

CYBERSEC EXPO & FORUM 2026
PRELIMINARY THEMATIC SCOPE
15-16 June 2026

A space where the public sector, business, industry and the world of technology come together to forge digital resilience.

15 JUNE 2026		
08:00-09:00 – guest registration		
09:00-10:30 BALLROOM C Opening session: Geopolitics of Cyber Security and Technological Sovereignty		
10:30-11:00 – break		
11:00-12:00 BALLROOM C Pragmatic Approach to Building Cyber Defence. Expectations vs. Reality	11:00-12:00 BALLROOM B Cybersecurity of Central and Local Administration	11:00-12:00 LOWER LOBBY STAGE Cyber Image of Polish Business 2026
12:00-12:30 – break		
12:30-13:30 BALLROOM C Partnership for Cyber Defence	12:30-13:30 BALLROOM B The National Cyber Security System and NIS2 in Practice	12:30-13:30 LOWER LOBBY STAGE Money for Cyber: from Legislation to Opportunities for Business
13:30-14:30 – break		
14:30-15:30 BALLROOM C AI in Practice: 2026 – the Year of Implementation	14:30-15:30 BALLROOM B Protecting Critical Infrastructure. Lessons for the Future	14:30-15:30 LOWER LOBBY STAGE Disinformation and social resilience
15:30-16:00 – break		
16:00-17:00 BALLROOM C Technologies of the Future. Where to Invest to Succeed?	16:00-17:00 BALLROOM B Skills and Education for the Future	16:00-17:00 LOWER LOBBY STAGE Between Specialization and Universality. How Should the State Organize Itself to Combat Cyber Crime?
18:30 Ballroom C ACCOMPANYING EVENTS Gala		
19:15 Ballroom A ACCOMPANYING EVENTS Banquet		

16 JUNE 2026		
08:00-09:30 – guest registration		
09:30-10:30 BALLROOM C The state, the Military, and Business – Partnership or Competition for Talent?	09:30-10:30 BALLROOM B CISOs and CIOs under Pressure. Leadership Challenges.	09:30-10:30 LOWER LOBBY STAGE Cyber Security in Finance
10:30-11:00 – break		
11:00-12:00 BALLROOM C The Cyber Resilience Act and Certification: New Obligations, New Product Security Standards	11:00-12:00 BALLROOM B Cyber Security and Dual-Use Technologies – How to Strengthen the Polish Ecosystem?	11:00-12:00 LOWER LOBBY STAGE Cyber Security of the Energy Sector
12:00-12:30 – break		
12:30-13:30 BALLROOM C Education as a Shield. The Academic Sector in Times of Change.	12:30-13:30 BALLROOM B Cyber Diplomacy and Poland's Technological Ambition. Can Poland Become an Exporter of Cyber Security?	12:30-13:30 LOWER LOBBY STAGE Cyber Security in Healthcare
13:30-14:30 – break		
14:30-15:30 BALLROOM C Smart Cities. How will Technology Reshape Urban Environments?	14:30-15:30 BALLROOM B Cyber Security in Industry	

15 June 2026 | 09:00-10:30 | Ballroom C |  on-line transmission |  simultaneous interpreting PL|EN

OPENING SESSION

Geopolitics of Cyber Security and Technological Sovereignty

Europe is functioning between global technological powerhouses that define the standards of safety, legislative models, and digital architecture. Is the EU doomed to dependence or is it developing its own agency in cyberspace? Debate on technological sovereignty, competitive industry and protection of democratic values in conditions of growing geopolitical pressure. The perspective of European institutions, businesses, and experts.

Opening:

- **Wojciech Kuśpik**, CEO of the PTWP Group
- **Leszek Pietraszek**, Chairman of the Board, Upper Silesian-Dąbrowa Basin Metropolis
- **Wojciech Saługa**, Marshal of the Silesian Voivodeship
- **Bogumił Sobuła**, Vice President of Katowice

Speech (10'):

- **Dariusz Standerski**, Secretary of State, Ministry of Digital Affairs

Speech (10'):

- **Borys Budka**, Member of the European Parliament, Head of EP ITRE Committee

The discussion, which were invited to participate (alphabetic order):

- **Andy Garth**, Director of Government Affairs, ESET
- **Radosław Nielek**, Director, NASK

