20–21
MAY
2024

www.cyber.ukw.edu.pl

BOOK OF ABSTRACTS

Organizer:

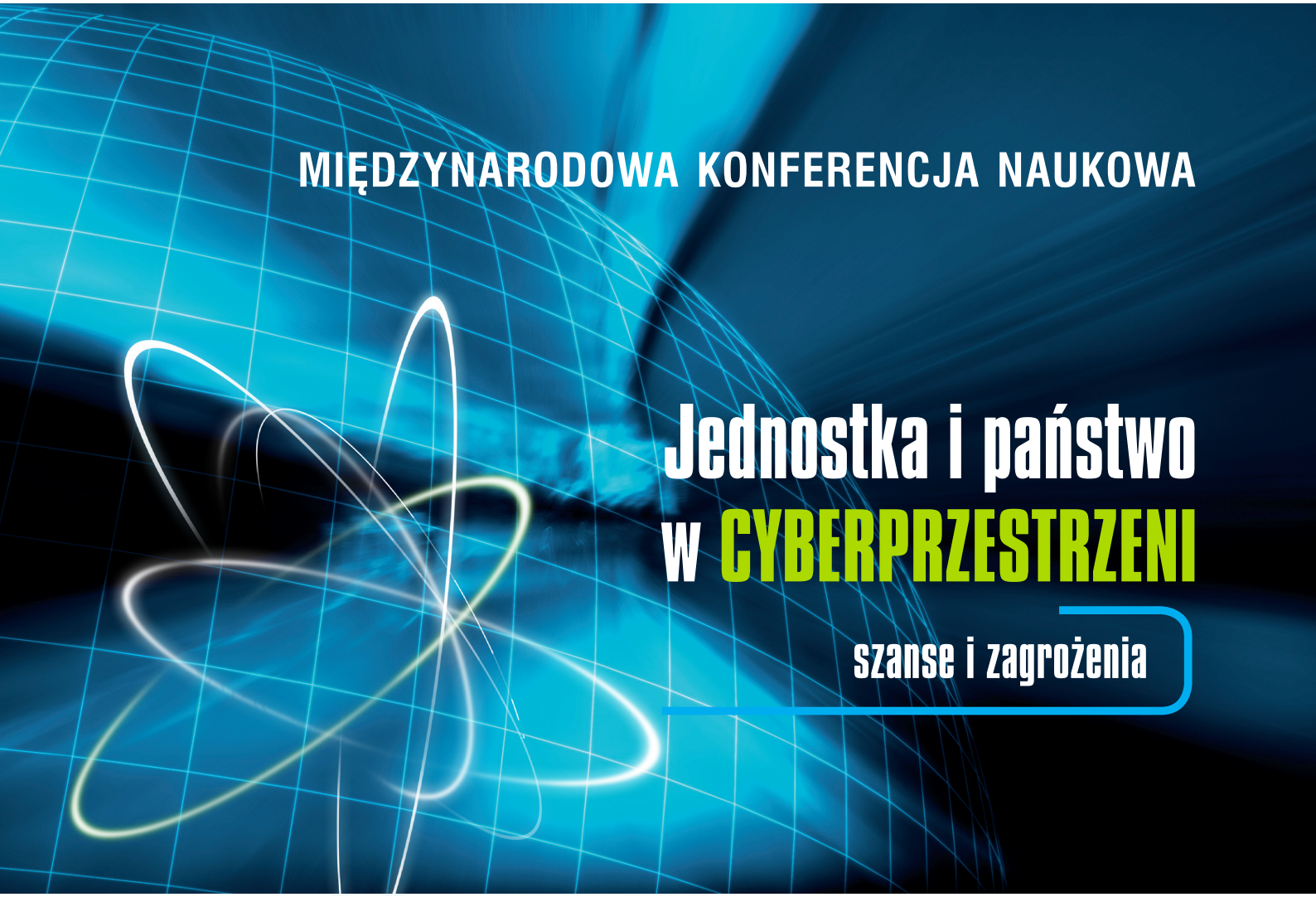
Honorary Patronage:

Co-organizers:

The conference is financed by the Ministry of Science and Higher Education under the contract no. KONF/SP/0234/2023/01 as part of the "Excellent Science II" Program, the "Conference support" module. Value of the funding: PLN 155,100.00, total value PLN 177,900.00.

20–21
MAJA
2024

www.cyber.ukw.edu.pl



MIĘDZYNARODOWA KONFERENCJA NAUKOWA

Jednostka i państwo w CYBERPRZESTRZENI

szanse i zagrożenia

KSIĘGA ABSTRAKTÓW

Organizator:

Patronat Honorowy:

Współorganizatorzy:

Projekt pt. „Międzynarodowa Konferencja Naukowa pt. Jednostka i państwo w cyberprzestrzeni - szanse i zagrożenia”, został dofinansowany w ramach programu Ministerstwa Nauki i Szkolnictwa Wyższego pod nazwą „Doskonała Nauka II” w ramach modułu „Wsparcie konferencji”.
Wartość dofinansowania: 155 100,00 PLN, całkowita wartość 177 900,00 PLN.

Part 1 – Plenary session

The Individual and the State in Cyberspace

– state of art, chances, and threats

Część 1 – Sesja plenarna

Jednostka i państwo w świecie wirtualnym

- stan obecny, szanse i zagrożenia

Giovani Ercolani

The Anthropological Gaze: Animal Identitarium, Security Knowledge, Power, Cyberspace, and Critical Thinking

Spojrzenie antropologiczne: identitarium zwierzęce, wiedza o bezpieczeństwie, władza, cyberprzestrzeń, a myślenie krytyczne

The human being is an ‘animal identitarium’ meaning that his outstanding attribute and essence is a striving for identity. This identity is sacred, provides a meaning of life and a sense of belonging to him/her, however, humankind lives inside the 'description’ of the world which contributes to the formation of his/her own symbolic universe which participates in the fabrication of his/her identity. As history has demonstrated during its course identity has been constructed on the emotion of anxiety, fear, and the man-

Człowiek jest „identitarium zwierzęcym”, co oznacza, że jego wyróżniającą cechą i istotą jest dążenie do tożsamości. Tożsamość ta jest uświęcona, nadaje życiu sens i tworzy poczucie przynależności, jednakże ludzkość żyje w ramach „opisu” świata, który przyczynia się do kształtowania własnego uniwersum symboli, uczestnicząc w tworzeniu ludzkiej tożsamości. Jak pokazuje historia, tożsamość budowano na odczuciach lęku, niepokoju, a także na tworzeniu konfliktu społecznego w relacji „my – inni”.

ufacturing of the ‘we-other’ conflicting relationship.

In this identity construction process the security concept (securitas: without anxiety) does play an important role because on its definition (source of anxiety), and on the identification of the security provider (securitizer), identity itself and power relations are have been set up in society. Identity and security are two concepts which have always been interrelated.

Nevertheless, security is a myth, and security knowledge, which now is based on the perception of the existential threat of 'the risk of...', through the rite of securitization process, is transformed into truth, technological knowledge, ideologies, cultural systems, and post-political biopolitics. Moreover, the securitization process acts as official-authorized description of the world (with power and political repercussions). If the ‘individual-animal identitarium’, until the advent of technological innovation, was living inside the description of the world, now the individual lives the totality of his/her life into the cyberspace which is a virtual space-dimension, represents a new, innovative, technological description of the world, and it is elevated to the only ‘veritas’ (truth).

The securitization-description of the COVID pandemic has demonstrated how an existential security threat has been managed (I call it a case of ‘e-securitization’, meaning the e-governing of security), and has shown how, using as a database grounded on the individuals responses to ‘orders’ emanated by the ‘power-security-knowledge-truth-moral’ structures (vaccines-pharmakon; healer), the same very States have produced lists of the doubters-sinners-heretics. During the pandemic time individuals were bombarded

W procesie konstruowania tożsamości koncepcja bezpieczeństwa (*securitas*: bez lęku) odgrywa ważną rolę, ponieważ na jej definicji (źródło niepokoju) oraz na identyfikacji dostawcy bezpieczeństwa, tj. sekurytyzatora ustala się sama tożsamość i relacje władzy w społeczeństwie. Tożsamość i bezpieczeństwo to dwa pojęcia od zawsze ze sobą związane.

Jednakże bezpieczeństwo jest mitem, a wiedza o bezpieczeństwie, która obecnie opiera się na postrzeganiu egzystencjalnego zagrożenia „ryzyka [...]”, poprzez rytuał sekurytyzacji, przekształca się w prawdę, wiedzę techniczną, ideologie, kultury i w postpolityczną biopolitykę. Co więcej, proces sekurytyzacji pełni funkcję usankcjonowanego oficjalnie opisu świata (ze swoimi reperkusjami w zakresie władzy i polityki). Jeśli „identitarium jednostka-zwierzę” do pojawienia się innowacji technicznych żyło w ramach opisu świata, to obecnie jednostka przeżywa całość swojego życia w cyberprzestrzeni, która jest wirtualnym wymiarem przestrzeni i stanowi nowy, nietradycyjny, technologiczny opis świata, który zostaje wyniesiony do rangi jedynej „veritas” (prawdy).

Sekurytyzacyjny opis pandemii Covid-19 zademonstrował w jaki sposób zarządzano egzystencjalnym zagrożeniem bezpieczeństwa (nazywam to przypadkiem „e-sekurytyzacji”, czyli e-zarządzania bezpieczeństwem). Pokazała też jak, biorąc za podstawę bazę danych opartą na reakcjach poszczególnych jednostek na „rozkazy” wydawane przez struktury „władzy – bezpieczeństwa – wiedzy – prawdy – moralności” (szczepionki–*farmakon*; uzdrowiciel), te same państwa stworzyły również listy wątpiących – grzeszników – heretyków. W okresie pandemii co godzinę bombardowano ludzi biuletynami wojen-

every hour with war bulletins in which the preachers-healers of this holy crusade were promoting their actions, their pharmakon, and were asserting the legal punishment toward the transgressors-heretics: a structural anxiety was put in practice.

As a result of this 'reality' (security knowledge-description) and 'truth,' and in order to produce a sane society, individuals have been transformed into a 'Q-CODE' which has become their identity and has recorded their sins, immorality, lifestyle, and insanity. The '"Q-CODE'-individual" (1) lives his/her life inside the cyberspace which is ruled by security knowledge which creates structural anxiety; and (2) his/her existence reminds Mr. Truman Burbank in his (sane-utopian) Seahaven Island where his whole human experience is 24/7 under the inquisitive scrutiny of camera-control.

All the above has been imposed by States (post-Athenian democracies) which were operating, for the benefit of the whole population, in the name of science and security. Basically, they were governing without any doubts and were imposing their own 'science' (e-governance: security knowledge) and 'truth' (e-truth), which, as a sacred interpretative paradigm, enforced a radical protocol of action-dogma most of the time contravening national constitutional laws thanks to the proclaimed 'state of emergency'.

Recent critical-antagonist scientific information have produced strong evidences of lethal side effects of vaccines and how some drug companies have retained the arrogant right to not disclose information about the effect of their vaccines for the next decades, rendering vain and ridicule the State power against multibillionaire multinational companies.

nymi, w których kaznodzieje – uzdrowiciele tej świętej krucjaty promowali swoje działania – swój farmakon – domagając się kar wobec przestępców-heretyków. Niepokój strukturalny wykorzystano zatem w praktyce.

W wyniku tej „rzeczywistości" (opisu wiedzy o bezpieczeństwie) oraz „prawdy", a także w celu stworzenia zdrowego społeczeństwa, jednostki zostały przekształcone w „KOD Q", który stał się ich tożsamością i zapisał ich grzechy, niemoralność, styl życia oraz szaleństwo. Jednostka „KOD-Q" po pierwsze żyje w cyberprzestrzeni rządzonej wiedzą o bezpieczeństwie, która wywołuje strukturalny niepokój, po drugie natomiast jej istnienie przypomina los filmowego Trumana Burbanka, mieszkańca (zdrowo-utopijnej) wyspy Seahaven, gdzie całe jego doświadczenie przebiega pod wnikliwą obserwacją kamery 24 godziny na dobę, 7 dni w tygodniu.

Wszystko to zostało narzucone z góry przez państwa (demokracje postateńskie), działające na rzecz całej populacji w imię nauki i bezpieczeństwa. Zarządzanie przebiegało bez żadnych wątpliwości, z narzuceniem własnej „nauki" (e-zarządzanie: wiedza o bezpieczeństwie) i „prawdy" (e-prawda), która jako uświęcony paradygmat interpretacyjny wymuszała przyjęcie radykalnych protokołów działania – dogmatów, w większości przypadków naruszając tym samym przepisy konstytucji krajowych, ze względu na ogłoszony „stan wyjątkowy".

Najnowsze krytyczno-antagonistyczne informacje naukowe dostarczyły mocnych dowodów na śmiertelne skutki uboczne szczepionek oraz na to, jak niektóre firmy farmaceutyczne z pełną arogancją zachowały swoje prawa do nieujawniania informacji o działaniu swoich szczepionek na następne dziesięciolecia, co udaremniło i ośmieszyło władzę

Until today no one among state agencies or international agencies (i.e., WHO) have been able to point directly to the responsible of the COVID pandemic and to denounce the causes of death in thousands of vaccinated 'people-individual-homo sacer-Q-CODE.' However, it looks like that the 'state of emergency' is going to be imposed as the new form of government for the coming years.

As a result of this process, I believe that the humankind is back into the Plato's cave in which lives his/her 'e-life' into the virtual and vulnerable world of the cyberspace, in its authorized description of the world, and in perennial 'state of emergency'. This 'e-cave' is the anthropological space-dimension of his/her 'e-life,' his/her 'e-identity,' his/her meaning of life; this 'e-cave' represents the cave of the soul making governed by the unquestionable 'e-truth'.

Here, in order to question the manufacturing of identity, meaning of life, security knowledge, and 'truth' is presented the epistemological and critical tool of the anthropological gaze, which, as instrument of critical thinking, is based on Socratic questioning, on the same curiosity and doubts that permitted Truman to take the courage to face the 'imposed-authorized' reality (e-reality) and 'e-truth', and to find a way to save his soul out of the new 'cyberspace-e-cave'. Leitmotiv of this endeavour is what Dante wrote in his 'Divine Comedy' (Inferno, canto 26): 'Consider your origins: you were not made to live as brutes, but to follow virtue and knowledge.'

Is there any virtue and knowledge in the cyberspace? Or it represents only an instrument, in the hands of 'Power,' to reproduce the Plato's cave soul making system?

Key words: animal identitarium, e-securitization, security, myth, anthropological gaze

państw wobec multimiliardowych międzynarodowych korporacji.

Do dziś żadna spośród agencji państwowych ani międzynarodowych (np. WHO) nie była w stanie wskazać bezpośrednio sprawców pandemii Covid ani potępić przyczyny śmierci tysięcy zaszczepionych „ludzi – jednostek – homo sacer – KODÓW-Q". Wygląda jednak na to, że na najbliższe lata „stan wyjątkowy" zostanie wprowadzony jako nowa forma rządów.

Jak sądzę, w wyniku tego procesu ludzkość wróciła do jaskini Platona, w której żyje swoim „e-życiem" w wirtualnym i wrażliwym świecie cyberprzestrzeni, z jego autoryzowanym opisem świata, w wiecznym „stanie wyjątkowym". Ta „e-jaskinia" jest antropologicznym wymiarem-przestrzenią ludzkiego „e-życia", „e-tożsamości", sensu życia; ta „e-jaskinia" to także jaskinia tworzenia duszy, zarządzana przez niekwestionowaną „e-prawdę".

Aby zakwestionować produkcję tożsamości, sensu życia, wiedzy o bezpieczeństwie i „prawdy", zaprezentowano tu epistemologiczno-krytyczne narzędzie w postaci spojrzenia antropologicznego, oparte na kwestionowaniu sokratejskim, na tej samej ciekawości i wątpliwościach, które pozwoliły Trumanowi zdobyć się na odwagę, aby zmierzyć się z „narzuconą-autoryzowaną" rzeczywistością (e-rzeczywistością) i „e-prawdą" i znaleźć sposób na wyprowadzenie swojej duszy od nowej „cyberprzestrzennej e- jaskini".

Motywem przewodnim tego przedsięwzięcia jest to, co Dante napisał w „Boskiej komedii" (Piekło, pieśń 26):

Rozważcie bytu waszego nasiona:
Nie na to przecie jesteście stworzeni,
Byście pędzili żywot jak bydlęta,

Lecz dążyć macie do wiedzy i cnoty! [przekład: A. R. Stanisławski.].

Czy w cyberprzestrzeni istnieje wiedza i cnota? A może stanowią one jedynie narzędzia w rękach „Władzy" służące do odtworzenia systemu kreowania duszy z jaskini Platona?

