I OGÓLNOPOLSKA STUDENCKO-DOKTORANCKA KONFERENCJA NAUKOWA

BEZPIECZEŃSTWO 2.0

25 MAJA 2026 R.

I Ogólnopolska Studencko-Doktorancka Konferencja Naukowa „Bezpieczeństwo 2.0” poświęcona jest współczesnym przemianom środowiska bezpieczeństwa w warunkach cyfryzacji, rozwoju sztucznej inteligencji, ekspansji mediów społecznościowych oraz narastającej złożoności zagrożeń społecznych, informacyjnych i infrastrukturalnych. Dzisiejsze bezpieczeństwo coraz rzadziej daje się opisywać wyłącznie za pomocą tradycyjnych kategorii militarnych, politycznych czy instytucjonalnych. Coraz częściej obejmuje ono również cyberprzestrzeń, przepływy informacji, odporność społeczeństwa na manipulację, ochronę danych, bezpieczeństwo użytkowników technologii cyfrowych oraz zdolność państwa do reagowania na zagrożenia hybrydowe.

Program konferencji pokazuje, jak szeroki i wielowymiarowy jest dziś obszar badań nad bezpieczeństwem. W sześciu panelach tematycznych poruszone zostaną zagadnienia cyberbezpieczeństwa i sztucznej inteligencji, dezinformacji, mediów społecznościowych, wojny informacyjnej, bezpieczeństwa użytkowników w społeczeństwie cyfrowym, infrastruktury krytycznej, bezpieczeństwa państwa, bezpieczeństwa społecznego, migracji, polityki międzynarodowej oraz wpływu nowych technologii na funkcjonowanie jednostki, społeczeństwa i instytucji publicznych.

Szczególne miejsce w tej problematyce zajmuje bezpieczeństwo informacyjne. Dezinformacja, deepfake’i, phishing, manipulacyjne interfejsy cyfrowe, algorytmy mediów społecznościowych oraz ekonomia uwagi pokazują, że współczesne zagrożenia coraz częściej oddziałują nie tylko na systemy techniczne, ale również na zaufanie, emocje, percepcję i decyzje obywateli. W tym kontekście należy zwrócić uwagę na nowy wymiar walki informacyjnej, jakim jest walka kognitywna. Jej istotą nie jest już wyłącznie rozpowszechnianie fałszywych informacji, lecz wpływanie na sposób, w jaki ludzie postrzegają rzeczywistość, interpretują fakty, definiują zagrożenia, oceniają instytucje i podejmują decyzje. Walka kognitywna przenosi zatem konflikt do sfery świadomości, uwagi, emocji i procesów poznawczych, czyniąc człowieka nie tylko odbiorcą informacji, ale również bezpośrednim polem oddziaływania.

Konferencja gromadzi 36 prelegentów reprezentujących 11 uczelni i ośrodków akademickich z 4 państw: Polski, Ukrainy, Słowacji i Litwy. Reprezentowane są: Uniwersytet Rzeszowski, Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Uniwersytet Jana Kochanowskiego w Kielcach, Uniwersytet w Siedlcach, Uniwersytet Jagielloński, Akademia WSB w Dąbrowie Górniczej, Uniwersytet Warmińsko-Mazurski w Olsztynie, Uniwersytet Jana Długosza w Częstochowie, Wołyński Uniwersytet Narodowy im. Łesi Ukrainki, Constantine the Philosopher University in Nitra oraz Panevėžio kolegija / State Higher Education Institution.

Tak szerokie grono uczestników pozwala spojrzeć na problematykę bezpieczeństwa z różnych perspektyw badawczych i doświadczeń akademickich. Dzisiejsza konferencja jest zatem nie tylko miejscem prezentacji wyników badań, ale także przestrzenią wymiany refleksji nad tym, jak zmienia się samo rozumienie bezpieczeństwa. W epoce sztucznej inteligencji, wojny informacyjnej, cyfrowej podatności użytkowników, presji demograficznej i technologicznej rywalizacji bezpieczeństwo staje się kategorią łączącą wymiar techniczny, społeczny, psychologiczny, polityczny i strategiczny.