POLSKIE TOWARZYSTWO WSPIERANIA PRZEDSIĘBIORCZOŚCI SA

 PTWP SA, Plac Sławika i Antalla 1, 40-163, Katowice  tel. +48 32/ 209 13 03  www.ptwp.pl  ptwp@ptwp.pl

NIP: 954-21-99-882 **REGON:** 273754180 **KRS:** 0000316388 Sąd Rejonowy Katowice-Wschód w Katowicach, Wydział VIII Gospodarczy - Krajowego Rejestru Sądowego **Kapitał zakładowy:** 803 455,00 zł

- **[Online] Jacek Siewiera**, Lt. Col. of the Polish Army, Atlantic Council Expert, Head of the National Security Bureau from 2022 to 2025
- **Dariusz Standerski**, Secretary of State, Ministry of Digital Affairs
- **Tomasz Zdzikot**, Vice-Chairman of the Security and Defence Council of the President of the Republic of Poland

Moderated by:

- **Nikola Bochyńska**, Journalist, WNP.pl

15 June 2026 | 11:00-12:00 | Lower Lobby Stage |  on-line transmission

Cyber Image of Polish Business 2026

Cyber attacks are growing in numbers, scale and diversity. What challenges do Polish companies face? Is the employee still the weakest link in the chain of cyber security? How often do Polish entities deal with consequences of ransomware?

The latest information of the situation of Polish cyberspace, taking into account business and managerial staff, will be presented in a report titled "Cyber Image of Polish Business 2026" by ESET and DAGMA IT Security. The discussion, apart from the state of technologies and procedures, will also concentrate on the perception of threats by organisations and their ability to navigate the constantly evolving minefield of cyber threats. The report will first be published at Cybersec EXPO & Forum

Presentation (10'):

- DAGMA report

The discussion, which were invited to participate (alphabetic order):

- **Marcin Dudek**, Manager, CERT Poland, NASK
- **Andrzej Dulka**, President, Polish Chamber of Information Technology and Telecommunications (PiliT)
- **Paweł Jurek**, Director of Business Development, DAGMA IT Security
- **Agnieszka Ulanowska**, Director, Internal Supervision and IT Security Department, VeloFunds TFI SA, ISACA Warsaw Chapter
- **Mirosław Wróblewski**, President, Personal Data Protection Office

Moderated by:

- **Nikola Bochyńska**, Journalist, WNP.pl

15 June 2026 | 11:00-12:00 | Ballroom B |  on-line transmission |  simultaneous interpreting PL|EN

Cybersecurity of Central and Local Administration

Central administration and local government face similar challenges: the implementation of NIS2, increasing legislative pressure and growing threats to public services and critical infrastructure. How to create a consistent system of state cyber resilience — from strategy and legislation, through joint SOC and smart city protection, to cross-sectoral cooperation? Debate on the digital foundations of a secure state functioning under permanent pressure. The state and local government in one system: SOC, Zero Trust and new models of cooperation.

The discussion, which were invited to participate (alphabetic order):

- **Michał Gramatyka**, Secretary of State, Ministry of Digital Affairs
- **Monika Ingram**, Director, Cybersecurity Research Center, Łukasiewicz-Al
- **Stanisław Korman**, Member of the Management Board, Upper Silesian-Dąbrowa Basin Metropolis
- **Jakub Olszowiec**, Strategy, R&D and PMO Director, Polish Security Printing Works
- **Jacek Orłowski**, Manager, Department of Cooperation with the Electronic Document Management Environment Entities, NASK

Moderated by:

- **Elżbieta Rutkowska**, Journalist, WNP.pl

15 June 2026 | 11:00-12:00 | Ballroom C |  on-line transmission |  simultaneous interpreting PL|EN

Pragmatic Approach to Building Cyber Defence. Expectations vs. Reality

Creating SOC and CSIRT, implementing procedures, testing business continuity plans — in practice. Debate on the difference between strategies and organisational reality: staff shortages, limited budgets, resistance to change. What are the proven methods of increasing cyber resilience and how to avoid falling into the most popular traps? Trust comes first, Directions for development and cooperation in cyber security.

