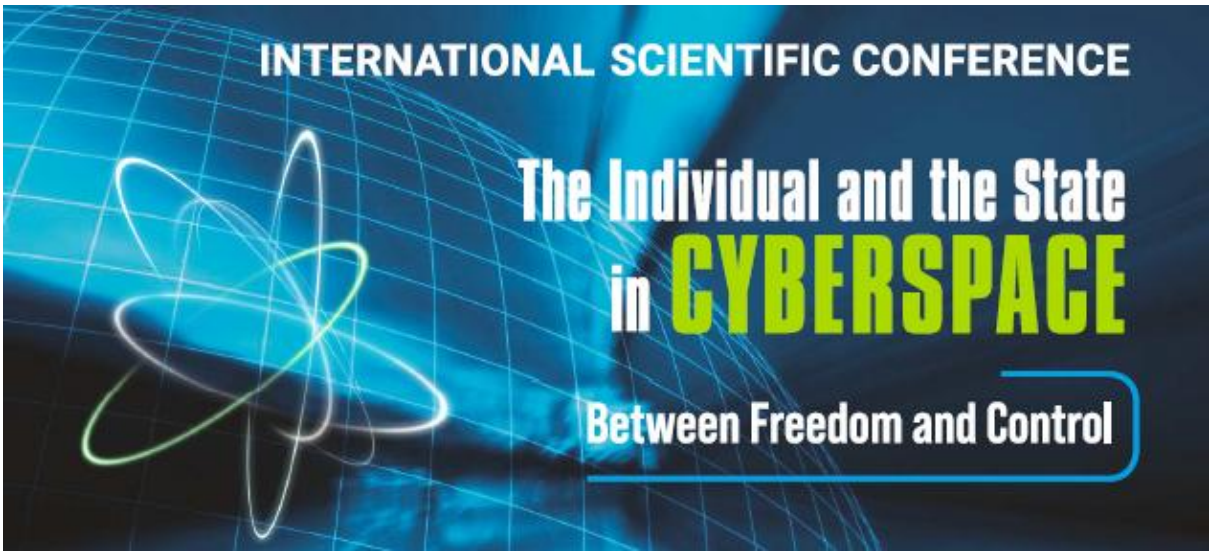
www.cyber.ukw.edu.pl

Redakcja/ Editors:
Marcin Jastrzębski, Izabela Kapsa & Kamila Sierzputowska

KSIĘGA ABSTRAKTÓW



BOOK OF ABSTRACTS

Organizatorzy / Organizers

Uniwersytet Kazimierza Wielkiego w Bydgoszczy | Wydział Nauk o Polityce i Administracji

Regionalny Ośrodek Debaty Międzynarodowej 2025–2026 wielkopolskie i kujawsko-pomorskie

Partnerzy Konferencji / Conference Partners

2026 ROK LUDZI FILMU Z KUJAW I POMORZA

Samorząd Województwa Kujawsko-Pomorskiego

KUJAWY POMORZE

Urząd Marszałkowski Województwa Kujawsko-Pomorskiego w Toruniu

Dofinansowano z budżetu Samorządu Województwa Kujawsko-Pomorskiego

2026 ROKIEM NSZZ SOLIDARNOŚĆ RI I BYDGOSKIEGO MARCA 1981

ORLEN

Patronat Honorowy/ Honorary Patronage

Ministerstwo Cyfryzacji

Wojewoda Kujawsko-Pomorski Michał Sztybel

Marszałek Województwa Kujawsko-Pomorskiego Piotr Całbecki

Prezydent Bydgoszczy Rafał Bruski

Patronat Honorowy Rektora Uniwersytetu Kazimierza Wielkiego prof. dr. hab. Bernarda Mendlika

NASK

Polskie Towarzystwo Nauk Politycznych

Patronat medialny/ Media Patronage

TVP3 Bydgoszcz

PiK Polskie Radio

20 lat UKW

Uniwersytet Kazimierza Wielkiego w Bydgoszczy

PROGRAM KONFERENCJI

PROGRAMME OF THE CONFERENCE

Miejsce obrad: BIBLIOTEKA UKW **Venue: Library of Kazimierz Wielki University**

Język panelu wskazany jest przez język, w którym podano tytuł panelu (polski lub angielski).

The language of each panel is indicated by the language used in the panel title (Polish or English).

Środa, 27 maja / Wednesday, May 27

12:00-12:30 - UROCZYSTE OTWARCIE KONFERENCJI / OPENING CEREMONY

12.30-13.30 - KEYNOTE SPEAKER: Prof. Andra Siibak, University of Tartu (Estonia), *Whose values and whose power matter in cyberspace?*

14.15-15.45 - SESJE PANELOWE / PANEL SESSIONS

2.1. Artificial Intelligence, Governance and Human Rights in the Digital Age

2.2. Cyberbezpieczeństwo i odporność organizacji w dobie transformacji cyfrowej

2.3. Między wolnością a kontrolą: społeczne i polityczne wyzwania cyberprzestrzeni

2.4. Dostępność cyfrowa i inkluzja społeczna w procesach transformacji cyfrowej

16:15 - 17:15 - KEYNOTE SPEAKER: Prof. Włodzisław Duch, Nicolaus Copernicus University in Toruń (Poland), *Artificial Intelligence: Threats and Hopes*

Czwartek, 28 maja / Thursday, May 28

12:30-14:00 - SESJE PANELOWE / PANEL SESSIONS

3.1. *Global Cyber Governance and the Politics of Digital Security*

3.2. *Media cyfrowe, edukacja i aktywizm w erze AI*

3.3. *Państwo i obywatel wobec zagrożeń wojny informacyjnej*

3.4. *Prawo, nadzór i ochrona jednostki w cyberprzestrzeni*

14:30-16:00 SESJE PANELOWE / PANEL SESSIONS

4.1. *Digital Society Between Innovation and Social Challenges*

4.2. *Sztuczna inteligencja, algorytmy i przyszłość demokracji*

4.3. *Cyberbezpieczeństwo i cyfryzacja usług publicznych*

16:00 - Podsumowanie i zamknięcie konferencji / Closing ceremony

Komitet Naukowy / Scientific Committee

- Przewodnicząca: dr hab. Izabela Kapsa, prof. ucz. (Uniwersytet Kazimierza Wielkiego w Bydgoszczy)
- prof. dr hab. Jolanta Itrich-Drabarek (Uniwersytet Warszawski)
- prof. dr hab. Magdalena Musiał-Karg (Uniwersytet im. Adama Mickiewicza w Poznaniu, Prezes PTNP)
- prof. dr hab. Paweł Malendowicz (Uniwersytet Kazimierza Wielkiego w Bydgoszczy, Prezes PTNP o/Bydgoszcz)
- ks. prof. dr hab. Piotr Roszak (Uniwersytet Mikołaja Kopernika, Uniwersyteckie Interdyscyplinarne Centrum Studiów nad Technologiami w Społeczeństwie)
- prof. dr hab. Marek Szewczyk (Uniwersytet Kaliski)
- Prof. Dr. Kamil Kardis (Prešovská Univerzita v Prešove)
- Prof. Dr. Jaroslav Usiak (Univerzita Mateja Bela v Banskej Bystrici)
- dr hab. Kamil Glinka, prof. UWr (Uniwersytet Wrocławski)
- dr hab. Michał Jacuński, prof. UWr (Przewodniczący Sekcji Badań nad Digitalizacją Procesów Demokratycznych PTNP, Chair Akcji COST CA23114)
- dr hab. Michał Kosman, prof. ucz. (Uniwersytet Kazimierza Wielkiego w Bydgoszczy, W-ce prezes PTNP o/Bydgoszcz)
- dr hab. Artur Laska, prof. ucz. (Uniwersytet Kazimierza Wielkiego w Bydgoszczy)
- dr hab. Arkadiusz Lewandowski, prof. ucz. (Uniwersytet Kazimierza Wielkiego w Bydgoszczy)
- Assoc. Prof. Dr. Linert Lireza (Aleksander Moisiu University of Durres)
- Assoc. Prof. Dr. Lorenzo Medici† (The Università degli Studi di Perugia)
- Assoc. Prof. Dr. Felix-Christopher von Nostitz (Université Catholique de Lille)
- Dr. Dmytro Khutkyy (Tartu Ülikool)
- dr Kamila Sierzputowska (Uniwersytet Kazimierza Wielkiego w Bydgoszczy)
- dr Agnieszka Pazderska (Uniwersytet Kazimierza Wielkiego w Bydgoszczy)
- dr Joanna Wieczorek-Orlikowska (Uniwersytet Kazimierza Wielkiego w Bydgoszczy)

Komitet Organizacyjny / Organizing Committee

- Przewodnicząca: dr Kamila Sierzputowska (Uniwersytet Kazimierza Wielkiego w Bydgoszczy)
- dr Marcin Jastrzębski (Uniwersytet Kazimierza Wielkiego w Bydgoszczy)
- dr Łukasz Mikołajczyk (Uniwersytet Kaliski)
- dr Jan Wiśniewski (Koordynator RODM wielkopolskie i kujawsko-pomorskie, Uniwersytet Mikołaja Kopernika w Toruniu)

KEYNOTE SPEAKER: Prof. **Andra Siibak,** University of Tartu (Estonia), ***Whose values and whose power matter in cyberspace?***

Andra Siibak is a Professor of Media Studies, and a Deputy Head of Research and Development at the Institute of Social Studies, University of Tartu. Her research focuses on opportunities and risks (e.g. surveillance, privacy issues, fake news, deepfakes, social engineering scams) surrounding the use of digital technologies and the internet, as well as inter-generational family life and communication practices in the era of datafication and platformisation. Together with Giovanna Mascheroni she has co-authored two monographs "*Datafied Childhoods: Data Practices and Imaginaries in Children's Lives*" (2021, Peter Lang), and "*Children and AI: Changing Digital Childhoods?"* (forthcoming in 2026, Palgrave). She is a member of Film, Media, and Visual Studies section of *Academia Europaea* and currently serves as the Vice President of the Association of Internet Researchers (AoIR).

KEYNOTE SPEAKER: Prof. **Włodzisław Duch,** Nicolaus Copernicus University in Toruń (Poland), ***Artificial Intelligence: Threats and Hopes***

Professor Włodzisław Duch is a faculty member in the Department of Applied Computer Science at Nicolaus Copernicus University, where he leads the Neurocognitive Laboratory. He is also the head of the Neuroinformatics and Artificial Intelligence group within the University Centre of Excellence Dynamics, Mathematical Analysis and Artificial Intelligence.

He has worked in many countries, including the United States, Japan, and Germany. He served as a visiting professor at the School of Computer Engineering, Nanyang Technological University (2003–2009), and later as a Nanyang Professor (2010–2012).

For two terms, he served as President of the European Neural Networks Society (2006–2008 and 2008–2011). In 2013, he was elected to the College of Fellows of the International Neural Networks Society. He is also a Fellow of the International Neural Networks Society (INNS), the Asia-Pacific Artificial Intelligence Association, the International Artificial Intelligence Industry Alliance, the World Academy of Artificial Consciousness, and a Life Senior Member of IEEE.

He served as Vice-Rector for Research and Informatization at Nicolaus Copernicus University (2012–2014), and later as Undersecretary of State (Deputy Minister) at the Ministry of Science and Higher Education of Poland, where he was responsible for science policy in Poland (2014–2015).

Extensive information about his activities, full CV, scientific publications, and lecture materials can be found on websites available by searching for "Wlodzislaw Duch" in Google or other internet search engines, as well as on YouTube.

Dr **Christopher Farrands**, Nottingham Trent University (UK), ***"Sovereign AI": myths, rhetorics and pragmatism***

Dr Chris Farrands is now retired from full time work, having most recently been the head of the International Relations team at Nottingham Trent University. Educated at University of Wales Aberystwyth and London School of Economics, he has worked extensively on technology and international political economy as well as on security and conflict issues and on the theory of international relations. He has also worked extensively for the Economist Intelligence Unit and Oxford Analytica on technology policy and technology cooperation in the European Union. He currently continues to do a small amount of graduate teaching together with research and examining.

Abstract: The paper will explore how the strategies of large firms with near monopoly characteristics ('monopoly competition') manage their relations with states and customers so as to ensure dominant positions in specific markets. It will explore how intellectual property and knowledge ownership including with respect to big data and AI enable large firms to shape the social space as well as the competitive environment in ways which undermine possibilities of individual agency and the potential for civil society responses. The paper will include case study work to be clarified in due course.

Keywords: large firms in cyberspace; intellectual property; corporate strategy; impacts on governance structures and individual agency

Assoc. Prof. Dr hab. **Łukasz Perlikowski** & MA **Oussama el Ouadie**, Nicolaus Copernicus University in Toruń (Poland), ***Artificial Intelligence between dialectics and demonstration***

Assoc. Prof. Dr hab. **Łukasz Perlikowski** pursued his studies in political science at Nicolaus Copernicus University in Toruń, where he completed both my BA and MA at the Faculty of Political Science and International Relations. Following his graduation, he began a PhD programme and successfully defended his doctoral dissertation in 2017, receiving honours for his critique of deliberative democracy through the lens of political philosophy and argumentation theory. Seven years later, he earned his habilitation degree for his research on political stability and subsequently attained the position of Associate Professor at Nicolaus Copernicus University. A defining aspect of his academic career is his commitment to fostering the international exchange of ideas and experiences. From 2022 to 2024, he served as Mobility Coordinator at the Faculty of Political Science and Security Studies at Nicolaus Copernicus University. His teaching activities are primarily focused on international studies for foreign students.

MA **Oussama el Ouadie**

The co-author of the presentation is Oussama El Ouadie (MA), student of International Politics and Diplomacy program at Faculty of Political Science and Security Studies NCU in Toruń.

Abstract: The two main approaches to knowledge that have been present in scientific and philosophical reflection since the dawn of civilization can be described using the Latin terms dialectica and demonstratio. Demonstrative knowledge, characteristic primarily of the exact sciences, assumes that there is an inviolable objective truth, and that the task of science, or more broadly, scientific thinking, is to present this truth as accurately as possible and to present it in the form of knowledge. The prime example here is mathematics, which provides proofs of true statements. In demonstratio, therefore, we are talking primarily about proof. The nature of proof is that its task is to establish as accurately and reliably as possible the relationship between a given statement and the corresponding state of affairs. Mathematical theorems are closely related to proofs that anchor them in the realm of truth. This is the level of precision to which all the so-called natural sciences aspire. Doubt and alternative ways of looking at a given problem are not always an advantage in this context. Certainty of knowledge is the greatest value we can obtain here. This alternative to demonstrative reasoning is dialectical reasoning. Dialectics concerns issues in which conjecture and uncertainty reign. A significant part of the reality inhabited by humankind exceeds the limits of objective cognition due to its complexity. Our argument regarding the assessment of AI is as follows. When we talk about artificial intelligence, we will focus on chatbots, which, regardless of the manufacturer's brand, present the same operating logic. They differ in quality and accuracy, but not in the conventions they operate within. Our argument is that by recognizing the emergence of AI chatbots as a revolutionary breakthrough in thinking, or even conscious machines, we are confusing two orders. This error consists of attributing demonstrative reasoning to the scope of tasks that belong to dialectical reasoning. The chat incarnation of artificial intelligence achieves a masterful level of demonstrative reasoning that is unattainable for humans. Bots resemble outstanding scholars, or even savants skilled in performing calculations of monstrous scale. In demonstrative reasoning, knowledge must be precise, and the certainty of the results testifies to the quality of the reasoning. It is contrary to the case of dialectical reasoning, which views the train of thought primarily as a process rather than as the shortest path to specific knowledge; it has always been, and continues to be, a source of creativity that allows us to identify problems and formulate the conditions and methods for solving them. Works based directly on chatbot query results are easy to recognize without complex tools. This is because they lack the dialectical factor. Instead, we receive knowledge and information – the tip of the iceberg visible above the surface of the water. The dialectical part, consisting of the paths to this knowledge, remains unknown to readers, authors, and the AI tools themselves, for which data remains the main raw material.
Keywords: artificial intelligence, ChatGPT, chatbots, dialectis, demonstratio, theory of argumentation

Dr hab. **Maciej Potz**, University of Łódź (Poland), ***Human rights under pressure: a future-oriented conception of universal rights***

Dr hab., profesor uczelni w Katedrze Systemów Politycznych WSMiP UŁ. Jego zainteresowania naukowe obejmują m.in. teorię polityki, politologię religii, biopolitologię oraz wpływ innowacji technologicznych i zmian społecznych na przyszłość polityki. W latach 2022-26 kierownik

projektu pt. "Polityka zakonna: władza i status w zakonach. Badanie empiryczne polskiego monastycyzmu" w ramach konkursu OPUS NCN. W roku akademickim 2021/22 Visiting Scholar w Uniwersytecie Stanforda w USA w ramach programu im. Bekkera NAWA.

Abstract: Rapid technological progress, including advances in AI and bioengineering, raises concerns about the threats these processes pose to human rights in areas such as freedom, equality, privacy, or employment. However, future political community will itself change in profound ways. Fundamentally, it may consist of various categories of beings, human and non-human – such as animals, cyborgs, AI-algorithms, embodied or not – with mental characteristics similar to, or surpassing, those of humans, by virtue of which these beings may acquire moral and political status.

In this context, the anthropocentric conception of "human rights" may itself become an oppressive and exclusionary idea promoting the interests of one category of beings – one species – over others who may, too, have a valid moral claim to rights. The claim rests on characteristics such as sentience, self-consciousness, empathy or intelligence, that entitle to full or partial attribution of rights.

In the posthuman society, human rights will need to be replaced with a more inclusive system protecting all members of its political pluriverse. I develop such future-oriented universal conception of rights based on fundamental principles of interest protection, non-speciesism, capacity differentiation and substrate-independence. I also postulate extending political representation to all sentient beings, while enabling political participation of moral agents (intelligent and self-conscious beings). Such blueprint for a just universal citizenship will equip future political systems with normative/legal means to address challenges brought by transhumanism and technological progress.

Keywords: human rights; universal rights; speciesism; future society; future politics; transhumanism.

Dr **Mentor Beqa**, PhD, Aleksandër Moisiu University, Durrës (Albania), ***From Digital Governance to Algorithmic Authority: Rethinking the State in Cyberspace***

Dr. Mentor Beqa is a Senior Lecturer in International Politics and Research Methods at the Faculty of Law and Political Sciences, "Aleksandër Moisiu" University, Durrës, and Executive Director of the Institute of Political Studies "Sami Frashëri." His academic trajectory combines training in journalism (University of Tirana), international security (University of Geneva), and political science (PhD in International Relations, European University of Tirana), forming an interdisciplinary foundation that informs both his empirical and theoretical work.
His scholarly contribution is situated at the intersection of digitalisation, governance, and democracy, with a particular focus on how technological transformations reshape state authority, public administration, and political communication. His recent research engages with questions of algorithmic governance, digital public services, and the reconfiguration of democratic legitimacy under conditions of increasing technological mediation. In parallel, he maintains an active research agenda on national and international security, with specific attention to regional security dynamics, strategic policy, and the evolving architecture of cooperation in the Western Balkans.