Mamy nadzieję, że konferencja „Bezpieczeństwo 2.0” stanie się okazją do pogłębionej dyskusji nad tym, jak wzmacniać odporność państwa, społeczeństwa i jednostki wobec zagrożeń, które już dziś kształtują nasze środowisko bezpieczeństwa, a w kolejnych latach będą nabierały jeszcze większego znaczenia.

Oliwia Radkiewicz
Juliusz Sikorski

PANEL I A
SZTUCZNA INTELIGENCJA W CYBERPRZESTRZENI: MIĘDZY INNOWACJĄ A ZAGROŻENIEM

MODERACJA: MAGDALENA BIERNACKA

Ewelina Zielińska
„Cyberbezpieczeństwo w dobie sztucznej inteligencji – nowe wyzwania i zagrożenia“

Rozwój sztucznej inteligencji istotnie wpływa na współczesne cyberbezpieczeństwo, generując zarówno nowe możliwości, jak i zagrożenia. Celem referatu jest analiza roli AI w kształtowaniu bezpieczeństwa w cyberprzestrzeni oraz identyfikacja najważniejszych wyzwań z tym związanych. Szczególną uwagę poświęcono wykorzystaniu sztucznej inteligencji w automatyzacji cyberataków, takich jak phishing, deepfake czy działania dezinformacyjne, a także jej zastosowaniu w systemach ochrony i wykrywania zagrożeń.
W referacie podkreślono dualny charakter sztucznej inteligencji oraz konieczność dostosowania strategii bezpieczeństwa do dynamicznych zmian technologicznych. Wskazano również na znaczenie regulacji prawnych oraz rozwijania kompetencji cyfrowych. Wnioski pokazują, że AI redefiniuje podejście do cyberbezpieczeństwa, wymagając wdrażania nowych metod ochrony oraz zwiększonej współpracy międzysektorowej.

Klaudia Zygmunt
„Deepfake - realne zagrożenie w cyfrowym świecie”

Współczesne bezpieczeństwo informacyjne mierzy się z poważnym wyzwaniem związanym z weryfikacją wiarygodności i autentyczności przekazów. Rozwój sztucznej inteligencji sprawił, że narzędzia służące do manipulacji obrazem, dźwiękiem i tekstem stały się powszechnie dostępne, a tworzone za ich pomocą treści są często trudne do odróżnienia od rzeczywistości. Zjawisko deepfake polega na generowaniu hiperrealistycznych materiałów audiowizualnych, które mogą stać się potężnym narzędziem w rękach aktorów państwowych, grup przestępczych oraz innych podmiotów prowadzących działania manipulacyjne. W kontekście bezpieczeństwa międzynarodowego i społecznego deepfake przestaje być jedynie ciekawostką technologiczną, stając się realnym zagrożeniem dla stabilności państw i zaufania społecznego.

A**nastasiia Dombrovska**
„Bezpieczeństwo cyfrowe społeczeństwa w dobie sztucznej inteligencji”

Dynamiczny rozwój sztucznej inteligencji w ostatnich latach znacząco przekształca funkcjonowanie współczesnych społeczeństw, wpływając zarówno na poziom innowacyjności, jak i na charakter pojawiających się zagrożeń cyfrowych. Celem niniejszego wystąpienia jest analiza wpływu technologii opartych na AI na bezpieczeństwo cyfrowe społeczeństwa, ze szczególnym uwzględnieniem nowych form cyberzagrożeń oraz wyzwań związanych z ochroną danych, prywatnością i integralnością informacji.
W referacie omówione zostaną m.in. takie zjawiska, jak automatyzacja cyberataków, wykorzystanie sztucznej inteligencji do tworzenia zaawansowanych form dezinformacji, w tym deepfake’ów, a także rosnąca rola algorytmów w procesach decyzyjnych mających znaczenie dla bezpieczeństwa publicznego. Jednocześnie wskazane zostaną potencjalne korzyści wynikające z zastosowania AI w obszarze cyberbezpieczeństwa, w tym rozwój systemów wczesnego wykrywania zagrożeń oraz narzędzi wspierających analizę incydentów.
Ważnym elementem analizy będzie również rola edukacji cyfrowej oraz świadomości społecznej w budowaniu odporności na zagrożenia technologiczne. W konkluzji podkreślona zostanie konieczność wypracowania zrównoważonych strategii regulacyjnych i technologicznych, które pozwolą na efektywne wykorzystanie potencjału sztucznej inteligencji przy jednoczesnym minimalizowaniu ryzyka dla bezpieczeństwa społeczeństwa.