Słowa kluczowe: identitarium zwierzęce, e-sekurytyzacja, bezpieczeństwo, mit, spojrzenie antropologiczne

Agnieszka Demczuk

Disinformation in Poland: Diagnosis and Counteracting

Dezinformacja w Polsce: diagnoza i przeciwdziałanie

There are already many reports and publications that warn how disinformation harms the election campaigns and how is destructive for liberal democracy. The aimed of disinformation is polarizing and radicalizing of democratic and pluralistic society especially in an election time; disinformation is harmful factor to not only undermine but even systematically destroy national security (also had destroyed health security on the pandemic time – "We're not just fighting a pandemic; we're fighting an infodemic. Fake news spreads faster and more easily than this virus and is

W obiegu informacyjnym dostępnych jest już wiele raportów i publikacji na temat tego, jak dezinformacja szkodzi kampaniom wyborczym i jak jest destrukcyjna dla demokracji liberalnej. Jej celem jest polaryzacja i radykalizacja pluralistycznego i demokratycznego społeczeństwa, zwłaszcza w czasie wyborów; dezinformacja jest szkodliwym czynnikiem, który nie tylko podważa, ale systematycznie niszczy bezpieczeństwo publiczne (w czasie pandemii zniszczyła bezpieczeństwo zdrowotne – jak powiedział Tedros Adhanom Ghebreyesus z WHO „Nie tylko walczymy

just as dangerous," said Tedros Adhanom Ghebreyesus, WHO); last but not least disinformation also kills other common democratic values, such as human rights and freedoms and a rule of law. We are witnesses of trend of globalisation and democratisations disinformation à la Kremlin; except Russin propagandist and bots, non-state actors, from right-wing extremists in Internet (alt-right internet) to populist parties, take over Kremlin narratives ("Putin Playbook", vide Institute for Strategic Dialogue Report, 2019) using automatic influence mechanisms and online black-market manipulative infrastructure. Disinformation remained a little-known phenomenon in Poland for many years. Both the political class and the public paid little attention to that problem. In 2015, anti-immigrant narratives contributed significantly to Law and Justice party gaining power. The situation did not change for the following years, even on COVID-19-related infodemic time. Poland remained one of the least vaccinated countries in the EU; over 120 of thousand people died because of COVID-19 infection. Russia's full-scale invasion of Ukraine in 2022 demonstrated the power of Kremlin propaganda in Poland again. Thousands of social media accounts have shifted from anti-vaccine narratives to anti-Ukrainian content. In the first period of the war, however, Polish society proved immune to Russian propaganda. But the following months, especially 2024 and farmers protests show us how sentiments towards the need to help Ukraine and Ukrainians can change. So, we need to complex and holistic policy of counteracting disinformation in Poland. We need a systemic approach covering such areas of public life as education, public attitudes, and the legal framework. A clear strategy for dealing with

z pandemią, walczymy również z infodemią. Fałszywe wiadomości rozprzestrzeniają się szybciej i łatwiej niż ten wirus i są tak samo niebezpieczne"); wreszcie dezinformacja zabija także inne wartości takie jak prawa człowieka, wolności czy rządy prawa. Jesteśmy świadkami trendu globalizacji i demokratyzacji dezinformacji a la Kreml; oprócz rosyjskich propagandystów i botów, niepaństwowi aktorzy od skrajnie prawicowych w Internecie (alt-internet) po partie populistyczne używają narracji prokremlowskich („Podręcznik Putina", zobacz raport Instytutu Dialogu Strategicznego, 2019) wykorzystując mechanizmy automatycznego wpływu i czarnorynkowej infrastruktury manipulacyjnej online. Dezinformacja przez wiele lat pozostawała w Polsce zjawiskiem mało znanym. Zarówno klasa polityczna, jak i społeczeństwo nie zwracały na ten problem zbytniej uwagi. W 2015 roku narracje antyimigranckie znacząco przyczyniły się do zdobycia władzy przez Prawo i Sprawiedliwość. Sytuacja nie uległa zmianie przez kolejne lata, nawet w czasach infodemii COVID-19. Polska pozostała jednym z najmniej zaszczepionych państw w UE; z powodu zakażenia COVID-19 zmarło ponad 120 tys. osób. Rosyjska inwazja na Ukrainę na pełną skalę w 2022 r. po raz kolejny pokazała siłę kremlowskiej propagandy w Polsce. Tysiące kont w mediach społecznościowych przeniosło się z narracji antyszczepionkowych na treści antyukraińskie. Jednak w pierwszym okresie wojny społeczeństwo polskie okazało się odporne na rosyjską propagandę. Jednakże kolejne miesiące, szczególnie rok 2024 i protesty rolników pokazują, jak mogą zmieniać się nastroje wobec konieczności pomocy Ukrainie i Ukraińcom. Potrzebujemy więc kompleksowej i całościowej polityki przeciwdziałania

this threat is also necessary. Counteracting disinformation should involve all discourse actors in the fight against it.

dezinformacji w Polsce. Potrzebujemy podejścia systemowego, obejmującego takie obszary życia publicznego, jak edukacja, postawy społeczne i ramy prawne. Niezbędna jest także jasna strategia poradzenia sobie z tym zagrożeniem. Przeciwdziałanie dezinformacji powinno bowiem angażować w walkę z nią wszystkich aktorów dyskursu.

Christopher Farrands

Individual and state in cyberspace? The impact of big tech firms, governance structures and intellectual property control on individual- state relations

Jednostka i państwo w cyberprzestrzeni? Wpływ dużych firm technologicznych, struktur zarządzania i kontroli własności intelektualnej na relacje jednostka-państwo

This paper aims to explore the business strategies and governance issues which frame how questions about 'the individual and the state in cyberspace' might be addressed. It argues that the business environment of cyberspace is dominated by a few very large firms, that, in this oligopoly environment, 'free competition' simply does not apply; instead, intense forms of oligopoly competition structure ways in which firms operate. The major firms shaping the climate in which artificial intelligence (AI) is being developed and applied

Celem niniejszego artykułu jest zbadanie strategii biznesowych i kwestii związanych z zarządzaniem, które nadają ramy odpowiedziom na pytania o „jednostkę i państwo w cyberprzestrzeni". Autor argumentuje, że środowisko biznesowe cyberprzestrzeni zdominowane jest przez kilka bardzo dużych korporacji, a w tym środowisku oligopolu „wolna konkurencja" po prostu nie ma zastosowania; zamiast tego intensywne formy konkurencji oligopolowej kształtują sposoby działania firm. Największe firmy

control not only the market, but also the intellectual property and data management keys to understanding the possibilities of cyberspace as it evolves. One should be wary of talking about AI as if it is a single entity given its diversity, but the core underlying technologies, the production of advanced semiconductors, software engineering and very sophisticated automated production processes will set parameters which shape future possibilities. In these fields, there is an extraordinary concentration of capacity. Barriers to entry are very high, not least because the machinery to produce many of the key features of these technologies is so expensive, but also because the skills and staff who can contribute to its growth are rare and highly specialised. Furthermore, the existing players have large cash pools and can buy smaller competitors almost at will as they deploy intellectual property rules to their greatest advantage. The first half of the paper is therefore an analysis of business strategies and their relations to government.

The second half of the paper interrogates some of the consequences of this analysis. How, then, should the governance of this vital area be organised? The idea that markets might be more open and that large tech firms should be broken up clash here both with aa desire to see major firms succeed and create more jobs and more investment in their supply chains and with geopolitics. The geopolitics itself is changing as relations between the U.S., E.U., China and Japan evolve. The paper will explore these dilemmas in more detail. It also asks whether there is anything to learn from the management (some would say 'lack of management') of the governance of the global internet as it emerged in the 1990s. It asks what the consequences are of asking

tworzą klimat, w którym rozwija się i stosuje sztuczną inteligencję (AI), kontrolując nie tylko sam rynek, ale też własność intelektualną i zarządzanie danymi, kluczowe dla zrozumienia możliwości ewoluującej cyberprzestrzeni. Ze względu na różnorodność AI należy zachować ostrożność, jeśli chodzi o mówienie o niej tak, jakby stanowiła ona pojedynczy podmiot, ale podstawowe technologie leżące u jej podstaw, czyli produkcja zaawansowanych półprzewodników, inżynieria oprogramowania oraz wyrafinowane zautomatyzowane procesy produkcyjne wyznaczą parametry, które ukształtują przyszłe możliwości. W tych dziedzinach istnieje niezwykła koncentracja potencjałów. Bariery wejścia są bardzo wysokie, nie tylko dlatego, że maszyny do wytwarzania wielu kluczowych cech tych technologii są bardzo drogie, ale także dlatego, że umiejętności i personel, który może przyczynić się do ich rozwoju, są dobrami rzadkimi o wysokim stopniu specjalizacji. Co więcej, obecni gracze dysponują dużymi zasobami finansowymi i są w stanie kupować pomniejszych konkurentów niemal według własnego uznania, wdrażając zasady własności intelektualnej tak, żeby zapewnić sobie jak największe korzyści. Pierwsza część artykułu to zatem analiza strategii biznesowych i ich powiązań z rządem.

W części drugiej omówiono niektóre konsekwencje tej analizy. Jak zatem należy zorganizować zarządzanie tym istotnym obszarem? Pomysł, że rynki mogłyby być bardziej otwarte i że duże firmy technologiczne powinny zostać rozbite, koliduje tutaj zarówno z pragnieniem, aby duże firmy odniosły sukces, tworzyły więcej miejsc pracy i inwestowały więcej w swoje łańcuchy dostaw, a także z geopolityką. Sama geopolityka zmienia się wraz

apparently simple ethical and political questions such as ‘do we own our own data and should we?’ for our relationship as citizens and consumers in a rapidly transforming technological environment. And it draws some conclusions about needs for education in that arguably not-so-brave new world.

z ewolucją stosunków pomiędzy USA, UE, Chinami i Japonią. Artykuł omawia te dylematy bardziej szczegółowo. Zadaje pytanie, czy można się czegoś nauczyć z zarządzania (niektórzy powiedzieliby „braku zarządzania”) globalnym Internetem, jaki pojawił się w latach 90. XX wieku. Stawia też pytanie o konsekwencje stawiania pozornie prostych pytań etycznych i politycznych, takich jak „czy jesteśmy właścicielami naszych danych i czy powinniśmy być?” – dla naszych relacji jako obywateli i konsumentów w szybko zmieniającym się środowisku technologicznym. Wyciąga też wnioski co do potrzeb edukacyjnych w tym nowym, choć być może niekoniecznie wspaniałym świecie.

Diana Etsko

The confusing and contradictory character of the competences of the local public administration in the field of education and health

Zagmatwany i sprzeczny charakter kompetencji lokalnej administracji publicznej w obszarze oświaty i zdrowia

The inconsistency of local public administration powers in the field of education and health is a current issue rooted in legislative contradictions, which regulate the powers of local public authorities in the field of education and health. The traditional opposition be-

Niespójność kompetencji publicznej administracji samorządowej w obszarach oświaty i zdrowia to problem aktualny, mający swe źródło w sprzecznościach legislacyjnych, które regulują kompetencje władz samorządowych. W tradycyjnej opozycji pomię-

tween the provisions of the Law on Administrative Decentralization and the Law on Local Public Administration, on the one hand, which do not provide for any competences for local public authorities in the given field, and, on the other hand, the contradictory legislation, which establishes a large number of attributions for local public authorities. In order to know how the field of public education is managed by the local authorities, we will invoke some legislative acts. In December 2006, the General Regulatory Framework for administrative decentralization and the distribution of powers between public authorities was adopted. In accordance with Law no. 435/28.12.2006 and Law no. 436/28.12. 2006 education is not a priority of local public authorities. In the context of the distribution of competences between public authorities, the sphere of education and training falls under the attributions of local public administration authorities of level II.

Upon careful retrospective analysis, we will reveal inconsistent wording, which creates confusion in the approach to this subject. An accurate approach is needed for an understanding proper to the full recognition of the pre-established competences, otherwise the law, despite good intentions, does not carry reliability. Each assignment must have a convenient understanding of its own duties that it consistently upholds. The understanding we strive to have, in relation to the competences of local public authorities, inevitably affects the quality of services in the field of education and public health. By the way in which the field of education was targeted, by virtue of structural affinities, the competence approach is not visible in the stated context. Thus, the possible gaps are generated by the abstraction of the meaning of the term

dzy ustawą o decentralizacji administracyjnej i ustawą o administracji samorządowej z jednej strony, które nie przewidują żadnych kompetencji władz samorządowych w danym zakresie, a z drugiej strony, sprzecznego ustawodawstwa, które ustanawia dużą liczbę uprawnień władz lokalnych. Aby dowiedzieć się, jak samorządy lokalne zarządzają dziedziną edukacji publicznej, przywołamy niektóre akty prawne. W grudniu 2006 r. przyjęto ogólne ramy regulacyjne dotyczące decentralizacji administracyjnej i podziału uprawnień pomiędzy organami publicznymi. Zgodnie z ustawą nr. 435/28.12.2006 oraz ustawą nr. 436/28.12.2006, edukacja nie jest priorytetem lokalnych władz publicznych. W kontekście podziału kompetencji pomiędzy władzami publicznymi, sfera kształcenia i szkoleń wpisuje się w kompetencje lokalnych władz administracji publicznej II stopnia.

Na podstawie wnikliwej analizy retrospektywnej, ujawniliśmy niespójność sformułowań skutkującą zamieszaniem w podejściach do omawianego zagadnienia. Dla właściwego zrozumienia wcześniej ustalonych kompetencji potrzebne jest prawidłowe podejście, gdyż w przeciwnym razie prawo, pomimo jak najlepszych intencji, nie jest miarodajne. Każde zadanie musi umożliwiać zrozumienie nakładanych obowiązków, których wykonywanie zastrzega. Rozumienie, do którego dążymy, w odniesieniu do kompetencji władz lokalnych, nieuchronnie wpływa na jakość usług w zakresie edukacji i zdrowia publicznego. Ze względu na uwarunkowania obszaru edukacji oraz powiązania strukturalne, podejście kompetencyjne nie jest widoczne w podanym kontekście. Możliwe jest zatem tworzenie się luk z uwagi na abstrakcyjność terminu „utrzymanie", obejmującego m.in. ubezpieczenia majątkowe, remonty kapita-

"maintenance": material insurance, capital repairs, current repairs. According to him, from the adopted theoretical point of view, the law is irrelevant and does not provide conditions for realization nor does it aim at the conditions of possibility between the obligation of the municipalities to materially and financially ensure the functioning of the educational institutions and the existence of mechanisms to influence and effectively control the leaders these institutions, through the methods provided by the labor legislation: hiring, firing, sanctioning, etc. The more distant the Law is from a concise and accurate approach through the prism of realities, the more it generates conflicting situations when, for example, on the one hand, 75-90% of local budgets are intended to finance education, and on the other on the other hand, the local public authorities have no real competence and influence over the management of the respective educational institutions.

The legislation oscillates from one pole to the other in assigning powers to local public authorities in the field of public health. Thus, the legislation, in the targeted field, represents an axis defined at one pole by the powers assigned, exclusively, to the state and central public authorities, and at the other by a series of powers assigned to local public authorities in the field of health protection.

łowe, jak również bieżące naprawy. W związku z tym, z przyjętego teoretycznego punktu widzenia, ustawa jest nieistotna i nie tworzy warunków dla realizacji, ani też nie ma na celu stworzenia możliwości pomiędzy obowiązkiem gmin w zakresie materialnego i finansowego zapewnienia funkcjonowania placówek oświatowych a istnieniem mechanizmów wpływu i skutecznej kontroli kierownictwa tych instytucji z użyciem metod przewidzianych przez prawo pracy: zatrudniania, zwalniania, nakładania kar, itp. Im bardziej Prawo odbiega od zwięzłego i trafnego podejścia poprzez pryzmat realiów, tym więcej sytuacji konfliktowych generuje, gdy np. z jednej strony 75-90% lokalnych budżetów przeznaczonych jest na finansowanie oświaty, a z drugiej, władze lokalne nie mają realnych kompetencji ani wpływu na zarządzanie instytucjami edukacyjnymi.

Prawodawstwo oscyluje od jednego bieguna do drugiego w zakresie powierzania uprawnień władzom lokalnym w dziedzinie zdrowia publicznego. Zatem ustawodawstwo w tym obszarze stanowi oś wyznaczaną z jednej strony przez uprawnienia przyznane wyłącznie państwu i władzom centralnym, z drugiej zaś przez szereg uprawnień przyznanych władzom lokalnym w zakresie ochrony zdrowia.

Valentin Constantinov

The confusing and contradictory character of the competences of the local public administration in the field of education and health

Wyzwania i perspektywy rozwoju e-administracji w dobie globalizacji i integracji europejskiej na przykładzie Mołdawii

E-administration is currently one of the modern elements of governance. At the beginning, several assumptions were made, along with the development and formulation of the principles of e-administration. The prospects offered by this form of administration suddenly aroused the interest of not only the local public administration, but also of the general public, particularly as the era of globalization posed new challenges. Moldova very quickly put the mobility and dynamics of these new forms into practice. Furthermore, many elements of the new administration were also formed during the recent pandemic. Despite this, however, there are also problems in implementing this form of activity, including Internet access, citizen training and ownership of the digital technology that is able to secure all that is needed. As Moldova has become a candidate country for accession to the EU, solving these problems is also a priority for the present and future governments in our country.