Dr. Beqa has published in peer-reviewed academic journals and contributed to policy-oriented research at national, regional, and international levels. His work is characterised by an effort to bridge theoretical innovation – particularly in international political theory and research methodology – with applied policy analysis, especially in contexts of institutional transformation and uncertainty.

In recent years, his research has expanded to include communism and transitional justice in post-communist societies, examining the long-term institutional and societal consequences of authoritarian legacies. In this capacity, he was elected by the Albanian Parliament as a member of the Governing Board of the Institute for the Study of the Crimes and Consequences of Communism (ISKK), where he has served as Chair since April 2025.

His broader academic interests include digital governance, democracy, international politics, geopolitics, European integration, and transitional justice, with an overarching emphasis on how structural transformations – technological, political, and institutional – interact in shaping contemporary governance and security environments.

Abstract: The rapid integration of algorithmic systems into public administration and governance processes has generated a qualitative shift in the architecture of state authority. While existing literature predominantly conceptualizes digital technologies as instruments that enhance state capacity, this paper argues that certain configurations of artificial intelligence and automated decision-making systems are progressively acquiring attributes of authority themselves. This transformation challenges the conventional understanding of the state as a centralized, human-driven locus of decision-making grounded in legal-rational legitimacy. The paper develops a conceptual framework to capture this transition from digital governance to algorithmic authority. It distinguishes between three analytical stages: (1) digital augmentation, where technologies function as administrative tools; (2) algorithmic mediation, where decision-making is structured through computational systems; and (3) algorithmic ascendance, where systems operate with a degree of autonomy that reshapes accountability, discretion, and legitimacy. Through this framework, the paper examines how authority is redistributed across human and non-human actors, leading to forms of governance that are increasingly opaque, diffused, and temporally accelerated.

Methodologically, the paper adopts a conceptual-analytical approach grounded in contemporary debates on governmentality, performativity, and digital sovereignty. It engages with empirical illustrations from recent developments in AI-assisted governance to demonstrate how algorithmic systems are framed as neutral, objective, and efficient, thereby reinforcing their acceptance as legitimate decision-making entities. Particular attention is paid to the tension between claims of enhanced efficiency and the erosion of transparency and contestability. By reframing algorithmic systems as emerging sites of authority rather than mere tools, the paper contributes to ongoing debates on the transformation of the state in the digital age. It proposes that the central question is no longer how states use technology, but how authority itself is being reconstituted within hybrid human-algorithmic assemblages in cyberspace.

Keywords: algorithmic authority; digital governance; artificial intelligence; state transformation; legitimacy; governmentality; algorithmic decision-making; cyber-politics; digital sovereignty; hybrid governance systems

Prof. PhD LLM. DSc **Ilin Savov**, Trakia University (Bulgaria), ***Cyber Risk and Protection in the Age of Quantum Communication***

Director of Scientific Institute of security and alimentary sustainability at Trakia University. He is full professor, doctor and doctor of science on the field of "National Security". In 2000, he began his professional career as an intelligence officer in the security services of the Republic of Bulgaria. In 2013 he defended his first doctorate degree at the Academy of Ministry of Interior of Republic of Bulgaria. In 2021 he defended his second doctorate degree “Doctor of Science” at Military Academy of Republic of Bulgaria. From 2022 to December 2023, he was a Commissioner, Deputy rector of the Academy of the Ministry of the Interior. He trains investigative police officers and operatives in crime prevention structures in Bulgaria, Latvia, Lithuania, Estonia, the Czech Republic, Poland, Romania, Greece and other countries. He conduct classes and lectures as full professor at Trakia University, Sofia University, Plovdiv University, New Bulgarian University, Academy of the Ministry of Interior and Military Academy in Republic of Bulgaria. Author of over 90 publications (10 monographic books) on the field of intelligence and defense of national security. He is an established expert on national and international security issues, as well as operational-search and operational-technical activities for protection against international organized criminial groups. Delivers a number of reports at prestigious scientific forums in the Republic of Bulgaria and abroad. As a scientist, he conducts research on regulations legal issues in the area of management and functioning of the security services and the Ministry of the Interior, alimentary sustainability, cyber security, human trafficking, migration processes, the use and control of special intelligence tools and traffic data in the Republic of Bulgaria, the EU and the USA. He is a member of the Union of Scientists in the Republic of Bulgaria and the International Police Association (IPA).

Abstract: The accelerating convergence between quantum technologies, artificial intelligence and global digital interconnectivity is reshaping the foundations of cybersecurity, institutional resilience and strategic protection. This report examines the emerging cyber risks associated with the transition toward quantum communication infrastructures and the broader implications for governments, critical sectors and private organisations operating in an increasingly hostile digital environment. The analysis focuses on the growing vulnerability of traditional cryptographic mechanisms in the context of future quantum computing capabilities. Particular attention is given to the strategic risk known as “harvest now, decrypt later”, where encrypted information collected today may become readable in the future once cryptographically relevant quantum computers mature. The presentation explores why this challenge is no longer a distant theoretical concern, but an active strategic issue already influencing national policies, international standards, cyber resilience planning and long-term data protection strategies. The transition to the quantum era will not occur through a single technological breakthrough, but through a gradual restructuring of trust systems, security models and institutional decision-making processes. For this reason, preparation, strategic sequencing and interdisciplinary cooperation are becoming critical factors for sustainable cyber protection in the next decade.

Keywords: quantum technologies; cybersecurity; post-quantum cryptography; harvest now, decrypt later; cyber resilience; critical infrastructure; data protection; institutional resilience

Cyberbezpieczeństwo i odporność organizacji w dobie transformacji cyfrowej

dr inż. **Łukasz Apiecionek**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Wybrane mechanizmy sztucznej inteligencji do wykrywania zagrożeń systemów informatycznych***

Kierownik Katedry Cyberbezpieczeństwa na Wydziale Informatyki, Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Przewodniczący rady kierunku cyberbezpieczeństwo. Adiunkt na Wydziale Informatyki Uniwersytetu Morskiego w Gdyni. Wykładowca z zakresu cyberbezpieczeństwa i sztucznej inteligencji.

Abstrakt: W artykule przedstawiono rozmyte mechanizmy sztucznej inteligencji do klasyfikacji danych na potrzeby cyberbezpieczeństwa. Systemy informatyczne są narażone na ataki mające na celu nieuprawnione pozyskanie danych lub zakłócenie działania systemu. W związku z tym rośnie znaczenie metod analizy danych uwzględniających niepewność informacji. Celem badań była implementacja mechanizmów sztucznej inteligencji: rozmytej głębokiej sztucznej sieci neuronowej, hybrydowej sieci konwolucyjnej, klasyfikacji k najbliższych sąsiadów oraz redukcji wymiarów poprzez analizę składowych głównych. Badania koncentrują się na konstrukcji mechanizmów umożliwiających wykrywanie wzorców ataków i klasyfikację pakietów sieciowych uwzględniając niepewność danych. Opracowane mechanizmy działają z wykorzystaniem skierowanych liczb rozmytych reprezentujących dane niepewne. Wykonane eksperymenty potwierdziły skuteczność zastosowanego podejścia, wskazując na zasadność wykorzystania mechanizmów sztucznej inteligencji w analizie zagrożeń cybernetycznych, jednocześnie pozwalając na redukcję wymaganych architektur rozwiązań. Redukcja architektur nie odbywa się kosztem jakości rozwiązań. Dzięki temu, możliwa jest implementacja mechanizmów na urządzeniach brzegowych, szczególnie na platformach mobilnych pracujących z zasilaniem bateryjnym, gdzie oszczędza się moc obliczeniową niezbędną do ich działania.

Słowa kluczowe: skierowane liczby rozmyte, sieci neuronowe, cyberbezpieczeństwo

dr hab. inż. **Joanna Panek**, prof. WAT, Wojskowa Akademia Techniczna,

Od VUCA do BANI: implikacje dla bezpieczeństwa i odporności łańcuchów dostaw

Dawniej Joanna Nowakowska-Grunt, jest pracownikiem Wydziału Bezpieczeństwa, Logistyki i Zarządzania Wojskowej Akademii Technicznej. Specjalizuje się w problematyce zarządzania łańcuchem dostaw, bezpieczeństwa systemów logistycznych oraz implementacji standardów ESG. Autorka licznych publikacji z zakresu odporności i zrównoważonego zarządzania łańcuchami dostaw.

Abstrakt: Współczesne łańcuchy dostaw funkcjonują w warunkach narastającej niestabilności, która wykracza poza klasyczne ujęcie VUCA. O ile koncepcja VUCA opisuje środowisko zmienne, niepewne, złożone i niejednoznaczne, o tyle nowsze podejście BANI wskazuje na jego kruchość, nieliniowość oraz nieuchwytność poznawczą. Celem artykułu jest analiza implikacji

przejścia od logiki VUCA do BANI dla bezpieczeństwa i odporności łańcuchów dostaw. Podjęto w nim próbę identyfikacji kluczowych wyzwań zarządczych oraz mechanizmów adaptacyjnych, takich jak redundancja, dywersyfikacja, cyfryzacja i integracja kryteriów ESG oraz wskazano, że w warunkach BANI podejścia tradycyjne oparte na optymalizacji i predykcji okazują się być niewystarczające, a kluczowe znaczenie zyskuje zdolność organizacji do absorpcji zakłóceń, uczenia się oraz elastycznego reagowania na wyzwania otoczenia. Wyniki analizy podkreślają konieczność redefinicji paradygmatu zarządzania łańcuchem dostaw w kierunku budowania odporności systemowej i bezpieczeństwa operacyjnego.

Słowa kluczowe: bezpieczeństwo łańcuchów dostaw, VUCA, BANI

Między wolnością a kontrolą: społeczne i polityczne wyzwania cyberprzestrzeni

dr inż. **Katarzyna Kazimierska**, dr inż. **Mateusz Wirwicki**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Sztuczna inteligencja w służbie państwa i obywatela – szanse, zagrożenia i granice zaufania***

Katarzyna Kazimierska – Prodziekan ds. kształcenia na Wydziale Mechatroniki Uniwersytetu Kazimierza Wielkiego w Bydgoszczy, specjalizująca się w zastosowaniach sztucznej inteligencji, analizie danych oraz nowoczesnych technologiach cyfrowych. Certyfikowany trener AI, prowadzi szkolenia dla środowisk akademickich, biznesowych i prawniczych, koncentrując się na praktycznym wykorzystaniu AI, bezpieczeństwie danych oraz wyzwaniach regulacyjnych. Absolwentka programu MIT Professional Education „Breakthrough Innovation: Harnessing AI to Create Value".

Mateusz Wirwicki zajmuje się wdrażaniem sztucznej inteligencji w pracy naukowej, dydaktyce oraz działalności organizacji. Koncentruje się na tym, jak wykorzystywać narzędzia AI w sposób świadomy i efektywny, uwzględniając ich możliwości, ale również ograniczenia, takie jak generowanie nieprecyzyjnych lub błędnych treści. Prowadzi szkolenia i warsztaty dla firm, środowiska edukacyjnego oraz administracji, skupiając się na rozwijaniu praktycznych umiejętności pracy z AI – od tworzenia skutecznych zapytań po ocenę wiarygodności uzyskiwanych wyników. W swoich działaniach uwzględnia także zagadnienia związane z bezpieczeństwem informacji, etyką oraz odpowiedzialnym wykorzystaniem danych, podkreślając rolę krytycznego podejścia do technologii w dynamicznie zmieniającym się środowisku cyfrowym.

Abstrakt: Wystąpienie koncentruje się na praktycznym wykorzystaniu sztucznej inteligencji w pracy naukowej i edukacji oraz jej wpływie na funkcjonowanie jednostki w cyberprzestrzeni. Pokazuje przejście od „hype'u" do realnej wartości AI, wyjaśniając, jak działają modele językowe oraz dlaczego generują błędy i halucynacje. Omówione zostają kluczowe narzędzia AI oraz zasady ich świadomego doboru w zależności od zadania. Szczególny nacisk położono na kompetencje użytkownika – umiejętność formułowania zapytań (*prompt engineering*), krytycznej weryfikacji informacji oraz odpowiedzialnego korzystania z danych. Wystąpienie

porusza również kwestie bezpieczeństwa, prywatności i etyki, wskazując, że AI może być zarówno narzędziem wsparcia, jak i źródłem ryzyka. W kontekście relacji jednostka–państwo podkreślono znaczenie świadomego i krytycznego korzystania z AI jako kluczowej kompetencji cyfrowej.

Słowa kluczowe: sztuczna inteligencja, modele językowe, *prompt engineering*, bezpieczeństwo i prywatność, kompetencje cyfrowe

dr **Przemysław Kwiatkowski**, WSB Merito Toruń, ***UE wobec zwalczania dezinformacji w sieci: architektura regulacyjna, egzekwowanie prawa i wyzwania technologiczne***

Doktor nauk humanistycznych w dziedzinie nauk o polityce, amerykanista oraz ekspert ds. stosunków międzynarodowych i bezpieczeństwa. Z Uniwersytetem WSB Merito w Toruniu jest związany nieprzerwanie od 2008 roku, gdzie aktualnie pełni funkcję Prodziekana Wydziału Finansów i Zarządzania. W swojej pracy z powodzeniem łączy wiedzę akademicką z praktycznym doświadczeniem zdobytym podczas realizacji projektów we współpracy z partnerami zagranicznymi.

Abstrakt: Cele artykułu jest prezentacja aktualnej konstrukcji europejskiej architektury zwalczania dezinformacji, wskazując na radykalne przejście od miękkich zaleceń do twardego egzekwowania prawa. Centralnym filarem tego systemu jest Akt o usługach cyfrowych (DSA), który nakłada na największe platformy internetowe (VLOP) rygorystyczny obowiązek mitygacji ryzyk systemowych, przewidując kary sięgające do 6% ich rocznego, globalnego obrotu. Zagrożenia drastycznie potęguje rozwój sztucznej inteligencji. Z jednej strony generuje ona masowy, motywowany korzyściami finansowymi syntetyczny szum ("AI Slop"), z drugiej – wzmacnia asymetryczne, zagraniczne ingerencje wrogich aktorów (zarówno państwowych, jak i niepaństwowych), które Unia zwalcza prewencyjnie uderzając w infrastrukturę sprawców m.in. poprzez "Deterrence Playbook". Odpowiedzią na zagrożenia związane z tzw. deepfake jest z kolei AI Act, wymuszający wyraźne oznaczanie treści syntetycznych. Mimo koordynacji na szczeblu unijnym (np. w ramach nowej Europejskiej Tarczy Demokracji), słabym ogniwem pozostaje powolna transpozycja przepisów na poziomie krajowym – luki te, widoczne chociażby na przykładzie Polski, nadal pozwalają korporacjom na masowe ignorowanie zgłoszeń dezinformacji.

Słowa kluczowe: dezinformacja i FIMI, Akt o usługach cyfrowych, Europejska Tarcza Demokracji, AI Slop

dr **Joanna Grubicka**, Uniwersytet Pomorski w Słupsku, ***Bezpieczeństwo personalne jednostki w cyberprzestrzeni w kontekście ochrony infrastruktury krytycznej – między autonomią a systemem kontroli***

Doktor nauk technicznych w dyscyplinie automatyka i robotyka, absolwentka Instytutu Badań Systemowych PAN w Warszawie. Adiunkt w Instytucie Bezpieczeństwa i Socjologii Uniwersytetu Pomorskiego w Słupsku oraz kierownik Zakładu Bezpieczeństwa Cyberprzestrzeni

w Katedrze Bezpieczeństwa Narodowego. Członkini Polskiego Towarzystwa Informatycznego, Oddział Kujawsko-Pomorski. Należy do zespołów redakcyjnych czasopism naukowych *Social Development & Security* oraz *Studia nad Bezpieczeństwem*. Współpracuje z Pracownią Badań Społecznych Pionu Rozwoju Społeczeństwa Informacyjnego NASK w Warszawie przy realizacji projektów badawczych. Autorka i współautorka publikacji naukowych z zakresu niezawodności obiektów technicznych, społeczeństwa cyfrowego i bezpieczeństwa cyfrowego. Współautorka monografii *Bezpieczeństwo cyfrowe. Perspektywa organizacyjna* (Difin, 2023), *Przestrzeń cyfrowa w ponowoczesności. Jednostka – technologia – profilaktyka* (Difin, 2024) oraz *Innowacje a cyfryzacja. Między teorią a praktyką* (CeDeWu, 2025), a także autorka monografii *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni – studium z zakresu bezpieczeństwa personalnego* (Wydawnictwo Uniwersytetu Pomorskiego w Słupsku, 2025). Jej zainteresowania badawcze koncentrują się wokół wpływu nowoczesnych technologii na organizacje i społeczeństwo oraz problematyki bezpieczeństwa w cyberprzestrzeni.

Abstrakt: Dynamiczny rozwój technologii informacyjno-komunikacyjnych oraz postępująca cyfryzacja infrastruktury krytycznej prowadzą do zasadniczej zmiany charakteru współczesnych zagrożeń bezpieczeństwa. Infrastruktura krytyczna, obejmująca m.in. sektor energetyczny, transportowy, zdrowotny czy administracyjny, staje się coraz częściej celem zaawansowanych cyberataków, których skutki wykraczają poza wymiar techniczny i instytucjonalny, bezpośrednio oddziałując na bezpieczeństwo personalne jednostki. Wzrost liczby incydentów cybernetycznych oraz ich rosnąca złożoność wskazują, że cyberzagrożenia mają charakter systemowy i wielowymiarowy, obejmując zarówno aspekty technologiczne, jak i społeczne oraz psychologiczne. Celem wystąpienia jest analiza relacji pomiędzy cyberbezpieczeństwem infrastruktury krytycznej a bezpieczeństwem personalnym jednostki w kontekście napięcia pomiędzy potrzebą zapewnienia ochrony a stosowaniem mechanizmów kontroli państwa. W rozważaniach przyjęto perspektywę sekuritologiczną oraz podejście systemowe, które umożliwiają ukazanie współzależności między jednostką, środowiskiem cyfrowym oraz instytucjonalnymi strukturami bezpieczeństwa. Szczególną uwagę poświęcono roli regulacji prawnych, w tym dyrektywy NIS2, oraz mechanizmom nadzoru i zarządzania ryzykiem, które – mimo że zwiększają poziom ochrony infrastruktury – mogą jednocześnie prowadzić do ograniczenia autonomii jednostki i intensyfikacji kontroli w cyberprzestrzeni. W wystąpieniu wskazano, że zagrożenia dla infrastruktury krytycznej generują realne konsekwencje dla życia, zdrowia, prywatności oraz poczucia bezpieczeństwa jednostki, czyniąc ją kluczowym i najbardziej wrażliwym elementem systemu bezpieczeństwa. Podkreślono również, że skuteczna ochrona przed cyberzagrożeniami wymaga zintegrowanego podejścia, łączącego rozwiązania technologiczne, regulacyjne oraz edukacyjne, przy jednoczesnym zachowaniu równowagi pomiędzy bezpieczeństwem a wolnością w cyberprzestrzeni.