Julia Szypuła
„AI – zagrożenia dla bezpieczeństwa społecznego”

Wpływ sztucznej inteligencji na nasze codzienne życie systematycznie rośnie. Dotyczy to zarówno sposobów pozyskiwania informacji, jak i tego, jak komunikujemy się, pracujemy oraz podejmujemy decyzje. Postęp w dziedzinie sztucznej inteligencji przynosi wiele korzyści, jednak jednocześnie rodzi coraz więcej obaw związanych z bezpieczeństwem społecznym.

Prelekcja będzie próbą wykazania, że sztuczna inteligencja stanowi wyzwanie nie tylko z perspektywy przyszłości, lecz także teraźniejszości. Poruszone zostaną takie kwestie, jak dezinformacja, treści typu deepfake, manipulacja opinią publiczną oraz rosnący wpływ algorytmów na decyzje jednostek i relacje społeczne. Omówione zostaną również zagadnienia związane z utratą prywatności oraz narastającą zależnością od technologii.
Celem wystąpienia jest nie tylko zwrócenie uwagi na zagrożenia wynikające z rozwoju sztucznej inteligencji, lecz także podkreślenie potrzeby jej odpowiedzialnego projektowania i wykorzystywania. Istotne znaczenie mają w tym kontekście edukacja cyfrowa oraz rozwijanie świadomości społecznej w zakresie bezpiecznego korzystania z nowych technologii.

Khrystyna Duchak
„Wpływ sztucznej inteligencji na dezinformację w mediach społecznościowych”

W swoim wystąpieniu zamierzam przedstawić, w jaki sposób rozwój sztucznej inteligencji wpływa na tworzenie i rozpowszechnianie dezinformacji w mediach społecznościowych. Szczególna uwaga zostanie poświęcona temu, dlaczego dzięki narzędziom takim jak generatory treści czy technologia deepfake fałszywe informacje są obecnie łatwiejsze do tworzenia, a zarazem trudniejsze do rozpoznania.
Analizie poddane zostaną mechanizmy działania dezinformacji oraz rola algorytmów platform społecznościowych w zwiększaniu zasięgu tego typu treści. W wystąpieniu wskazane zostanie, że rozwój sztucznej inteligencji znacząco zwiększa skalę problemu dezinformacji, czyniąc jego ograniczanie coraz większym wyzwaniem dla społeczeństw, instytucji publicznych oraz podmiotów odpowiedzialnych za bezpieczeństwo informacyjne.

Filip Rawski
„Dezinformacja 2.0: Wpływ sztucznej inteligencji na poczucie bezpieczeństwa informacyjnego pokolenia Z”