E-administracja jest obecnie jednym z nowoczesnych elementów rządzenia. Na początku przyjęto kilka założeń, a także opracowano i sformułowano zasady e-administracji. Perspektywy, jakie daje ta forma administracji wzbudzają zainteresowanie nie tylko lokalnej administracji publicznej, ale także ogółu społeczeństwa, zwłaszcza że era globalizacji stawia nowe wyzwania. Mołdawia bardzo szybko wprowadziła mobilność i dynamikę tych nowych form w życie. Co więcej, podczas ostatniej pandemii powstało także wiele elementów nowej administracji. Mimo to pojawiają się problemy z realizacją tej formy działalności, m.in. z dostępem do Internetu, szkoleniem obywateli i posiadaniem technologii cyfrowej, która jest w stanie zabezpieczyć wszystko, co potrzebne. Ponieważ Mołdawia stała się krajem kandydującym do przystąpienia do UE, rozwiązanie tych problemów jest także priorytetem dla obecnych i przyszłych rządów tego kraju.

Part 2 – Plenary session

Cybersecurity – the perspective of states and international organizations

Część 2 – Sesja plenarna

Bezpieczeństwo w cyberprzestrzeni – perspektywa państw i organizacji międzynarodowych

Miron Lakomy

Online Extremism Revisited: Mapping the Salafi-jihadist information ecosystem on the surface web

Ponowne spojrzenie na ekstremizm online: Mapowanie ekosystemu informacyjnego salafickich dżihadystów w sieci powierzchniowej

This presentation overviews some of the core findings of a NAWA-backed VEOMAP research project, realized in 2023 and 2024, in the ITSTIME center in Milan, Italy. Based on advanced open-source intelligence methods combined with social network analysis, it explores the structure and evolution of the Salafi-jihadist information ecosystem available on or detectable from the surface web between mid-2023 and March 2024. Among

Prezentacja niniejsza zawiera przegląd wybranych najważniejszych wniosków z projektu badawczego VEOMAP, realizowanego ze wsparciem NAWA w latach 2023 i 2024 w ośrodku ITSTIME, w Mediolanie. W oparciu o zaawansowane metody wywiadowcze z wykorzystaniem źródeł otwartych (open-source), w połączeniu z analizą sieci społecznościowych bada strukturę i ewolucję ekosystemu informacyjnego dżihadystów salafickich

others, the presentation discusses features of the core hotspots for Salafi-jihadist communication in this environment, as well as the strategies of propaganda dissemination adopted by both major and minor violent extremist organizations. It explains the current standards in operations security measures adopted by terrorist media operatives. On top of this, drawing from online observation and content analysis of the essential Salafi-jihadist domains, it covers the scale and structure of terrorist propaganda production during this period.

dostępnego w sieci powierzchniowej bądź możliwego do wykrycia w sieci od połowy roku 2023 do marca 2024. W prezentacji omówiono między innymi funkcje głównych punktów komunikacji dżihadystów w tym środowisku, a także strategii rozpowszechniania propagandy przyjętych zarówno przez główne, jak i pomniejsze brutalne organizacje ekstremistyczne. Omawiane są też aktualne standardy środków bezpieczeństwa operacji przyjęte przez terrorystycznych agentów medialnych. Ponadto, opierając się na obserwacjach internetowych i analizie treści najważniejszych domen dżihadystów salafickich, omawiana jest również skala i struktura produkcji propagandy terrorystycznej w podanym okresie.

Katarzyna Chałubińska-Jentkiewicz

Between freedom and security - new rules of responsibility in cyberspace

Między wolnością a bezpieczeństwem - nowe reguły odpowiedzialności w cyberprzestrzeni

Shota Gvineria

The Role of Cyber Defense in Contemporary Security: Military Considerations and Insights from the War in Ukraine

Rola cyberobrony we współczesnym systemie bezpieczeństwie: kwestie wojskowe oraz wnioski z wojny na Ukrainie

The contemporary security landscape is heavily influenced by the integration of cyberspace, where the role of cyber defense has become pivotal, especially in military contexts. It is essential to explore the role of cyber defense in modern security environments, focusing particularly on military considerations and insights gleaned from the war in Ukraine. Cyberspace now stands as a crucial domain for military operations, offering both opportunities for offensive actions and vulnerabilities for exploitation by adversaries. Consequently, robust cyber defense strategies are essential to safeguard national security interests and maintain operational readiness. The armed conflict in Ukraine provides a poignant case study, revealing how cyber effects are wielded as integral components of hybrid warfare tactics. From distributed denial-of-service assaults targeting critical infrastructure to sophisticated malware campaigns disrupting communications, the conflict underscores the diverse array of cyber threats. Moreover, it emphasizes the importance of dominating information and com-

Współczesny krajobraz bezpieczeństwa jest pod dużym wpływem integracji cyberprzestrzeni, w której kluczowa stała się rola cyberobrony, szczególnie w kontekście wojskowym. Niezbędne jest zbadanie roli cyberobrony we współczesnych środowiskach bezpieczeństwa, ze szczególnym uwzględnieniem kwestii wojskowych i spostrzeżeń pochodzących z wojny na Ukrainie. Cyberprzestrzeń stanowi obecnie kluczową dziedzinę operacji wojskowych, obejmując zarówno możliwości działań ofensywnych, jak i luki w zabezpieczeniach, które mogą zostać wykorzystane przez przeciwników. W związku z tym solidne strategie cyberobrony są niezbędne do ochrony interesów bezpieczeństwa narodowego i utrzymania gotowości operacyjnej. Konflikt zbrojny na Ukrainie stanowi przejmujące studium przypadku, ujawniając w jaki sposób efekty cybernetyczne są wykorzystywane jako integralne elementy wojny hybrydowej. Od rozproszonych ataków na infrastrukturę krytyczną w postaci „odmowy dostępu” (denial-of-service) po wyrafinowane kampanie z użyciem szkodliwego

munications space and the role of information as a strategic capability. In addition to analyzing specific cyber threats encountered in Ukraine, it is critical to discuss broader implications for cyber policy, doctrine, and strategy. It stresses the imperative of seamlessly integrating cyber capabilities within traditional military operations and underscores the importance of collaboration among government agencies, private sector entities, and international allies to effectively counter cyber threats. Distilling insights from the war in Ukraine is the key towards developing future cyber policies and cyber defense strategies that can enhance resilience in national security contexts. The lessons learned highlight the need for perpetual adaptation and innovation in cyber defense practices to thwart evolving threats and uphold strategic advantage in an era dominated by information warfare.

oprogramowania zakłócającego komunikację – konflikt uwydatnia różnorodną gamę zagrożeń cybernetycznych. Ponadto podkreśla on znaczenie dominacji w przestrzeni informacyjno-komunikacyjnej oraz rolę informacji jako potencjału strategicznego. Obok analizy konkretnych zagrożeń cybernetycznych występujących na Ukrainie, niezwykle ważne jest omówienie szerszych implikacji dla polityki, doktryny i strategii cybernetycznej. Podkreśla konieczność płynnej integracji zdolności cybernetycznych w ramach tradycyjnych operacji wojskowych i znaczenie współpracy pomiędzy agencjami rządowymi, podmiotami sektora prywatnego i sojusznikami międzynarodowymi w celu skutecznego przeciwdziałania zagrożeniom cybernetycznym. Wyciąganie wniosków z wojny na Ukrainie jest kluczem do opracowania przyszłych polityk w zakresie polityk i strategii cyberobrony, które mogą zwiększyć odporność w kontekście bezpieczeństwa narodowego.

Obecne wnioski podkreślają potrzebę ciągłej adaptacji i innowacji w zakresie praktyk cyberobrony, aby udaremniać ewoluujące zagrożenia i utrzymywać przewagę strategiczną w epoce zdominowanej przez wojnę informacyjną.

Jacek Raubo

When cyber became a strategic dilemma for defense and security?

Kiedy cyberprzestrzeń stała się strategicznym dylematem dla obronności i bezpieczeństwa?

Today, the cyber domain is recognized as an entirely legitimate space for military and intelligence activities and all activities related to national security. However, this mental and technological revolution occurred dynamically, and it is necessary to indicate, above all, critical points in the perception of cyber topics in the category of strategic reflection space. Moreover, a spectrum of questions can build images of war in cyberspace separated from other (classical) domains. It is also important to consider to what extent contemporary intelligence analysis processes, including intelligence collection, may be determined by cyberspace.

Obecnie domena cyber uznawana jest za całkowicie legalną przestrzeń działań wojskowych, wywiadowczych i wszelkich działań związanych z bezpieczeństwem narodowym. Ta rewolucja mentalno-technologiczna dokonała się jednak dynamicznie i należy wskazać przede wszystkim punkty krytyczne w postrzeganiu zagadnień cyberprzestrzeni w refleksji strategicznej. Co więcej, spektrum pytań może budować obrazy wojny w cyberprzestrzeni oddzielonej od innych (klasycznych) domen. Warto też zastanowić się, w jakim stopniu współczesne procesy analizy wywiadu, w tym gromadzenia danych wywiadowczych, mogą być determinowane przez cyberprzestrzeń.

Ilin Savov

Digital Era and CyberCrimes

Era cyfrowa a cyberprzestępczość

The digital transformation that global societies and industries have been undergoing has revolutionized the manner in which human-computer interaction is conducted. While there have been numerous benefits and opportunities provided via the means of cyberspace, another phenomenon has also risen in conjunction with the transition towards the cyber environment, and that phenomenon is cybercrime. While witnessing the heavy dependence that has been placed on technology, malicious entities have sought to leverage their technological savviness in order to gain lucrative profits via the sophistication of attack strategies and mechanisms. The digital age enables the rise of cybercrime to become an alarming reality. From large-scale corporate data breaches to individual identity theft, the virtual world is a fertile ground for criminal activity. Armed with cutting-edge technology and sophisticated tactics, cyber organized crime groups are exploiting vulnerabilities in our interconnected systems, causing significant financial loss, emotional distress and even threats to national security. As our lives become increasingly intertwined with technology, understanding the nuances of cybercrime and its far-reaching consequences is

Transformacja cyfrowa, jaką przechodzą globalne społeczeństwa i gałęzie przemysłu, zrewolucjonizowała sposób interakcji człowiek-komputer. Mimo iż cyberprzestrzeń zapewnia liczne korzyści i możliwości, w związku z przejściem do środowiska cybernetycznego pojawiło się także inne zjawisko, a mianowicie cyberprzestępczość. Będąc świadkami dużej zależności od technologii, szkodliwe podmioty próbowały wykorzystać swoją wiedzę technologiczną w celu uzyskania dużych zysków za pomocą wyrafinowanych strategii i mechanizmów ataku. Era cyfrowa sprawia, że wzrost cyberprzestępczości staje się niepokojącą rzeczywistością. Od naruszeń danych korporacyjnych na dużą skalę po kradzież tożsamości osób – świat wirtualny jest podatnym gruntem dla działalności przestępczej. Uzbrojone w najnowocześniejszą technologię i wyrafinowane taktyki zorganizowane grupy cyberprzestępcze wykorzystują luki w naszych wzajemnie połączonych systemach, powodując znaczne straty finansowe, niepokój emocjonalny, a nawet zagrożenia dla bezpieczeństwa narodowego. Ponieważ nasze życie w coraz większym stopniu splata się z technologią, zrozu-

not just a necessity, but an urgent priority. The phenomenon of cyber crime has become a global concern, as individuals, businesses, and governments find themselves vulnerable to a wide range of cyber threats. Cybercrime encompasses a broad range of criminal activities conducted through the use of digital technologies. From hacking and identity theft to phishing and ransom ware attacks, cybercriminals exploit vulnerabilities in computer systems and networks to carry out their malicious activities. The anonymity, speed, and global reach afforded by the internet make cybercrime an attractive and lucrative prospect for criminals. Efforts to combat cyber crime are underway on multiple fronts. Collaboration between governments, law enforcement agencies, and international organizations is crucial to address the global nature of cyber crime. Strengthening cyber security infrastructure, raising public awareness about online threats, and promoting responsible online behavior are essential steps. Innovative technologies, such as artificial intelligence and blockchain, are also being employed to enhance security measures and detect cyber threats in real-time.

mienie niuansów cyberprzestępczości i jej dalekosiężnych konsekwencji jest nie tylko koniecznością, ale pilnym priorytetem. Zjawisko cyberprzestępczości stało się problemem globalnym, ponieważ osoby fizyczne, przedsiębiorstwa i rządy są narażone na szeroką gamę zagrożeń cybernetycznych. Cyberprzestępczość obejmuje szeroki zakres działań przestępczych prowadzonych z wykorzystaniem technologii cyfrowych. Od włamań i kradzieży tożsamości po ataki typu phishing i oprogramowanie ransomware – cyberprzestępcy wykorzystują luki w systemach i sieciach komputerowych w celu prowadzenia szkodliwych działań. Anonimowość, szybkość i globalny zasięg, jaki zapewnia Internet, sprawiają, że cyberprzestępczość jest atrakcyjną i lukratywną perspektywą dla przestępców. Wysiłki mające na celu zwalczanie cyberprzestępczości trwają na wielu frontach. Aby zaradzić globalnemu charakterowi cyberprzestępczości, kluczowa jest współpraca pomiędzy rządami, organami ścigania i organizacjami międzynarodowymi. Wzmocnienie infrastruktury bezpieczeństwa cybernetycznego, podnoszenie świadomości społecznej na temat zagrożeń w Internecie i promowanie odpowiedzialnych zachowań to istotne kroki. Innowacyjne technologie, takie jak sztuczna inteligencja i blockchain, są również wykorzystywane w celu poprawy bezpieczeństwa oraz wykrywania zagrożeń cybernetycznych w czasie rzeczywistym.

Panel sessions 1

The State in Cyberspace: current challenges

Sesja panelowa 1

Państwo w cyberprzestrzeni: aktualne wyzwania

Jaroslav Usiak

Hybrid Warfare and Disinformation: Challenges for Central European Democracies

Wojna hybrydowa i dezinformacja: wyzwania dla demokracji środkowoeuropejskich

The article focuses on analysing hybrid threats and disinformation campaigns and their impact on the democracies of Central Europe as well as public opinion and citizen participation. Over recent years, hybrid threats and disinformation have become significant risks not only to Central European democratic systems. These threats often include a mix of traditional military operations and non-traditional methods such as cyber-attacks spreading false information and political propaganda and foreign influences. In the contribution, the main features of hybrid threats and disinformation activities are outlined and within that, their objectives and methods are defined also some examples of

Artykuł skupia się na analizie zagrożeń hybrydowych i kampanii dezinformacyjnych oraz ich wpływie na demokracje Europy Środkowej, a także opinię publiczną i partycypację obywateli. W ostatnich latach zagrożenia hybrydowe i dezinformacja stały się poważnym ryzykiem nie tylko dla środkowoeuropejskich systemów demokratycznych. Zagrożenia te często obejmują połączenie tradycyjnych operacji wojskowych i nietradycyjnych metod, takich jak cyberataki rozpowszechniające fałszywe informacje, propagandę polityczną i wpływy zagraniczne. W artykule nakreślono główne cechy zagrożeń hybrydowych i działań dezinformacyjnych, w ramach, których zdefiniowano ich cele i metody,

their recent use in the Central European region and their impact are delineated. The submitted article addresses the impact of defined phenomena on public opinion citizens and their attitudes: It also focuses on processes as these informations are spread through social or online media. Selected case studies try to present also the impact of disinformation on political processes participation and also opens a polemic of implications for the democratic society as such. The article attempts to offer an overview of strategies adopted by Central European countries in response to these threats. The conclusion of the article emphasizes the need to expand professional and public discussion in the context of protecting democratic values under the influence of disinformation and hybrid threats and propaganda.
Key words: Hybrid threats; Disinformation campaigns; Central European democracies; Public opinion; Political propaganda; Foreign influences

a także przedstawiono kilka przykładów ich niedawnego zastosowania w regionie Europy Środkowej oraz ich wpływ. Nadesłany artykuł porusza kwestię wpływu zdefiniowanych zjawisk na opinię publiczną obywateli i ich postawy: Skupia się także na procesach rozprzestrzeniania się tych informacji za pośrednictwem mediów społecznościowych lub internetowych. Wybrane studia przypadków starają się także przedstawić wpływ dezinformacji na uczestnictwo w procesach politycznych, a także otwierają polemikę implikacji dla społeczeństwa demokratycznego jako takiego. W artykule podjęto próbę przeglądu strategii przyjętych przez kraje Europy Środkowej w odpowiedzi na te zagrożenia. W konkluzji artykułu podkreślono potrzebę rozszerzenia dyskusji zawodowej i publicznej w kontekście ochrony wartości demokratycznych pod wpływem dezinformacji oraz zagrożeń i propagandy hybrydowej.
Słowa kluczowe: zagrożenia hybrydowe; Kampanie dezinformacyjne; demokracje środkowoeuropejskie; Opinia publiczna; Propaganda polityczna; Wpływy obce