Słowa kluczowe: cyberbezpieczeństwo, infrastruktura krytyczna, bezpieczeństwo personalne, cyberzagrożenia, kontrola państwa, NIS2, cyberprzestrzeń

dr **Ewa Maria Włodyka**, Politechnika Koszalińska, ***Między integracją a dezinformacją: uchodźcy z Ukrainy w polskiej cyberprzestrzeni jako wyzwanie dla e-administracji i odporności cyfrowej państwa***

Politolożka, adiunkt w Katedrze Nauk o Polityce Wydziału Humanistycznego Politechniki Koszalińskiej. Realizuje badania w obszarze nauk o polityce i administracji: m.in. samorząd terytorialny, administracja publiczna i e-administracja, partycypacja obywatelska. samorządowiec. Kierownik projektu badawczego MINIATURA 8 (NCN) w 2025r., w ramach którego analizowała potencjał konsolidacji struktur lokalnych Ukrainy z wykorzystaniem sztucznej inteligencji oraz kapitału społecznego reemigrantów. Autorka licznych publikacji i konferencji naukowych.

Abstrakt: Napływ uchodźców z Ukrainy po 2022 roku ujawnił kluczową rolę cyberprzestrzeni w procesach integracji społecznej, komunikacji publicznej oraz zarządzania państwem. Celem referatu jest analiza funkcjonowania migrantów ukraińskich w polskiej cyberprzestrzeni w kontekście e-governance, cyberdemokracji oraz odporności cyfrowej państwa. Uwaga w wystąpieniu zostanie skierowana na wykorzystanie narzędzi cyfrowych przez administrację publiczną oraz aktywności samych migrantów w okresie kryzysu migracyjnego z 2022 roku. Analiza wskazuje, że poziom kompetencji cyfrowych migrantów oraz jakość komunikacji publicznej mają istotne znaczenie dla skutecznej integracji oraz bezpieczeństwa informacyjnego państwa. Wnioski obejmują rekomendacje dla polityk publicznych w zakresie zarządzania wielopoziomowego i cyberbezpieczeństwa. W jakim zakresie problem dezinformacji jako element zagrożeń hybrydowych dotknął administrację i środowisko migrantów z Ukrainy? Jaki wpływ mają doświadczenia z okresu przebywania w Polsce ukraińskich imigrantów dla wzmacniania demokratycznych mechanizmów sprawowania władzy i stabilizację społeczeństwa obywatelskiego? Na te i inne pytania badawcze w ramach referatu zostaną w odpowiedzi przedstawione częściowe wyniki badania naukowego, przeprowadzonego w ramach grantu NCN Miniatura 8 pt.: "Potencjał konsolidacji samorządu terytorialnego w Ukrainie z perspektywy ukraińskich imigrantów w Polsce, z uwzględnieniem implementacji sztucznej inteligencji w administracji publicznej samorządu", realizowanego w 2025r. Analiza wskazuje, że poziom kompetencji cyfrowych migrantów oraz jakość komunikacji publicznej mają istotne znaczenie dla skutecznej integracji oraz bezpieczeństwa informacyjnego państwa. Wnioski obejmują rekomendacje dla polityk publicznych w zakresie zarządzania wielopoziomowego i cyberbezpieczeństwa.

Słowa kluczowe: e-administracja, migracja, Polska, Ukraina, administracja publiczna, samorząd terytorialny, odporność cyfrowa, kompetencje cyfrowe

mgr **Anna Szorc**, dr hab. **Aleksandra Błachnio** prof. ucz., Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Postawy wobec uchodźców przykładem wolności czy utraty kontroli? Raport z adaptacji nowego narzędzia***

mgr **Anna Szorc**, psycholog badający postawy wobec uchodźców w kontekście współczesnych procesów migracyjnych w Europie. Koncentruje się na adaptacji narzędzi psychometrycznych do warunków polskich oraz ich zastosowaniu w analizie postaw społecznych. W badaniach łączy perspektywę psychologiczną z analizą kontekstu społeczno-politycznego i informacyjnego.

Dr hab. **Aleksandra Błachnio** [ORCID 0000-0003-0756-7416] kierownik Katedry Psychologii Osobowości na Uniwersytecie Kazimierza Wielkiego w Bydgoszczy oraz pracownik Akademii

Nauk Społecznych w Elblągu. Naukowo interesuje się jakością życia, starzeniem się, globalizacją, rewolucją cyfrową i odpornością psychiczną. Autorka kilku monografii: *Potencjał osób w starości. Poczucie jakości życia w procesie starzenia się* (2019); *Starość non profit*: *wolontariat na Uniwersytetach Trzeciego Wieku w Polsce i na świecie* (2012); *Człowiek autorski w erze globalizacji* (2011). Tłumaczka *Psychologii starzenia* się Stuarta-Hamiltona z 2006 czy redakcji Sędka, Hessa i Tourona *Wielościenność ścieżek starzenia się poznawczego. Wpływy motywacyjne i kontekstowe* z 2025 roku.

Abstrakt: Od 2022 r. obserwujemy dynamiczne zmiany w geopolityce europejskiej. Wojna Rosji z Ukrainą wpisała w biografię narodu polskiego na trwałe doświadczenie kohabitacji z uchodźcami. Niemniej zmienia się ono od braterskiej solidarności po gorące debaty publiczne nad konsekwencjami społeczno-ekonomicznymi migracji. W toczących się sporach krytycznymi są postawy wobec uchodźców. Brakuje rzetelnych i aktualnych narzędzi do ich pomiaru. Stąd celem wystąpienia jest popularyzacja polskiej adaptacji narzędzia Short Attitudes Towards Refugees Scale (SATRS). W odróżnieniu od klasycznych ujęć, koncentrujących się głównie na dystansie społecznym, SATRS obejmuje kompletny tj. poznawczy, emocjonalny oraz behawioralny pomiar postaw umożliwiając pogłębioną i wielowymiarową analizę problemu. Obok zaprezentowania procesu adaptacji kulturowej narzędzia, akcent położony jest na praktyczne walory SATRS. Monitorowanie zmian postaw w czasie sprzyja kontroli skuteczności działań informacyjnych, kształtowaniu polityki wobec kryzysu migracyjnego i bezpieczeństwa informacyjnego państwa. Wystąpienie wpisuje rzetelną diagnozę psychologiczną w aktualny obszar transformacji społecznych i cyfrowych kraju.

Słowa kluczowe: kryzys migracyjny, bezpieczeństwo, postawy wobec uchodźców, adaptacja kulturowa

Dostępność cyfrowa i inkluzja społeczna w procesach transformacji cyfrowej

dr hab. **Małgorzata Sikora-Gaca**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Od transferu do inkluzji: dostępność cyfrowa jako nowy wymiar polskiej polityki rozwojowej wobec państw Partnerstwa Wschodniego***

Politolożka, adiunkt na Wydziale Nauk o Polityce i Administracji Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Jej zainteresowania badawcze koncentrują się wokół polityki rozwojowej, oficjalnej pomocy rozwojowej (ODA), współpracy Unii Europejskiej z państwami Partnerstwa Wschodniego oraz roli Polski jako dawcy pomocy rozwojowej. Autorka monografii „Od pomocy dla krajów rozwijających się do partnerstwa na rzecz rozwoju. Analiza politologiczna problemu wraz ze studium przypadku relacji polsko-mołdawskich w latach 1998–2023", w której analizuje ewolucję globalnego i regionalnego systemu pomocy rozwojowej oraz znaczenie transformacyjnego know-how Polski. W swoich najnowszych

badaniach podejmuje problematykę dostępności (w tym dostępności cyfrowej) jako elementu polityk publicznych i działań rozwojowych, łącząc perspektywę politologiczną z praktyką wdrażania projektów rozwojowych.

Abstrakt: Artykuł podejmuje problematykę dostępności cyfrowej jako nowego, dotychczas niedostatecznie rozpoznanego wymiaru polityki rozwojowej, realizowanej przez Polskę wobec państw Partnerstwa Wschodniego. W literaturze przedmiotu dominują analizy koncentrujące się na wielkości transferów finansowych, efektywności oficjalnej pomocy rozwojowej (ODA) oraz instytucjonalnych uwarunkowaniach współpracy międzynarodowej. Znacznie rzadziej podejmowany jest natomiast wątek jakościowego wymiaru rozwoju, w tym dostępności i inkluzywności projektów realizowanych w obszarze cyfryzacji.

Celem artykułu jest odpowiedź na pytanie, czy i w jakim zakresie dostępność cyfrowa stanowi element systemowy polskiej polityki rozwojowej wobec państw Partnerstwa Wschodniego, a także identyfikacja jej znaczenia jako narzędzia ograniczania wykluczenia cyfrowego. W ujęciu teoretycznym artykuł odwołuje się do koncepcji rozwoju inkluzywnego oraz traktowania polityki rozwojowej jako instrumentu polityki zagranicznej i soft power. W warstwie empirycznej zastosowano analizę jakościową wybranych projektów rozwojowych realizowanych w państwach Partnerstwa Wschodniego, ze szczególnym uwzględnieniem Republiki Mołdawii jako studium przypadku.

Wyniki przeprowadzonych analiz wskazują, że dostępność cyfrowa nie stanowi jeszcze w pełni zinstytucjonalizowanego komponentu polskiej pomocy rozwojowej, a jej obecność w projektach ma charakter fragmentaryczny i niesystemowy. Jednocześnie rosnące znaczenie cyfryzacji usług publicznych oraz e-administracji powoduje, że brak uwzględnienia standardów dostępności może prowadzić do pogłębiania wykluczenia społecznego w przestrzeni cyfrowej. W odpowiedzi na zidentyfikowane luki autorka proponuje model trójpoziomowego ujęcia dostępności w polityce rozwojowej, obejmujący wymiar infrastrukturalny, kompetencyjny oraz instytucjonalny. Wnioski z badań wskazują na konieczność włączenia dostępności cyfrowej do głównego nurtu projektowania i realizacji działań w ramach ODA, co stanowi warunek przejścia od modelu transferowego do modelu inkluzywnego rozwoju.

Słowa kluczowe: polityka rozwojowa, dostępność cyfrowa, Official Development Assistance (ODA), Eastern Partnership, digital inclusion

dr **Barbara Panciszko-Szweda**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy,

Dostępność cyfrowa na obszarach wiejskich w Polsce – wyzwania w kontekście zapewnienia dostępu do usług publicznych

Doktor nauk społecznych w dziedzinie nauk o polityce, magisterium europeistyki (2013) i ekonomii (2014) uzyskane na Uniwersytecie Wrocławskim, adiunkt w Katedrze Polityki Innowacyjności i Zrównoważonego Rozwoju na Uniwersytecie Kazimierza Wielkiego w Bydgoszczy; zainteresowania badawcze: zrównoważony rozwój obszarów wiejskich, koncepcja *smart villages*, Wspólna Polityka Rolna Unii Europejskiej, bezpieczeństwo żywnościowe, nowe technologie w rolnictwie i produkcji żywności zwłaszcza inżynieria genetyczna, integracja europejska oraz polityka dostępności; ekspert w obszarze planowania rozwoju lokalnego.

Abstrakt: Uchwalenie w 2016 r. Dyrektywy zobowiązującej instytucje publiczne do zapewniania dostępności cyfrowej spowodowało konieczność transpozycji jej przepisów do krajowych porządków prawnych. W 2019 r. przyjęto w Polsce ustawę, która implementowała zapisy dyrektywy (EU) 2016/2102. Tym samym dostępność cyfrowa stała się obowiązkiem dla instytucji publicznych. Pomimo tego nadal wiele stron internetowych, aplikacji mobilnych i dokumentów tekstowych nie spełnia wymogów WCAG (Web Content Accessibility Guidelines). Stąd celem wystąpienia jest identyfikacja wyzwań, jakie stoją przed instytucjami publicznymi na terenach wiejskich w Polsce w kontekście zapewniania dostępności osobom ze szczególnymi potrzebami. Autorka stawia następujące pytania badacze: Jakie grupy społeczne na wsi skorzystają na praktycznej realizacji zapisów prawnych związanych z dostępnością cyfrową? Jakie są główne bariery w zapewnianiu dostępności cyfrowej na terenach wiejskich? Dlaczego dostępność do usług publicznych z wykorzystaniem technologii cyfrowych ma szczególne znaczenie na obszarach wiejskich? Punktem wyjścia do rozważań jest koncepcja *smart villages*.
Słowa kluczowe: dostępność cyfrowa, obszary wiejskie, *smart villages*

dr **Monika Opioła – Cegiełka**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy,

Cyfrowe dziedzictwo pamięci. Szanse i zagrożenia dla upamiętniania w erze AI

Historyczka i filolożka romańska, adiunkt na Wydziale Historycznym Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Jej zainteresowania badawcze obejmują kulturę i politykę pamięci (zwłaszcza dychotomię pamięci i historii), historię kobiet i ruchów kobiecych XIX i XX wieku oraz historię prasy międzywojennej. Entuzjastka nowych technologii i uczestniczka szkoleń z zakresu AI w edukacji.

Abstrakt: Rozwój sztucznej inteligencji otwiera nowe możliwości w zakresie ochrony, udostępniania i popularyzacji dziedzictwa historycznego. Narzędzia oparte na HTR, jak Transkribus, rewolucjonizują pracę z archiwami poprzez automatyczną transkrypcję historycznych rękopisów, ułatwiając dostęp do źródeł dotąd trudno dostępnych. Projekt Dimensions in Testimony USC Shoah Foundation pokazuje zaś, jak AI może służyć upamiętnianiu w sposób etyczny – umożliwiając interaktywne rozmowy z ocalałymi z Holokaustu bez manipulowania ich świadectwem. Równocześnie te same technologie stwarzają poważne zagrożenia dla integralności pamięci zbiorowej. Śledztwa BBC i AFP z 2025 roku ujawniły, że międzynarodowe sieci spamerów masowo publikują na platformach społecznościowych generowane przez AI fałszywe zdjęcia ofiar Holokaustu, czerpiąc zyski z systemów monetyzacji treści. Zjawisko „AI slop" podważa autentyczność cyfrowego dziedzictwa i dezorientuje odbiorców — w tym rodziny ocalałych. Referat stawia pytanie o warunki, w jakich AI może służyć rzetelnej pamięci historycznej, a nie jej wypaczaniu.
Słowa kluczowe: dziedzictwo cyfrowe, pamięć zbiorowa, upamiętnianie, sztuczna inteligencja, dezinformacja historyczna

dr **Agnieszka Pazderska**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Rola internetu i AI w ewolucji zasady równości w obliczu narastającej polaryzacji oraz barier cyfrowych***

Adiunkt badawczo-dydaktyczny w Katedrze Myśli Politycznej i Ruchów Społecznych na Wydziale Nauk o Polityce i Administracji Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Autorka publikacji naukowych dotyczących w szczególności slaktywizmu, aktywności politycznej w internecie oraz wartości i aspiracji życiowych młodych dorosłych. Główne zainteresowania badawcze: aktywność młodych dorosłych w internecie, wykorzystywanie mediów społecznościowych w polityce.

Abstrakt: Przedmiotem analizy jest rola internetu oraz sztucznej inteligencji w kształtowaniu zasady równości w warunkach narastającej polaryzacji społecznej i utrzymujących się barier cyfrowych. Przyjęto hipotezę, że technologie cyfrowe, mimo deklarowanego potencjału demokratyzującego, często sprzyjają utrwalaniu nierówności. Punktem wyjścia jest omówienie pojęcia równości oraz sposobów jej realizacji w przestrzeni cyfrowej, gdzie formalna dostępność nie zawsze oznacza realną inkluzywność. Analizie poddane zostaną zjawiska cyfrowej przepaści i wykluczenia cyfrowego, które ograniczają możliwość pełnego uczestnictwa w życiu publicznym. Następnie przeanalizowany będzie wpływ algorytmów na polaryzację polityczną, w tym powstawanie baniek filtrujących i komór echa wzmacniających skrajne postawy poprzez personalizację treści. Szczególna uwaga zostanie poświęcona temu, jak asymetria kompetencji cyfrowych wpływa na zdolność użytkowników do krytycznej oceny informacji oraz świadomego korzystania z narzędzi technologicznych. W końcowej części przedstawione zostaną kierunki działań mogących ograniczać nierówności cyfrowe, obejmujące rozwój infrastruktury oraz upowszechnianie edukacji cyfrowej.

