoft, Google, NASK, PIIT and CyberDefence24. In total, the conference brought together over 35 institutional, academic, public and business organisations. Such broad representation confirms that issues relating to cyberspace cannot be confined to a single discipline or sector. Contemporary cyber threats are cross-cutting in nature and therefore require cooperation between universities, law enforcement agencies, government, the technology sector, the banking sector, the education sector and civil society.

The conference programme was structured around multiple themes. It comprised plenary sessions, parallel panels, an anniversary debate, a police panel, an international session, expert presentations, workshops and presentations by young researchers. As a result, the event combined theoretical reflection with the practical aspects of digital security. One of the most important areas of debate was the strategic challenges to national security in the context of information technology. Participants analysed the role of cyberspace as a new dimension of conflicts, international rivalry and hybrid operations. Of particular significance were the presentations on the Ukraine–Russia war, the Israeli–Palestinian conflict, the European Union's and NATO's cyberspace security policies and national information resilience. The discussions emphasised that modern warfare is not limited to military operations and attacks on technical infrastructure. Influence operations, disinformation, the manipulation of public opinion and actions aimed at undermining public trust in state institutions are becoming increasingly significant. Cyberspace has therefore become not only a field for the technical protection of systems, but also a space for the battle over citizens' awareness, emotions, interpretations and decisions.

The second key pillar of the conference was artificial intelligence. Of particular significance was the opening lecture devoted to the thesis 'AI without order = cyberchaos.' This presentation highlighted the fundamental importance of data management

for the security of AI-based systems. During the proceedings it was pointed out that AI can be both a tool for development and a source of new threats. On the one hand, it supports data analysis, education, simulations, automation, quality management and decision-making processes. On the other hand, it can be used to generate disinformation, deepfakes, automate fraud, personalise social engineering attacks and create more sophisticated forms of cyberattacks. An important conclusion from the conference was that the effective use of AI requires not only technical expertise, but also organisational governance, ethical accountability, data transparency, legal regulation and user education. Without these elements, artificial intelligence may exacerbate information chaos and increase society's vulnerability to manipulation. A key item on the agenda was a police panel dedicated to crime in the digital age. Participants discussed technologies, threats and challenges facing law enforcement agencies. This panel was particularly valuable as it combined academic knowledge with the operational experience of officers and experts dealing with real-world cases of cybercrime. Topics covered included the securing of cryptocurrencies during searches, mobile device forensics, data extraction, anti-forensic techniques, methods for bypassing device encryption and practical evidential issues. Representatives from the Central Bureau for Combating Cybercrime demonstrated how rapidly the criminal environment is changing and how crucial specialist technical knowledge is becoming. The panel confirmed that cybercrime is no longer a marginal or purely technical phenomenon. It is one of the key challenges to the security of the state, the economy and citizens. Criminals exploit artificial intelligence, cryptocurrencies, anonymisation tools, mobile devices, social engineering and the cross-border nature of the internet. This requires the continuous refinement of investigative methods, international cooperation and the integration of legal, technical and criminological expertise.

Another key area of the conference was cooperation between the business sector, public administration and law enforcement agencies. Representatives from Allegro, OLX, DHL eCommerce, mBank and Samsung discussed their practical experiences in combating online fraud, phishing, e-commerce abuse, cross-border crime and customer protection. The topic of the psychology of fraud was particularly important. It was emphasised that cyber-attacks very often do not begin by breaching technical security measures, but by exploiting human emotions: fear, haste, trust, curiosity, time pressure or the need for quick profit. Technology can support security, but it cannot replace user awareness and organisational culture. In this context, it was particularly significant to note that technological security can create an illusion of protection if it is not accompanied by education and responsible process design. Effective

protection of bank customers, e-commerce platform users and digital service users requires combining technical safeguards with public communication, behavioural analysis and preventative measures.