Ewelina Kasprzyk

The Cyber Game-Changer: How AI Works Both Against and For Cybersecurity

Zmiana zasad gry w cyberprzestrzeni: jak sztuczna inteligencja działa przeciwko cyberbezpieczeństwu, jak i dla niego

The cyber threat landscape remains in constant flux, propelled by the rapid advancements in technology available for both state and non-state actors. Artificial intelligence (AI) plays a pivotal role in this process, fueling the evolution of cyber capabilities, tactics, and methods. With AI's prowess, cyberattacks are not only escalating in scale and speed but also becoming increasingly sophisticated. Moreover, AI-based tools are significantly reducing entry barriers for novice and less-skilled threat actors and amplifying the efficacy of their attacks. The cybersecurity community should not only mitigate the hazards associated with AI but also harness its transformative capabilities to fortify cybersecurity defenses. AI-based solutions for anomaly detection, alert triage, proactive security automation and even autonomous cyber operations can significantly raise our cyber defence level, for example by enhancing analysis of CTI and tackling the expertise and skills gap. AI can be used to fight the very problem it creates – this

Krajobraz zagrożeń cybernetycznych podlega ciągłym zmianom, napędzanym szybkim postępem technologii dostępnym zarówno dla podmiotów państwowych, jak i niepaństwowych. Sztuczna inteligencja (AI) odgrywa kluczową rolę w tym procesie, napędzając ewolucję możliwości, taktyk i metod cybernetycznych. Dzięki możliwościom sztucznej inteligencji cyberataki nie tylko nasilają się pod względem skali i szybkości, ale także stają się coraz bardziej wyrafinowane. Co więcej, narzędzia oparte na sztucznej inteligencji znacznie zmniejszają bariery wejścia dla początkujących i mniej wykwalifikowanych cyberprzestępców oraz zwiększają skuteczność ich ataków. Społeczność zajmująca się cyberbezpieczeństwem powinna nie tylko łagodzić zagrożenia związane ze sztuczną inteligencją, ale także wykorzystywać jej możliwości transformacyjne w celu wzmacniania obrony cyberbezpieczeństwa. Rozwiązania oparte na sztucznej inteligencji do wykrywania anomalii, selekcji alertów, proaktywnej automatyzacji bezpieczeństwa, a nawet autonomicznych operacji cybernetycznych mogą znacznie podnieść nasz po-

presentation will try to explain how AI works both against and for cybersecurity.

ziom cyberobrony, na przykład poprzez usprawnienie analizy CTI i eliminowanie luk w wiedzy specjalistycznej i umiejętnościach. Sztuczną inteligencję można wykorzystać do walki z problemem, który stwarza – w tej prezentacji postaramy się wyjaśnić, w jaki sposób sztuczna inteligencja działa zarówno przeciwko, jak i dla cyberbezpieczeństwa.

Arkadiusz Nyzio

Poland, SIGINT, and the reform of intelligence services

Polska, SIGINT i reforma służb wywiadowczych

For years, there has been a rather chaotic debate in Poland concerning cybersecurity and clandestine data interception. In recent months there have been ideas floating around to create a sixth intelligence service (Cybersecurity Agency) or to establish a fourth Computer Security Incident Response Team (CSIRT INT), and all this takes place against the background of the urgent need to implement the Electronic Communications Code Directive (Poland has already exceeded the transposition deadline by over three years). Currently, signals intelligence powers are dispersed among several Polish intelligence services and the need to integrate this area

Od lat w Polsce toczy się dość chaotyczna debata dotycząca cyberbezpieczeństwa i nielegalnego przechwytywania danych. W ostatnich miesiącach pojawiały się pomysły na powołanie szóstej już służby wywiadowczej (Agencja Cyberbezpieczeństwa) lub czwartego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT INT), a wszystko to działo się w kontekście pilnej konieczności wdrożenia dyrektywy o Europejski kodeks łączności elektronicznej (Polska przekroczyła już termin transpozycji o ponad trzy lata). Obecnie uprawnienia wywiadu sygnalizacyjnego są rozproszone pomiędzy kilka polskich służb wywiadowczych i

should be considered, following the example not only of the well-known British Government Communications Headquarters or the American National Security Agency, but also of the Czech Národní Úřad pro Kybernetickou a Informační Bezpečnost. In the paper, I present current proposals for further developments concerning electronic interceptions in Poland, analyse the crucial aspects of the ongoing debate and propose possible directions for unavoidable reforms.

należy rozważyć potrzebę integracji tego obszaru, idąc za przykładem nie tylko znanej brytyjskiej Centrali Łączności Rządowej czy amerykańskiej Agencji Bezpieczeństwa Narodowego, ale także czeskiego organu o nazwie Národní Úřad pro Kybernetickou i Informační Bezpečnost.

W artykule przedstawiam aktualne propozycje dalszego rozwoju sytuacji w zakresie przechwytu sygnałów elektronicznych w Polsce, analizuję najważniejsze aspekty toczącej się debaty i proponuję możliwe kierunki nieuniknionych reform.

Piotr Walewicz

Social media as the arena for environmental policy disputes: the case of European Green Deal

Media społecznościowe areną sporów dotyczących polityki środowiskowej: przypadek Europejskiego Zielonego Ładu

The presentation is a preliminary report from the ongoing realization of research funded by the National Science Centre, Poland, grant number 2023/07/X/HS5/00685 (“Polityczne narracje na temat Europejskiego Zielonego Ładu: krytyczno-analityczne studium wypowiedzi europejskich polityków w mediach społecznościowych”).

Firstly, it outlines the importance of studying narratives within both environmental policy

Prezentacja stanowi wstępny raport z bieżącej realizacji badań finansowanych przez Narodowe Centrum Nauki, grant nr 2023/07/X/HS5/00685 („Polityczne narracje na temat europejskiego zielonego ładu: krytyczno-analityczne studium dotyczące polityków w mediów społecznościowych”).

Po pierwsze, podkreśla znaczenie badania narracji zarówno w ramach studiów nad polityką środowiskową, jak i badań nad mediami

studies as well as social media and Internet studies without neglecting neither the ideological nor material aspects of political reality.

Secondly, it reveals the preliminary findings of the analysis of narratives about the European Green Deal told by Polish politicians on Facebook.

Lastly, it hypothesizes about the eventual conclusions of the whole research as well as tries to give some predictions on how the narratives on EGD can be shaped in the near future.

społecznościowymi i Internetem, nie zaniedbując ani ideologicznych, ani materialnych aspektów rzeczywistości politycznej.

Po drugie, ukazuje wstępne wnioski z analizy narracji na temat Europejskiego Zielonego Ładu prowadzonych przez polskich polityków na Facebooku.

Na koniec stawia hipotezy na temat ostatecznych wniosków z całego badania, a także stara się przedstawić pewne przewidywania dotyczące tego, jak narracje na temat Zielonego Ładu mogą kształtować się w najbliższej przyszłości.

Panel sessions 2

Contemporary cybersecurity threats

Sesja panelowa 2

Współczesne zagrożenia bezpieczeństwa

Remigiusz Rosicki

Disinformation, terrorist crimes and sabotage in the context of changing the scope of criminalization of the crime of espionage in Poland in 2023

Dezinformacja, przestępstwa o charakterze terrorystycznym, sabotaż i dywersja w kontekście zmiany zakresu kryminalizacji przestępstwa szpiegostwa w Polsce w 2023 roku

The talk presents the significance of changing the scope of criminalization of espionage in Poland in 2023. New types of espionage offenses are presented, along with reference to existing regulations regarding crimes against information protection (i.e. cybercrimes).

Głównym celem wystąpienia jest prezentacja istoty oraz sensu zmiany zakresu kryminalizacji przestępstwa szpiegostwa w Polsce w 2023 roku. Podczas wystąpienia zaprezentowane zostaną nowe typy przestępstwa szpiegostwa wraz z odniesieniem do istniejących już regulacji dotyczących przestępstw przeciwko ochronie informacji (tj. cyberprzestępstw).

Kinga Machowicz

Threats to freedom of expression in cyberspace

Zagrożenia dla wolności wypowiedzi w cyberprzestrzeni

Freedom of expression in cyberspace is exposed to more widespread threats, as well as specific threats, than is the case with expressions occurring in cyberspace. The aim of the presentation is twofold: 1. to identify and briefly characterize threats to freedom of expression which result from intentionally misleading information in cyberspace and/or exerting pressure on the recipient of the communication, 2. to identify potential ways to counteract these threats.

Wolność wypowiedzi w cyberprzestrzeni jest narażona na więcej rozpowszechnionych zagrożeń, jak również zagrożeń specyficznych niż ma to miejsce w przypadku wypowiedzi umieszczanych poza cyberprzestrzenią. Celem wystąpienia jest: 1. zidentyfikowanie i krótkie scharakteryzowanie zagrożeń dla wolności wypowiedzi, które wynikają z celowego wprowadzania w błąd informacjami publikowanymi w cyberprzestrzeni i/lub wywoływania presji na odbiorcę przekazu, 2. określenie potencjalnych sposobów przeciwdziałania tym zagrożeniom.

Ewa Szatlach

The right to be forgotten as a defense tool against fake news

Prawo do bycia zapomnianym jako narzędzie obrony przed fake newsami

In May 2014, the Court of Justice of the EU stated that every private person has the right to request that search engine operators such as Google remove search results containing their name and surname. The operator must comply with such a request if the links in it lead to information that is "inappropriate, exaggerated, inadequate or irrelevant" or is fake news. The goal of the study presented in the article is to show the process of creating the right to be forgotten.

W maju 2014 roku Trybunał Sprawiedliwości UE stwierdził, że każda osoba prywatna ma prawo do zażądania usunięcia wyników wyszukiwania zawierających jej imię i nazwisko przez operatorów wyszukiwarek takich jak na przykład Google. Operator musi zrealizować takie żądanie, jeśli występujące w nim linki prowadzą do informacji, które są „nieodpowiednie, przesadzone, nieadekwatne lub nieistotne” lub są fake newsami. Celem badawczym artykułu jest przedstawienie procesu tworzenia prawa do bycia zapomnianym.

Arkadiusz Lewandowski

New technologies and cyberspace in the perspective of contemporary theories of the crisis of liberal democracy

Nowe technologie i cyberprzestrzeń w perspektywie współczesnych teorii kryzysu demokracji liberalnej

The aim of the presentation is to discuss the role and importance of new technologies and cyberspace in contemporary theories addressing both the causes and essence of the crisis of democracy. The talk will present the main assumptions of the most important theories addressing the current crisis, with emphasis on the issues related to the use of new technologies as an important element of political processes. Examples will include subjective deprivation, a sense of threat to national identities and, finally, polarization within societies. The sources and determining factors of the crisis of contemporary democracy diagnosed by the authors of individual theories refer, be it directly or indirectly, to new technologies and processes taking place in cyberspace. An attempt will be made to systematize and categorize the relationship between new technologies and the crisis of democracy.

Celem wystąpienia jest określenie znaczenia oraz roli nowych technologii i cyberprzestrzeni we współczesnych teoriach opisujących zarówno przyczyny jak i istotę kryzysu demokracji. W ramach wystąpienia przedstawione zostaną główne założenia najważniejszych teorii dotyczących współczesnego kryzysu z naciskiem na te kwestie, które odnoszą się do problematyki nowych technologii jako istotnego elementu procesów politycznych. Przykładem tego typu procesów są: subiektywna deprywacja, poczucie zagrożenia narodowych tożsamości czy wreszcie polaryzacja wewnątrz społeczeństw. Diagnozowane przez autorów poszczególnych teorii źródła oraz czynniki determinujące kryzys współczesnej demokracji w sposób bezpośredni lub pośredni odnoszą się do nowych technologii i procesów zachodzących w cyberprzestrzeni. Wystąpienie będzie próbą systematyzacji i typologizacji w obrębie relacji nowe technologie – kryzys demokracji.

Marcin Jastrzębski

Potential threats to human existence from artificial intelligence. Analysis of the current discourse of its creators

Potencjalne zagrożenia dla ludzkiej egzystencji ze strony sztucznej inteligencji. Analiza aktualnego dyskursu jej twórców

In recent years, the development of artificial intelligence (AI) has exceeded the boundaries of the science of artificial intelligence and its technical applications, also becoming a topic of discussion on the future of human existence within the social sciences. The present article analyzes the current discourse of AI creators, focusing on potential threats to human existence. The study is based on the analysis of scientific publications, conference deliberations, interviews, and media statements of experts in the field. The study identified the main areas of threats, from job loss, increasing social inequalities, the risk of excessive dependence on AI, to the occurrence of a technological singularity, i.e. a superintelligence beyond human understanding or control, which could entail the domination and even extinction of humanity. Moreover, the article evaluates the approaches and proposals of AI developers to minimize these threats, including legal regulations and ethical principles to ensure the safe and sustainable development of AI. The article empha-

W ostatnich latach rozwój sztucznej inteligencji (SI) przekroczył granice nauki o sztucznej inteligencji i jej technicznych zastosowań, stając się także tematem dyskusji toczonej w ramach m.in. nauk społecznych dotyczącej przyszłości ludzkiej egzystencji. Niniejszy artykuł analizuje aktualny dyskurs twórców SI, koncentrując się na potencjalnych zagrożeniach dla ludzkiej egzystencji. Badanie opiera się na analizie publikacji naukowych, dyskusjach konferencyjnych oraz wywiadach i wypowiedziach medialnych z ekspertami w dziedzinie SI. W wyniku przeprowadzonych analiz identyfikowane są główne obszary zagrożeń, od takich jak utrata miejsc pracy, zwiększenie nierówności społecznych, czy potencjalne ryzyko nadmiernego uzależnienia od SI po zjawisko osobliwości technologicznej (singularity), czyli możliwości powstania superinteligencji, która przekroczyłaby zdolności ludzkiego zrozumienia i kontrolowania, która mogłaby doprowadzić do zdominowania a nawet zagłady ludzkości. Ponadto, artykuł ocenia podejścia i propozy-

sizes the need for further interdisciplinary discussion and cooperation between scientists and creators of AI as well as representatives of other scientific disciplines, legislators, and representatives of societies in order to effectively mitigate potential threats resulting from the development of AI.

cje twórców SI w kwestii minimalizowania tych zagrożeń, włączając w to uregulowania prawne i zasady etyczne, które mają na celu zapewnienie bezpiecznego i zrównoważonego rozwoju SI. W artykule podkreślono potrzebę dalszej interdyscyplinarnej dyskusji oraz współpracy pomiędzy naukowcami - twórcami SI oraz przedstawicielami innych dyscyplin naukowych, twórcami prawa, i przedstawicielami społeczeństw w celu skutecznego niwelowania potencjalnych zagrożeń wynikającymi z rozwoju SI.

Panel sessions 3

Cybersecurity and digital resilience of internet users

Sesja panelowa 3

Cyberbezpieczeństwo i odporność cyfrowa użytkowników internetu

Joanna Grubicka

Cyber threats as a significant risk to an individual personal security in cyberspace

Cyberzagrożenia jako istotne ryzyko dla bezpieczeństwa personalnego jednostki w cyberprzestrzeni

The presented speech will discuss a practical approach to shaping a security system, using the examples of open-source intelligence (OSINT), Dark Web and generative artificial intelligence (GSI). In the current information environment, where security threats are becoming increasingly complex and unpredictable, it is important to use innovative tools and strategies to effectively protect against a variety of risks. OSINT enables the collection, analysis and use of information from publicly available sources, which allows for monitoring activities and identifying threats. On the other hand, the Dark Web is a hidden part of the Internet that can be used for illegal activities, but also pro-

W prezentowanym wystąpieniu zostanie omówienie praktyczne podejście do kształtowania systemu bezpieczeństwa, korzystając z przykładów Open Source Intelligence (OSINT), Dark Web oraz generatywnej sztucznej inteligencji (GSI). W obecnym otoczeniu informacyjnym, gdzie zagrożenia dla bezpieczeństwa stają się coraz bardziej złożone i nieprzewidywalne, istotne jest wykorzystanie innowacyjnych narzędzi i strategii w celu efektywnej ochrony przed różnorodnymi ryzykami. OSINT umożliwia zbieranie, analizę i wykorzystanie informacji z publicznie dostępnych źródeł, co pozwala na monitorowanie działań oraz identyfikację zagrożeń. Z drugiej strony, Dark Web stanowi

vides information about potential threats. However, GSI uses advanced machine learning algorithms to generate data and recognize behavioral patterns, which allows forecasting trends and detecting anomalies. The combination of these tools and technologies creates new opportunities for monitoring, analysis and response to security threats, while requiring constant adaptation to the changing cyberspace environment. The presentation will discuss in detail the identified threat directions and proposed countermeasures that can be used to minimize the risk for entities using new technologies. Ultimately, the goal of the Innovation Incubator 4.0 project is to promote awareness and education in the area of cybersecurity and support innovative solutions to protect against threats in the digital era.

ukrytą część internetu, która może być wykorzystywana do nielegalnych działań, ale także dostarcza informacji o potencjalnych zagrożeniach. Natomiast, GSI wykorzystuje zaawansowane algorytmy uczenia maszynowego do generowania danych i rozpoznawania wzorców zachowań, co pozwala na prognozowani trendów i wykrywanie anomalii. Połączenie tych narzędzi i technologii tworzy nowe możliwości w zakresie monitorowania, analizy i reakcji na zagrożenia bezpieczeństwa, wymagając równocześnie ciągłego dostosowywania się do zmieniającego się środowiska cyberprzestrzeni. Podczas prezentacji zostaną omówione szczegółowo zidentyfikowane kierunki zagrożeń oraz zaproponowane środki zaradcze, które mogą być stosowane w celu zminimalizowania ryzyka dla jednostek korzystających z nowych technologii. Ostatecznie, celem projektu Inkubatora Innowacyjności 4.0 jest promowanie świadomości i edukacji w zakresie cyberbezpieczeństwa oraz wspieranie innowacyjnych rozwiązań mających na celu ochronę przed zagrożeniami w erze cyfryzacji.