Celem niniejszego wystąpienia jest analiza ewolucji zagrożeń informacyjnych w dobie dynamicznego rozwoju generatywnej sztucznej inteligencji oraz ich wpływu na bezpieczeństwo poznawcze przedstawicieli pokolenia Z. W realiach „Bezpieczeństwa 2.0” tradycyjne paradygmaty ochrony informacji stają się niewystarczające wobec masowego wykorzystania takich narzędzi, jak deepfake’i, zaawansowane farmy botów czy algorytmiczne mikrotargetowanie kognitywne.
W wystąpieniu podjęta zostanie próba odpowiedzi na pytanie, w jaki sposób powszechność treści generowanych przez AI wpływa na zaufanie młodych dorosłych do mediów cyfrowych oraz jakie konsekwencje niesie to dla stabilności bezpieczeństwa wewnętrznego państwa. Analiza została oparta na metodzie syntezy oraz krytycznego przeglądu raportów wiodących instytucji badawczych, w tym m.in. NASK, raportu „Dezinformacja oczami Polaków”, NATO StratCom COE oraz Reuters Institute.
Wnioski z analizy wskazują, że tzw. dywidenda kłamcy, czyli możliwość podważania autentyczności prawdziwych materiałów poprzez odwołanie się do rzekomej manipulacji technologicznej, oraz narastająca polaryzacja społeczna stanowią kluczowe wyzwania dla administracji publicznej.

PANEL I B
WOJNA INFORMACYJNA W EPOCE MEDIÓW SPOŁECZNOŚCIOWYCH I AI

MODERACJA: JULIUSZ SIKORSKI

Karol Walczak
„Dezinformacja w erze AI - nowe zagrożenia dla społeczeństwa”

Sztuczna inteligencja potrafi dziś w ciągu kilku sekund stworzyć fałszywe wideo, artykuł czy wypowiedź polityka, nadając im pozory autentyczności. Jak to możliwe i dlaczego jest to tak niebezpieczne? Celem wystąpienia będzie ukazanie, w jaki sposób deepfake’i oraz chatboty zmieniły oblicze dezinformacji – od manipulacji wyborczych po działania prowadzone w ramach wojen informacyjnych. Omówione zostaną również konkretne sposoby, dzięki którym każdy użytkownik może skuteczniej rozpoznawać tego typu zagrożenia i się przed nimi chronić.

Gabriela Ruszel
„Dezinformacja jako czynnik obniżający poczucie bezpieczeństwa społecznego w Polsce – analiza zjawiska i mechanizmów”

Dezinformacja jest zjawiskiem coraz częściej obecnym we współczesnej przestrzeni informacyjnej, szczególnie w mediach społecznościowych, gdzie treści mogą rozprzestrzeniać się bardzo szybko, często bez uprzedniej weryfikacji ich wiarygodności. Celem niniejszego wystąpienia jest analiza wpływu fałszywych lub wprowadzających w błąd informacji na poczucie bezpieczeństwa społecznego w Polsce.
W wystąpieniu omówione zostanie pojęcie dezinformacji oraz różnica między rzeczywistym charakterem zagrożeń a ich społecznym postrzeganiem. Zwrócona zostanie uwaga na fakt, że ludzie często oceniają poziom bezpieczeństwa nie na podstawie obiektywnych danych, lecz informacji, które do nich docierają – zwłaszcza tych nacechowanych emocjonalnie.
Analiza koncentrować się będzie na mechanizmach oddziaływania dezinformacji, takich jak wywoływanie strachu, wielokrotne powielanie tych samych treści w internecie oraz funkcjonowanie mediów społecznościowych, które wzmacniają najbardziej angażujące przekazy. Przedstawione zostaną również wybrane przykłady z Polski, związane m.in. z wojną w Ukrainie, migracją oraz sytuacjami kryzysowymi.
W wystąpieniu wskazane zostanie, że dezinformacja może prowadzić do wzrostu niepokoju społecznego, spadku zaufania do instytucji publicznych oraz nasilenia poczucia zagrożenia, nawet jeśli nie znajduje ono pełnego uzasadnienia w rzeczywistej sytuacji. W podsumowaniu podkreślone zostanie znaczenie krytycznego podejścia do informacji oraz edukacji medialnej jako sposobów ograniczania wpływu fałszywych treści na społeczeństwo.