Słowa kluczowe: równość, AI, polaryzacja, cyfrowa przepaść, wykluczenie cyfrowe

dr **Magdalena Bierzyńska-Sudoł**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Mechanizmy ekskluzji cyfrowej seniorów w warunkach cyfryzacji usług publicznych***

Doktor nauk społecznych w dyscyplinie nauki o polityce i administracji, adiunkt na Wydziale Nauk o Polityce i Administracji Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Autorka licznych artykułów naukowych oraz monografii. Jako pracownik Katedry Polityki Innowacyjności i Zrównoważonego Rozwoju prowadzi badania nad kluczowymi wyzwaniami społeczno-ekonomicznymi związanymi z procesami demograficznymi i migracyjnymi, srebrną gospodarką, innowacyjnością, cyberprzestrzenią i jej społecznymi aspektami, a także społecznościami i interakcjami wirtualnymi. Członkini Polskiego Towarzystwa Nauk Politycznych, Światowej Rady Badań nad Polonią oraz Bydgoskiego Towarzystwa Naukowego. [ORCID: 0000-0002-7279-6103, magda77@ukw.edu.pl; m.bierzynska.sudol@gmail.com]

Abstrakt: Postępująca cyfryzacja usług publicznych stanowi jeden z najważniejszych procesów transformacyjnych współczesnych państw. Elektroniczne formy kontaktu z administracją, cyfrowe systemy ochrony zdrowia, bankowość internetowa czy platformy świadczeń społecznych mają zwiększać efektywność instytucji publicznych oraz poprawiać dostęp

obywateli do usług. Jednocześnie proces ten ujawnia nowe nierówności społeczne związane z kompetencjami cyfrowymi, dostępem do technologii oraz zdolnością do samodzielnego funkcjonowania w środowisku cyfrowym. Szczególnie narażoną grupą są osoby starsze. Celem wystąpienia jest analiza mechanizmów prowadzących do ekskluzji cyfrowej seniorów w warunkach rosnącej cyfryzacji usług publicznych. W referacie ekskluzja cyfrowa zostanie przedstawiona nie tylko jako problem technologiczny, lecz przede wszystkim jako zjawisko społeczne i polityczne wpływające na poziom uczestnictwa obywatelskiego, dostęp do praw socjalnych oraz jakość życia osób starszych. Analizie poddane zostaną bariery infrastrukturalne, kompetencyjne, ekonomiczne, psychologiczne i instytucjonalne ograniczające zdolność seniorów do korzystania z cyfrowych kanałów komunikacji z państwem.
W konkluzji przedstawiono konsekwencje ekskluzji cyfrowej dla realizacji zasady równego dostępu do usług publicznych oraz rekomendacje dotyczące projektowania bardziej inkluzyjnych polityk publicznych wobec starzejących się społeczeństw. Podkreślając, że skuteczna cyfryzacja administracji powinna uwzględniać nie tylko rozwój technologii, ale również zróżnicowane potrzeby i możliwości obywateli należących do najstarszych grup wieku.
Słowa kluczowe: seniorzy, ekskluzja cyfrowa, cyfryzacja usług publicznych, nierówności cyfrowe, wykluczenie społeczne, polityka publiczna, administracja elektroniczna, starzenie się społeczeństwa.

lic. **Ewa Wielewska**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Poziom dostępności cyfrowej jednostek samorządu terytorialnego – badania empiryczne***

Studentka kierunku Zarządzanie sferą publiczną prowadzonego przez Wydział Nauk o Polityce i Administracji UKW. Na co dzień współpracuje z jednostkami administracji publicznej wdrażając i rozwijając aplikacje internetowe wspierające udostępnianie informacji publicznych, kontakt z mieszkańcami i partycypację obywatelską. Członkini Rady Działalności Pożytku Publicznego Miasta Bydgoszczy kadencji 2023-2026, od kwietnia 2025 pełniąca rolę Przewodniczącej.
Abstrakt: Niniejsze wystąpienie analizuje poziom dostępności cyfrowej stron internetowych i aplikacji mobilnych wybranych podmiotów publicznych – gmin w województwie kujawsko-pomorskim do 20 tys. mieszkańców. Podstawę prawną wdrożeń stanowi Ustawa z 4 kwietnia 2019 roku. W związku z tym, że funkcjonuje ona jako przepisy obligatoryjne dla sektora publicznego od ponad 5 lat, interesujący wydaje się poziom jej rzeczywistej implementacji we wspomnianej przestrzeni. Na potrzeby badania stworzono uproszczony kwestionariusz audytowy, w którym wskazano podstawowe wytyczne właściwe dla standardu WCAG 2.1. odnoszące się do dostępności cyfrowej. W procesie badawczym wykorzystano również specjalistyczne narzędzia audytowe. Weryfikacji poddano warstwę techniczną treści cyfrowych, a także ich stronę redakcyjną, odnoszącą się m. in. do zastosowania języka prostego i treści w ETR. W oparciu o powyższe wypracowano rekomendacje dla JST w zakresie wdrażania zasad dostępności cyfrowej.
Słowa kluczowe: dostępność cyfrowa, samorząd terytorialny, małe gminy, WCAG

Global Cyber Governance and the Politics of Digital Security

Assoc. Prof. **Valentina Sommella**, PhD, University of Perugia (Italy), ***The Digital Silk Road and China's Role in the Global Innovation System***

Associate Professor of History of International Relations. She teaches Global Governance and International Organizations and Geopolitics of China and East Asia. Before joining the Department of Political Science at the University of Perugia, she taught the History of International Relations at La Sapienza University of Rome and was Visiting Research Fellow at University College Dublin. Her main research interests lie in the foreign policy of liberal Italy; Italian foreign policy in the interwar years; relations between the Allies during and after WWII; and, more recently, the rise of China as a global power in the international system. She has participated in several research projects and has published three monographs and numerous articles in international journals, for example *Un console in trincea. Carlo Galli e la politica estera dell'Italia liberale, 1905-1922* (Soveria Mannelli: Rubbettino, 2016), *Dalla non belligeranza alla resa incondizionata. Le relazioni politico-diplomatiche italo-francesi tra Asse e Alleati* (Rome: Aracne, 2008) and *Un'alleanza difficile. Churchill, de Gaulle e Roosevelt negli anni della guerra* (Rome: Aracne, 2005)

Abstract: First announced in September 2013 at the Nazarbayev University of Astana, the capital of Kazakhstan, the Belt and Road Initiative (BRI, yi dai yi lu 一带一路) has grown over the years to become an ambitious plan that can be declined in multiple directions: from the classic geopolitical strategic land and sea routes to the Arctic and the new space frontier, and up to the most sophisticated articulations of a Digital Silk Road (shuzi sichou zhilu 数字丝绸之路), a Green BRI (lüse yi dai yi lu 绿色一带一路) and a Health Silk Road (jiankang sichou zhilu 健康丝绸之路). The aim of this paper is to take a look at the objectives of the Digital Silk Road, its tools, ongoing projects and its global geopolitical implications.

Keywords: Belt and Road Initiative; Digital Silk Road; China; geopolitics; digital infrastructure; global connectivity; technological expansion; cyber governance

Prof. Dr. **Jaroslav Usiak**, Matej Bel University in Banska Bystrica (Slovakia), ***Recoding Security in Cyberspace: The Paradox of State Control and Civil Liberties in Slovakia***

Prof. Jaroslav Ušiak, PhD. is Vice-Dean for Science, Research, and Development at the Faculty of Political Sciences and International Relations at Matej Bel University in Banská Bystrica, he also professor at the Department of Security Studies. His scientific work focuses on security threats, securitization theory, extremism, and radicalism. He has extensive experience in international research projects focused on the prevention of extremism, the fight against disinformation, and strengthening the defences of democratic regimes. E-mail: jaroslav.usiak@umb.sk

Abstract: Following Slovakia's integration into Euro-Atlantic structures, the concept of security was primarily linked to the principles of militant (or defensive) democracy: protecting the liberal order from external hybrid threats, particularly in the information space. The defence of democratic values and cyberspace was seen as a key element of national security. However, recent years have brought a fundamental shift in the interpretation of "threats" within Slovak political discourse, reflecting a broader regional trend within the Visegrad Four (V4). We are witnessing a dual securitisation of the cyber-social space. Whilst the legitimate effort to defend against real external disinformation campaigns continues to exist, government actors have increasingly adopted security and cyber-defence language as a tool of domestic political control. Concepts such as "hybrid threat" or "foreign influence" are instrumentalised to combat domestic opposition, critical independent media, and non-governmental organisations (NGOs). Legislation restricting civil society is framed as "defending sovereignty" against informational subversion, representing a fatal target displacement where the defensive arsenal of the state is turned against democratic plurality. Based on a critical analysis of political discourse and legislative documents from 2022 to 2025, this paper explores the tension between freedom and control in the digital age. It analyses Slovakia as a critical Central European laboratory, standing between the fully consolidated illiberal system of Hungary and the robust democratic resilience of the Czech Republic. The paper argues that this "re-coding" of security threats has a highly destructive and ambivalent outcome. Whilst it ostensibly protects the state from cognitive manipulation, it establishes mechanisms of authoritarian control. By cutting off critical civic infrastructure and destroying cooperation with the third sector, the state loses its essential expertise. Ultimately, this approach creates a "Hollow State" paradox: a state that appears immensely powerful and repressive towards its own citizens but remains institutionally debilitated and incapable of facing actual external crises and sophisticated hybrid attacks.
*This work was supported by the Slovak Research and Development Agency under Contract No. APVV-24-0174.

Keywords: Slovakia; securitisation; hybrid threats; cyber-social space; civil society; democratic resilience; authoritarian control

Dr **Kamila Sierzputowska**, PhD, Kazimierz Wielki University (Poland), ***Protecting Poland's information space: the role of state institutions, the private sector and civil society***

Assistant Professor at the Department of Political Systems and Digital State, Faculty of Political Science and Administration, Kazimierz Wielki University in Bydgoszcz, Poland. She holds a Ph.D. in Political Science with a specialization in International Relations.

She is a Member of the Council for International Disinformation Resilience operating under the auspices of the Ministry of Foreign Affairs of the Republic of Poland, contributing to national and international initiatives aimed at strengthening societal resilience against information threats, foreign influence operations, and hybrid threats. She also serves as the Rector's Plenipotentiary for the Protection of Classified Information and is a member of the Rector's Commission for Promotion and Cooperation at Kazimierz Wielki University.

Her research focuses on cybersecurity, cyber resilience, cyber stability, international security, and international relations. Her scholarly interests also encompass state resilience, information security, digital governance, strategic communication, disinformation resilience, and cyber security policy, as well as the evolving challenges facing NATO and the broader Euro-Atlantic security environment. A significant part of her research is dedicated to Estonia as a pioneer of digital transformation in public administration, particularly in the areas of e-governance, digital state development, and cybersecurity.

Dr. Sierzputowska has authored numerous scientific publications, including articles in Polish and international peer-reviewed journals as well as chapters in academic monographs. She is the Managing Editor of *Transformation Through Training*, the official magazine of the NATO Joint Force Training Centre. She actively participates in international academic and policy discussions concerning cybersecurity, digital transformation, democratic resilience, and international security. As a member of several national and international professional associations, she contributes to interdisciplinary research and expert dialogue on the future of digital states, cyber governance, and resilience policies.

Her international academic experience includes research visits, scientific internships, and professional exchanges in Italy, Slovenia, Slovakia, Israel, and Türkiye. She has also presented her research at numerous national and international conferences and workshops.

In addition to her academic activities, Dr. Sierzputowska conducts training and educational programmes for NATO institutions in the fields of political systems, strategic communication, resilience, and security studies. She serves as the Coordinator of International Student Internships at the NATO Military Police Centre of Excellence and has extensive experience in the management, coordination, and implementation of projects financed through national and international public funding mechanisms.

Abstract: The contemporary information space has become a key arena of political, economic, and military competition. The growing scale of disinformation campaigns, cyberattacks, and influence operations conducted by state and non-state actors poses a significant threat to Poland's national security.

The aim of this article is to analyze the role of state institutions, the private sector, and civil society in protecting the Polish information space.

The study argues that effective protection requires a multi-sectoral approach based on cooperation between public administration, technology companies, the media, and non-governmental organizations. Particular attention is paid to state actions in the areas of cybersecurity, countering disinformation, and building social resilience. The importance of digital platforms and private entities in identifying and limiting harmful content is also discussed. The article emphasizes the role of civil society in developing media literacy, digital education, and strengthening citizens' awareness of information threats.

The conclusions indicate that only coordinated actions by all stakeholders can effectively increase Poland's resilience to contemporary threats in the information domain.

Keywords: information security, disinformation, cybersecurity, societal resilience, state institutions, national security, information warfare

Dr **Mehmet Mert Kaleci**, PhD, Düzce University (Turkey), ***The Politics of Cyber Governance in Türkiye: A Descriptive Mapping of State and Civil Society Discourses***

Lecturer at Düzce University (Türkiye), where he teaches courses on diplomacy, foreign policy analysis, international relations, Turkish politics, and globalization. He also contributes to the Research Deanery, supporting institutional research policy development, international cooperation, and EU-funded project initiatives. His research focuses on new institutionalism, discursive institutionalism, and state transformation. His work examines the relationship between political authority and institutional change, with particular attention to the role of ideas, discourse, and advocacy and discursive coalitions in shaping policy processes. He is involved in the COST Action Science in Diplomacy Network (CA24169). More recently, he has begun to engage with questions related to science diplomacy, digital governance, and the institutional implications of emerging technologies.

Abstract: The enactment of Law No. 7545 in 2025, establishing the National Cybersecurity Presidency (SGB), marks an important development in Türkiye's evolving digital governance framework. This paper provides a descriptive mapping of the Turkish cyber-governance landscape, focusing on debates surrounding state-led cybersecurity policies and individual digital rights. Drawing on official statements, reports, and policy documents of key stakeholders – ranging from government institutions such as the Information and Communication Technologies Authority (BTK) and the National Cybersecurity Presidency to civil society organisations including the Freedom of Expression Association (İFÖD) – the study examines how different actors frame issues of cybersecurity, regulation, and digital rights. From a political science perspective, the analysis categorizes these discourses and highlights how policies often associated with the concept of the "Cyber Homeland" intersect with concerns about surveillance, transparency, and data governance. The paper provides a descriptive snapshot of the Turkish case as of 2026.

Keywords: Cyber Governance; Cybersecurity Policy; Digital Rights; Civil Society; Stakeholder Discourses; Türkiye

MA **Geoffrey Lefebvre**, Nicolaus Copernicus University in Toruń (Poland), ***The Proliferation of Cyberattacks in France: Implications for Political Trust and Institutional Legitimacy***

I hold a bachelor's degree in political science from the University of Picardy Jules Verne in Amiens (France) and a master's degree in international relations and diplomacy from Nicolaus Copernicus University in Torun (Poland). I am currently a doctoral candidate in political science at the Doctoral School of Social Sciences, Doctoral Schools, Nicolaus Copernicus University in Torun. My research focuses primarily on electoral behavior, abstention, political participation, and populism.

Abstract: In the era of data digitization, cyberattacks are multiplying in Western Democracies. Whether it is the work of a foreign power aiming to destabilize states, or of a criminal organization, the increasing number of these attacks has a direct impact on citizens. Taking as

a case study recent cyberattacks on France, including the hacking of the French Shooting Federation, as well as massive data leaks related to government agencies, this paper aims to take stock of the recent attacks suffered in France and their concrete implications for the population and their security. From a theoretical perspective, this paper also focuses on the medium- and long-term implications of these attacks on our democratic systems. Drawing on theories of political legitimacy and political trust, this paper argues that the repetition of these incidents contributes to undermining citizens' trust in the state's ability to protect sensitive data, thereby contributing to an erosion of democratic legitimacy and fueling populist rhetoric. Finally, in conclusion, this article examines the risks and limits that the trend toward the digitization of our official data, as well as the issue of electronic voting, may pose in the future.

Keywords: Cybersecurity ; Political Trust ; Democratic Legitimacy ; France

MA **Isti Marta Sukma**, Warsaw University (Poland), ***Do Alliances Make Policies Alike? Cybersecurity Policy Convergence Within the Five Eyes***

PhD candidate at the University of Warsaw researching emerging technologies (cybersecurity, AI, quantum computing) at the intersection of geopolitics and public policy, with a focus on the Indo-Pacific and EU. My work advances theory building in political science and develops predictive models to monitor and anticipate policy processes and political outcomes, integrating power, institutions, and material constraints. I use mixed and computational methods, including NLP and transformer-based models, to analyze large-scale policy and strategic documents and assess how frontier technologies reshape governance and state capacity.

Abstract: This paper asks whether alliance membership produces similar cybersecurity policies. Using NLP-based textual similarity analysis of national cybersecurity strategy documents from Five Eyes member states, it measures the degree to which Australia, Canada, New Zealand, the United Kingdom, and the United States have converged in policy content - not merely in policy adoption. The paper then asks why: does similarity reflect states learning from each other's experience, emulating a perceived best-practice model, or following shared alliance templates? Distinguishing these mechanisms matters because they imply different degrees of national policy autonomy. Preliminary findings suggest convergence extends beyond shared instruments to shared threat framings, pointing toward institutional emulation as the dominant diffusion mechanism within the alliance.

Keywords: policy diffusion, Five Eyes, cybersecurity policy, alliance, emulation, textual similarity, NLP

dr **Maksymilian Galon**, Uniwersytet Jagielloński, ***Elektroniczna partycypacja w praktyce dydaktycznej***

Adiunkt w katedrze Współczesnych Systemów Politycznych i Partyjnych na co dzień zajmujący się Internetem (zwłaszcza jego rolą w zarządzaniem państwem) oraz procesami kreatywnymi (głównie metodą Design Sprint) .

Abstrakt: Wystąpienie przedstawia wyniki eksperymentu dydaktycznego poświęconego partycypacji w sieci, realizowanego w ramach zajęć akademickich przez trzy semestry. Jego głównym celem jest praktyczna weryfikacja przekonania, że prowadzenie profilu w mediach społecznościowych jest działaniem prostym i intuicyjnym.

W ramach projektu studentki i studenci zakładają oraz prowadzą wybrany profil społecznościowy przez jeden semestr, z możliwością kontynuacji działań do czterech semestrów. Pozwala im to poznać mechanikę funkcjonowania platform społecznościowych, zasady tworzenia i dystrybucji treści, budowania zaangażowania odbiorców oraz analizy danych generowanych podczas prowadzenia profilu. Uczestnicy uczą się także korzystania z narzędzi wspierających produkcję treści cyfrowych, takich jak CapCut, OpenShot czy Audacity.

Teoretycznym punktem odniesienia są koncepcja drabiny partycypacji Sherry R. Arnstein oraz refleksje nad sieciowością i przemianami władzy zawarte w książce *Netokracja* Alexandra Barda i Jana Söderqvista. Eksperyment ukazuje media społecznościowe jako przestrzeń uczenia się uczestnictwa, sprawczości i odpowiedzialności w środowisku cyfrowym.

Słowa kluczowe: elektroniczna partycypacja, Tik Tok, Instagram, projekty dydaktyczne

dr **Łukasz Brzeziński**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Od kompetencji do autokracji poznawczej: narcyzm cyfrowy i iluzja wiedzy w edukacji wspieranej przez AI***

Jest doktorem nauk społecznych, psychologiem oraz pedagogiem. Jego kwalifikacje potwierdzają również certyfikaty International Professional Trainer (ACI®), Erickson Professional Coach (ICF) oraz Trener Biznesu (GAUM). Właściciel firmy VIAE MENTIS Łukasz Brzeziński. Jako trener specjalizuje się w szkoleniach z zakresu komunikacji, prezentacji, savoir-vivre i budowania zespołów. Prowadzi także warsztaty rozwijające umiejętność kreatywnego myślenia i skutecznego rozwiązywania problemów. W roli coacha towarzyszy swoim klientom w procesach rozwojowych i wizerunkowych – inspiruje, motywuje i pomaga w przełamywaniu barier, które powstrzymują ich przed realizacją planów życiowych i biznesowych. W pracy psychologicznej kieruje się uważnością, autentycznym szacunkiem i wiarą w potencjał drugiego człowieka. Opiera się na sprawdzonych podejściach, łącząc naukową rzetelność z empatycznym zrozumieniem ludzkich potrzeb.