Izabela Kapsa, Aleksandra Błachnio,
Kamila Litwic-Kaminska, Łukasz Brzeziński,
Jakub Kopowski

Digital resilience of individuals, based on the example of UKW students – conclusions from empirical research

Odporność cyfrowa jednostek na przykładzie studentów UKW – wnioski z badań empirycznych

Digital resilience refers to the ability of individuals, communities and organizations to adapt to and cope with digital threats such as cyberattacks, data breaches and system failures, including awareness of these threats, the ability to recognize and avoid risks, and take effective actions in the event of an attack or cyber incident. The talk will include and analysis of digital resilience of the student body of Kazimierz Wielki University, based on the results of a study conducted in 2022-2023 (N=735) by a Polish team selected to work in the DigiPsyRes project (Increasing resilience to digital and psychological threats in times of crisis by creating networks peers in an online environment). Key aspects of digital resilience will be presented, including awareness of threats, the ability to deal with them, as well as practices for the safe use of digital technologies. The presentation of conclusions from the study will allow for a better understanding of the current challenges related to digital resilience in the context of the young

Odporność cyfrowa odnosi się do zdolności jednostek, społeczności i organizacji do dostosowywania się i radzenia sobie z zagrożeniami cyfrowymi, takimi jak cyberataki, naruszenia danych i awarie systemów, obejmując świadomość tychże zagrożeń, umiejętność rozpoznawania i unikania ryzyka oraz skuteczne działania w przypadku ataku czy incydentu cybernetycznego. Wystąpienie będzie poświęcone analizie odporności cyfrowej studentów Uniwersytetu Kazimierza Wielkiego, na podstawie wyników badań empirycznych przeprowadzonych w latach 2022-2023 (N=735) przez polski zespół powołany do pracy w projekcie DigiPsyRes (Zwiększanie odporności na zagrożenia cyfrowe i psychologiczne w czasach kryzysu poprzez tworzenie sieci rówieśniczych w środowisku online). Przedstawione zostaną kluczowe aspekty odporności cyfrowej, w tym świadomość zagrożeń, umiejętność radzenia sobie z nimi oraz praktyki bezpiecznego korzystania z technologii cyfrowych. Prezentacja wnio-

generation and to indicate potential directions of educational and social activities aimed at strengthening this dimension of individual resilience.

sków z badań empirycznych pozwoli na lepsze zrozumienie obecnych wyzwań związanych z odpornością cyfrową w kontekście młodego pokolenia oraz na wskazanie potencjalnych kierunków działań edukacyjnych i społecznych mających na celu wzmocnienie tegoż wymiaru odporności jednostek.

Ewa Kabza, Dominik Chodkowski

Cyberbullying

Cyfrowe nękanie (cyberbullying)

Characteristics of cyberbullying:
- aggressive, intentional, and repetitive activity of an (anonymous) person or group of people that occurs over some time, using electronic forms of contact, against a victim who cannot easily defend against attacks (OECD 2018),
- forms of “digital harassment”.

Legal effects of cyberbullying under Polish law and their limited usefulness in the case of peer-against-peer violence:
- the crime of persistent harassment (Article 190a of the Penal Code); and art. 190, 191, 202, 212, 216, 267, 268a of the Penal Code; art. 197, 141 of the Code of Petty Offences,
- the crime of persistent harassment (Article 190a of the Penal Code); and art. 190, 191,

Charakterystyka zjawiska cyberbullingu:
- cyberbulling to agresywne, intencjonalne, powtarzalne i rozłożone w czasie działanie (anonimowej) osoby bądź grupy osób, używających elektronicznych form kontaktu przeciwko ofierze, która nie ma możliwości łatwej obrony przed atakami (OECD 2018),
- formy „cyfrowego nękania”.

Skutki prawne stosowania cyberbullingu w świetle prawa polskiego i ich ograniczona przydatność w przypadku przemocy rówieśniczej:
- przestępstwo uporczywego nękania (art. 190a kk); oraz art. 190, 191, 202, 212, 216, 267, 268a kk; art. 197, 141 kw,
- przestępstwo uporczywego nękania (art. 190a kk); oraz art. 190, 191, 202, 212, 216, 267, 268a kk; art. 197, 141 kw,

202, 212, 216, 267, 268a Penal Code; art. 197, 141 of the Code of Petty Offences,
- violation of the victim's personal rights,
- Act on support and social rehabilitation of minors,
- "penalties" imposed on students in the light of the provisions of the Education System Act and school statutes.
"Social" responsibility:
- reporting offensive comments and entries to page administrators,
- balancing the child's right to privacy and confidentiality of correspondence and the proper exercise of parental authority,
- prevention.
The effects of cyberbullying.
Foreign examples of regulations:
- USA, e.g. in California (EDC § 234); Florida (Title XLVIII. K-20 Education Code § 1006.147); Missouri (MRS Title XI. § 160.775.),
- Austria - § 107c StGB,
- Italy – Legge n. 71/2017,
- Spain – art. 169 and art. 173 of the Código Penal.

- naruszenie dóbr osobistych ofiary,
- ustawa o wspieraniu i resocjalizacji nieletnich,
- „kary" nakładane na ucznia w świetle przepisów ustawy o systemie oświaty i w statutach szkoły.
„Społeczna" odpowiedzialność:
- zgłaszanie obraźliwych komentarzy, wpisów administratorom stron,
- wyważenie prawa do prywatności dziecka i tajemnicy korespondencji oraz właściwego sprawowania władzy rodzicielskiej,
- profilaktyka.
Skutki stosowania cyberbullingu.
Zagraniczne przykłady regulacji:
- USA np. w Kalifornia (EDC § 234); Floryda (Title XLVIII. K-20 Education Code § 1006.147); Missouri (MRS Title XI. § 160.775.),
- Austria - § 107c StGB,
- Włochy – Legge n. 71/2017,
- Hiszpania – art. 169 i art. 173 Código Penal.

Magdalena Biernacka, Aleksandra Pelczar

Sexual abuse of children in cyberspace – challenges and protection of the individual in the era of digitalization

Wykorzystywanie seksualne dzieci w cyberprzestrzeni – wyzwania i ochrona jednostki w erze cyfryzacji

In the current era of digitalization, humanity faces ever-increasing challenges that require action at national and international levels. One of the most disturbing problems is the sexual exploitation of children in cyberspace. This phenomenon, which is a direct result of the rapid development of technology and network globalization, as well as the ongoing armed conflict between Russia and Ukraine, poses new challenges for society. To effectively respond to this threat, it is necessary to adopt an interdisciplinary approach that combines knowledge from various fields of science, including: technology, psychology and law. In this speech, the authors will attempt to present the profile of perpetrators of sexual violence against children in the online environment. Current protection mechanisms and preventive methods used to combat sexual crimes against children in cyberspace will also be discussed. Particular attention will be paid to such phenomena as cyberpornography, cyberpedophilia, cyber-

W obecnej erze cyfryzacji, ludzkość stoi przed stale rosnącymi wyzwaniami, które wymagają działań na poziomie krajowym oraz międzynarodowym. Jednym z najbardziej niepokojących problemów jest wykorzystanie seksualne dzieci w cyberprzestrzeni. To zjawisko, będące bezpośrednim efektem szybkiego rozwoju technologii oraz globalizacji sieci, a także trwającego konfliktu zbrojnego pomiędzy Rosją, a Ukrainą stawia przed społeczeństwem nowe wyzwania. Aby skutecznie odpowiedzieć na to zagrożenie, konieczne jest przyjęcie interdyscyplinarnego podejścia, które łączy w sobie wiedzę z różnych dziedzin nauki m.in. technologii, psychologii oraz prawa. W niniejszym wystąpieniu autorzy podejmą próbę przedstawienia sylwetki sprawców przemocy seksualnej w środowisku online wobec dzieci. Omówione zostaną także aktualne mechanizmy ochrony oraz metody prewencyjne stosowane w zakresie zwalczania przestępstw seksualnych skierowanych przeciwko dzieciom w cyberprzestrzeni. Szczególna uwaga

prostitution and grooming, all of which constitute cybercrimes.

zostanie również poświęcona takim zjawiskom jak cyberpornografia, cyberpedofilia, cyberprostytucja oraz grooming, które zaliczane są do kategorii cyberprzestępstw.

Wojciech Trempała

The Novacene – James Lovelock on the post-Anthropocene, evolution and superintelligence

Era Nowocenu – James Lovelock o post-antropocenie, ewolucji i superinteligencji

James Lovelock (born 1919 – died 2022) is one of the greatest minds of the 20th and first two decades of the 21st century. Author of numerous patents, inventor of devices for chemical measurements in the environment, some of which are used by NASA for space exploration. All of his honors and decorations would be too numerous to list. His most famous concept – the Gaia Hypothesis – is a set of ideas crucial for the development of humanistic and social research on the environmental crisis. He has also been a source of inspiration for numerous "green" movements, and for the world of pop culture. The aim of the talk, however, will be to present and analyze Lovelock's proposals advanced in a less known book, published three years before his death, entitled *Novacene: The Coming Age of Hyperintelligence* (2019).

James Lovelock (ur. 1919 – zm. 2022) to jeden z najwybitniejszych umysłów XX i pierwszych dwóch dekad wieku XXI. Autor licznych patentów, wynalazca urządzeń do pomiarów chemicznych w środowisku, w tym takich, które były wykorzystywane przez NASA do badań kosmosu. Trudno wyliczyć wszystkie honory i odznaczenia, których jest on laureatem. Jego najsłynniejsza koncepcja - „Hipoteza Gai" - to zbiór idei kluczowych dla rozwoju humanistycznych i społecznych badań nad kryzysem środowiskowym. Ponadto inspiracja dla licznych ruchów zielonych, jak i świata popkultury. Celem wypowiedzi będzie jednak prezentacja i analiza tez wyłożonych przez Lovelocka w mniej znanej, opublikowanej na 3 lata przed jego śmiercią, książce pod tytułem: Novacene: The Coming Age of Hyperintelligence (2019). Czym będzie

What will be the characteristics of the new system of human life based on cybernetics? What does the disappearance of biological life forms mean for humanity? Will artificial intelligence enslave the homo sapiens or will it save the world from ecological catastrophe? This is merely a handful of the questions that the British scientist tried to answer. The pace at which artificial intelligence has been developing in recent years and the debate on the political, social and ethical consequences of this development mean that Lovelock's voice should not be omitted in this discussion. On the contrary, it deserves wider popularization.

charakteryzował się nowy system życia gatunku ludzkiego oparty na cybernetyce? Co oznacza dla ludzkości zanik znaczenia biologicznych form życia? Czy sztuczna inteligencja zniewoli homo sapiens czy też uratuje świat przed katastrofą ekologiczną? To tylko nieliczne pytania, na które starał się udzielić odpowiedzi brytyjski uczony. Tempo z jaką w ostatnich latach rozwija się sztuczna inteligencja oraz sama debata na temat politycznych, społecznych i etycznych konsekwencji tego rozwoju powoduje, że głos Lovelocka nie powinien być w tej dyskusji pomijany. Wręcz przeciwnie, zasługuje na szerszą popularyzację.

Panel sessions 4

Cyberspace as a new dimension of state competition

Sesja panelowa 4

Cyberbezpieczeństwo jako nowy wymiar rywalizacji państw

Joanna Antczak

Cybersecurity of the Weimar Triangle countries – selected aspects

Cyberbezpieczeństwo państw Trójkąta Weimarskiego – wybrane aspekty

The global landscape of cyberthreats has undergone significant evolution, including a range of sophisticated attacks targeting various countries and sectors. There is a need for systemic coordination on the national level in order to effectively analyze the need for expenditure and minimize costs. Knowledge of the costs incurred by the private sector in the area of cybersecurity is necessary for those in power. A good decision-making structure is the key to a rational and more effective cybersecurity spending policy at the national level, both on the government/public and private side. At the national level, it is necessary to precisely

Krajobraz globalnych cyberzagrożeń znacznie ewoluował, demonstrując szereg wyrafinowanych ataków wymierzonych w różne sektory i kraje. Występuje konieczność koordynacji systemowej w skali państwa, tak aby skutecznie analizować konieczność wydatków, minimalizować koszty. Niezbędna jest wiedza dla rządzących w zakresie ponoszonych kosztów przez sektor prywatny w zakresie cyberbezpieczenstwa. Dobra struktura decyzyjna stanowi klucz dla racjonalnej i zarazem bardziej efektywnej polityki nakładów na cyberbezpieczeństwo w skali państwa, zarówno po stronie rządowej/publicznej, jak i prywatnej. W skali państwa niezbędne jest

define competences in three areas: detecting, protecting and responding to threats at all levels of the state and at the same time initiating and coordinating activities at all levels. The strategies of the Weimar Triangle countries jointly emphasize the importance of cybersecurity in protecting interconnected digital systems and the proactive measures needed to counter potential cyber threats and mitigate their effects through national initiatives and international cooperation.

dokładne określenie kompetencji w trzech obszarach: wykrywania, chronienia oraz reagowania na zagrożenia na wszystkich płaszczyznach państwowym i jednocześnie inicjowanie i koordynowanie działań na wszystkich poziomach. Strategie państw Trójkąta Weimarskiego łącznie podkreślają znaczenie cyberbezpieczeństwa w ochronie wzajemnie połączonych systemów cyfrowych oraz proaktywne środki niezbędne do przeciwdziałania potencjalnym cyberzagrożeniom i łagodzenia ich skutków poprzez inicjatywy krajowe i współpracę międzynarodową.

Kamila Sierzputowska

In the direction of cyber -security? NATO and cybersecurity support mechanisms

W kierunku cybestabilności? NATO a mechanizmy wsparcia cyberbezpieczeństwa

The threats that are associated with cyberspace include all entities of the modern safety environment, including NATO. Due to the fact that cyber threats are becoming more frequent, more complex NATO was forced to take specific steps in the field of cyberbrona to face the evolving challenges.
The subject of the study presented in the article are the activities and mechanisms of NATO cybersecurity contributing to the de-

Zagrożenia, które związane są z cyberprzestrzenią obejmują wszystkie podmioty współczesnego środowiska bezpieczeństwa, w tym również NATO. Z uwagi na to, że zagrożenia cybernetyczne stają się coraz częstsze, bardziej złożone NATO zmuszone było podjąć określone kroki w dziedzinie cyberobrony, aby zmierzyć się z wziąć ewoluującymi wyzwaniami. Przedmiotem badania przedstawionym w artykule są działania i mechanizmy

velopment of this organization's ability. They include a number of strategies and actions taken as a result, aimed at protecting allies against threats associated with cyberspace. The need to strengthen the ability to defend against cybernetic attacks was first recognized by the alliance leaders during their peak in Prague in 2002. Since then, cybernetic issues have occupied an increasingly prominent place in NATO peak programs. In 2008, the first NATO policy in the field of cyberbron was adopted. However, 6 years later, cyberbrona became an integral part of collective defense, declaring that cyberrataki could lead to reference to Article 5 of the NATO founding treaty about collective defense. Even in 2016, Member States recognized the cyber space as the area of armed activities and, to a greater extent, undertook to strengthen cyberbron in relation to their national networks and infrastructure and to treat it as a priority. The basic thesis of the article indicates mechanisms that are a comprehensive set of activities aimed at increasing the cybersecurity of NATO and its members.

As part of the organization's cyber policy, the principles and guidelines of cybernetic activities were set out, including cooperation with allies and reaction to cyber attacks, defensive and proactive activities.