Mariia Pavliukh
„Anatomia polskiej dezinformacji: kluczowe antyukraińskie fałszerstwa i narracje (2024-2026)”

W polskiej przestrzeni informacyjnej coraz częściej pojawiają się fałszywe przekazy oraz działania dezinformacyjne dotyczące wojny rosyjsko-ukraińskiej i obywateli Ukrainy. Rosyjska dezinformacja zmierza do rozpowszechniania nieprawdziwych informacji na temat Ukraińców, a jej celem jest m.in. wzbudzanie nieufności oraz pogłębianie napięć między Polakami a Ukraińcami.
Istotnym wyzwaniem staje się zatem rozwijanie umiejętności rozpoznawania fałszywych informacji, przeciwdziałania manipulacjom oraz wzmacniania odporności społecznej na działania dezinformacyjne.

Martyna Bąchorek
„CONATEL jako instrument dezinformacji medialnej w Wenezueli”

Praca poświęcona jest analizie CONATEL – Comisión Nacional de Telecomunicaciones – jako narzędzia systematycznej kontroli przestrzeni medialnej oraz przepływu informacji w Wenezueli. Omówione zostanie funkcjonowanie instytucji regulacyjnych w kontekście reżimów hybrydowych, a także ich wpływ na pluralizm medialny i swobodę przepływu informacji. Szczególną uwagę poświęcono mechanizmom przechwycenia instytucjonalnego, za pomocą których formalnie neutralny organ regulacyjny został zinstrumentalizowany przez rządy Hugo Cháveza i Nicolása Maduro w celu eliminowania niezależnych mediów oraz utrwalania hegemonii narracyjnej władzy.
Celem pracy jest analiza mechanizmów funkcjonowania CONATEL jako narzędzia autorytarnej kontroli informacji oraz określenie skali jego wpływu na ekosystem medialny Wenezueli. Problem badawczy został sformułowany w postaci pytania: w jaki sposób CONATEL funkcjonuje jako instrument dezinformacji i kontroli narracji? Hipoteza badawcza zakłada, że CONATEL stanowi świadome narzędzie wojny informacyjnej, działające w ramach szerszego systemu represji medialnych charakterystycznego dla reżimów hybrydowych Ameryki Łacińskiej.
W artykule wykorzystano analizę literatury naukowej i materiałów źródłowych, kwerendę raportów organizacji pozarządowych, metodę desk research oraz studium przypadku Wenezueli. Wnioski płynące z analizy mają znaczenie wykraczające poza kontekst wenezuelski, ponieważ wskazują na uniwersalne mechanizmy przekształcania niezależnych instytucji regulacyjnych w narzędzia autorytarnej kontroli informacji.

A**leksandra Kielar**
„Media społecznościowe jako narzędzie rozpowszechniania dezinformacji – analiza zagrożeń dla bezpieczeństwa państwa”

Dynamiczny rozwój mediów społecznościowych w XXI wieku doprowadził do istotnej transformacji przestrzeni informacyjnej, czyniąc ją jednym z kluczowych obszarów oddziaływania politycznego i społecznego. Platformy takie jak Facebook, X czy TikTok umożliwiają szybkie i masowe rozpowszechnianie treści, co sprzyja nie tylko swobodnemu przepływowi informacji, lecz także intensyfikacji zjawiska dezinformacji.

Celem niniejszego referatu jest analiza roli mediów społecznościowych jako narzędzia rozpowszechniania dezinformacji oraz identyfikacja wynikających z tego zagrożeń dla bezpieczeństwa państwa. W pracy omówione zostaną mechanizmy funkcjonowania platform cyfrowych, w szczególności algorytmy rekomendacyjne, które sprzyjają amplifikacji treści o charakterze emocjonalnym i kontrowersyjnym. Szczególna uwaga zostanie poświęcona wpływowi dezinformacji na opinię publiczną, procesy wyborcze oraz poziom zaufania społecznego do instytucji państwowych.
Analiza obejmie również wybrane przykłady operacji informacyjnych oraz kampanii dezinformacyjnych, w tym działalność Cambridge Analytica, które unaoczniają skalę i potencjalne konsekwencje manipulacji informacyjnej.
Wnioski wskazują, że dezinformacja w mediach społecznościowych stanowi istotne zagrożenie dla stabilności państw, wpływając na procesy demokratyczne oraz bezpieczeństwo informacyjne. Zjawisko to wymaga wypracowania skutecznych mechanizmów przeciwdziałania zarówno na poziomie krajowym, jak i międzynarodowym.