Abstrakt: Narcyz zakochał się we własnym odbiciu. Dziś tym lustrem nie jest już woda, lecz sztuczna inteligencja. Autor podejmuje krytyczną analizę roli AI w edukacji, stawiając pytanie: czy technologia rzeczywiście wspiera proces uczenia się, czy raczej wzmacnia iluzję kompetencji. Punktem wyjścia jest koncepcja „narcyzmu cyfrowego" rozumianego jako

mechanizm kulturowo-poznawczy, w którym tożsamość opiera się na percepcji własnej wiedzy, a nie jej rzeczywistym posiadaniu. AI funkcjonuje tu jako „lustro", wzmacniając pewność siebie użytkownika poprzez personalizację treści, generowanie wysokiej jakości odpowiedzi oraz eliminację wysiłku poznawczego. W efekcie dochodzi do przesunięcia władzy poznawczej - od realnej kompetencji ku zarządzaniu jej pozorem, co autor określa mianem autokracji poznawczej. Szczególnym zagrożeniem jest autodecepcja, czyli utożsamienie wiedzy wygenerowanej z własnym rozumieniem. Wystąpienie wskazuje konsekwencje tego zjawiska dla ucznia, relacji edukacyjnych oraz systemu kształcenia, proponując jednocześnie kierunki przeciwdziałania oparte na metapoznaniu.

Słowa kluczowe: narcyzm cyfrowy, autodecepcja, edukacja, uczenie się, AI

dr **Wojciech Trempała**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Między nadmiarem a niedostępnością: Selektywna ekspozycja informacyjna młodych a ograniczenia partycypacji społecznej w życiu miasta***

Politolog, doktor nauk społecznych w zakresie socjologii, adiunkt w Katedrze Polityki Innowacyjności i Zrównoważonego Rozwoju, Prodziekan ds. Kształcenia. Autor publikacji na temat kulturowych i politycznych implikacji współczesnego kryzysu środowiskowego oraz wartości i aspiracji życiowych młodych mieszkańców miasta Bydgoszczy. Od 2018 roku wspólnie z zespołem realizuje projekt pod tytułem: „Bydgoscy maturzyści o sobie i świecie. Kim są? Czego chcą? Jak postrzegają społeczeństwo?" - którego jest jednym z inicjatorów. Kierownik i autor koncepcji badawczej *Kompleksowej diagnozy potrzeb oraz potencjału młodych mieszkanek i mieszkańców Miasta Bydgoszczy (w wieku 13–35 lat) w zakresie partycypacji w życiu społecznym i obywatelskim*.

Abstrakt: Celem wystąpienia jest analiza zjawiska selektywnej ekspozycji informacyjnej młodych mieszkańców miasta w kontekście ich partycypacji społecznej. Punktem wyjścia jest założenie, że internet – przy odpowiedniej polityce informacyjnej i kompetencjach medialnych – może wzmacniać zaangażowanie obywatelskie, jednak w warunkach ich deficytu prowadzi do chaosu informacyjnego i ograniczonej widoczności treści lokalnych. Badanie koncentruje się na pytaniu, w jaki sposób nadmiar informacji oraz jednoczesna niedostępność kluczowych komunikatów wpływają na formy i poziom uczestnictwa młodych w życiu miasta. Analizie poddano źródła informacji wykorzystywane przez młodych, ich subiektywne poczucie poinformowania, kryteria selekcji treści oraz rolę algorytmicznych mechanizmów mediów społecznościowych. Podstawę empiryczną stanowią wyniki badań ilościowych (N=2289) oraz wywiadów fokusowych przeprowadzonych wśród osób w wieku 13–35 lat w Bydgoszczy. Wyniki wskazują na paradoks współczesnej komunikacji: mimo szerokiej oferty partycypacyjnej znaczna jej część pozostaje niewidoczna dla odbiorców. Wśród rekomendacji podkreślono potrzebę rozwoju edukacji obywatelskiej i medialnej, wzmocnienia komunikacji bezpośredniej oraz współpracy instytucjonalnej na rzecz zwiększenia dostępności informacji oraz budowania lokalnej tożsamości.

Słowa kluczowe: polityka miejska, młodzież, marketing terytorialny, partycypacja obywatelska, social media

dr hab. **Magdalena Mateja**, prof. UMK, Uniwersytet Mikołaja Kopernika w Toruniu,

Między empatią a nadużyciem: wybrane patologie cyfrowego aktywizmu na rzecz zwierząt

Jestem medioznawczynią, dr hab. nauk o polityce, profesorką w Katedrze Komunikacji, Mediów i Dziennikarstwa UMK w Toruniu. Moje zainteresowania badawcze obejmują m.in. komunikację wizualną i perswazyjną, komunikowanie polityczne oraz badania nad dziennikarstwem. Należę do Polskiego Towarzystwa Komunikacji Społecznej i Polskiego Towarzystwa Badań nad Filmem i Mediami. Jestem autorką monografii "Mowa umowna. O felietonach Kisiela" oraz "Między newsem a mitem. Prasa wobec śmierci polityka", a także autorką, współautorką lub współredaktorką kilkudziesięciu innych publikacji naukowych. Jako popularyzatorka nauki brałam udział w licznych festiwalach naukowych, wykładach okolicznościowych, szkoleniach oraz warsztatach. Od ponad dekady współpracuję z mediami, w których komentuję tematy odnoszące się do mediów masowych lub komunikowania politycznego. Współpracuje również z Klubem Miłośników Filmu „Mozaika" w Bydgoszczy, gdzie wygłaszam prelekcje o kinie współczesnym.

Abstrakt: Cyfrowy aktywizm na rzecz zwierząt odgrywa istotną rolę w komunikacji społecznej, jednak obok działań pomocowych ujawniają się praktyki budzące poważne wątpliwości etyczne. Celem referatu jest analiza wybranych patologii cyfrowego aktywizmu prozwierzęcego, ze szczególnym uwzględnieniem strategii retorycznych opartych na intensywnej emocjonalizacji przekazu oraz mechanizmów psychologii tłumu w środowisku sieciowym. Rama teoretyczna badań odwołuje się do klasycznej teorii retoryki (zob. pathos), koncepcji retoryki emocji oraz ujęć komunikacji afektywnej w mediach cyfrowych. Analizowane treści – publikowane głównie w mediach społecznościowych – wykorzystują silnie nacechowany język perswazji, narracje katastroficzne oraz drastyczne obrazy chorych i cierpiących zwierząt jako argumenty afektywne. Przekazy te często łączone są z presją moralną i czasową oraz rozbudowanym katalogiem form wpłat, co stanowi sugestię, że brak wsparcia finansowego prowadzi do śmierci zwierzęcia lub jego dalszego cierpienia.Analiza uwzględnia także mechanizmy psychologii tłumu, takie jak emocjonalna zaraźliwość, społeczny dowód słuszności i konformizm, wzmacniane przez algorytmy mediów społecznościowych. Metodologicznie badanie opiera się na jakościowej analizie treści (tekstów i fotografii) oraz analizie dyskursu. Wyniki wskazują na ryzyko instrumentalizacji empatii i erozji zaufania wobec organizacji trzeciego sektora.

Słowa kluczowe: cyfrowy aktywizm, retoryka emocji, psychologia tłumu, organizacje prozwięrzęce, zbiórka internetowa

dr **Bartłomiej Różycki**, Uniwersytet Mikołaja Kopernika w Toruniu, ***Desokupa TV - kanał influencerski czy nowy głos hiszpańskiej prawicy?***

Politolog, adiunkt na Wydziale Nauk o Polityce i Bezpieczeństwie Uniwersytetu Mikołaja Kopernika w Toruniu, współpracujący także z Instytutem Studiów Politycznych Polskiej Akademii Nauk. Swoje zainteresowania badawcze koncentruje wokół wykorzystania narracji

historycznych w polityce, szczególnie w kontekście współczesnej Hiszpanii, a także symboli przeszłości funkcjonujących w przestrzeni publicznej i przekształcaniu krajobrazu symbolicznego w wyniku transformacji ustrojowej.

Abstrakt: Daniel Esteve stał się rozpoznawalną postacią hiszpańskiego życia publicznego jako założyciel firmy Desokupa, zajmującej się eksmisjami osób nielegalnie zajmujących nieruchomości. Upolitycznienie i rozgłos nadany tematowi tzw. Okupas, wykraczający również poza granice Hiszpanii, stał się osią dyskursu publicznego wokół z jednej strony nienaruszalności własności prywatnej, z drugiej kohezji i bezpieczeństwa społecznego. W kontekście rosnącej również w Hiszpanii popularności haseł skrajnie prawicowych, działalność Daniela Esteve zaczęła wiązać się z postawami antyimigranckimi, wykraczającymi poza pierwotnie zajmującą go kwestię Okupas. Jego zyskujący w ostatnich dwóch latach popularność kanał w serwisie YouTube, Desokupa TV, stał się instrumentem promowania postaw polaryzujących, zorientowanych wokół krytyki elit politycznych oraz upatrywania przyczyn problemów społecznych Hiszpanii w słabości instytucji państwowych. Kwestią otwartą pozostaje związek działalności medialnej Daniela Esteve z hiszpańską polityką – na ile Desokupa TV stanowi formę promocji specyficznej działalności biznesowej, a na ile stała się instrumentem kształtowania hiszpańskiego prawicowego dyskursu publicznego.

Słowa kluczowe: Daniel Esteve, Okupas, Hiszpania, dyskurs skrajnej prawicy, YouTube

Państwo i obywatel wobec zagrożeń wojny informacyjnej

dr hab. **Agnieszka Demczuk**, prof. UMCS, Uniwersytet Marii Curie Skłodowskiej,

Ochrona przed dezinformacją. Rola państwa: od biernego obserwatora do aktywnego gracza

Agnieszka Elżbieta Demczuk, dr hab., prawniczka i politolożka, profesorka Uniwersytetu Marii Curie-Skłodowskiej w Lublinie w zakresie nauk o polityce i administracji, od 2008 r. pracuje w Katedrze Systemów Politycznych i Praw Człowieka w Instytucie Nauk Politycznych i Administracji Publicznej; kierowniczka sekcji praw człowieka w PAN oddział Lublin; w latach 2024-2025 członkini Komisji ds. badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy RP w latach 2004-2024. Od 2020 r. kierowniczka Zespołu Badań Propagandy i Dezinformacji na UMCS; w latach 2004-2008 pracowała w Helsińskiej Fundacji Praw Człowieka w Warszawie. Autorka prac na temat ochrony praw człowieka, wolności wypowiedzi, dezinformacji i propagandy, infodemii COVID-19 i szerzej rożnych aspektów funkcjonowania społeczeństwa informacyjnego. W 2022 r. brała udział w pracach nad raportem „Przeciwdziałanie dezinformacji w Polsce. Rekomendacje systemowe", przygotowanym przez 40 polskich ekspertów i zawierającym 60 rekomendacji, przedstawionym Senatowi RP w 2023 r. W latach 2020-2023 brała udział w projekcie badawczym Horyzont 2020 pt. „Przestrzeganie praw podstawowych w wykorzystaniu technologii cyfrowych w usługach e-zdrowia" (REINITIALISE, nr 952357).

Abstrakt: Od ponad dekady dezinformacja stanowi skuteczną broń w wojnie kognitywnej Rosji przeciwko państwom NATO i UE, w tym Polsce, której celem jest zmiana nie tylko tego, co obywatele myślą, ale także jak myślą i jak działają. Dezinformacja nie jest jedynie problemem obserwowanym w stosunkach międzynarodowych. Dezinformacją posługują się również krajowi, tj. partie polityczne, dziennikarze, organizacje pozarządowe. Dezinformacja zanieczyszcza zarówno cyberprzestrzeń, jak i media tradycyjne. Intoksykacja ludzkich umysłów trwa stopniowo, acz metodycznie i konsekwentnie poprzez wprowadzanie do opinii publicznej fałszywych teorii naukowych, teorii spiskowych, wielkiego kłamstwa, fałszywych paradygmatów i koncepcji wywierających wpływ na zarządzanie państwem w celu osłabienia jego morale, wartości, potencjału obronnego, informacyjnego, ekonomicznego itd. Degradacji ulegają procesy i instytucje demokratyczne, prawa człowieka, dyskurs publiczny oraz kultura publiczna. W tym kontekście, rodzą się pytania: czy państwo powinno być biernym obserwatorem i hołdować purytańskiej zasadzie o niemal absolutnej wolności wypowiedzi, czy włączyć się aktywnie w zwalczanie i zapobieganie dezinformacji, (współ)tworzyć regulacje prawne (np. na poziomie UE – DSA, DMA, AI Act), finansować kampanie społeczne, powoływać komisje ds. badania wpływów obcych służb na życie publiczne, wreszcie prowadzić proaktywną politykę medialną. Co ciekawe, przypadek Polski jest tu niemal modelowy. W ostatniej dekadzie można było zauważyć zmianę podejścia państwa w relacjach z obywatelem, próbą stopniowego zwiększania swojej roli w ochronie przed dezinformacją. Czy tego rodzaju działania wystarczą? Jakie dają rokowania na przyszłość? Czy nie jest już za późno, na skuteczną ochronę polskiego społeczeństwa przed dezinformacją, bo wyniki badań opinii publicznej jednoznacznie wskazują na coraz wyższy wzrost nastrojów (anty)-szczepionkowych, -migrackich, -unijnych i -ukraińskich.
Słowa kluczowe: dezinformacja, propaganda, wojna kognitywna, cyberprzestrzeń, sieci społecznościowe, Polska

dr hab. **Wojciech Kotowicz**, Uniwersytet Warmińsko-Mazurski w Olsztynie, ***Między wolnością a bezpieczeństwem: kontrola przekazu w cyberprzestrzeni w państwach bałtyckich wobec rosyjskiej wojny informacyjnej***

Zainteresowania naukowe: dezinformacja, zagrożenia hybrydowe, Rosja, państwa bałtyckie, polityka zagraniczna, bezpieczeństwo międzynarodowe i narodowe. autor kilku monografii m.in.: Obwód kaliningradzki w warunkach enklawowości, Olsztyn 2020; Stosunki polsko-litewskie - wybrane problemy 2024. Kilkanaście staży naukowych m. in.: Rosja, Litwa, Łotwa, Estonia, Mołdawia, Armenia. Udział w kilkunastu grantach naukowych, m.in.: „Wpływ rosyjskiej dezinformacji na kształtowanie opinii publicznej w krajach Europy Wschodniej – analiza i strategie przeciwdziałania", finansowanego przez Centrum Dialogu im. Juliusza Mieroszewskiego w ramach III Otwartego Konkursu, 2025 (kierownik projektu); „Edukacja społeczeństwa w zakresie dezinformacji: Polska, Litwa, Łotwa i Estonia”, "Dyplomacja publiczna 2024", MSZ; "Empowering border communities: education and strategies against disinformation. Practical recommendations", dofinansowany z Programu Współpracy INTERREG Litwa-Polska 2021-2027.

Abstrakt: Referat podejmuje analizę prawnych mechanizmów ograniczania przekazu w cyberprzestrzeni w Litwie, Łotwie i Estonii, ukazując napięcie między konstytucyjnie gwarantowaną wolnością słowa a obowiązkiem państwa do zapewnienia bezpieczeństwa narodowego. Państwa bałtyckie, ze względu na swoje położenie geopolityczne oraz doświadczenia historyczne, należą do najbardziej aktywnych w Europie w zakresie przeciwdziałania dezinformacji, w tym propagandzie rosyjskiej. Wystąpienie obejmuje analizę działań podejmowanych zarówno w warunkach „zwykłego" funkcjonowania państwa (blokowanie kanałów medialnych, decyzje regulatorów, sankcje administracyjne), jak i potencjalnych instrumentów przewidzianych na czas stanów nadzwyczajnych, w tym wojny. Celem referatu jest ocena, czy przyjęte rozwiązania mieszczą się w standardach demokratycznego państwa prawa, a także czy model „odporności informacyjnej" prowadzi do trwałej redefinicji granic wolności słowa w cyberprzestrzeni.
Słowa kluczowe: cyberbezpieczeństwo, dezinformacja, państwa bałtyckie, wolność słowa, Rosja

dr hab. **Krzysztof Żęgota**, Uniwersytet Warmińsko-Mazurski w Olsztynie, ***Niewidzialny front: jak Rosja prowadzi cyberwojnę przeciw Europie***

Dr hab., profesor uczelni w Instytucie Nauk Politycznych Uniwersytetu Warmińsko-Mazurskiego w Olsztynie. Badacz polityki zagranicznej i bezpieczeństwa Federacji Rosyjskiej wobec Polski i państw bałtyckich oraz społeczno-politycznych uwarunkowań rozwoju obwodu królewieckiego Federacji Rosyjskiej. Autor monografii Obwód kaliningradzki Federacji Rosyjskiej a bezpieczeństwo międzynarodowe Europy Środkowo-Wschodniej. Między geopolityką a konstruktywizmem (FNCE, Poznań 2021). Członek Polskiego Towarzystwa Nauk Politycznych i Polskiego Towarzystwa Geopolitycznego.
Abstrakt: Wystąpienie analizuje skalę, charakter i ewolucję rosyjskich operacji cybernetycznych wymierzonych w państwa europejskie w ostatnich latach, szczególnie po 2022 roku. Punktem wyjścia jest koncepcja wojny hybrydowej, w ramach której działania w cyberprzestrzeni uzupełniają klasyczne instrumenty polityki i presji strategicznej. Przedstawione zostaną główne typy ataków – od operacji szpiegowskich i sabotażowych po kampanie cybernetyczne i działania dezinformacyjne – wraz z ich celami oraz skutkami dla bezpieczeństwa państw i społeczeństw. Szczególna uwaga zostanie poświęcona atakom na infrastrukturę krytyczną oraz procesy demokratyczne jako kluczowym obszarom oddziaływania. Wnioski koncentrują się na rosnącym znaczeniu odporności cyfrowej oraz potrzebie skoordynowanej odpowiedzi państw europejskich na zagrożenia płynące z „niewidzialnego frontu".
Słowa kluczowe: cyberbezpieczeństwo, wojna bybrydowa, Rosja, Europa

mgr **Antoni Chelyuskin**, Uniwersytet Mikołaja Kopernika w Toruniu, ***Wpływ prokremlowskiej narracji na jednostkę w cyberprzestrzeni***

Absolwent UMK: studia magisterskie (politologia), zainteresowania geopolityką, szczególnie pojęciem soft power oraz ideologią "ruski mir" oraz zainteresowania językami obcymi. Posiadam

kilka publikacji naukowych (Rosyjska Cerkiew prawosławna a imperialna polityka Kremla; Język rosyjski jako narzędzie w propagowaniu idei "ruskiego mitu")

Abstrakt: Wpływ prorosyjskiej narracji (zarazem propagandy) na jednostkę w cyberprzestrzeni stanowi istotny przedmiot badań w kontekście współczesnych zagrożeń informacyjnych. W tym w kontekście zagrożenia dla państwa przez oddziaływanie na jednostkę. Rozwój technologii cyfrowych, w tym AI, zwiększył skalę i skuteczność oddziaływania treści dezinformacyjnych. Algorytmy AI umożliwiają tworzenie realistycznych komunikatów, obrazów oraz materiałów wideo, co utrudnia ich weryfikację i sprzyja manipulacji.