Key words: *NATO, cyberthreats, cyberdefense, cybersecurity, cyberspace*

cyberbezpieczeństwa NATO przyczyniające się do rozwoju zdolności tej organizacji. Obejmują szereg strategii i działań podjętych w jej wyniku, mających na celu ochronę sojuszników przed zagrożeniami związanymi z cyberprzestrzenią. Konieczność wzmocnienia zdolności do obrony przed atakami cybernetycznymi po raz pierwszy została uznana przez przywódców Sojuszu podczas ich szczytu w Pradze w 2002 roku. Od tego czasu zagadnienia cybernetyczne zajmowały coraz bardziej poczesne miejsce w programach szczytów NATO. W 2008 roku przyjęto pierwszą politykę NATO w dziedzinie cyberobrony. Natomiast, już 6 lat później cyberobrona stała się nieodłączną częścią obrony zbiorowej deklarując, że cyberataki mogą prowadzić do powołania się na Artykuł 5 traktatu założycielskiego NATO mówiący o obronie zbiorowej. Jeszcze w 2016 roku państwa członkowskie uznały przestrzeń cybernetyczną za obszar działań zbrojnych i w większym stopniu zobowiązały się do wzmacniania cyberobrony w odniesieniu do swoich krajowych sieci i infrastruktury oraz traktowania jej jako priorytet.

Zasadnicza teza artykułu wskazuje na mechanizmy stanowiące kompleksowy zestaw działań mających na celu zwiększenie cyberbezpieczeństwa NATO i jego członków. W ramach polityki cybernetycznej organizacji określone zostały zasady i wytyczne działań cybernetycznych, w tym współpracy z sojusznikami i reakcji na ataki cybernetyczne, działań defensywnych, jak i proaktywnych.

Słowa klucze: NATO, *cyberzagrożenia, cyberobrona, cyberbezpieczeństwo, cyberprzestrzeń*.

Karol Piękoś

Threats originating in cyberspace as one of the grounds for introducing a state of emergency

Zagrożenia pochodzące z cyberprzestrzeni jako jedna z przesłanek wprowadzenia stanu nadzwyczajnego

Contemporary threats to state security are characterized by complexity. The rapid development of civilization has also made cyberspace a place full of potential threats. Due to this problem in Poland, in 2011 changes were made to the laws regarding states of emergency. The Polish Constitution of April 2, 1997 provides for the possibility of introducing: martial law, a state of emergency and a state of natural disaster. As a result of the 2011 amendment, each of these may be imposed due to activities in cyberspace. This presentation will analyze the potential consequences of hostile actions carried out in cyberspace from the perspective of regulating states of emergency.

Współczesne zagrożenia dla bezpieczeństwa państw, charakteryzują się złożonością. Szybki rozwój cywilizacyjny spowodował, że również cyberprzestrzeń stała się miejscem pełnym potencjalnych zagrożeń. Wobec tego problemu w Polsce, w 2011 r. dokonano zmian w ustawach dotyczących stanów nadzwyczajnych. Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. przewiduje możliwość wprowadzenia: stanu wojennego, stanu wyjątkowego jak i stanu klęski żywiołowej. W wyniku nowelizacji z 2011 r. każdy z nich może zostać wprowadzony z powodu działań w cyberprzestrzeni. W przedmiotowym wystąpieniu zostanie podjęta próba analizy potencjalnych konsekwencji wrogich działań, prowadzonych w cyberprzestrzeni z perspektywy regulacji stanów nadzwyczajnych.

Marcin Wałdoch

The Cyberspace Component in the AUKUS Agreement

Komponent cyberprzestrzeni w porozumieniu AUKUS

The Trilateral Agreement on Military and Technological Cooperation of Australia, Great Britain and the United States (AUKUS) turned out to be a particularly important instrument in the development of cooperation between these countries and their selected partners in cyberspace, particularly in building cybersecurity instruments. A component of the AUKUS treaty (Pillar II) contains particularly important provisions on cooperation in cyberspace and the development of defensive and offensive means. The talk will present the positions of the AUKUS signatory countries and the potential for expanding cooperation at the level of Pillar II, under which more and more countries around the world, including New Zealand, are willing to cooperate.

Umowa o współpracy w zakresie militarnym i technologicznym - Australii, Wielkiej Brytanii i Stanów Zjednoczonych (AUKUS), okazała się być szczególnie ważnym instrumentem w rozwoju współpracy pomiędzy wymienionymi państwami oraz ich wybranymi partnerami w zakresie cybeprzestrzeni, a szczególnie budowania instrumentów cyberbezpieczeństwa. Komponent umowy AUKUS w tzw. filarze II zawiera szczególnie ważne zapisy o współpracy w zakresie cyberprzestrzeni i rozwijania środków defensywnych i ofensywnych. W trakcie wystąpienia przedstawione zostaną stanowiska państw sygnatariuszy AUKUS oraz potencjał rozszerzenia współpracy właśnie na płaszczyźnie filaru II, w ramach którego chęć współpracy zgłasza coraz więcej państw świata, w tym Nowa Zelandia.

Marcin Leźnicki

Bioethics in the digital age. Ethical considerations on ongoing digitization

Bioetyka w erze cyfrowej. Etyczne rozważania na temat postępującej digitalizacji

Along with the dynamic development of digital technologies, cyberspace has become an integral part of our everyday life. The use of increasingly advanced technologies has opened up countless opportunities for us, but it has also highlighted new bioethical challenges that we must meet in the perspective of the rapidly changing digital reality. The article presents selected threats in the area of bioethics posed by the dynamic development of digital technologies that penetrate our lives. Examples of (bio)ethical issues considered in the context of the development of cyberspace include: the problem of individual autonomy in the era of algorithms, security of medical data in the digital world, ethical aspects of the development and application of artificial intelligence in medicine (including the responsible use of AI algorithms in diagnosing and treating diseases and conducting research), limits of the development of genetic engineering in the era of digital technologies (also in the context of the discussion on responsibility for the possible effects of genetic manipulation in cyberspace), or even

Wraz z dynamicznym rozwojem technologii cyfrowych, cyberprzestrzeń stała się nieodłączną częścią naszego codziennego życia. Wykorzystanie coraz to bardziej zaawansowanych technologii otworzyło przed nami niezliczone możliwości ale równocześnie uwidoczniło nowe wyzwania bioetyczne, którym musimy sprostać w perspektywie zmieniającej się szybko rzeczywistości cyfrowej. W artykule zaprezentowano wybrane zagrożenia z obszaru bioetyki, jakie niesie za sobą dynamiczny rozwój przenikających nasze życie technologii cyfrowych. Wśród przykładowych zagadnień (bio)etycznych rozpatrywanych w kontekście rozwoju cyberprzestrzeni wymienić można m.in. problem autonomii jednostki w erze algorytmów, bezpieczeństwa danych medycznych w świecie cyfrowym, etycznych aspektów rozwoju i zastosowania sztucznej inteligencji w medycynie (w tym m.in. odpowiedzialnego wykorzystania algorytmów AI w diagnozowaniu i leczeniu chorób oraz prowadzeniu badań naukowych), granic rozwoju inżynierii genetycznej w dobie technologii cyfrowych (m.in.

the possibility of maintaining privacy in the era of "collective" cyberspace. These issues require not only theoretical reflection, but also practical actions aimed at ensuring an appropriate level of privacy protection, data security and, finally, the application of ethical standards in the use of modern technologies, so that technological progress goes hand in hand with the moral and ethical progress of society.

w kontekście dyskusji poświęconej odpowiedzialności za ewentualne skutki manipulacji genetycznej w cyberprzestrzeni), czy choćby możliwości utrzymania etyki prywatności w erze „zbiorowej" cyberprzestrzeni. Wyszczególnione wątpliwości wymagają podjęcia nie tylko refleksji teoretycznej, ale także praktycznych działań mających na celu zapewnienie odpowiedniego poziomu ochrony prywatności, bezpieczeństwa danych a wreszcie zastosowania etycznych norm w wykorzystaniu nowoczesnych technologii, tak aby postęp technologiczny szedł w parze z postępem moralnym i etycznym społeczeństwa.

Panel sessions 5

Socio-economic challenges of cyberspace

Sesja panelowa 5

Społeczno-ekonomiczne wyzwania cyberprzestrzeni

Ewa Matuska

The human-centric HR model in talent and competence management in the era of digital transformation

Humano-centryczny model HR w zarządzaniu talentami i kompetencjami w dobie transformacji cyfrowej

With the introduction of cloud computing, mobile applications and AI solutions, employees may not only work from anywhere with access to the same information, but above all, they can work more efficiently. The increase in productivity is not so much a matter of more work being done in a given time, but of its better quality - values delivered to customers that are better tailored to their needs thanks to agile management practices. Digital transformation has also created a new set of skills that companies need to stay competitive and keep their data secure. Employees must constantly improve their competences, especially digital ones. HR depart-

Wraz z wprowadzeniem chmury obliczeniowej, aplikacji mobilnych oraz rozwiązań z zakresu AI pracownicy mogą nie tylko pracować z dowolnego miejsca i mieć dostęp do tych samych informacji, niezależnie od ich fizycznej lokalizacji, ale przede wszystkim pracować wydajniej. Wzrost produktowości firm to nie tyle kwestia większej ilości pracy wykonanej w danym czasie, co lepsza jej jakość – lepiej dopasowane wartości dostarczane klientom dzięki zwinnym praktykom zarządzania. Transformacja cyfrowa stworzyła też nowy zestaw umiejętności, których firmy potrzebują, aby pozostać konkurencyjnymi i zapewnić bezpieczeństwo swoich danych. Pra-

ments are responsible for providing useful training and creating programs enabling the retention of trained talents. According to recent research, the pool of digital talents in organizations turns out to be larger than expected, and the so-called knowledge workers who identify as creators and heavy users of AI are surprisingly looking for something other than additional technical skills: socio-emotional skills, meaningful work, and a supportive environment. How can organizations provide this? Is the so-called Is the human-centric HR model helpful here?

cownicy muszą stale doskonalić swoje kompetencje, zwłaszcza cyfrowe. Działy HR zaś mają za zadanie dostarczać użytecznych szkoleń i tworzyć programy umożliwiające zatrzymanie wyszkolonych talentów w firmie. Według ostatnich badań pula talentów cyfrowych w organizacjach okazuje się większa niż oczekiwano, a tzw. pracownicy wiedzy, którzy identyfikują się jako twórcy i intensywni użytkownicy sztucznej inteligencji, zaskakująco poszukują czegoś innego niż dodatkowe umiejętności techniczne: umiejętności społeczno-emocjonalnych, znaczącej pracy i wspierającego środowiska. W jaki sposób organizacje mogą im tego dostarczać? Czy tzw. humano-centryczny model HR jest tu pomocny?

Małgorzata Cieślik-Florczyk

Creating the company image. A networking group as a form of a network community

Kreowanie wizerunku przedsiębiorstwa. Grupa networkingowa jako forma społeczności sieciowych

Building a company's brand is one of the basic elements influencing its development. A brand can be created using various tools. One of them is networking groups Understood in this way, branding allows the com-

Budowanie marki przedsiębiorstwa stanowi jeden z podstawowych elementów wpływających na rozwój przedsiębiorstwa. Markę można kreować z wykorzystaniem różnych narzędzi. Jednym z nich są grupy networkon-

pany to stand out from the competition, which in turn has a positive impact on the profitability of the business. This goal can be achieved using a variety of tools, including networking groups. The aim of the work is to demonstrate how participation in networking groups contributes to building a brand and how an online image created in this way can contribute to the development of a brand on the Internet.

gowe. Budowanie marki stanowi jeden z podstawowych elementów rozwoju każdego przedsiębiorstwa. Rozumiany w ten sposób branding pozwala wyróżnić się przedsiębiorstwu na tle konkurencji, co z kolei ma pozytywnie wpłynąć na zyskowność prowadzonego biznesu. Cel ten można osiągnąć za pomocą różnorodnych narzędzi. Przykładem tego typu narzędzi są grupy networkingowe. Celem pracy jest wykazanie, w jaki sposób uczestnictwo w grupach networkingowych przyczynia się do budowania marki i w jaki sposób tak tworzony wizerunek w sieci może przyczynić się do rozwoju marki w Internecie.

Wojciech Mincewicz

Models of state policies towards cryptocurrencies after 15 years of operation: from legalism to prohibition

Modele polityk państw wobec kryptowalut po 15-latach funkcjonowania: od legalizmu do zakazów

The advent of Bitcoin and other decentralized virtual currencies operating in a cryptographically secured peer-to-peer network, based on trust and consensus which partially fulfill the functions of money, significantly influenced the relationship between the state and the individual in the monetary sphere. Since

Powstanie Bitcoina, a następnie kolejnych zdecentralizowanych, funkcjonujących w sieci o architekturze peer-to-peer, zabezpieczonych kryptograficznie, opartych na zaufaniu i konsensusie, walut wirtualnych, spełniających w niepełny sposób niektóre funkcje pieniądza w sposób istotny wpłynął na rela-

2009, economic circulation outside state control has become possible, and has resulted in the creation of commercial exchange independent of state institutions, tax-free, and uncontrolled by the state. In this situation, it is justified to ask about the reactions of state and non-state actors, which should formulate a model of action. Already in 2014, there were voices in the academic debate that the further development of state policy toward cryptocurrencies would be similar to how the Internet was treated at the beginning of its existence. For the first few years, the authorities perceived the Internet, electronic trading, e-commerce and other spheres of operation of the World Wide Web as a special type of traditionally conducted activity. This approach was only partly successful. The process of evolving policy changes towards cryptocurrencies is similar. After 15 years of existence, it is possible to distinguish at least five model policies that countries pursue, and the first part of the speech will be devoted to analyzing them, indicating the scope of them. The second part will present the results of the author's own research, where, based on the designed empirical indicators, the key research question revolved around an attempt to design the state policy toward cryptocurrencies in Poland expected by users.

cje pomiędzy państwem, a jednostką w sferze monetarnej. Od 2009 roku możliwy staje się obieg ekonomiczny poza kontrolą państwa, a w efekcie tworzenie niezależnej od instytucji państwowych, nieopodatkowanej i niekontrolowanej przez państwo wymiany handlowej. W tej sytuacji zasadnym staje się pytanie o reakcje aktorów państwowych i pozapaństwowych, które powinny sformułować model działań. Już w 2014 roku w debacie akademickiej pojawiły się głosy, że dalszy rozwój polityki państw wobec kryptowalut będzie zbliżony do tego, jak był traktowany Internet na początku swojego istnienia. Przez kilka początkowych lat władze postrzegały Internet, obrót elektroniczny, e-handel oraz inne sfery funkcjonowania sieci WWW, jako szczególny rodzaj tradycyjnie prowadzonej działalności. Podejście takie zakończyło się połowicznym sukcesem. W podobny sposób przebiega proces ewolucji zmian polityk wobec kryptowalut. Po 15-latach istnienia możliwe jest wyróżnienie co najmniej pięciu modelowych polityk, które prowadzą państwa i analizie tychże poświęcona zostanie pierwsza część wystąpienia, wskazując na zakres tychże. W drugiej części przedstawione zostaną natomiast wyniki badań własnych autora, gdzie na podstawie zaprojektowanych wskaźników empirycznych kluczowym pytaniem badawcze oscylowało wokół próby zaprojektowania oczekiwanej przez użytkowników polityki państwa wobec kryptowalut w Polsce.

Magdalena Bierzyńska-Sudoł

The role and significance of cyberspace in the integration of migrants in the modern world

Rola i znaczenie cyberprzestrzeni w integracji migrantów we współczesnym świecie

The modern world is characterized by an increasing influx of migrants from various parts of the world. Their integration in the new society is becoming one of the most important challenges, and cyberspace is becoming one of the key tools in this process. The Internet and digital technologies currently play a very important role in the integration of migrants, who can maintain contact with their families and friends, have access to online courses and e-learning platforms, and can develop professionally and improve their qualifications, which significantly facilitates the process of adaptation to a new social, cultural and professional environment. The Internet provides access to information about local customs, rights and obligations. Social media give migrants the opportunity to build online communities, share experiences and support each other. Migrant groups on online platforms also help in solving problems related to looking for a job or apartment and organizing cultural events. However, it is worth remembering that access to the Internet is not equal for all migrants, and thus it is important that

Współczesny świat charakteryzuje się coraz większym napływem migrantów z różnych części świata. Integracja tych osób w nowym społeczeństwie staje się jednym z ważniejszych wyzwań, a jednym z kluczowych narzędzi w tym procesie staje się cyberprzestrzeń. Jako obszar internetu i technologii cyfrowych, pełni obecnie bardzo istotną rolę w integracji migrantów. Dzięki sieci mogą oni zachować kontakt ze swoimi rodzinami i przyjaciółmi, mają dostęp do kursów online i platform e-learningowych, mogą oni rozwijać się zawodowo i podnosić kwalifikacje, co znacząco ułatwia proces adaptacji do nowego środowiska społecznego, kulturowego i zawodowego. Internet umożliwia dostęp do informacji o lokalnych zwyczajach, prawach i obowiązkach. Media społecznościowe, dają migrantom możliwość budowania społeczności online, dzielenia się doświadczeniami i wspierania się nawzajem. Grupy migrantów na platformach internetowych pomagają również w rozwiązywaniu problemów związanych z poszukiwaniem pracy czy mieszkania oraz organizowaniu wydarzeń kulturalnych. Jednak warto pamiętać, że dostęp do

actions be taken to ensure equal access to the Internet for all migrants.

internetu nie jest równy dla wszystkich migrantów. Dlatego ważne jest, aby prowadzone były działania mające na celu równomierne zapewnienie dostępu do internetu dla wszystkich migrantów.