Magdalena Lewicka
„Rola mediów społecznościowych w kształtowaniu odporności państwa na ataki informacyjne”

Współczesne środowisko bezpieczeństwa charakteryzuje się rosnącym znaczeniem przestrzeni informacyjnej, w której media społecznościowe odgrywają kluczową rolę w kształtowaniu opinii publicznej, przepływie informacji oraz budowaniu świadomości społecznej. Jednocześnie platformy te stały się narzędziem wykorzystywanym do prowadzenia działań dezinformacyjnych, manipulacji przekazem oraz wpływania na procesy polityczne i społeczne. Celem niniejszej pracy jest analiza roli mediów społecznościowych w budowaniu odporności państwa na ataki informacyjne oraz identyfikacja mechanizmów wzmacniających bezpieczeństwo informacyjne społeczeństwa. W badaniu omówiono zarówno zagrożenia wynikające z rozpowszechniania fałszywych treści, działalności botów informacyjnych czy kampanii wpływu, jak i możliwości wykorzystania mediów społecznościowych do szybkiej komunikacji kryzysowej, edukacji medialnej oraz przeciwdziałania dezinformacji. Analiza wskazuje, że skuteczna odporność państwa na ataki informacyjne wymaga współpracy instytucji publicznych, sektora prywatnego, platform cyfrowych oraz świadomego społeczeństwa. Kluczowe znaczenie mają rozwój kompetencji medialnych obywateli, transparentna komunikacja władz oraz wdrażanie strategii cyberbezpieczeństwa i ochrony przestrzeni informacyjnej.

PANEL II A
BEZPIECZEŃSTWO UŻYTKOWNIKÓW W SPOŁECZEŃSTWIE CYFROWYM

MODERACJA: NIKODEM KLATA

Jakub Paciorek
„Phishing jako najpowszechniejsze zagrożenie cyberbezpieczeństwa”

Phishing od lat pozostaje jedną z najskuteczniejszych i najczęściej stosowanych metod ataku w cyberprzestrzeni. Pomimo rosnącej świadomości społecznej liczba skutecznych ataków systematycznie wzrasta, a phishing stanowi ponad połowę wszystkich zgłaszanych incydentów bezpieczeństwa.
Celem referatu jest analiza ewolucji technik phishingowych oraz ocena poziomu świadomości polskich użytkowników internetu w zakresie tego zagrożenia. W pierwszej części wystąpienia omówione zostaną różne rodzaje ataków phishingowych: od klasycznego phishingu e-mailowego, przez spear phishing, po vishing, czyli ataki prowadzone z wykorzystaniem połączeń głosowych. Uwzględnione zostaną także nowe formy phishingu, w tym działania wykorzystujące generatywną sztuczną inteligencję do tworzenia wiarygodnych i trudniejszych do rozpoznania wiadomości.
W drugiej części referatu przedstawione zostaną wyniki analizy dostępnych raportów z ostatnich lat, pozwalające ocenić skalę zjawiska oraz poziom przygotowania użytkowników do rozpoznawania i unikania tego typu zagrożeń.

Ewa Kogut
„Phishing i dezinformacja jako współczesne wyzwania cyberbezpieczeństwa w Polsce”

Phishing i dezinformacja należą do kluczowych współczesnych wyzwań cyberbezpieczeństwa w Polsce. Phishing, opierający się na mechanizmach socjotechniki, wykorzystuje fałszywe komunikaty oraz podrobione strony internetowe w celu wyłudzenia danych lub środków finansowych. Dezinformacja natomiast polega na manipulowaniu opinią publiczną poprzez rozpowszechnianie fałszywych lub wprowadzających w błąd treści.