Szczególną rolę w tym procesie odgrywają tzw. rosyjskie trolle internetowe, działające zarówno jako zorganizowane grupy, jak i zautomatyzowane boty. Ich aktywność polega na ciągłym rozpowszechnianiu określonych narracji, wzmacnianiu podziałów społecznych oraz podważaniu zaufania do instytucji publicznych i mediów. Działania te często są ukierunkowane na podatne grupy odbiorców, w tym środowiska antysystemowe, w których prokremlowskie przekazy znajdują grunt dzięki istniejącej nieufności wobec struktur państwowych i międzynarodowych.

Oddziaływanie propagandy (nie tylko rosyjskiej) w cyberprzestrzeni na jednostkę widoczne w zmianie postaw, radykalizacji poglądów oraz obniżeniu krytycznego podejścia do informacji. Mechanizmy takie jak efekt bańki informacyjnej czy potwierdzenia przekonań wzmacniają skuteczność tych działań. W rezultacie jednostka może nieświadomie internalizować zmanipulowane treści, co wpływa na jej decyzje społeczne i polityczne.

Słowa kluczowe: Jednostka, cyberprzestrzeń, państwo, prorosyjskie narracji, dezinformacja

mgr **Joanna Baranowska**, Wyższa Szkoła Gospodarki, ***Jednostka wobec cyberwojny. Czy obywatel jest nowym polem***

Politolożka, absolwentka nauk politycznych Akademii Bydgoskiej. Zawodowo związana z Wyższą Szkołą Gospodarki w Bydgoszczy, gdzie pełni funkcję wykładowczyni oraz metodyczki kształcenia zdalnego, koncentrując się na nowoczesnych rozwiązaniach dydaktycznych i efektywnym wykorzystaniu technologii w edukacji. Członkini Polskiego Towarzystwa Nauk Politycznych, aktywnie zaangażowana w rozwój badań nad współczesnymi wyzwaniami w obszarze bezpieczeństwa. Jej zainteresowania naukowe obejmują przede wszystkim szeroko rozumiane kwestie bezpieczeństwa, ze szczególnym uwzględnieniem relacji polsko-amerykańskich oraz ich znaczenia w kontekście międzynarodowym. Prywatnie miłośniczka literatury kryminalnej, w której odnajduje inspirację do analitycznego spojrzenia na rzeczywistość i mechanizmy rządzące światem.

Abstrakt: Współczesne konflikty zbrojne coraz wyraźniej przenoszą się do świata cyfrowego, gdzie granice między frontem a zapleczem ulegają zatarciu. Celem niniejszego wystąpienia jest analiza tezy, że w warunkach cyberwojny jednostka – obywatel – staje się nowym polem bitwy. W przeciwieństwie do tradycyjnych działań militarnych, cyberkonflikty angażują nie tylko infrastrukturę krytyczną czy instytucje państwowe, lecz także codzienne praktyki komunikacyjne, percepcję informacji oraz tożsamość cyfrową użytkowników. Referat podejmuje próbę zdefiniowania mechanizmów oddziaływania na jednostkę w cyberprzestrzeni, takich jak dezinformacja, naciski psychologiczne, manipulacja

algorytmiczna czy eksploatacja danych osobowych. Szczególna uwaga zostanie poświęcona roli mediów społecznościowych jako narzędzi wpływu oraz przestrzeni prowadzenia działań hybrydowych. W tym kontekście obywatel przestaje być wyłącznie biernym odbiorcą skutków konfliktu, a staje się jego aktywnym uczestnikiem – zarówno jako cel, jak i potencjalne narzędzie oddziaływania.

Celem wystąpienia jest nie tylko opisanie zjawiska, ale również wskazanie implikacji dla polityk publicznych, edukacji cyfrowej oraz budowania odporności społecznej. W konkluzji zostanie postawione pytanie o granice odpowiedzialności państwa i jednostki w obliczu konfliktów, które coraz częściej toczą się w przestrzeni niematerialnej, lecz wywierają realne skutki społeczne i polityczne.

Słowa kluczowe: cyberwojna, cyberbezpieczeństwo, wojna informacyjna, dezinformacja, konflikty hybrydowe

Prawo, nadzór i ochrona jednostki w cyberprzestrzeni

dr hab. **Remigiusz Rosicki**, prof. UAM, Uniwersytet im. Adama Mickiewicza w Poznaniu, ***Prawne aspekty przestępstwa pozorowanej pornografii dziecięcej (problem deepfake'ów)***

Profesor uczelni na Uniwersytecie im. Adama Mickiewicza wPoznaniu. Posiada stopnie doktora nauk politycznych oraz doktora nauk prawnych. W celu poszerzenia swoich kompetencji akademickich ukończył liczne studia podyplomowe, m.in. z zakresu prawa karnego i procedury karnej ze szczególnym uwzględnieniem nowych technologii, prawa gospodarczego oraz prawa karnego skarbowego i gospodarczego. Jego zainteresowania badawcze obejmują ocenę prawną technologii, politykę i prawo karne, politykę i prawo energetyczne oraz metodologię porównawczą.

Abstrakt: Zakres wystąpienia dotyczy treści i znaczenia elementów charakteryzujących jeden z typów przestępstwa pornografii skryminalizowanego w art. 202 § 4b polskiego Kodeku karnego, czyli tzw. dziecięcej pornografii pozorowanej. Przez przestępstwo to rozumie się produkowanie, rozpowszechnianie, prezentowanie, przechowywanie lub posiadanie treści pornograficznych przedstawiających wizerunek osoby małoletniej. W wystąpieniu podjęty zostanie także problem deepfake'ów.

Słowa kluczowe: treści pornograficzne w internecie, deepfake, pornografia dziecięca, pozorowana pornografia dziecięca

dr **Ewa Kabza**, Uniwersytet Mikołaja Kopernika w Toruniu, ***Telefon dla dziecka – błogosławieństwo czy przekleństwo?***

Doktor nauk prawnych (2020), adiunkt w Katedrze Prawa Cywilnego WPiA UMK w Toruniu. Zainteresowania naukowe: prawo rodzinne, spadkowe, medyczne, komparatystyka prawnicza

Abstrakt: Referat ma na celu przedstawienie wpływu/powszechnej dostępności telefonów na życie dzieci (w tym np. na częstotliwość występowania przemocy rówieśniczej), omówienie projektu nowelizacji ustawy Prawo oświatowe (wprowadzającej zakaz korzystania z telefonów w publicznych szkołach podstawowych) oraz wskazanie na rozwiązania w przedmiotowej sprawie w prawie zagranicznym.
Słowa kluczowe: dzieci i smartfony; zakaz telefonów w szkołach; przemoc rówieśnicza; cyberprzemoc; prawo oświatowe; publiczne szkoły podstawowe; regulacje prawne; rozwiązania zagraniczne

dr **Anita Kubanek**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Naruszenie prawa konsumenta do autonomii decyzyjnej w przestrzeni cyfrowej***

Absolwentka Wydziału Administracji i Nauk Społecznych Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Doktorat z nauk prawnych uzyskała na Wydziale Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu broniąc pracę pt. „Ograniczenie praw jednostki przez zastosowanie środków przymusu bezpośredniego w celu zapewnienia bezpieczeństwa i porządku publicznego". Ukończyła studia Master Business of Administration (MBA) w Wyższej Szkole Bankowej w Toruniu/Franklin University. Autorka licznych publikacji naukowych. Przez wiele lat związana z branżą zbrojeniową, gdzie uczestniczyła w budowaniu strategii Polskiego Holdingu Obronnego i Polskiej Grupy Zbrojeniowej. Posiada bogate doświadczenie praktyczne i szkoleniowe w zakresie PR, HR, marketingu oraz organizacji i zarządzania. Certyfikowany tutor i trener biznesu. Uczestniczka i realizator licznych projektów unijnych, w tym projektów związanych m.in. z podwyższeniem kompetencji studentów, badaniem wydajności pracowników 50+, komercjalizacją wyników badań naukowych, przedsiębiorczością i zakładaniem działalności gospodarczej. Uczestniczka licznych szkoleń podnoszących kompetencje, konferencji i spotkań networkingowych. Jest opiekunem Koła Naukowego "Prawo&Biznes" oraz na Wydziale była przez kilka lat odpowiedzialna za promocję, stronę www i social media. Uczestniczka Bydgoskiego Festiwalu Nauki. Uczestniczyła w programie wymiany międzynarodowej ERASMUS+ jako prelegent w Portugalii, Turcji i Teneryfie. Zawodowo jest również związana z sektorem biznesu. Ostatnio w kręgu jej zainteresowań pojawiło się zagadnienie prawnych aspektów wykorzystania sztucznej inteligencji w działalności gospodarczej.

dr **Marcin Jastrzębski**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Technologia rozpoznawania twarzy: prawa i wolności jednostki a granice cybernetycznego nadzoru***

Dr Marcin Jastrzębski jest adiunktem na Wydziale Nauk Politycznych i Administracji Uniwersytetu Kazimierza Wielkiego w Bydgoszczy (UKW), gdzie pracuje w Katedrze Systemów Politycznych i Państwa Cyfrowego. Jego szerokie zainteresowania badawcze łączą prawo i nauki polityczne, koncentrując się na prawie międzynarodowym publicznym, międzynarodowych i polskich systemach ochrony praw człowieka oraz wolnościach politycznych – w szczególności na prawie do wolnych wyborów. Jego najnowsze prace analizują złożone relacje między

cyberprzestrzenią, sztuczną inteligencją, a erozją systemów ochrony praw człowieka, kryzysem demokracji oraz ewolucją współczesnych systemów politycznych, ze szczególnym uwzględnieniem wpływu mechanizmów wyborczych na kształtowanie się scen politycznych. Jako aktywny członek społeczności akademickiej odbył liczne międzynarodowe staże badawcze w ramach programu Erasmus+, w tym na uniwersytetach w Muğli (Turcja), Teneryfie oraz Grenadzie (Hiszpania). Poza działalnością akademicką posiada doświadczenie praktyczne jako członek i przedstawiciel UKW w Bydgoskiej Radzie ds. Praw Człowieka i Równego Traktowania przy Prezydencie Miasta Bydgoszczy, gdzie działa na rzecz przełożenia teorii praw człowieka na lokalną praktykę administracyjną.

Abstrakt: Technologia rozpoznawania twarzy (FRT) staje się coraz powszechniejszym narzędziem nadzoru cybernetycznego, wykorzystywanym zarówno przez organy państwa, jak i podmioty prywatne. Artykuł analizuje napięcie między efektywnością systemów FRT w zakresie zapewnienia bezpieczeństwa publicznego a ochroną podstawowych praw i wolności jednostki, takich jak prawo do prywatności (art. 8 EKPC), ochrona danych osobowych (RODO) oraz godność osobista. Autor wskazuje, że masowe, nieukierunkowane stosowanie rozpoznawania twarzy w przestrzeni publicznej – bez wyraźnej podstawy prawnej, nadzoru sądowego i mechanizmów proporcjonalności – może stanowić ingerencję o charakterze systemowym i nieproporcjonalnym, wykraczającą poza granice dopuszczalne w demokratycznym społeczeństwie. W opracowaniu omówiono kluczowe orzeczenia sądów europejskich (m.in. ETPC w sprawach dotyczących nadzoru masowego) oraz regulacje aktu w sprawie sztucznej inteligencji (AI Act), który klasyfikuje systemy biometrycznej identyfikacji w czasie rzeczywistym jako obarczone wysokim ryzykiem, a nawet zakazane, z wyjątkami ściśle określonymi. W konkluzji autor postuluje konieczność wyznaczenia wyraźnych „granic cybernetycznego nadzoru" – poprzez wymóg indywidualnej autoryzacji sądowej, ograniczenia czasowe i terytorialne oraz obowiązek transparentności i skutecznych środków odwoławczych.

Słowa kluczowe: rozpoznawanie twarzy, nadzór cybernetyczny, prywatność, prawa człowieka

dr **Daniel Damian Kasprzycki**, Wyższa Szkoła Kształcenia Zawodowego, ***Cyfrowy panoptykon 2.0: czy nadzór państwowy w sieci jest jeszcze narzędziem bezpieczeństwa, czy już formą kontroli społecznej?***

Doktor nauk społecznych, absolwent Akademii Marynarki Wojennej w Gdyni. Ekspert ds. bezpieczeństwa i wojskowości. Absolwent Instytutu Bezpieczeństwa i Spraw Międzynarodowych Dolnośląskiej Szkoły Wyższej we Wrocławiu (obecnie: Uniwersytet Dolnośląski DSW), które ukończył z wyróżnieniem w 2014 r. i studiów doktoranckich na Wydziale Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni, ukończonych z wyróżnieniem w 2021 r. Wychowanek prof. dr. hab. Piotra Mickiewicza.

W swojej karierze zawodowej pracował w różnych firmach krajowych i zagranicznych piastując stanowiska menedżerskie. Autor i współautor licznych monografii i artykułów naukowych publikowanych w uznanych czasopismach krajowych i zagranicznych, uczestnik krajowych i międzynarodowych konferencji naukowych. Jego badania naukowe koncentrują się na studiach nad współczesnymi konfliktami zbrojnymi, strategiami wojskowymi i zagrożeniami

asymetrycznymi – równolegle prowadzi badania nad cyberprzestrzenią jako polem współczesnej rywalizacji strategicznej ze szczególnym uwzględnieniem różnych aspektów dezinformacji i propagandy oraz konfliktów kognitywnych. W swojej pracy badawczej ceni sobie podejście interdyscyplinarne, łącząc perspektywy politologiczne, historyczne oraz nauk o bezpieczeństwie. Jego działalność dydaktyczna obejmuje prowadzenie zajęć z zakresu m.in. geopolityki, strategii, teorii bezpieczeństwa, zwalczania terroryzmu i historii wojskowości. Promotor prac licencjackich i prac magisterskich (na kilku różnych uczelniach), w tym wielu prac wyróżnionych.

Abstrakt: Rozwój technologii cyfrowych w istotny sposób przeobraził relacje między jednostką a państwem, szczególnie w kontekście mechanizmów nadzoru. Współczesny „cyfrowy panoptykon 2.0" wykracza poza tradycyjne modele kontroli, opierając się na zaawansowanej analizie danych, algorytmizacji procesów decyzyjnych oraz wykorzystaniu narzędzi predykcyjnych. Celem niniejszego referatu jest próba odpowiedzi na pytanie, czy nadzór państwowy w cyberprzestrzeni zachowuje charakter proporcjonalnego instrumentu zapewniania bezpieczeństwa, czy też ulega przekształceniu w formę systemowej kontroli społecznej.

Analizie poddane zostaną wybrane praktyki monitorowania, w tym retencja danych, stosowanie oprogramowania inwigilacyjnego oraz systemy identyfikacji biometrycznej, a także rola podmiotów prywatnych w procesach gromadzenia i udostępniania informacji. Istotnym punktem odniesienia będą również regulacje Unii Europejskiej oraz problem granic dopuszczalnej ingerencji państwa w sferę praw jednostki. Uwzględniona zostanie także koncepcja „efektu mrożącego", wpływającego na zachowania użytkowników w przestrzeni cyfrowej.

Przeprowadzone rozważania prowadzą do wniosku, iż granica między bezpieczeństwem a kontrolą ulega stopniowemu zatarciu, co rodzi potrzebę ponownego określenia standardów ochrony praw jednostki w warunkach społeczeństwa cyfrowego.

Słowa kluczowe: nadzór cyfrowy, panoptykon, cyberprzestrzeń, prywatność, bezpieczeństwo państwa, kontrola społeczna, big data, sztuczna inteligencja, prawa jednostki, inwigilacja, chilling effect

Digital Society Between Innovation and Social Challenges

Prof. Dr. **Darko Hinić**, University of Kragujevac (Serbia), Assoc. Prof. Dr hab. **Aleksandra Błachnio**, Kazimierz Wielki University in Bydgoszcz (Poland), Doc. Dr. **Gorana Rakić Bajić**, Union University (Serbia), ***Online disinhibition in students' social networks use and online gaming***

Darko Hinić - Full professor of General Psychology at the Department of Psychology, Faculty of Science, University of Kragujevac, Serbia. His research interests include social psychology, environmental psychology, and psychology of online behaviour.

Abstract: According to the concept of online disinhibition, Internet users are becoming more relaxed to freely express their attitudes online by time. They take greater emotional risks, express their opinions and make comments more readily. In the offline world, such a way of communication is often not possible due to fear of criticism or social rejection. This study is a part of an ongoing project (NAWA BPS/ZAP/2024/1/00102/I/1), exploring aspects of Internet use in student population, including online disinhibition. The sample included 1372 students (70% female), from all state universities in Serbia. They answered the socio-demographic questionnaire, Internet use questionnaire and DAR-5. On average, the participants reported not to behave differently online than offline; 27.2% found it easier to express disagreement in online communication and 18.1% to verbally attack someone online. Online disinhibition had a low positive correlation with the intensity of social networks use and online gaming (especially among players of certain genres). The implications of the results will be further discussed in the presentation, with a special focus on potential directions of preventive educational activities.
Keywords: online disinhibition, students, social networks, gaming.

Assoc. Prof. Dr hab. **Izabela Kapsa**, Assoc. Prof. Dr hab. **Aleksandra Błachnio**, Kazimierz Wielki University in Bydgoszcz (Poland), Prof. Dr. **Darko Hinić**, University of Kragujevac (Serbia)

, Digital Safety, and Online Experiences among University Students – Cross-Cultural Variations

Izabela Kapsa [ORCID: 0000-0003-2342-3682] is an Associate Professor and Head of the Department of Political and Digital State at Kazimierz Wielki University in Bydgoszcz, Poland. She is a political scientist and psychologist specializing in the role of digital technologies in shaping civic participation, public opinion, and democratic engagement.

Her research focuses on e-participation, digital governance, and citizens' resilience to disinformation and information warfare. She examines young people's political preferences, digital resilience, and forms of political engagement in the context of new technologies. She applies mixed-methods approaches, including survey research and quantitative data analysis.