Panel sessions 6

Virtually local - application of new technologies in public administration

Sesja panelowa 6

Wirtualnie lokalnie - zastosowanie nowych technologii w administracji publicznej

Alina Kaszkur

New technologies and the resilience of cities

Nowe technologie a odporność miast

The growing scale and specificity of contemporary threats, also in cyberspace, require from those in power not only the ability to quickly react and make decisions, but above all, take pre-emptive actions. At the city level, this responsibility falls on the local authorities. Cities therefore need not only decision-makers who are well prepared for these circumstances, but also an appropriate resilience strategy. The talk presents the concept of urban resilience, with particular emphasis on the technological aspects influencing it.

Rosnąca skala i specyfika współczesnych zagrożeń, także w cyberprzestrzeni, wymaga od rządzących nie tylko umiejętności szybkiego reagowania i podejmowania decyzji, ale przede wszystkim działań wyprzedzających. Na poziomie miast odpowiedzialność ta spada na władze lokalne. Miasta potrzebują zatem nie tylko dobrze przygotowanych na te okoliczności decydentów, ale także stworzenia i wdrożenia odpowiedniej strategii odporności. Proponowane wystąpienie będzie miało na celu przybliżenie koncepcji odporności miejskiej, ze szczególnym uwzględnieniem wpływających na nią aspektów technologicznych.

Adam Ilciów

Resilient, intelligent, balanced. Concepts of city development in the face of technology and potential threats

Rezylientne, inteligentne, zrównoważone. Koncepcje rozwoju miast wobec technologii i potencjalnych zagrożeń

Technologies are constantly being developed, innovations are initiated, known solutions find new applications, and increasingly larger groups of stakeholders are involved in the development of technologies. The changes taking place are particularly visible in urban centers. Investments in infrastructure, environmental protection, safety and city management affect the quality of life of residents. The use of modern technologies in developing the smart city concept shows what cities of the future may become. Unfavorable megatrends, such as demographic changes, increasing urbanization, or constantly growing demand for energy intensify potential threats and encourage sustainable and responsible use of resources. The answer may lie in the concepts of urban development, particularly in the resilient city.

Technologie są stale rozwijane, innowacje inicjowane, znane rozwiązania znajdują nowe zastosowania, w rozwój technologii włączane są coraz większe grupy interesariuszy. W ośrodkach miejskich w szczególności widoczne są dokonujące się zmiany. Inwestycje w infrastrukturę, ochronę środowiska, bezpieczeństwo i aspekty związane z zarządzaniem miastem wpływają na jakość życia mieszkańców. Zastosowania nowoczesnych technologii w rozwijaniu koncepcji smart city wskazują jakimi mogą stać się miasta przyszłości. Niekorzystne megatrendy, jak zmiany demograficzne, wzrost urbanizacji, czy stale rosnące zapotrzebowanie na energię, intensyfikują potencjalne zagrożenia i skłaniają do zrównoważonego i odpowiedzialnego dysponowania zasobami. Odpowiedzią mogą być koncepcje rozwoju miast, w tym miasta rezylientnego.

Martyna Rajek-Kwiatek

Citizensourcing as a tool for local development - case analysis from Polish cities

Citizensourcing jako narzędzie rozwoju lokalnego – analiza przypadków z polskich miast

The aim of the presentation is to analyze the use of citizensourcing as a tool supporting local development in the context of Polish cities. Citizensourcing, understood as the involvement of residents in decision-making and development processes using information and communication technologies, is an important element in creating social inclusion and administrative efficiency. Therefore, based on case studies from selected cities in Poland, the author will attempt to discuss how city decision-makers implement citizensourcing strategies to stimulate civic activity, support innovation and solve current urban problems. The analysis will cover both successes and challenges faced by citizensourcing projects, which may limit their effectiveness. It is thus also necessary to appropriately adapt the methods and tools to the specific conditions of a particular urban environment. Only properly managed citizensourcing can significantly contribute to increasing social participation, improving public services, integrating urban communities, and increasing social trust in local authorities. Also

Celem wystąpienia jest analiza wykorzystania citizensourcingu jako narzędzia wspierającego rozwój lokalny w kontekście polskich miast. Citizensourcing, rozumiany jako zaangażowanie mieszkańców w procesy decyzyjne i rozwojowe przy wykorzystaniu technologii informacyjno-komunikacyjnych, stanowi istotny element w kreowaniu inkluzji społecznej oraz efektywności administracyjnej. W związku z tym i w oparciu o studia przypadków z wybranych miast w Polsce, autorka podejmie próbę omówienia tego, w jaki sposób decydenci miejscy implementują strategie citizensourcingu, aby stymulować aktywność obywatelską, wspierać innowacje i rozwiązywać bieżące problemy miejskie. Analiza obejmie zarówno sukcesy, jak i wyzwania związane z wdrażaniem projektów citizensourcingowych, które mogą wpływać na ograniczenie ich efektywności. Stąd też koniecznością jest także odpowiednie dostosowanie metod i narzędzi do specyficznych warunków danego środowiska miejskiego. Tylko odpowiednio zarządzany citizensourcing może bowiem zna-

important is openness, availability and scalability of citizensourcing projects as the primary factors of their effectiveness and durability. In conclusion, the author will present recommendations for city decision-makers interested in implementing similar projects and maximizing the benefits of civic involvement. The conclusions can also serve as a guide for other cities that plan to introduce citizensourcing as a permanent element of their development strategy.

cząco przyczyniać się do zwiększenia partycypacji społecznej, poprawy usług publicznych, integracji społeczności miejskich czy wzrostu zaufania społecznego do władz lokalnych. Ważne jest też znaczenie otwartości, dostępności i skalowalności projektów citizensourcingowych jako nadrzędnych czynników ich efektywności i trwałości.
W konkluzji autorka przedstawi rekomendacje dla decydentów miejskich zainteresowanych implementacją podobnych projektów i maksymalizacją korzyści wynikających z obywatelskiego zaangażowania. Wnioski mogą też służyć jako drogowskaz dla innych miast, które planują wprowadzenie citizensourcingu jako stałego elementu strategii rozwoju.

Paweł Nowak

The impact of the COVID-19 pandemic on increasing the digital accessibility of local government units in Poland

Wpływ pandemii COVID-19 na zwiększenie dostępności cyfrowej jednostek samorządu terytorialnego w Polsce

The Covid-19 pandemic forced the transfer of local government public services to the virtual sphere. Remote handling of matters in offices became the norm rather than the exception. The 2016 EU Directive on public sector websites and mobile applications and the

Pandemia Covid-19 wymusiła przeniesienie samorządowych usług publicznych do świata wirtualnego. Zdalna obsługa spraw w urzędach stała się raczej normą niż wyjątkiem. Dyrektywa UE z 2016 r. w sprawie stron internetowych i aplikacji mobilnych sektora

European Digital Accessibility Act 2019 introduced an obligation to provide these services electronically and make them accessible to people with disabilities. The aim of the present study was to determine whether the Covid-19 pandemic resulted in the implementation of European solutions in the Polish legal system and whether this implementation resulted in the adaptation of digital activities of local government units (LGUs) to the needs of people with disabilities. The study was conducted in the fourth quarter of 2022 in two trial forms: 1. in the form of a survey (approx. 250 local government units), which included meeting formal requirements, the level of readiness of officials to create documents and digitally available content, and the organizational readiness of offices. 2. In the form of an analysis of the source code of the websites of 66 Polish cities with county rights – due to the availability of the results of the same sample from 2015. The results showed that local government units in Poland: 1. met the formal and organizational requirements for digital accessibility, 2. did not make every effort to prepare employees to create digitally accessible documents and content, 3. the websites examined had worse source code in 2022 in terms of meeting the WCAG standard than in 2015. It seems reasonable to conclude that the Covid-19 pandemic had a formal, but not real, impact on the digital availability of services provided by Polish local government units.

publicznego oraz europejska ustawa o dostępności cyfrowej z 2019 r. wprowadziły obowiązek świadczenia tych usług drogą elektroniczną i dostępności dla osób niepełnosprawnych. Celem przeprowadzonego przez autorów badania było ustalenie czy pandemia Covid-19 spowodowała wdrożenie rozwiązań europejskich w polskim porządku prawnym oraz czy wdrożenie to przełożyło się na faktyczne dostosowanie działań cyfrowych jednostek samorządu terytorialnego (JST)) do potrzeb osób niepełnosprawnych. Badanie przeprowadzono w IV kwartale 2022 r. w dwóch formach próbnych: 1. w formie ankiety (ok. 250 JST), która obejmowała spełnianie wymogów formalnych, poziom gotowości urzędników do tworzenia dokumentów i treści dostępnych cyfrowo, i gotowość organizacyjną urzędów. 2. W formie analizy kodu źródłowego stron internetowych 66 polskich miast na prawach powiatu – w związku z dostępnością wyników tej samej próby z 2015 roku. Przeprowadzone badania wykazały, że JST w Polsce: 1. spełniły wymogi formalne i organizacyjne dostępności cyfrowej, 2. nie dołożyły wszelkich starań, aby przygotować pracowników do tworzenia dokumentów i treści dostępnych cyfrowo, 3. badane strony internetowe miały w 2022 r. gorszy kod źródłowy pod względem spełnienia standardu WCAG niż w 2015 r. Zasadny wydaje się wniosek, że pandemia Covid-19 miała formalny, a nie realny wpływ na dostępność cyfrową usług świadczonych przez polskie JST.

Barbara Panciszko-Szweda,
Małgorzata Sikora-Gaca

Using digital tools to improve accessibility for people with special needs in rural areas

Wykorzystanie narzędzi cyfrowych do poprawy dostępności osób ze szczególnymi potrzebami na obszarach wiejskich

People with special needs (people with disabilities, elderly people, temporary or permanent mobility problems, mental limitations, pregnant women or parents with small children) struggle with numerous problems related to accessibility. People living in rural areas (especially peripheral ones), where access to basic and specialized medical care is at a lower level than in cities, are particularly exposed to social exclusion and marginalization; the issue of access to rehabilitation, educational, transport and job services is similar. The research problem outlined in this way leads the authors to formulate the following hypothesis: the development of information and communication technology is an opportunity for people with special needs to increase their access to diagnostic, medical and rehabilitation services in rural areas. The presentation will answer the following questions: what are the main barriers in access to diagnostic, rehabilitation and medical ser-

Osoby ze szczególnymi potrzebami (z niepełnosprawnościami, osoby starsze, z czasowymi lub trwałymi problemami z poruszaniem się, ograniczeniami mentalnymi, kobiety w ciąży czy rodzice z małymi dziećmi) borykają się z licznymi problemami związanymi z dostępnością. Szczególnie narażone na wykluczenie i marginalizację społeczną są osoby zamieszkujące obszary wiejskie (zwłaszcza peryferyjne), gdzie dostęp do podstawowej i specjalistycznej opieki medycznej jest na niższym poziomie niż w mieście; analogicznie wygląda kwestia dostępu do usług rehabilitacyjnych, edukacyjnych, transportowych czy miejsc pracy. Tak zarysowany problem badawczy skłania autorki do postawienia hipotezy badawczej: rozwój technologii informacyjno-komunikacyjnej stanowi szansę dla osób ze szczególnymi potrzebami na zwiększenie ich dostępu do usług diagnostycznych, medycznych i rehabilitacyjnych na obszarach wiejskich. W ramach wystą-

vices in rural areas in Poland? What are the benefits of using digital tools in this area? What are the most important threats resulting from the use of such tools in the area of improving accessibility for people with special needs? What good practices can be identified to improve access to these services?

pienia udzielone zostaną odpowiedzi na następujące pytania badawcze: jakie są główne bariery w dostępie do usług diagnostycznych, rehabilitacyjnych i medycznych na obszarach wiejskich w Polsce? Jakie korzyści mogą wyniknąć z zastosowania narzędzi cyfrowych w tym obszarze? Jakie są najważniejsze zagrożenia wynikające z zastosowania takich narzędzi w obszarze poprawy dostępności osób ze szczególnymi potrzebami? Jakie dobre praktyki z zakresu poprawy dostępności do tych usług można wskazać?

Szymon Ostrowski

Digitization in local government: comparing Scotland and Wales' digitization strategies

Cyfryzacja w samorządach lokalnych: porównanie strategii cyfryzacji Szkocji i Walii

The paper analyzes the digitalization strategies of local governments in Scotland and Wales and compares them in order to identify similarities and differences. Problems related to the development of digitalization and communication exclusion turned out to be urgent during the coronavirus pandemic and equally important for states and local governments. The study highlights the strengths and weaknesses of the Welsh and Scottish ap-

Celem wystąpienia jest analiza strategii cyfryzacji samorządów lokalnych Szkocji i Walii oraz ich porównanie w celu wskazania podobieństw i różnic. Problemy związane z rozwojem cyfryzacji i wykluczeniem komunikacyjnym okazały się palące w czasie pandemii koronawirusa i jednakowo istotne dla państw jak i samorządów lokalnych. Badanie wskaże mocne i słabe strony walijskiego i szkockiego podejścia do tej kwestii. Problem badawczy

proaches to this issue. The research problem is “How local governments can tackle the need to develop telecommunications infrastructure and the problem of communication exclusion?” The hypothesis was that the local governments in Wales and Scotland approached the problem in very complex ways. The research method was the analysis of primary sources and comparative analysis.

stanowi pytanie w jaki sposób samorządy lokalne mogą mierzyć się z potrzebą rozwoju infrastruktury telekomunikacyjnej i problemem wykluczenia komunikacyjnego? Hipotezę stano stwierdzenie, że samorządy Walii i Szkocji podchodzą do problemu w sposób bardzo złożony. Metoda badawcza badania to analiza źródeł pierwotnych i analiza porównawcza.

Panel sessions 7

Social media as a tool of political influence

Sesja panelowa 7

Media społecznościowe jako narzędzie wpływu politycznego

Nartsiss Shukuralieva

Telegram as the site of the revolt of Yevgeny Prigozhin and the Wagner Group

Telegram jako miejsce buntu Jewgienija Prigożyna i Grupy Wagnera

The paper focuses on a new element of the tactics of the rebellion of the Russian oligarch Yevgeny Prigozhin and the Wagner Group on June 23-24, 2023, which is the use of social media. As censorship and narrative control in mainstream media increases, Telegram is becoming one of the few uncensored online spaces in Russia that can be freely accessed from within Russia without the use of techniques of censorship circumvention. Telegram has become not only the main source of information for Russians about Prigozhin's rebellion, but also an independent space *for* this rebellion. It allowed soldiers to publicly criticize corrupt practices, the actions of their

Wystąpienie skupia się na nowym elemencie taktyki buntu rosyjskiego oligarchy Jewgienija Prigożyna i Grupy Wagnera z 23-24 czerwca 2023 r., którym jest wykorzystanie mediów społecznościowych. Wraz ze wzrostem cenzury i kontrolą narracji w mediach głównego nurtu, Telegram staje się w Rosji jedną z niewielu nieocenzurowanych przestrzeni internetowych, do których można uzyskać swobodny dostęp z Rosji bez konieczności stosowania różnych technik obchodzenia cenzury. Telegram stał się nie tylko głównym źródłem informacji dla Rosjan o buncie Prigożyna, ale także samoistną przestrzenią tego buntu. Umożliwiał żołnierzom upublicznianie

commanders, and improper procedures. It also removed any geographical constraints for the rebels. In this context, the mediatization of Prigozhin's rebellion reached an unprecedented scale. Millions of viewers could watch the escalation of the conflict with the Ministry of Defense, the march on Moscow and the withdrawal of the Wagnerites to field camps almost in real time via social media.

krytyki praktyk korupcyjnych, a także działań ich dowódców oraz niewłaściwych procedur wojskowych. Wyzwolił także buntowników z ograniczeń geograficznych. W tym kontekście mediatyzacja buntu J. Prigożyna i grupy Wagnera osiągnęła niespotykaną dotąd skalę. Miliony widzów za pośrednictwem mediów społecznościowych niemal w czasie rzeczywistym mogło obserwować eskalację konfliktu z Ministerstwem Obrony, marsz na Moskwę oraz wycofywanie się wagnerowców do obozów polowych.