Współwystępowanie tych zjawisk wzmacnia lęk i niepewność, zwiększając skuteczność ataków oraz utrudniając odbiorcom odróżnianie informacji wiarygodnych od fałszywych. Praca analizuje wpływ phishingu i dezinformacji na bezpieczeństwo obywateli oraz jakość przestrzeni publicznej, a także omawia podejmowane działania zapobiegawcze, takie jak edukacja cyfrowa, systemy ostrzegawcze i kampanie informacyjne.
Wskazano, że skuteczna ochrona wymaga łączenia rozwiązań technicznych z rozwijaniem krytycznego myślenia oraz odpowiedzialnych postaw obywateli w środowisku cyfrowym.

Wiktoria Izdebska
„Starzenie się ludności w Polsce wobec nowoczesnych zagrożeń: ochrona seniora przed oszustwami phishingowymi oraz deepfake'ami”

Starzenie się ludności w Polsce stawia nowe wyzwania w zakresie bezpieczeństwa cyfrowego. Osoby starsze, coraz częściej korzystające z bankowości elektronicznej, e-administracji, komunikatorów oraz mediów społecznościowych, stają się szczególnie narażone na nowoczesne formy cyberoszustw. Do najpowszechniejszych zagrożeń należą przede wszystkim ataki phishingowe, polegające na wyłudzaniu danych logowania, kodów dostępu czy numerów kart płatniczych poprzez podszywanie się pod instytucje finansowe, administrację publiczną lub operatorów usług. Równolegle rośnie ryzyko związane z wykorzystaniem technologii deepfake, która może służyć do manipulacji emocjonalnej, m.in. w oszustwach typu „na wnuczka” czy „na policjanta”.
W pracy przedstawiona zostanie analiza osobistych, technicznych i społecznych uwarunkowań podatności seniorów na tego typu ataki. Wskazane zostaną kluczowe czynniki ryzyka, takie jak niższa świadomość cyberbezpieczeństwa, brak lub fragmentaryczny charakter edukacji cyfrowej, większa ufność wobec instytucji oraz lęk przed utratą kontaktu z rodziną, który może prowadzić do nagłych i emocjonalnych reakcji na fałszywe komunikaty. Dokonany zostanie także przegląd istniejących rozwiązań edukacyjnych, technologicznych i instytucjonalnych, których celem jest zwiększenie odporności seniorów na zagrożenia cyfrowe.

Gabriela Kazimierska
„Dark Patterns – jak interfejsy aplikacji manipulują użytkownikiem i zagrażają jego prywatności”

Współczesne projektowanie produktów cyfrowych coraz częściej wykracza poza ramy estetyki i użyteczności, wkraczając w obszar psychologicznego oddziaływania na zachowania użytkowników. Niniejsze wystąpienie poświęcone jest problematyce ciemnych wzorców projektowych, znanych jako dark patterns, które stanowią zestaw celowych zabiegów stosowanych w architekturze interfejsu w celu nakłonienia użytkownika do działań niezgodnych z jego pierwotną wolą lub interesem.
Podczas prelekcji przeanalizowane zostanie, w jaki sposób twórcy aplikacji wykorzystują naturalną skłonność człowieka do upraszczania decyzji, aby skłaniać użytkowników do dodatkowych płatności, utrudniać im usunięcie konta czy nakłaniać do zaakceptowania inwazyjnych ustawień prywatności. Problem ten zostanie przedstawiony nie tylko jako wyzwanie projektowe, lecz przede wszystkim jako istotne zagrożenie dla ochrony danych osobowych, ponieważ skomplikowane menu i podstępne komunikaty mogą służyć budowaniu bazy informacji o użytkowniku bez jego pełnej świadomości.
Odwołując się do przykładów z życia codziennego, takich jak popularne serwisy streamingowe i portale aukcyjne, wskazane zostaną mechanizmy, które zamieniają wolny wybór w iluzję sterowaną przez algorytmy. Całość rozważań prowadzić będzie do refleksji nad etyką w świecie IT oraz potrzebą wypracowania krytycznego spojrzenia na interakcje, jakie każdego dnia podejmujemy z ekranami naszych smartfonów.