She is actively engaged in international academic collaboration and delivers training in communication and digital competences. She has participated in multiple international projects, including research on e-voting systems and digital and psychological resilience. email: izabela.kapsa@ukw.edu.pl

Aleksandra Błachnio [ORCID 0000-0003-0756-7416] affiliated with Kazimierz Wielki University in Bydgoszcz, and University of Applied Sciences in Elbląg. In 2020, she achieved a postdoctoral degree in psychology from the University of Gdańsk. Her interests are diverse, encompassing quality of life, aging, globalization, personality and resilience. Author of several monographs: *Potential of People in Old Age: Sense of Quality of Life in the Process of Aging* (2019); *Non-Profit Old Age: Volunteering at Third Age Universities in Poland and Around the World* (2012); *Self - Author in the Era of Globalization* (2011); *Volunteering at Third Age Universities* (2008); *Self-Author in the Third Wave of Civilization* (2006). Translator of '*Psychology of Aging'* by Stuart-Hamilton in 2006 or '*Multiple Pathways of Cognitive Aging. Motivational and Contextual Influences*' edited by Sędek, Hess, & Touron in 2025.

Darko Hinić - Full professor of General Psychology at the Department of Psychology, Faculty of Science, University of Kragujevac, Serbia. His research interests include social psychology, environmental psychology, and psychology of online behaviour.

Abstract: University students live their online and offline lives simultaneously. The aim of the study is to analyse and compare possible relations between students' readiness to apply digital safety measures, and their online social experiences across different cultures (Serbia, Italy, and Poland). We primarily focus on negative experiences in social interactions. The survey included 523 students, 66% female, Mage = 22.37±2.51. All the participants completed a demographic questionnaire, a questionnaire on applying Active/Passive digital safety measures, and Negative online experiences. The results are discussed according to the Hofstede's Cultural Dimensions Theory. Our results support the thesis that with the use of digital technologies, especially in the area of social interaction, certain differences can still be found in cultural characteristics and social norms of the users. We believe that it would be useful to further examine these differences in order to come up with recommendations on how to better understand online behaviours and empower users of DT to better respond to possible negative online experiences.

Keywords: digital safety measures; negative online experiences; psychological resilience

Dr **Morena Boja**, PhDAleksandër Moisiu University, Durrës (Albania), ***Artificial intelligence in higher education: A study of how UAMD students use AI for learning***

Dr. Morena Boja is a lecturer at Aleksandër Moisiu University of Durrës at the Faculty of Political Science and Law, Department of Public Administration. She teaches a range of courses, including Central and Local Government, Public Economic Policy, Macroeconomics, and Microeconomics. Her research focuses on the digital transformation of governance, with particular attention to the digitalization of public administration and local government. Additional research interests include the management of public funds, digital political marketing, and the role of digitalization in strengthening transparency and accountability at both central and local government levels. Dr. Boja also explores how digital platforms can be used to enhance community engagement, support civic initiatives, and improve communication between citizens and public institutions, particularly in facilitating the submission of complaints, petitions, and participatory processes

Abstract: Artificial intelligence (AI) has increasingly transformed multiple sectors of society, including higher education. The growing integration of digital technologies into the learning process has made the use of AI-based tools a common practice among university students. This study aims to analyse the extent to which students at Aleksandër Moisiu University of Durrës (UAMD) use artificial intelligence for educational purposes. The research focuses on students from different faculties and study cycles, including bachelor's, master's, and doctoral programs. To address the research objectives, a structured questionnaire was developed and distributed to students. The collected data will be analysed using SPSS to identify patterns of AI use in academic activities. The study examines how artificial intelligence tools are used to support academic tasks, facilitate knowledge acquisition, and contribute to the development of students' learning skills. The findings indicate a significant increase in the use of AI tools among students, particularly for summarising academic materials, explaining complex concepts, and

supporting academic writing. At the same time, the research highlights several challenges, including limited critical evaluation of AI-generated information and the potential risk of over-reliance on technological tools. Furthermore, the study explores students' perceptions regarding the possible integration of artificial intelligence as an institutional educational tool within the university. This issue requires careful consideration and collaboration between academic staff and policymakers to balance the benefits of AI in facilitating learning with the need to strengthen students' critical thinking skills through academic discussions, debates, and case-based learning.

Keywords: artificial intelligence, higher education, students, digital learning tools, academic performance, universities

Doç. Dr. **Ülke Evrim Uysal**, Istanbul Beykent University (Turkey), ***The Sovereign vs. the Seamless: A Comparative Study of Digital Urbanism in Barcelona and Singapore***

Researcher and lecturer at Istanbul Beykent University. He received his Bachelor's Degree from Department of Political Science and Public Administration, Middle East Technical University and Department of History, Istanbul University; Master's Degree from Department of Public Administration, University of Istanbul and Doctoral Degree from Department of Social Research, University of Helsinki. His main research areas are urban history, urban regeneration, urban tourism and city branding.

Abstract: This study provides a comparative analysis of two contrasting models of digital governance: Singapore's Centralised Efficiency model and Barcelona's Distributed Sovereignty model. Drawing on the urban theory of 'the right to the city' by Lefebvre and 'the digital panopticon by Foucault', it examines how each city mediates the relationship between the individual and the state through cyberspace.

In Singapore, the state uses a digital twin and Singpass ecosystem to create a 'frictionless' urban experience where individuals are integrated into a top-down framework of precision governance. In contrast, Barcelona's 'Digital City' initiative uses decentralised technologies (e.g. DECODE, Decidim) to give individuals ownership of their data, thereby fostering a data commons. While Singapore prioritises urban optimisation and national security, Barcelona emphasises technological sovereignty and participatory democracy. The study concludes that both models represent a significant departure from traditional urbanism, moving towards a 'phygital' reality in which political agency is defined by one's relationship with data. The research concludes that the future of global urbanism lies in the tension between these two poles: the desire for an efficient, state-managed city versus the demand for a transparent, citizen-owned digital realm.

Keywords: Data sovereignty, platform urbanism, participatory democracy, digital twin, Singapore, Barcelona

Dr **Majlinda Velcani** PhD, Dr **Evelina Lusha**, PhD, Aleksandër Moisiu University, Durrës (Albania), ***Digitalization of public services: evaluation of efficiency and use by citizens***

PhD **Majlinda Velçani** is a lecturer at the Department of Public Administration, at the "Aleksandër Moisiu" University, Durrës. She graduated in Law at the Faculty of Law, University of Tirana. She completed her Doctoral Studies at the University of National and World Economy in Sofia, Bulgaria, at the Department of Public Law, in the profile "Theory of State and Law. Political and Legal Studies". She is a member of several international and national scientific research projects. Member of the scientific boards of international scientific journals and of the organizational boards of national and international conferences. She has received Certification from the Center for International Relations and Balkan Studies for conducting trainings in the field of "Social Harmony and Conflict Resolution". Majlinda Velçani is the author and co-author of dozens of publications in scientific journals and participant in regional, national and international conferences.

Dr. **Evelina Lusha** is a lecturer and researcher at Aleksandër Moisiu University in Durrës, Albania, specializing in international relations, public governance, and sustainable development. Her work focuses on the intersection of intellectual capital, policy-making, and institutional performance, particularly in the context of European integration and emerging global challenges. She has contributed to a range of international publications and conferences, addressing topics such as digital transformation, supply chain resilience, and economic governance. Through her research, Dr. Lusha aims to bridge theory and practice by advancing policy-relevant insights that support institutional reform, innovation, and long-term sustainability in developing and transition economies.

Abstract: This study seeks to examine the digitalization process of public services in Albania, emphasizing an evaluation of their efficiency and the extent of citizen usage. The digital transformation of public services represents a key aspect of modernizing local administration and enhancing the interaction between institutions and residents. Over recent decades, advancements in information and communication technologies have altered how public entities deliver services and engage with citizens. The digitalization of public services has emerged as a strategic focus for governments globally, as it offers the potential for heightened administrative efficiency, cost reductions, greater transparency, and enhanced user experience. In this light, the local administration in Albania has made significant progress towards achieving digital transformation, aiming to modernize its processes and make services more accessible to citizens. Municipalities, being the initial point of contact for citizens with public administration, are crucial in executing digitalization projects. The establishment of electronic platforms and the automation of administrative tasks are vital steps towards fulfilling these objectives. Nevertheless, the success of digitalization should not solely be assessed by the availability of online services but also by how extensively they are utilized by citizens and the tangible impact on improving institutional efficiency. Despite the advancements made, the digitalization efforts at the local level in Albania face several hurdles. These challenges include varying levels of digital literacy among citizens, a lack of confidence in electronic services, infrastructural constraints, and the ongoing need to enhance administrative capabilities. Therefore, a thorough analysis is essential to evaluate not only the presence of digital services but also their actual performance and user perceptions. The research employs both qualitative and quantitative approaches, including an analysis of official documents, surveys of citizens, and interviews with local administration officials. The findings aim to underscore the concrete advantages of

digitalization, such as reduced service wait times, increased transparency, and better access, while also addressing the challenges related to digital literacy, public trust, and technological infrastructure. Through this analysis, the paper offers an evaluation of the current state of digital transformation and suggests practical recommendations for boosting the utilization and enhancing the quality of electronic services.

Keywords: digitalization, public services, efficiency, use by citizens, electronic governance

Sztuczna inteligencja, algorytmy i przyszłość demokracji

dr hab. **Artur Laska**, prof. ucz., Uniwersytet Kazimierza Wielkiego w Bydgoszczy,

Polityczne konsekwencje erozji suwerenności poznawczej w realiach martwego internetu i niesprawiedliwości epistemicznej

Politolog, profesor uczelni oraz dziekan Wydziału Nauk o Polityce i Administracji Uniwersytetu Kazimierza Wielkiego w Bydgoszczy, a także członek Komitetu Nauk Politycznych PAN. Specjalizuje się w teorii polityki oraz polityce miejskiej, w szczególności w zagadnieniach rozwoju, innowacyjności i przywództwa.

Abstrakt: Ekspansja sztucznej inteligencji i algorytmizacja sfery publicznej podważają fundamenty demokratycznej deliberacji. Referat stawia tezę, że zjawisko martwego internetu - środowiska zdominowanego przez zautomatyzowane treści - generuje strukturalną niesprawiedliwość epistemiczną, której politycznym skutkiem jest erozja suwerenności poznawczej obywatela. Analizę osadzono w teoriach M. Fricker, J. Habermasa i P. Bourdieu. Innowacją pojęciową jest przeniesienie kategorii suwerenności na grunt politologii. Referat stanowi efekt badań teoretycznych, opartych na wnioskowaniu abdukcyjnym, analizie pojęciowej oraz krytycznej syntezie literatury. Celem wystąpienia jest zbudowanie ramy eksplanacyjnej dla dalszych programów badawczych. Analiza prowadzi do wniosku, że erozja suwerenności poznawczej należy do kluczowych mechanizmów współczesnego kryzysu sfery publicznej, ponieważ zmienia relację między obiegiem wiedzy, sprawczością obywatelską i legitymizacją władzy.

Słowa kluczowe: suwerenność poznawcza, martwy internet, niesprawiedliwość epistemiczna, populizm, polaryzacja społeczna, media społecznościowe, algorytmizacja, sztuczna inteligencja

dr **Wojciech Mincewicz**, Szkoła Główna Gospodarstwa Wiejskiego w Warszawie,

Pomiar i typologia postaw wobec generatywnej sztucznej inteligencji

Doktor nauk społecznych w dyscyplinie nauka o polityce i administracji (2023, summa cum laude). Politolog, socjolog, broker informacji, wykładowca akademicki. Obecnie adiunkt badawczo-dydaktyczny w Katedrze Socjologii Instytutu Nauk Socjologicznych i Pedagogiki Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie. Autor ponad 40 recenzowanych publikacji akademickich opublikowanych w międzynarodowych oraz ogólnopolskich

czasopismach i wydawnictwach naukowych. Wygłosił ponad 50 referatów w trakcie międzynarodowych oraz ogólnopolskich kongresów i konferencji naukowych. Za osiągnięcia w pracy naukowej wyróżniony między innymi stypendium Ministra Nauk i Szkolnictwa Wyższego dla wybitnych młodych naukowców na lata 2024-2027 oraz nagrodą indywidualną Rektora SGGW (2025). Jego zainteresowania naukowe obejmują zagadnienia z zakresu polityczno-społecznych aspektów funkcjonowania kryptowalut i technologii blockchain, sztucznej inteligencji, bezpieczeństwa w cyberprzestrzeni, wywiadu jawnoźródłowego oraz partycypacji politycznej.

Abstrakt: W trakcie wystąpienia przedstawiony zostanie sposób pomiaru oraz typologia postaw wobec generatywnej sztucznej inteligencji na podstawie badań przeprowadzonych wśród dorosłych Polaków. W projekcie zastosowano skalę pomiarową obejmującą zestaw twierdzeń dotyczących ocen, obaw i akceptacji różnych zastosowań tej technologii, na podstawie której skonstruowano syntetyczny indeks postawy. Analiza uzyskanych wyników pozwoliła na uchwycenie kontinuum ocen oraz wyróżnienie kilku typów postaw – od wyraźnie sceptycznych, przez ambiwalentne, po afirmatywne. W referacie omówiono także wybrane czynniki społeczno-demograficzne różnicujące badane postawy. Wyniki stanowią próbę uporządkowania społecznych reakcji na rozwój generatywnej sztucznej inteligencji oraz wskazują na znaczenie kontekstu społecznego w ich kształtowaniu.

Słowa kluczowe: generatywna sztuczna inteligencja, postawy, opinie, typologia, pomiar

dr hab. **Arkadiusz Lewandowski**, prof. ucz., dr **Marcin Polakowski**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Niecierpliwa demokracja. Jednostka i państwo w dobie zmian technologicznych***

Arkadiusz Lewandowski, Wydział Nauk o Polityce i Administracji Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Autor bądź współautor kilkudziesięciu artykułów naukowych oraz monografii (m.in. Między upodmiotowieniem a upolitycznieniem. Polski samorząd terytorialny w realiach (kryzysu) demokracji liberalnej po 1989 roku (2022), Akcja Wyborcza Solidarność. Centroprawica w poszukiwaniu modelu współpracy (2016). Jego zainteresowania badawcze obejmują zagadnienia teorii współczesnego kryzysu demokracji liberalnej oraz elit parlamentarnych w Polsce. Współpracownik czasopism naukowych „Dyskurs & Dialog" (Redaktor naczelny) oraz „Studia Politicae Universitatis Silesiensis" (Zastępca redaktora naczelnego).

Marcin Polakowski, Wydział Nauk o Polityce i Administracji Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Autor m.in. monografii naukowej *Sceptycyzm w polityce. Studium myśli politycznej Michaela Oakeshotta* (2017), kilkunastu przekładów artykułów i książek naukowych z języka angielskiego na język polski oraz kilkudziesięciu artykułów naukowych. Jego zainteresowania badawcze koncentrują się na teorii populizmu, kondycji współczesnej demokracji oraz współczesnej teorii, filozofii i myśli politycznej.

Abstrakt: Dynamiczny rozwój nowych technologii fundamentalnie przekształcił sferę oczekiwań obywateli względem demokracji. Doświadczenie codziennej „natychmiastowości" wchodzi w głęboki konflikt z tradycyjną, powolną dynamiką instytucji demokratycznych.

Podczas gdy cyfrowe środowisko przyzwyczaja jednostkę do natychmiastowej gratyfikacji, procedury państwa wymagają czasu, co rodzi syndrom „niecierpliwej demokracji".
Wystąpienie, ma na celu operacjonalizację wymienionego zagadnienia. Odwołując się do koncepcji J. Haidta (metafora jeźdźca i słonia) oraz H. Rosy (teoria przyspieszenia), stawiamy tezę, że algorytmy platform społecznościowych systemowo wzmacniają afektywne reakcje jednostek, niszcząc przestrzeń dla deliberacji i kompromisu.
Zjawisko to prowadzi do kryzysu demokracji liberalnej oraz paradoksu podmiotowości: budująca swoją podmiotowość jednostka staje się jednocześnie obiektem algorytmicznej manipulacji. W efekcie współczesna polityka, poddana presji permanentnego monitorowania, traci zdolność do długofalowego planowania, stając się zakładnikiem reaktywnego zarządzania kryzysowego.
Słowa kluczowe: niecierpliwa demokracja, kryzys demokracji, nowe technologie, algorytmy.

dr **Jarosław Spychała**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, ***Sztuczna inteligencja a demokracja – przegląd wybranych stanowisk***

Doktor nauk humanistycznych w zakresie filozofii. Naukowo zajmuje historią filozofii i religii, a szczególnie zjawiskiem przenikania się religii i filozofii w zakresie wyobrażeń o pośmiertnych losach człowieka oraz ich wpływem na szeroko rozumianą komunikację (np. na komunikację marketingową, polityczną oraz na narracje filmowe czy literackie). Ponadto prowadzi badania poświęcone idei sztucznych istot w kulturze, w szczególności tradycji mitu Golema, oraz możliwościom zastosowania sztucznej inteligencji w edukacji, kulturze, polityce, demokracji i gospodarce.
Autor publikacji naukowych i popularnonaukowych z zakresu filozofii i historii religii, m.in: Heracles, Jesus Christ and Lord Vader at the Crossroads. The ethical message of the ΛΕΓΩ-ΛΟΓΟΣ method; Die Höhle. Der Weg der Rebellen; Mali Rebelianci, Jaskinia. Droga rebeliantów; Eracle, Gesù Cristo e Darth Vader al bivio. Il messaggio etico del metodo LEGO-LOGOS; Herakles, Jezus Chrystus i Lord Vader na rozstajnych drogach; Bulletproof – platońskie przesłanie ΛΕΓΩ-ΛΟΓΟΣ, ΛΕΓΩ-ΛΟΓΟΣ: czytać, myśleć, mówić.
Abstrakt: Celem artykułu jest omówienie wybranych stanowisk w kwestii wpływu AI na funkcjonowanie demokracji (m.in. Boden, 2020; Boine, 2024; Buchanan, 2022; Chamarthy, 2024; Chehoudi, 2025; Coeckelbergh, 2023; Crawford, 2024; Das, 2024; Innerarity, 2024; Jungherr, 2023; Kan, 2024; Kaplan, 2019; Kurzweil, 2024; Nemitz, 2023; Olson, 2025; Przegalińska, 2020; Puaschunder, 2020; Risse, 2021; Sudmann, 2019; Summerfield, 2024). Rozważania rozpoczynają się od opisania zmiany dokonującej się w dyskursie publicznym polegającej na przejściu od uproszczonych narracji apokaliptycznych w kierunku bardziej zniuansowanych narracji ujmujących wpływ AI na demokrację w kategoriach metafor „obusiecznego miecza" lub „janusowego oblicza" wskazujących zarówno potencjalne szanse jak i ryzyka płynące z szerokiego zastosowania technologii cyfrowych. Następnie szczegółowo zostaje omówione zagadnienie oddziaływanie AI na jakość demokracji, które ogniskuje się w czterech domenach: polityczny charakteru sztucznej inteligencji; wpływ AI na proces wyborczy; wpływ AI na proces deliberacji obywatelskiej; wpływ AI na sądownictwo, system

fiskalny i socjalny. Artykuł kończą wnioski i rekomendacje działań mogących zapobiegać negatywnym skutkom wpływu AI na demokrację.