Dawid Gralik

Historical narratives in social media as an element of information warfare

Narracje historyczne w mediach społecznościowych jako element wojny informacyjnej

The popularity of social media has created a new element of information wars, which are now present in every modern-day international conflict. While in the previous century, traditional media, such as the press, played a decisive role in shaping society's knowledge, today the Internet is an extremely important element. It is no different in shaping historical awareness and memory. This is clearly visible in the example of the Russo-Ukrainian conflict, where on the one hand, Russians

Popularność mediów społecznościowych stworzyła z nich nowy element wojen informacyjnych, które stały się elementem każdego współczesnego konfliktu międzynarodowego. O ile w poprzednim stuleciu decydującą rolę w kształtowaniu wiedzy społeczeństwa odgrywały tradycyjne media, np. prasa, o tyle współcześnie niezwykle ważnym elementem jest Internet. Nie inaczej wygląda to w przypadku kształtowania świadomości i pamięci historycznej. Widać to znakomicie

are trying to undermine the very existence of the Ukrainian state based on spurious historical arguments, and Ukrainians are shaping their own identity anew. In my paper, I would like to present how social media are used to create historical narratives and how they are utilized in information wars. Selected examples will present the role of state factors in shaping the narrative, as well as the way the message is shaped, along with its consequences. The paper will be based on the results of a study conducted as part of the OPUS NCN grant "Historical narrative in Web 2.0 as an element of the functioning of national identities in Central and Eastern Europe".

na przykładzie konfliktu rosyjsko-ukraińskiego, gdzie z jednej strony Rosjanie starają się na bazie argumentów historycznych podważyć sens istnienia państwa ukraińskiego, zaś Ukraińcy kształtują na nowo własną tożsamość. W swoim referacie chciałbym przedstawić w jaki sposób media społecznościowe są wykorzystywane do tworzenia narracji historycznych oraz używane w wojnach informacyjnych. Na wybranych przykładach zostanie przedstawiona rola czynników państwowych w kształtowaniu narracji, a także sposób kształtowania przekazu i jego konsekwencje. Referat zostanie oparty na wynikach badań prowadzonych w ramach grantu OPUS NCN „Narracja historyczna w Web 2.0 jako element funkcjonowania tożsamości narodowych w Europie Środkowo-Wschodniej".

Agata Olszanecka-Marmola, Maciej Marmola

TikTok as a tool of creating a political image: conclusions from research

TikTok jako narzędzie budowania wizerunku politycznego: wnioski z badań

TikTok has become the fastest growing social medium in recent years. Although there is serious concern about the utilization of

TikTok stał się w ostatnich latach najszybciej rozwijającym się medium społecznościowym. Choć istnieje poważna obawa dotycząca wy-

user data by this Chinese platform, its potential is beginning to be recognized by Polish politicians, who are using this medium to build their political image and win over the youngest voters. The aim of the paper is to diagnose how political messages on TikTok influence the evaluation of selected Polish politicians. To investigate this, we conducted a quasi-experimental study (N=197) with two measurements in one sample. Its results confirm that TikTok can be considered an effective tool in building a political image. The presented messages had a positive impact on the assessment of those politicians who skillfully used the character of TikTok by publishing entertaining content. An in-depth analysis showed that the susceptibility to changing opinions on politicians under the influence of TikTok content is related to gender and political preferences, while the political views of recipients are less important in this matter.

korzystywania danych użytkowników przez tę chińską platformę, to jego potencjał zaczynają zauważać polscy politycy, który stosują to medium do budowania politycznego wizerunku i przekonania do siebie najmłodszych wyborców. Celem wystąpienia jest zdiagnozowanie, w jaki sposób przekazy polityczne na TikToku wpływają na ocenę wybranych polskich polityków. Aby to sprawdzić przeprowadziliśmy badanie quasi-eksperymentalne (N=197) z dwukrotnym pomiarem w jednej próbie. Jego wyniki potwierdzają, że TikTok można uznać za skuteczne narzędzie w procesie budowania wizerunku politycznego. Zaprezentowane przekazy pozytywnie wpłynęły na ocenę tych polityków, którzy umiejętnie wykorzystywali specyfikę TikToka, publikując treści o charakterze rozrywkowym. Pogłębiona analiza wykazała, że podatność na zmianę ocen polityków pod wpływem treści z TikToka wiąże się z płcią i preferencjami politycznymi, a mniejsze znaczenie w tej kwestii mają poglądy polityczne odbiorców.

Piotr Walewicz

When profiles go to war – or profiling through the prism of political conflict

Profile idą na wojnę, czyli profilowość przez pryzmat politycznego konfliktu

The paper attempts to formulate a political science synthesis of two concepts that have appeared in recent years in the social sciences and humanities. The first is *profiling*, a new paradigm of creating human identity. Its authors, Hans-Georg Moeller and Paul J. D'Ambrosio, point out that in late modern times we no longer create identity by sincerely fulfilling a social role assigned from the outside, nor by authentic self-realization, but by building and updating various profiles – not only those on social media. The second concept is the concept of *LikeWar*, authored by P. W. Singer and Emerson T. Brooking, which reveals and explains new spaces of political conflict, new tools and tactics of conducting it. Both concepts, although they come from different epistemological positions, converge in the area of clashing profiles created by people in contexts of great political significance. Their synthesis can explain the importance of the currently dominant identity paradigm for political and ideological "wars" in social media.

Wystąpienie jest próbą politologicznej syntezy dwóch koncepcji, które pojawiły się w ostatnich latach w naukach społecznych i humanistycznych. Pierwszą jest profilowość (ang. profilicity), tzn. nowy paradygmat kreowania tożsamości człowieka. Jej autorzy, Hans-Georg Moeller i Paul J. D'Ambrosio, wskazują, że w późnej współczesności nie tworzymy już tożsamości przez szczere wypełnianie przypisanej z zewnątrz społecznej roli, ani przez autentyczne realizowanie siebie, ale przez budowanie i aktualizowanie przeróżnych profili – nie tylko tych w mediach społecznościowych. Drugą jest tzw. „wojna na lajki" (oryg. LikeWar), czyli koncepcja odsłaniająca i tłumacząca nowe przestrzenie konfliktu politycznego, nowe narzędzia i taktyki jego prowadzenia, której autorami są P. W. Singer i Emerson T. Brooking. Obie koncepcje, choć wychodzą z różnych pozycji epistemologicznych, spotykają się w obszarze ścierania się kreowanych przez ludzi profili w kontekstach o dużym znaczeniu politycznym. Ich synteza może wyjaśnić, jakie znaczenie dla „wojen" politycznych i światopoglądowych w mediach społecznościowych ma do-

minujący współcześnie paradygmat tożsamości.

Patryk Tomaszewski

Politicians, celebrities, journalists – who shapes the political opinions of young voters in Poland using social media

Politycy, celebryci, dziennikarze – kto kształtuje opinie polityczne młodych wyborców w Polsce używając do tego mediów społecznościowych

Radzym Jankiewicz

Perception of the conflict in Ukraine and the situation of refugees from Ukraine in Poland in the era of digital information - analysis of the role of online media

Percepcja konfliktu na Ukrainie i sytuacji uchodźców z Ukrainy w Polsce w erze informacji cyfrowej - analiza roli mediów internetowych

In the digital age, online media have become a key tool in shaping public opinion on international conflicts. This is particularly visible in the case of the current conflict in Ukraine, where cyberspace has transformed into an information battle arena. This work focuses on analyzing how information is presented, manipulated and used in digital media to influence international and domestic perceptions of the armed conflict in Ukraine and the situation of refugees from Ukraine who arrived in Poland after February 24, 2022.

W dobie cyfrowej, media internetowe stały się kluczowym narzędziem w kształtowaniu opinii publicznej na temat konfliktów międzynarodowych. Szczególnie widoczne jest to w przypadku obecnego konfliktu na Ukrainie, gdzie cyberprzestrzeń przekształciła się w arenę bitwy informacyjnej. Niniejsza praca skupia się na analizie, w jaki sposób informacje są prezentowane, manipulowane i wykorzystywane w mediach cyfrowych, by wpływać na międzynarodowe i krajowe postrzeganie konfliktu zbrojnego na Ukrainie oraz sytuacji uchodźców z Ukrainy, którzy przybyli do Polski po 24 lutym 2022 r.

Panel sessions 8

Cyberspace as a subject of interest for young researchers

Sesja panelowa 8

Cyberprzestrzeń jako przedmiot zainteresowania młodych badaczy

Oskar Stefański

Nordic right-wing populisms on the Internet. How do right-wing populists from Sweden and Finland operate on the Internet?

Nordyckie prawicowe populizmy w Internecie. W jaki sposób w przestrzeni internetowej działają prawicowi populiści ze Szwecji i Finlandii?

The activities of right-wing populists in Europe are a topic widely discussed in international scientific discourse. Right-wing populist movements from Northern Europe are not as common in the academic debate on this phenomenon. Nordic populisms are different from those of the rest of Europe, with the position of party leader as well as the social organization being completely separate from other European populist movements. The Swedish Democrats are known for their message reaching mainly young people and men from smaller, post-industrial municipalities, and True Finns operate similarly in Finland.

Działalność prawicowych populistów w Europie to temat szeroko poruszany w międzynarodowym dyskursie naukowym. Tematyka prawicowych ruchów populistycznych z Europy Północnej nie jest aż tak powszechna w naukowej debacie o tym zjawisku. Nordyckie populizmy są wyjątkowe względem reszty Europy, pozycja lidera partyjnego, a także organizacja społeczna są całkowicie odrębne od innych europejskich ruchów populistycznych. Szwedzcy Demokraci znani są ze swojego przekazu trafiającego głównie do młodzieży i mężczyzn pochodzących z mniejszych, postindustrialnych gmin, po-

What seems interesting is the question of how right-wing populists operate in the virtual space and how they create their message and image there. The aim of the presentation will be to answer the question "How do right-wing populists from Sweden and Finland operate in the Internet space?" In preparing the study, a case study method will be used, in which the activities of populist movements from Sweden and Finland will provide an example, as well as a comparative analysis, the aim of which will be to compare the activities of these movements on the Internet.

dobnie w Finlandii działają Prawdziwi Finowie. Interesującym wydaje się zagadnienie, w jakim sposób prawicowi populiści operują w przestrzeni wirtualnej i w jaki sposób kreują tam swój przekaz, jak i swój obraz. Celem wystąpienia, będzie odpowiedź na pytanie "W jaki sposób w przestrzeni internetowej działają prawicowi populiści ze Szwecji i Finlandii?" W przygotowaniu badania wykorzystana zostanie wykorzystana metoda studium przypadku, w której przykładem będzie działalność ruchów populistycznych ze Szwecji i Finlandii, a także analiza porównawcza, której celem będzie porównanie do siebie działalności tychże ruchów w sieci.

Anna Leda

Online radicalization: Current recruitment tactics of terrorist organizations

Radykalizacja online: Obecne taktyki rekrutacyjne organizacji terrorystycznych

The Internet remains a key tool for terrorist organizations, including its use for recruitment and radicalization of unwitting people around the world. Social media facilitate the spread of extremist ideologies on an unprecedented scale. Understanding radicalization and recruitment methods is crucial to countering the global threat of terrorism. Despite numerous reports on terrorist threats, there is little

Internet pozostaje kluczowym narzędziem dla organizacji terrorystycznych, m.in. do rekrutowania i radykalizowania nieświadomych ludzi na całym świecie. Media społecznościowe pozwalają promować ideologie ekstremistyczne na niespotykaną dotąd skalę. Zrozumienie metod radykalizacji i rekrutacji ma kluczowe znaczenie dla przeciwdziałania globalnemu zagrożeniu terroryzmem. Po-

current data on online recruitment and radicalization of victims. According to a report by the Executive Directorate of the UN Security Council's Counter-Terrorism Committee, terrorist groups have attempted to exploit some of the main challenges of COVID-19 restrictions, including social isolation and increased internet exposure, to spread disinformation, in order to strengthen their recruitment efforts and expand their influence. The main aim of the paper is to examine the current motivations and techniques of the recruitment process and propose countermeasures aimed at reducing their impact and increasing people's awareness.

mimo licznych raportów na temat zagrożeń terrorystycznych, niewiele jest aktualnych danych na temat rekrutacji online i radykalizacji ofiar. Według raportu Dyrekcji Wykonawczej Komitetu Antyterrorystycznego Rady Bezpieczeństwa ONZ, grupy terrorystyczne próbowały wykorzystać niektóre z głównych wyzwań związanych z ograniczeniami związanymi z pandemią COVID-19, w tym izolację społeczną i zwiększoną ekspozycję na Internet do rozprzestrzeniania dezinformacji, w celu wzmocnienia wysiłków rekrutacyjnych i rozszerzenia wpływów. Głównym celem referatu jest zbadanie obecnych motywacji i technik procesu rekrutacji oraz zaproponowanie środków zaradczych, których celem jest zmniejszenie ich wpływu i zwiększenia świadomości ludzi.

Julia Niesyn

Belgium, Brazil, Estonia – three different visions of electronic elections

Belgia, Brazylia, Estonia - 3 wizje wyborów elektronicznych

The aim of the presentation is to compare the evolution of electronic voting in selected countries (Belgium, Brazil and Estonia) and the advantages and disadvantages of the adopted solutions. These countries

Celem wystąpienie jest porównanie ewolucji głosowania elektronicznego w wybranych państwach świata (Belgia, Brazylia i Estonia) oraz wad i zalet przyjętych rozwiązań. Kraje te przeszły długą drogę, aby móc zaoferować obywa-

have come a long way to be able to offer citizens a safe and convenient way to vote. Also worth noting is the way electronic voting works in each of these countries, as well as the prospects and plans that they are striving for. Estonia, considered a pioneer of e-voting, wants to ensure that citizens can vote safely using smartphones. Moreover, it attaches great importance to the security and secrecy of voting. Brazilians vote fully online, but this does not mean they can vote from home. In Brazil, voting is done using an electronic ballot box, which means that citizens must go to a polling station. However, this has the undoubted advantage of knowing the election results immediately. Belgium has compulsory voting and the introduction of electronic voting was not intended to improve turnout. The government leaves the decision on how to conduct elections to the municipalities, which results in the fact that not every municipality votes in the same way.

telom bezpieczne oraz wygodne oddanie głosu. Na uwagę zasługuje sposób głosowania elektronicznego jaki działa, w każdym z podanych państw oraz perspektywy i plany, do których te kraje dążą. Estonia uważana za pioniera e-votingu chce doprowadzić do bezpiecznego głosowania obywateli za pomocą smartphonów. Ponadto przykłada bardzo dużą wagę do bezpieczeństwa i tajności głosowania. Brazylijczycy głosują w pełni online, jednak nie oznacza to, że mogą zagłosować z domu. W Brazylii głosuje się za pomocą urny elektronicznej, co oznacza, że obywatele muszą udać się do lokalu wyborczego. Ma to jednak niewątpliwą zaletę w postaci natychmiastowego poznania wyniku wyborów. W Belgii obowiązuje przymus wyborczy, wprowadzenie głosowania elektronicznego nie miało na celu poprawienia frekwencji. Rząd zostawia gminom decyzję o sposobie przeprowadzenie wyborów, co skutkuje faktem, że nie w każdej gminie głos oddaje się tak samo.

Geoffrey Lefebvre

The Social Media Shift: Impact on Contemporary Terrorism in France. Analyzing the Role of Online Platforms in Extremist Mobilization and Radicalization

Zmiana mediów społecznościowych: wpływ na współczesny terroryzm we Francji. Analiza roli platform internetowych w mobilizacji i radykalizacji ekstremistów

France has experienced numerous terrorist attacks throughout its history, whether it be the assassination of Henri IV, the OAS and the FLN during the Algerian War, or the various communist attacks, as seen across Europe during the "Years of Lead." However, Terrorism in France has undergone a transformative evolution, especially in the recent decades marked by unprecedented attacks. The emergence of social networks, encrypted messaging platforms, and the internet has profoundly altered the landscape of terrorist activities, facilitating recruitment and radicalization processes. This presentation aims to analyze this shift, particularly focusing on the period between 2015 and 2018, during which France experienced a surge in Islamic terrorist attacks. The emergence of social networks and encrypted messaging applications has transformed the terrorism landscape, facilitating recruitment and radicalization. Despite the efforts of French authorities and their international

Francja doświadczyła w swojej historii licznych ataków terrorystycznych, czy to zabójstwa Henryka IV, OPA i FLN podczas wojny algierskiej, czy też różnych ataków komunistycznych, które można było zaobserwować w całej Europie podczas „lat ołowiu”. Terroryzm we Francji przeszedł jednak transformację, szczególnie w ostatnich dziesięcioleciach naznaczonych bezprecedensowymi atakami. Pojawienie się sieci społecznościowych, platform szyfrowania wiadomości i Internetu głęboko zmieniło krajobraz działań terrorystycznych, ułatwiając procesy rekrutacji i radykalizacji. Niniejsza prezentacja ma na celu analizę tej zmiany, ze szczególnym uwzględnieniem okresu 2015–2018, w którym Francja doświadczyła gwałtownego wzrostu liczby islamskich ataków terrorystycznych. Pomimo wysiłków władz francuskich i międzynarodowych partnerów, mających na celu przeciwdziałanie temu zagrożeniu, terroryzm pozostaje stałym zagrożeniem,

partners to counter this threat, terrorism remains a persistent menace, as evidenced by recent attacks and thwarted attempts.

o czym świadczą niedawne ataki i udaremnione próby.