The discussion, which were invited to participate (alphabetic order):

- **Miroslav Čačík**, Filed CISO Advisor, ESET
- **Agnieszka Jankowska**, Chairwoman of the Council for Digital Affairs, Ministry of Digital Affairs, Director of Corporate and Public Affairs, T-Mobile Polska

- **Filip Kupiński**, Security Services Lead for Poland, Accenture
- **Piotr Potejko**, Safety Director, Veolia Group in Poland
- **Agata Ślusarek**, CTI Expert

Moderated by:

- **Michał Duszczyk**, Journalist, Rzeczpospolita

15 June 2026 | 12:30-13:30 | Ballroom C |  on-line transmission |  simultaneous interpreting PL|EN

Partnership for Cyber Defence

Cyber space has become one of the key fields of activity for the Alliance. How is NATO developing joint competencies in the field of cyber defence and mechanisms of responding to serious incidents? Discussion on the sharing of information on threats, joint exercises, and the role of the member states. What is the influence of Poland and Central and Eastern Europe on NATO agenda on cyber security?

The discussion, which were invited to participate (alphabetic order):

- **Tomasz Florczak**, CEO, ChallengeRocket
- **Reserve Brig. Gen. Włodzimierz Nowak**, Expert in the field of Cybersecurity
- **Joanna Pawełek-Mendez**, Minister-Counsellor for Cybersecurity, Security Policy Department, Ministry of Foreign Affairs
- **Tomasz Zdzikot**, Vice-Chairman of the Council for Security and Defence to the President of the Republic of Poland

Moderated by:

- **Marcin Piasecki**, Managing Editor, Rzeczpospolita

15 June 2026 | 12:30-13:30 | Ballroom B |  on-line transmission |  simultaneous interpreting PL|EN

The National Cyber Security System and NIS2 in Practice

The progress on implementing the National Cyber Security System and NIS2 — what can entrepreneurs expect in the nearest future. How to prepare today for what is coming: the identification of responsibilities, risk analysis and first steps towards compliance with new legislation. Implementation challenges faced by businesses — the interpretation of legislation, preparation of procedures, cooperation with suppliers, and management of the supply chain. The role of the management board and managerial staff in preparing the company to new requirements of cyber security.

Presentation (15'):

- **Przemysław Frąk**, Senior Presales Engineer, Axence

The discussion, which were invited to participate (alphabetic order):

- **Przemysław Frąk**, Senior Presales Engineer, Axence
- **Jarosław Homa**, Rector's Representative for Cybersecurity, deputy director of the Centre for Cybersecurity at the Silesian University of Technology
- **Joanna Karczewska**, IS Auditor, Cyber Security and Data Protection Expert
- **Karol Skupień**, President of the Board, National Chamber of Ethernet Communications (KIKE)
- **Dariusz Szostek**, Judge of the Constitutional Tribunal, Director, Cyber Science Centre, University of Silesia

Moderated by:

- **Elżbieta Rutkowska**, Journalist, WNP.pl

15 June 2026 | 12:30-13:30 | Lower Lobby Stage |  on-line transmission

Money for Cyber: from Legislation to Opportunities for Business

The growing scale of threats means increased spending on cyber security. How to create an effective financing system: from public mechanisms and legislation to mobilizing private capital? Debate on the available support instruments and on transforming legislative pressure and risk into a stimulus for developing domestic technologies and services.

The discussion, which were invited to participate (alphabetic order):

- **Marietta Gieroń**, Chairwoman, The Kościuszko Institute
- **Adrian Kapczyński**, Coordinator of the "Cybersecurity" research sub-area, Silesian University of Technology
- **Marianna Sidoroff**, Director, Digital Economy Department, Ministry of Development and Technology

- **Krzysztof Szubert**, Plenipotentiary of the Director for Commercialization and International Cooperation, National Institute of Telecommunications, Member of the Board of Directors, European Cyber Security Organisation Senior Associate Member, University of Oxford
- **Piotr W. Zawadzki**, Expert, Strategic Management Department, National Centre for Research and Development

Moderated by:

- **Hubert Bigdowski**, Journalist, WNP.pl

15 June 2026 | 14:30-15:30 | Lower Lobby Stage |  on-line transmission

Disinformation and social resilience

Information operations have become a tool of political and economic pressure. Propaganda and disinformation campaigns impact decisions made by consumers, market stability, public health, and public feeling. How to create a communication resilience of a state, business, and nation? Debate on response mechanisms, education and cooperation between public institutions and the private sector. Strategic communication and the role of state. How to respond to crises?