2. Education, young people and public safety

From the very first editions of the conference, one of its most important areas has been digital education and the safety of children and young people. In the 10th edition, this topic returned in an expanded format. Presentations covered, amongst other things, young people online, cyber threats in the light of empirical research, the psycho-pedagogical consequences of online fraud, the protection of pupils' online reputations and the relationship between children, teachers and cyberspace. Participants pointed out that young internet users operate in an environment that offers enormous educational and social opportunities, but at the same time poses numerous risks. These include cyberbullying, digital addiction, disinformation, loss of privacy, image-related pressure, algorithmic manipulation and exposure to harmful content. A key conclusion was the emphasis placed on the role of teachers, parents and educational institutions. The safety of children and young people cannot be limited to bans and controls. It should be based on developing digital literacy, critical thinking, responsibility for one's own image, the ability to recognise manipulation and the mindful use of technology. The anniversary conference also provided a platform for young researchers and students. Second and third-year students of the Cyberspace Engineering programme at the University of Pomerania in Słupsk, as well as students representing the University of Wrocław and the University of Radom, took an active part in the practical panel and workshops. Their presence was a key element of the conference programme, as it enabled the younger academic community to be involved in an interdisciplinary debate on contemporary digital threats. The students presented topics including ARP spoofing, brute-force attacks, OSINT, deepfake technology, disinformation on social media and the principles of safe internet use. These presentations were practical in nature and illustrated both the technical mechanisms of cyber-attacks and the social consequences of users' unwitting behaviour in cyberspace. This element of the programme was of particular educational significance. It demonstrated that training future cybersecurity specialists requires not only theoretical lectures, but also practical demonstrations, case studies, workshop-based activities and direct contact with experts. The participation of students from various academic institutions fostered the exchange of experiences, the development

of research skills and the creation of a community of young specialists interested in digital security. The students took part not only as conference attendees but also as active contributors to the debate. Their presentations confirmed that the younger generation of cybersecurity researchers and practitioners is capable of combining technical knowledge with social, educational and organisational reflection. The inclusion of students in the programme of the conference's anniversary edition was also an expression of the consistent effort to build up the workforce for the cybersecurity sector and to foster a culture of responsible participation in cyberspace.

2. The importance of patronage and cross-sector collaboration

Over the years the conference has grown thanks to collaboration across many sectors. Previous editions have benefited from the patronage and support of institutions such as NASK, UKE, the Ministry of Education and Science, the Ministry of National Defence, the NASK Academy and technology companies including Allegro, Samsung, Comarch, Microsoft, Google, OLX, Comdrev.pl and Xopero Backup & Recovery. The anniversary edition reaffirmed the importance of cross-sector collaboration. The presence of universities, state institutions, law enforcement agencies, technology firms, the banking sector, e-commerce platforms and industry organisations created the conditions for a debate of both a practical and strategic nature. Representatives of the Police and the Central Bureau for Combating Cybercrime held a special place amongst the participants; their presence highlighted the practical dimension of the conference and the importance of collaboration between academia and the institutions responsible for public safety. The security services were represented by, amongst others: the Municipal Police Commander in Słupsk, Junior Inspector Leszek Głuchowski; the Deputy Commander of the Police Academy in Słupsk, Sub-Inspector Daniel Krenc; the First Deputy Provincial Police Commander in Gdańsk, Junior Inspector Tomasz Juński; the Head of the Digital Crime Division at the Gdańsk Provincial Police Headquarters, Assistant Commissioner Marcin Grześkowiak; and the Head of the Forensic IT Division at the Gdańsk Branch of the Central Bureau for Combating Cybercrime, Assistant Commissioner Przemysław Smeja. Their participation was of particular significance to the substantive aspect of the event, as it enabled the combination of academic reflection with the practical experience of the services responsible for identifying, combating and documenting crimes committed in the digital environment. The presence of representatives from the Police and the CBZC confirmed that cybersecurity is not solely the

responsibility of IT specialists or public administration. It is a shared responsibility of the state, academia, business and society, requiring constant cooperation, the exchange of knowledge and the refinement of procedures for responding to rapidly evolving threats.

4. Conclusions

It is clear from the proceedings of the anniversary conference that one of the key challenges for contemporary security is building the information resilience of the state and society. Disinformation, information warfare and influence operations are no longer marginal phenomena; they have become a permanent feature of the security environment. Their impact extends not only to the political and military spheres, but also to the social, educational, economic and cultural spheres. Effective protection against information manipulation therefore requires the development of analytical skills, the strengthening of critical thinking, media accountability, inter-institutional cooperation and efficient mechanisms for identifying and neutralising false narratives. Artificial intelligence was also a key area of discussion; its development creates new opportunities for education, governance, security and data analysis, but at the same time gives rise to qualitatively new risks. AI-based technologies can support decision-making processes, the automation of activities and the protection of digital resources; however, without proper oversight, organisational governance, high-quality data and a regulatory framework, they may become a tool for manipulation, fraud, disinformation and the destabilisation of the information environment. In this context, the responsible design, implementation and monitoring of artificial intelligence systems take on particular significance.