Słowa kluczowe: sztuczna inteligencja, demokracja, władza algorytmiczna, deliberacja obywatelska, cyfrowy autorytaryzm, niesprawiedliwość algorytmiczna

dr **Joanna Wieczorek-Orlikowska**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy,

Niewidzialna władza algorytmów - podmiotowość polityczna w warunkach cyfrowej kontroli

Adiunkt na Wydziale Nauk o Polityce i Administracji Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Jej zainteresowania badawcze obejmują teorię polityki, myśl polityczną, społeczne studia nad nauką i technologią, posthumanizm oraz sztuczną inteligencję. W badaniach koncentruje się na przemianach podmiotowości politycznej, sprawstwa i władzy w kontekście dynamicznych zmian współczesnego świata.

Abstrakt: Referat podejmuje problem wpływu algorytmów i systemów opartych na sztucznej inteligencji na podmiotowość polityczną jednostki w cyberprzestrzeni. Przestrzeń cyfrowa, choć często opisywana jako obszar wolności, komunikacji i partycypacji obywatelskiej, coraz wyraźniej staje się także środowiskiem kontroli, profilowania, selekcji informacji oraz algorytmicznego sterowania zachowaniami użytkowników. Celem wystąpienia jest analiza tego napięcia z perspektywy teorii polityki. Szczególna uwaga zostanie poświęcona mechanizmom personalizacji treści, systemom rekomendacyjnym, mikrotargetowaniu politycznemu, automatyzacji decyzji oraz predykcyjnym formom zarządzania ryzykiem. Algorytmy zostaną ujęte nie jako neutralne narzędzia techniczne, lecz jako elementy szerszych sieci władzy, współkształtujących dostęp do informacji, widzialność określonych treści, możliwości uczestnictwa i zakres autonomii obywatelskiej. Główna teza referatu zakłada, że podmiotowość polityczna jednostki w cyberprzestrzeni nie zanika, lecz ulega przekształceniu. Sprawstwo obywatela jest coraz silniej zapośredniczone przez dane, platformy i nieprzejrzyste systemy algorytmiczne.

Słowa kluczowe: algorytmy; podmiotowość polityczna; cyberprzestrzeń; cyfrowa kontrola; sztuczna inteligencja; sprawstwo; władza;

dr **Marcin Leźnicki**, Uniwersytet Mikołaja Kopernika w Toruniu,

Biowładza w epoce cyfrowej: od medykalizacji do algorytmicznej kontroli ciała i zdrowia

Filozof i bioetyk, adiunkt związany z Uniwersytetem Mikołaja Kopernika w Toruniu. Jego zainteresowania badawcze koncentrują się wokół etyki szczegółowej i praktycznej, w tym bioetyki, aksjomedycyny, filozofii medycyny, deontologii lekarskiej, ekofilozofii oraz etyki środowiskowej. W swoich publikacjach podejmuje m.in. zagadnienia reprogenetyki, biomedykalizacji życia ludzkiego, genetycznego udoskonalania człowieka oraz etycznych i filozoficznych konsekwencji rozwoju biomedycyny. Istotne miejsce w jego refleksji zajmują również pytania o wartość życia ludzkiego, tożsamość osobową człowieka, granice interwencji technologicznych oraz miejsce człowieka wobec wyzwań transhumanizmu i posthumanizmu.

Abstrakt: Wystąpienie podejmuje problem przemian medykalizacji w warunkach cyfryzacji życia społecznego. Punktem wyjścia jest teza, że współczesna kontrola ciała i zdrowia coraz rzadziej ma charakter wyłącznie instytucjonalny, a coraz częściej przybiera postać rozproszonej, algorytmicznej biowładzy, która działa poprzez dane, profilowanie ryzyka, technologie monitorowania i systemy wspierania decyzji. W takim ujęciu medykalizacja nie oznacza już jedynie rozszerzania zasięgu medycyny, lecz także przekształcanie osoby w obiekt ciągłej klasyfikacji, oceny i optymalizacji. Szczególnie wyraźnie widać to w obszarze reprodukcji, estetyzacji ciała oraz praktyk genetycznego i technicznego ulepszania człowieka. Celem referatu jest pokazanie, że cyfrowa transformacja biomedycyny wzmacnia napięcie między autonomią jednostki a nowymi formami kontroli, które mogą prowadzić do subtelnej normalizacji selekcji, presji doskonalenia i redefinicji granic tego, co uznawane jest za „zdrowe" i „właściwe". W zakończeniu zaproponowana zostanie bioetyczna interpretacja tych procesów, oparta na obronie podmiotowości osoby, krytyce redukcji człowieka do danych oraz ostrożności wobec technicznej obietnicy pełnej optymalizacji życia.
Słowa kluczowe: biowładza, medykalizacja, kontrola algorytmiczna, autonomia ciała, zdrowie, bioetyka

Cyberbezpieczeństwo i cyfryzacja usług publicznych

dr **Joanna Antczak**, dr **Anna Owczarczyk**, Wojskowa Akademia Techniczna,

Zarządzanie cyberbezpieczeństwem w ochronie zdrowia

Joanna Antczak posiada stopień naukowy doktora nauk ekonomicznych jest adiunktem na Wydziale Bezpieczeństwa, Logistyki i Zarządzania Wojskowej Akademii Technicznej oraz od 1 grudnia 2024 r. pełni funkcję Zastępcy Dyrektora ds. Naukowych Instytutu Zarządzania. Zainteresowania badawcze koncentruje wokół zagadnień zarządzania jednostką gospodarczą w zmiennym i wymagającym otoczeniu. Obejmują one w szczególności: zarządzanie cyberbezpieczeństwem, zarządzanie finansami, controlling i jego zastosowanie w przedsiębiorstwie, a także bezpieczeństwo gospodarczo-obronne państwa, w tym bezpieczeństwo w cyberprzestrzeni. Istotnym obszarem jej badań jest również zrównoważony rozwój organizacji, ze szczególnym uwzględnieniem standardów godnej pracy oraz roli zarządzania zasobami ludzkimi w budowaniu odpowiedzialnych, odpornych i etycznych struktur.

Anna Owczarczyk - moje zainteresowania naukowe dotyczą ekonomicznych i organizacyjnych uwarunkowań funkcjonowania sektora publicznego, szczególnie ochrony zdrowia. Zajmuję się tematyką finansów ochrony zdrowia, poziomu i struktury wydatków zdrowotnych oraz ich efektywności. Interesują mnie także zmiany zachodzące w systemie ochrony zdrowia, zwłaszcza opieka koordynowana i zintegrowana, polityka zdrowotna oraz wpływ cyfryzacji na organizację i jakość świadczeń. Od kilku lat analizuję również kwestie zarządzania cyberbezpieczeństwem w podmiotach ochrony zdrowia. W swoich badaniach łączę perspektywę ekonomiczną, instytucjonalną i zarządczą.

Abstrakt: Cyberbezpieczeństwo w ochronie zdrowia jest dziś jednym z kluczowych wyzwań zarządczych. Placówki medyczne przetwarzają ogromne ilości danych wrażliwych, a jednocześnie coraz szerzej korzystają z systemów informatycznych, dokumentacji elektronicznej i usług cyfrowych. To zwiększa ryzyko ataków, wycieków danych i zakłóceń w pracy podmiotów leczniczych. Wystąpienie dotyczy zarządzania cyberbezpieczeństwem w ochronie zdrowia z perspektywy: systemu ochrony zdrowia oraz podmiotów świadczących usługi zdrowotne. Omówione zostaną najważniejsze zagrożenia, a także przykłady wybranych ataków na placówki zdrowotne. Przedstawione będą także podstawowe elementy skutecznego systemu ochrony. Ważnym elementem prezentacji będzie również pokazanie, że cyberbezpieczeństwo nie jest wyłącznie problemem technicznym, ale częścią jakości zarządzania i bezpieczeństwa pacjenta.
Słowa kluczowe: Cyberbezpieczeństwo, ochrona zdrowia, zarządzanie

mgr **Małgorzata Wenderlich**, Uniwersytet WSB Merito, ***Transformacja kontroli płatników składek w Zakładzie Ubezpieczeń Społecznych w warunkach cyfryzacji i analizy ryzyka***

Absolwentka politologii (specjalność regionalno-samorządowa) oraz administracji na Uniwersytecie Kazimierza Wielkiego w Bydgoszczy, a także finansów i rachunkowości w Wyższej Szkole Bankowej w Toruniu. Ukończyła liczne studia podyplomowe, w tym z zakresu rachunkowości budżetowej, audytu wewnętrznego i kontroli zarządczej w jednostkach sektora finansów publicznych oraz zarządzania. Obecnie kształci się w ramach Kolegium doktorskiego. Posiada kilkunastoletnie doświadczenie zawodowe zdobywane w administracji publicznej, w tym w rządowej administracji zespolonej, oraz w szkolnictwie wyższym, w dużej mierze związane z obszarem kontroli. Jej zainteresowania koncentrują się wokół zagadnień kontroli płatników składek, audytu oraz funkcjonowania finansów publicznych, ze szczególnym uwzględnieniem procesów cyfryzacji administracji publicznej.

Abstrakt: W warunkach postępującej cyfryzacji administracji publicznej oraz rosnącego znaczenia analizy ryzyka obserwuje się zmianę modelu kontroli płatników składek realizowanej przez Zakład Ubezpieczeń Społecznych. Coraz większe znaczenie ma przejście od kontroli powszechnej do selektywnej, opartej na typowaniu podmiotów.

Celem wystąpienia jest ocena wpływu cyfryzacji i analizy ryzyka na funkcjonowanie systemu kontroli. Badanie opiera się na analizie instytucjonalno-prawnej oraz danych empirycznych ZUS z lat 2019–2024, obejmujących liczbę kontroli, wartość ujawnionych nieprawidłowości oraz skuteczność typowania.

Wyniki wskazują na spadek liczby kontroli w 2020 r., a następnie ich stopniową odbudowę przy wzroście wartości ujawnianych nieprawidłowości. Zauważalny jest również wzrost znaczenia analizy ryzyka jako narzędzia selekcji, przy jednoczesnym zróżnicowaniu jej skuteczności. Wzrasta rola analizy ryzyka, choć jej skuteczność pozostaje zróżnicowana. Wnioski potwierdzają wzrost efektywności kontroli przy jednoczesnej potrzebie dalszego doskonalenia mechanizmów analitycznych.

Słowa kluczowe: kontrola administracyjna; Zakład Ubezpieczeń Społecznych; płatnicy składek; analiza ryzyka; cyfryzacja administracji publicznej; kontrola selektywna; ubezpieczenia społeczne; administracja publiczna; państwo regulacyjne

mgr **Oskar Stefański**, Uniwersytet Mikołaja Kopernika w Toruniu,

Transformacja energetyczna a cyberzagrożenia - jak przeciwdziałać zagrożeniom cyfrowym w procesie transformacji energetycznej?

Doktorant w Szkole Doktorskiej Nauk Społecznych Uniwersytetu Mikołaja Kopernika w Toruniu. Magister Stosunków Międzynarodowych. Członek zespołu Climatrix Lab w ramach Priorytetowego Obszaru Badawczego na UMK w Toruniu. Uczestnik na kilkudziesięciu konferencjach naukowych, w tym w pierwszej edycji Konferencji: "Jednostka i państwo w cyberprzestrzeni". Autor wielu artykułów naukowych z zakresu polityki nordyckiej i polityki energetycznej.

Abstrakt: Transformacja energetyczna dotyczy przejścia z systemu energetycznego opartego na nieczystych źródłach energii na system oparty na czystych źródłach energii. Za czystość źródeł energii rozumie się przede wszystkim ich niską emisję gazów cieplarnianych i niski negatywny wpływ na środowisko.

Cyberzagrożenia są potencjalną barierą o charakterze technologicznym, która może spowalniać transformację energetyczną. Przez następujący postęp technologiczny i zwiększającą się rolę nowych technologii w systemach energetycznych zagrożenia te mogą stanowić barierę dla procesu. Kluczowe jest sprawnie im przeciwdziałać, co jest współcześnie jednym z przedmiotów badań nad barierami w transformacji energetycznej. Celem wystąpienia jest przedstawienie sposobów przeciwdziałania barierom w transformacji energetycznej będącymi cyberzagrożeniami. Przedstawiony zostanie problem badawczy P: Jakie są zalecane w literaturze i dokumentach organizacji międzynarodowych sposoby przeciwdziałania cyberzagrożeniom w transformacji energetycznej? Zastosowana zostanie jakościowa analiza źródeł. Będą nimi źródła: literatura przedmiotu i dokumenty organizacji międzynarodowych dotyczące cyberzagrożeń w energetyce.

Słowa kluczowe: transformacja energetyczna, cyberzagrożenia, nowe zagrożenia cyfrowe

mgr **Maciej Ciepluch**, Uniwersytet Kazimierza Wielkiego w Bydgoszczy,

Cyberbezpieczeństwo w jednostkach samorządu terytorialnego

mjr SW w stanie spoczynku, magister politologii, licencjat administracji, asystent dydaktyczny Wydziału Nauk o Polityce i Administracji UKW

Abstrakt: W dniu 1 stycznia 1999 r. w Polsce została wprowadzona w życie reforma samorządu terytorialnego. Aktualnie w Polsce funkcjonuje 16 województw, 380 powiatów, 2479 gmin. Przedmiotowe jednostki realizują zadania publiczne na potrzeby mieszkańców. Urzędy pracują w coraz bardziej zdygitalizowanym świecie e-administracji. Samorząd terytorialny przetwarza m.in. dane osobowe i musi zapewnić ich ochronę. Dodatkowo należy skupić się nad metodami zapewniającymi bezpieczeństwo informacji w urzędach oraz ciągłości ich pracy. Krajowe rozwiązania muszą być wdrożone przez jednostki samorządu terytorialnego RP. W ten

sposób Polska zapewni swoje cyberbezpieczeństwo w dwóch filarach administracji publicznej. Obecnie wprowadzane są zmiany w ustawie o krajowym systemie cyberbezpieczeństwa. W wykładzie przedstawiono analizę znaczenia cyberbezpieczeństwa dla jednostek samorządu terytorialnego oraz kierunek zmian. Przedstawiono hipotezę mówiącą o budowaniu w RP nowoczesnego cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Jako metodę wykorzystano analizę literatury i innych materiałów.
Słowa kluczowe: cyberbezpieczeństwo, e-administracja, samorząd terytorialny

Spis abstraktów

Kwiatkowski Przemysław: UE wobec zwalczania dezinformacji w sieci: architektura regulacyjna, egzekwowanie prawa i wyzwania technologiczne

Laska Artur: Polityczne konsekwencje erozji suwerenności poznawczej w realiach martwego internetu i niesprawiedliwości epistemicznej

Lefebvre Geoffrey: The Proliferation of Cyberattacks in France: Implications for Political Trust and Institutional Legitimacy

Lewandowski Arkadiusz, Polakowski Marcin: Niecierpliwa demokracja. Jednostka i państwo w dobie zmian technologicznych

Leźnicki Marcin: Biowładza w epoce cyfrowej: od medykalizacji do algorytmicznej kontroli ciała i zdrowia

Mateja Magdalena: Między empatią a nadużyciem: wybrane patologie cyfrowego aktywizmu na rzecz zwierząt

Mincewicz Wojciech: Pomiar i typologia postaw wobec generatywnej sztucznej inteligencji

Opioła-Cegiełka Monika: Cyfrowe dziedzictwo pamięci. Szanse i zagrożenia dla upamiętniania w erze AI

Panciszko-Szweda Barbara: Dostępność cyfrowa na obszarach wiejskich w Polsce

Panek Joanna: Od VUCA do BANI: implikacje dla bezpieczeństwa i odporności łańcuchów dostaw

Pazderska Agnieszka: Rola internetu i AI w ewolucji zasady równości w obliczu narastającej polaryzacji

Perlikowski Łukasz, el Ouadie Oussama: Artificial Intelligence between dialectics and demonstration

Potz Maciej: Human rights under pressure: a future-oriented conception of universal rights

Rosicki Remigiusz: Prawne aspekty przestępstwa pozorowanej pornografii dziecięcej (problem deepfake'ów)

Różycki Bartłomiej: Desokupa TV – kanał influencerski czy nowy głos hiszpańskiej prawicy?

Savov Ilin: Cyber Risk and Protection in the Age of Quantum Communication

Sierzputowska Kamila: Protecting Poland's information space: the role of state institutions, the private sector and civil society

Sikora-Gaca Małgorzata: Od transferu do inkluzji: dostępność cyfrowa jako nowy wymiar polskiej polityki rozwojowej

Sommella Valentina: The Digital Silk Road and China's Role in the Global Innovation System

Spychała Jarosław: Sztuczna inteligencja a demokracja – przegląd wybranych stanowisk

Stefański Oskar: Transformacja energetyczna a cyberzagrożenia – jak przeciwdziałać zagrożeniom cyfrowym?

Sukma Isti Marta: Do Alliances Make Policies Alike? Cybersecurity Policy Convergence Within the Five Eyes

Szorc Anna, Błachnio Aleksandra: Postawy wobec uchodźców przykładem wolności czy utraty kontroli? Raport z adaptacji nowego narzędzia

Trempała Wojciech: Między nadmiarem a niedostępnością: selektywna ekspozycja informacyjna młodych a ograniczenia partycypacji społecznej

Usiak Jaroslav: Recoding Security in Cyberspace: The Paradox of State Control and Civil Liberties in Slovakia

Uysal Ülke Evrim: The Sovereign vs. the Seamless: A Comparative Study of Digital Urbanism in Barcelona and Singapore

Velcani Majlinda, Lusha Evelina: Digitalization of public services: evaluation of efficiency and use by citizens

Wenderlich Małgorzata: Transformacja kontroli płatników składek w ZUS w warunkach cyfryzacji i analizy ryzyka

Wieczorek-Orlikowska Joanna: Niewidzialna władza algorytmów – podmiotość polityczna w warunkach cyfrowej kontroli

Wielewska Ewa: Poziom dostępności cyfrowej jednostek samorządu terytorialnego – badania empiryczne

Włodyka Ewa Maria: Między integracją a dezinformacją: uchodźcy z Ukrainy w polskiej cyberprzestrzeni

Żęgota Krzysztof: Niewidzialny front: jak Rosja prowadzi cyberwojnę przeciw Europie