The discussion, which were invited to participate (alphabetic order):

- **Szymon Grabowski**, Senior Content Verification Analyst, Cyberspace Information Protection Division, NASK
- **Marcel Kiełtyka**, Member of the Management Board, Director of Communications and PR, Demagog Association, Member of the Consultative Council for Counteracting External Disinformation at the Ministry of Foreign Affairs
- **Michał Kowalczyk**, Research Director, Member of the Management Board, Institute for Market and Social Research (IBRiS)
- **Marcin Piasecki**, Managing Editor, Rzeczpospolita
- **Marta Zabłocka**, Fact-Checking Department, Polish Press Agency
- **Łukasz Zych**, Press Spokesperson, Upper Silesian-Dąbrowa Basin Metropolis

Moderated by:

- **Karolina Markowska**, Editor-in-Chief, PulsHR.pl

15 June 2026 | 14:30-15:30 | Ballroom B |  on-line transmission |  simultaneous interpreting PL|EN

Protecting Critical Infrastructure. Lessons for the Future

Energy, water, transport, and communications remain the primary targets of advanced attacks. What lessons can be drawn from the most serious incidents of recent years? A discussion on new regulatory and technical requirements, as well as on designing resilience from a systemic perspective — so as to protect not only individual assets, but entire chains of interdependence. Artificial Intelligence. Energy, cloud, AI gigafactories: how can critical infrastructure be protected in a digital state?

The discussion, which were invited to participate (alphabetic order):

- **Marcin Dudek**, Manager, CERT Poland, NASK
- **Krzysztof Dyl**, Vice President, Office of Electronic Communications
- **Agnieszka Jankowska**, Chairwoman of the Council for Digital Affairs, Ministry of Digital Affairs, Director of Corporate and Public Affairs, T-Mobile Polska
- **Dariusz Pałka**, Head of Standards and Architecture Department, Cybersecurity Division, GAZ-SYSTEM
- **Maj. res. Artur Szachno**, Head of the Digital Operations Department, Government Agency for Strategic Reserves,
- **Grzegorz Wawryniuk**, Director of the Product and Marketing Office, EXATEL
- **Dawid Zięcina**, Technical Department Director, DAGMA IT Security

Moderated by:

- **Aleksandra Helbin**, Editor-in-Chief, WNP.PL

15 June 2026 | 14:30-15:30 | Ballroom C |  on-line transmission |  simultaneous interpreting PL|EN

AI in Practice: 2026 – the Year of Implementation

The year 2026 marks a shift from declarations to real AI deployments — also under the pressure of the AI Act. Which systems will be regulated, and what obligations will companies face? A discussion on preparing organizations for audits, responsibility for models, and data security. How can regulatory compliance be combined with efficiency and the building of competitive advantage? Artificial intelligence is changing the rules of the game — it is both a tool of attack and defence. How can AI be leveraged in sensitive sectors — from the military to industry and healthcare?

The discussion, which were invited to participate (alphabetic order):

- **Gabriela Bar**, Legal Counsel, Founder of the Law Firm, Gabriela Bar Law & AI

- **Joanna Karczewska**, IS Auditor, Cyber Security and Data Protection Expert
- **Monika Karwacka**, Assistant professor, Head of the Digital Humanities team, University of Silesia in Katowice
- **Marcin Kowalski**, Research professor, Leader of the artificial intelligence research team at the Institute of Optoelectronics, Military University of Technology
- **Dariusz Szostek**, Judge of the Constitutional Tribunal, director, Cyber Science Centre, University of Silesia

Moderated by:

- **Marcin Mazur**, PR & Communication Officer, DAGMA IT Security

15 June 2026 | 16:00-17:00 | Lower Lobby Stage |  on-line transmission

Between Specialization and Universality. How Should the State Organize Itself to Combat Cyber Crime?

Is a model based on specialized structures, such as the Polish Cyber Crime Investigation Agency, more effective, or should cyber competences be developed across the entire system of services and public administration? A discussion on the role of central and regional units, cooperation with SOCs and CSIRTs, and existing organizational gaps. Is the fight against cybercrime properly embedded today within the National Cybersecurity System and the broader state security system? From data breach to indictment. When and how should law enforcement be involved in incident response? New faces of cyber crime: AI, deepfakes, and cybercrime-as-a-service. Cybercrime without borders. The role of Europol, international cooperation, and the impact of new regulations.