The issue of cybercrime and the practices of law enforcement agencies featured prominently in the debate. Contemporary digital crime is becoming increasingly complex, cross-border in nature and technologically advanced. It encompasses both traditional fraud carried out using new technologies and specialised activities utilising cryptocurrencies, mobile devices, anonymisation tools, anti-forensic techniques and the automation of attacks. Effectively countering these phenomena requires specialist expertise, modern digital forensics tools, cooperation with the private sector and the continuous improvement of evidential and operational procedures.

The conference also clearly demonstrated that an organisation’s security cannot be equated solely with the implementation of technical tools. The level of protection is also determined by people, procedures, internal communication, management

accountability, the quality of data management and the institution's ability to respond rapidly to incidents. A security culture should be understood as an integral part of an organisation's operations, encompassing risk awareness, staff accountability, clear standards of conduct and a systematic approach to information protection. Particular importance was also attached to systematic digital education. Cybersecurity begins with the user – whether a child, pupil, student, employee, senior citizen, consumer or citizen. Education should not be limited to imparting technical security principles, but should also cover recognising manipulation, protecting privacy, the informed management of one's own digital identity, the critical evaluation of information and responsibility for one's online actions. Only such an approach allows for the development of a mature digital society, capable not only of using technology but also of understanding its consequences and mitigating the associated risks. The proceedings as a whole confirmed that cybersecurity requires an interdisciplinary and cross-sectoral approach. Contemporary digital threats transcend the boundaries of individual institutions, academic disciplines and economic sectors. Identifying and mitigating them requires cooperation between the academic community, public administration, law enforcement agencies, business, education and civil society. This anniversary edition of the conference demonstrated that the shift 'from threats to solutions' necessitates combining scientific analysis with institutional practice, technological development, public education and responsible cybersecurity governance.

The 10th National Scientific Conference 'Modern Society Facing the Challenges and Threats of Cyberspace' confirmed that the issue of cybersecurity requires an ongoing dialogue between academia and practice. The event provided an opportunity to juxtapose the researchers' perspective with the experience of law enforcement officers, technology experts and representatives from the worlds of business, banking, e-commerce and education. For the academic community, the conference served as a forum for presenting research findings, theoretical concepts and interdisciplinary analyses. For practitioners, it provided a space to exchange experiences regarding real-world threats, countermeasures and organisational needs. For students, it was an opportunity to learn from experts and showcase their own projects and skills. The event also demonstrated that the University of Pomerania in Słupsk is consistently establishing itself as a key centre for reflection on cybersecurity, personal safety and the social consequences of digitalisation. The ten-year cycle of conferences has created a lasting platform for academic and expert collaboration.

5. Summary

The tenth anniversary edition of the conference was an event of particular scientific, organisational and symbolic significance. On the one hand, it summarised a decade of debates on cyberspace; on the other, it opened up new avenues for reflection on the future of digital security. At the heart of this reflection was the individual – as a user of technology, a citizen, an employee, a student, a consumer, a victim of cybercrime, but also as a creator of solutions and a key player in fostering a culture of security. The conference confirmed that cyberspace is today one of the most important environments in which people operate. It is within this space that social relations, educational processes, political decisions, business models, information conflicts, criminal threats and new forms of responsibility take shape. Therefore, security in cyberspace must be understood broadly – as technical, social, personal, informational, legal, organisational and cultural security. A special highlight of the anniversary was the monograph The Multidimensionality of Cyberspace, which draws on the achievements of previous editions of the conference and presents them in the form of an academic summary. This publication confirms that ten years of the conference have resulted not only in a series of events, but also in a lasting contribution to the development of research into human behaviour in cyberspace. The 10th edition of the conference was a success both in terms of content and organisation. It demonstrated that the future of cybersecurity depends on the ability to collaborate, think across disciplines, educate, design technology responsibly and build social and institutional resilience. The debate that began a decade earlier has not been concluded – on the contrary, it has entered a new phase in which the challenge lies not only in responding to threats, but also in shaping a secure, informed and resilient digital culture.