The discussion, which were invited to participate (alphabetic order):

- **Maciej Jan Broniarz**, Cyber Incident Response Expert
- **Agnieszka Gryszczyńska**, Faculty of Law and Administration, Cardinal Stefan Wyszyński University in Warsaw
- **Wojciech Olszowy**, Commander, Central Bureau for Combating Cybercrime
- **Agata Ślusarek**, CTI Expert

Moderated by:

- **Nikola Bochyńska**, Journalist, WNP.pl

15 June 2026 | 16:00-17:00 | Ballroom B |  on-line transmission |  simultaneous interpreting PL|EN

Skills and Education for the Future

The rapid development of technology requires new competencies and close cooperation between academia and business. How can we respond to the growing demand for experts in cybersecurity, AI, and breakthrough technologies? A discussion on the labour market, training and certification systems, and how to adapt education to the real needs of the economy and state security. Cybersecurity education as a key future competence. From digital hygiene at home to real, market-ready skills.

The discussion, which were invited to participate (alphabetic order):

- **Michał Gramatyka**, Secretary of State, Ministry of Digital Affairs
- **Adrian Kapczyński**, Coordinator of the "Cybersecurity" research sub-area, Silesian University of Technology
- **Michał Maurycy Mazur**, Founder, Our future Foundation
- **Iryna Volnytska**, President, SET University, Founder & CEO, IronCyber
- **Rafał Żelazny**, President, Chairman of the Board, Katowice Special Economic Zone

Moderated by:

- **Karolina Markowska**, Editor-in-Chief, PulsHR.pl

15 June 2026 | 16:00-17:00 | Ballroom C |  on-line transmission |  simultaneous interpreting PL|EN

Technologies of the Future. Where to Invest to Succeed?

The world of cyber security is evolving faster than ever. Artificial intelligence, quantum computing, the development of cloud computing, and the semiconductor market are redefining both the possibilities and the limits of digital resilience. From post-quantum encryption to automated incident response, new technologies bring both breakthrough opportunities and previously unknown risks. Will the winners of the future be those who invest in AI and sovereign cloud infrastructure, or those who prioritize the security of semiconductor supply chains? Experts will explore which directions in development and investment will be critical to maintaining — or gaining — a competitive edge in the coming decade.

The discussion, which were invited to participate (alphabetic order):

- **Rafał Duczmał**, Chairman of the Board, EuroHPC Joint Undertaking
- **Jan Kozak**, Director, Łukasiewicz Research Network – Institute of Artificial Intelligence and Cybersecurity, Łukasiewicz – AI
- **Filip Kupiński**, Security Services Lead for Poland, Accenture

- **Marek Niezgódka**, Director, Center for Computational Science and Technology, Silesian University of Technology
- **Bianka Siwińska**, President, Perspektywy Education Foundation, Member of Digitization Council, Ministry of Digital Affairs, Member of the Supervisory Board, Creotech Quantum

Moderated by:

- **Marcin Piasecki**, Managing Editor, Rzeczpospolita

16 June 2026 | 09:30-10:30 | Ballroom C |  on-line transmission |  simultaneous interpreting PL|EN

The state, the Military, and Business – Partnership or Competition for Talent?

Cyber security and defence technologies require top-tier expertise, increasingly contested by public administration, armed forces, and the private sector. How can we build a model of cooperation instead of competing for specialists? A discussion on dual-career programs, joint R&D initiatives, and the role of universities in developing talent for both national security and the economy.

[video] 1:1 conversation:

- **Gen. Karol Molenda**, Former Commander, Cyberspace Defense Forces Component Command

The discussion, which were invited to participate (alphabetic order):

- **Adam Dzwonkowski**, Defense & Intelligence Technology Lead, Microsoft
- **Maj. res. Robert Gałązka**, Project Manager, Polish-Ukrainian Projects Office, Development Department, Polska Grupa Zbrojeniowa
- **Col. Michał Majewski**, Deputy Director, Cybersecurity Training Center of Excellence
- **Marcin Starzyk**, Recruitment and HR Manager, Rekrut 24
- **Anna Timofiejczuk**, Department of Fundamentals of Machinery Design – RMT6, Silesian University of Technology
- **Col. Jarosław Wacko**, Chief Specialist, Cyberspace Defense Forces Component Command

Moderated by:

- **Paweł Szygalski**, Deputy Editor-in-Chief, WNP.pl

16 June 2026 | 09:30-10:30 | Ballroom B |  on-line transmission |  simultaneous interpreting PL|EN

CISOs and CIOs under Pressure. Leadership Challenges.

A panel focused on the role of CISO and CIO within organizations, balancing operational responsibility with board-level expectations. Participants will address common communication challenges: how to translate technical risks into business language, how to build trust and a mandate to act, and how to respond when cyber security leaders themselves become targets of personal, reputational, or legal attacks. Cyber security as a competitive advantage, not just a cost.

The discussion, which were invited to participate (alphabetic order):

- **Andrzej Bartosiewicz**, CEO & President, CISO #Poland Foundation
- **Przemysław Dęba**, CISO, Orange Poland
- **Andrzej Jarosz**, Director, IT and Cybersecurity Department, Koleje Małopolskie
- **Iwona Prószyńska**, Head of the Cybersecurity Strategic Communication Team, NASK
- **Kajetan Przybysz**, CISO, Public Transport Service

Moderated by:

- **Nikoła Bochyńska**, Journalist, WNP.pl

16 June 2026 | 09:30-10:30 | Lower Lobby Stage |  on-line transmission

Cyber Security in Finance

Banking and e-commerce are among the most frequent targets of cyber criminals. How can online transactions be secured, fraud detected, and data breaches effectively managed? A discussion on new trends in financial cyber crime, protecting customers from scams, and the growing regulatory requirements—including Digital Operational Resilience Act—which are redefining resilience standards in the financial sector. Financial security. From internal data leaks to combating scams.

The discussion, which were invited to participate (alphabetic order):

- **Jarosław Biegański**, Director of the Banking Security Department, Polish Bank Association
- **Adam Cieślak**, Commander of the Central Cybercrime Bureau from 2022 to 2026
- **Patryk Gęborys**, Director of the Cybersecurity Office, PZU SA

- **Ireneusz Jazownik**, Chief Information Security Officer, IBK Bank Poland
- **Magdalena Korona**, Cybersecurity Expert, mBank
- **Łukasz Miedziński**, Cybersecurity Area Director, ING Hubs Poland

Moderated by:

- **Elżbieta Rutkowska**, Journalist, WNP.pl

16 June 2026 | 11:00-12:00 | Ballroom B |  on-line transmission |  simultaneous interpreting PL|EN

Cyber Security and Dual-Use Technologies – How to Strengthen the Polish Ecosystem?

Cyber is inherently a “dual-use” domain – solutions developed for the military quickly find applications in business, and vice versa. How should grants, regulations, and support programs be designed to build a strong and competitive cyber security ecosystem in Poland? A debate on the role of the state, funding mechanisms, and public-private partnerships, as well as on how to effectively commercialize emerging technologies.

The discussion, which were invited to participate (alphabetic order):

- **Adam Dzwonkowski**, Defense & Intelligence Technology Lead, Microsoft
- **Wojciech Górecki**, Dual-use Expert, Cybersecurity Center, AGH University of Science and Technology
- **Col. Jan Kelner**, Dean, Military University of Technology (WAT)
- **Mariusz Kujawski**, CEO, ComCERT, Asseco Group
- **Reserve Brig. Gen. Włodzimierz Nowak**, Expert in the field of cybersecurity

Moderated by:

- **Piotr Myszor**, Journalist, WNP.pl

16 June 2026 | 11:00-12:00 | Ballroom C |  on-line transmission |  simultaneous interpreting PL|EN

The Cyber Resilience Act and Certification: New Obligations, New Product Security Standards

The Cyber Resilience Act shifts responsibility for security onto manufacturers and providers of digital solutions. What does this mean in practice for product design, vulnerability management, and update lifecycles? A discussion on new obligations, the role of certification, and how regulatory compliance can be leveraged as a competitive advantage.

The discussion, which were invited to participate (alphabetic order):

- **Andrzej Bartosiewicz**, CEO & President, CISO #Poland Foundation
- **Andrzej Dulka**, President, Polish Chamber of Information Technology and Telecommunications (PliiT)
- **Jarostaw Homa**, Rector's Representative for Cybersecurity, deputy director of the Centre for Cybersecurity at the Silesian University of Technology
- **Kinga Pawłowska-Nojszewska**, Attorney-at-law, MEDIA Law Firm
- **Wojciech Piszewski**, Partner, Sterberg
- **Krzysztof Silicki**, Director for Cybersecurity Strategic Development, NASK, Vice Chair of Management Board, European Union Agency for Network and Information Security ENISA
- **Mikołaj Śniatała**, Partner, Andersen
- **[Online] Aleksandra Wójtowicz**, New Technologies and Digitalization Analyst, The Polish Institute of International Affairs
-

Moderated by:

- **Karol Tokarczyk**, Senior Economic Analyst, Polityka Insight

16 June 2026 | 11:00-12:00 | Lower Lobby Stage |  on-line transmission

Cyber Security of the Energy Sector

Energy is the backbone of the economy and one of the primary targets of cyberattacks. How can critical infrastructure be protected in the era of energy transition, the growth of renewables, and the increasing digitalization of networks? A discussion on new technologies, the use of AI, the resilience of OT/IT systems, and how to build sector-wide security under geopolitical and regulatory pressure. AI in energy: from failure prediction to cyber defence.

The discussion, which were invited to participate (alphabetic order):

- **Radosław Dumański**, Expert at CERT PSE, Polskie Sieci Elektroenergetyczne SA

- **Mariusz Jurczyk**, CEO, TAURON Dystrybucja Pomiary, Board Advisor for Advanced Metering Infrastructure, TAURON Dystrybucja
- **Tomasz Małeck**, Vice President of the Management Board for Strategy, PGE
- **Aleksandra Walter**, Director, Digitalization and Security Department, Ministry of Energy
- **Marek Pisarczyk**, Head of the Telecommunications Department, Victor Energy

Moderated by:

- **Aleksandra Helbin**, Editor-in-Chief, WNP.PL

16 June 2026 | 12:30-13:30 | Ballroom C |  on-line transmission |  simultaneous interpreting PL|EN

Education as a Shield. The Academic Sector in Times of Change.

Universities are becoming an integral part of the national cyber security system. How can the guidelines of the National Cyber Security System be implemented in the academic environment — from securing IT systems to educating future professionals? A debate on university curricula, internal training, and implementation standards, as well as on how to reconcile regulatory requirements with the real organizational capacities of higher education institutions. Implementing the National Cyber Security System in practice. What does the role of a CISO look like in a large academic organization? Science and competencies for digital autonomy. From research to technology. Cyber sovereignty begins with a strong scientific base and the right skills.

The discussion, which were invited to participate (alphabetic order):

- **Krzysztof Mączka**, Data Protection Officer, ISMS Internal Auditor, Information Security and Personal Data Protection Department, WSB University
- **Tomasz Miłkowski**, retired Brigadier General of the State Protection Service, Director, Institute of Security Sciences, Humanitas University
- **Marek Pawełczyk**, Rector, Silesian University of Technology
- **Paweł Słoń**, Cooperation Expert, Cybersecurity Center, AGH University of Krakow
- **Michał Szczerbowski**, Data Protection Officer, University of Economics in Katowice

Moderated by:

- **Karolina Markowska**, Editor-in-Chief, PulsHR.pl

16 June 2026 | 12:30-13:30 | Ballroom B |  on-line transmission |  simultaneous interpreting PL|EN

Cyber Diplomacy and Poland's Technological Ambition. Can Poland Become an Exporter of Cyber Security?

Cyber security is becoming a new dimension of politics and the economy — an area where technological ambition can strengthen a nation's position. Does Poland have the potential to export cyber solutions, technologies, and expertise?

Experts will examine how international cooperation — at the governmental, startup, and investment levels — can help build an effective ecosystem supporting the global expansion of Polish companies. The discussion will cover, among others, the use of public and EU programs, the role of capital and managerial education, and the development of a recognizable "Polish cyber brand" on the global stage. This panel will focus on strategic thinking, ambition, and the opportunities that today determine a country's position in digital geopolitics.

The discussion, which were invited to participate (alphabetic order):

- **[Online] Michał Baranowski**, Undersecretary of State, Ministry of Economic Development and Technology
- **Artur Bicki**, CEO, Energy Logserver
- **Łukasz Gawron**, President of the Management Board, Polish Cybersecurity Cluster #CyberMadeInPoland
- **Paweł Hansdorfer**, Director of Foreign Markets, Asseco Data Systems
- **Joanna Pawełek-Mendez**, Minister-Counsellor for Cybersecurity, Security Policy Department, Ministry of Foreign Affairs

Moderated by:

- **Nikola Bochyńska**, Journalist, WNP.pl

16 June 2026 | 12:30-13:30 | Lower Lobby Stage |  on-line transmission

Cyber Security in Healthcare

The healthcare sector is among the most vulnerable to cyber threats. How can medical data, hospital systems, and medical devices be protected in the era of telemedicine and AI-driven diagnostics? A discussion on institutional resilience to cyber incidents, business continuity, and the need for security standards that keep pace with digital transformation. Cyber ambulance. Sectoral SOC.

The discussion, which were invited to participate (alphabetic order):

- **Krzysztof Brud**, Co-Founder, Board Advisor, Software Quality Expert, Soflab Technology
- **Janusz Cieszyński**, Member of the Polish Parliament, Minister of Digital Affairs in 2023, Undersecretary of State at the Ministry of Health from 2018 to 2020
- **Rafał Lityński**, Sectoral CSIRT Expert, CeZ
- **Klaudia Rogowska**, Director, Upper Silesian Medical Center of Prof. Leszek Giec of the Silesian Medical University in Katowice
- **Anna Sibilska**, Director, Information Security and Business Continuity Office, National Health Fund
- **Małgorzata Wywrot**, Project Manager, NIL IN - Network of Innovative Doctors, Polish Chamber of Physicians and Dentists, The School of Public Health, The Centre of Postgraduate Medical Education
- **Michał Zabojszcz**, Director, Independent Public Healthcare Institution of the Ministry of the Interior and Administration in Krakow

Moderated by:

- **Klara Klinger**, Editor-in-Chief, Rynek Zdrowia

16 June 2026 | 14:30-15:30 | Ballroom C |  on-line transmission |  simultaneous interpreting PL|EN

Smart Cities. How will Technology Reshape Urban Environments?

The NIS2 Directive, IoT, and municipal infrastructure. Water systems, transport, energy, and urban IoT are increasingly targeted by advanced attacks. How should local governments implement NIS2, manage supplier risks, and maintain system updates? A discussion on practical response scenarios, cyber hygiene, and investment priorities in smart cities.

1:1 conversation (15'):

- **Jacek Woźnikowski**, Director of the Department of Socio-Economic Development and Cooperation, Upper Silesian-Dąbrowa Basin Metropolis

The discussion, which were invited to participate (alphabetic order):

- **Agnieszka Olbrycht-Banach**, President of the Management Board, Silesian Metropolitan Network
- **Marcin Staniek**, Vice-Rector for Cooperation with the Socio-Economic Environment, Silesian University of Technology
- **Ewelina Włoch**, Head of the Digitalization and New Technologies Division, Rybnik City Hall
- **Łukasz Żółciak**, Smart City Officer, Investor Services Division, Katowice City Hall
- **Katarzyna Żółkiewska-Malicka**, Chief Security Officer (CSO), Maria Curie-Skłodowska University in Lublin, Director, ISSA Local, Poland

Moderated by:

- **Aneta Kaczmarek**, Editor-in-Chief, Portalsamorzadowy.pl

16 June 2026 | 14:30-15:30 | Ballroom B |  on-line transmission |  simultaneous interpreting PL|EN

Cyber Security in Industry

From Security by Design to incident response. As industrial processes become increasingly digitalized, the security of OT systems becomes critical to economic continuity. How can industrial environments — from energy to logistics — be protected in line with standards such as IEC 62443 and the principle of Security by Design? A discussion on IT/OT separation, the development of SOC/MDR capabilities, incident response, and how cyber security can strengthen the competitiveness of companies.

The discussion, which were invited to participate (alphabetic order):

- **Dawid Bazan**, Cybersecurity Lead Architect, Stellantis
- **Waldemar Chlebiak**, Head of Cyber Security, Siemens Poland
- **Mikołaj Śniatała**, Partner, Andersen
- **Dawid Wachowiak**, Digital Transformation and IT Director, TDJ
- **Zuzanna Wieczorek**, CEO, Tekniska

Moderated by:

- **Piotr Myszor**, Journalist, WNP.PL