Magdalena Kozłowska
„Wpływ gier komputerowych online na bezpieczeństwo użytkowników”

Rozwój gier komputerowych online stanowi jedno z najbardziej dynamicznych zjawisk współczesnej kultury cyfrowej, szczególnie wśród dzieci i młodzieży. Platformy gamingowe, oferujące interakcję w czasie rzeczywistym oraz możliwość nawiązywania kontaktów z innymi użytkownikami, tworzą nowe przestrzenie komunikacji, ale jednocześnie generują szereg zagrożeń dla bezpieczeństwa użytkowników. Celem niniejszego artykułu jest analiza wpływu gier online na różne aspekty bezpieczeństwa, w tym bezpieczeństwo cyfrowe, społeczne i psychologiczne.
W pracy omówione zostaną najważniejsze zagrożenia związane z korzystaniem z gier online, takie jak cyberprzemoc, kontakt z nieznajomymi, uzależnienie od gier czy ryzyko utraty danych osobowych. Zwrócona zostanie również uwaga na mechanizmy stosowane w grach, w tym systemy mikropłatności oraz elementy losowe, które mogą wpływać na zachowania użytkowników i prowadzić do niepożądanych konsekwencji finansowych.
Artykuł podejmuje także problematykę działań profilaktycznych, podkreślając znaczenie edukacji cyfrowej, kontroli rodzicielskiej oraz odpowiedzialności twórców gier za projektowanie bezpiecznych środowisk dla użytkowników. Analiza ma charakter przeglądowy i opiera się na dostępnej literaturze oraz raportach dotyczących zachowań użytkowników w środowisku online.
Wnioski wskazują, że choć gry komputerowe online pełnią istotne funkcje rozrywkowe i społeczne, konieczne jest podejmowanie działań zwiększających świadomość zagrożeń oraz rozwijanie skutecznych strategii ochrony użytkowników, zwłaszcza najmłodszych.

Arnas Šukys
Improving Inventory Management in a Manufacturing Company under Economic Security and Resilience Perspectives

This presentation examines the challenges of inventory management in a manufacturing company that supplies and services equipment for the food industry. In the context of global supply chain disruptions, effective inventory management is no longer just a logistical task but a cornerstone of economic resilience and operational security.
The findings suggest that improving inventory management is essential for strengthening the company's economic resilience. Proposed solutions include the integration of barcode systems and the digitalization of warehouse processes. Such improvements ensure better traceability, minimize human error, and create a safer, more predictable operating environment, ultimately enhancing the company's competitive advantage in a volatile market.

PANEL II B
INFRASTRUKTURA KRYTYCZNA I BEZPIECZEŃSTWO PAŃSTWA W EPOCE TECHNOLOGICZNEJ RYWALIZACJI

MODERACJA: KAROLINA CEDRO

Mikołaj Sadlej
„Funkcjonowanie infrastruktury krytycznej w Polsce w świetle prawa i współczesnych zagrożeń”

Referat koncentruje się na funkcjonowaniu infrastruktury krytycznej w Polsce w ujęciu prawnym oraz w kontekście współczesnych zagrożeń. W pierwszej części przedstawione zostaną definicja oraz zakres infrastruktury krytycznej na podstawie przepisów ustawy o zarządzaniu kryzysowym, ze szczególnym uwzględnieniem zasad jej ochrony, których rozwinięcie stanowi Narodowy Program Ochrony Infrastruktury Krytycznej.
W drugiej części zaprezentowane zostaną wybrane przykłady zagrożeń i ataków na infrastrukturę krytyczną w Polsce po wybuchu wojny w Ukrainie. Celem referatu jest ukazanie znaczenia obowiązujących regulacji prawnych oraz ocena ich skuteczności w obliczu dynamicznie zmieniającego się środowiska bezpieczeństwa.

Hubert Hawrot
„Cyberataki na infrastrukturę krytyczną. Analiza przypadków i rekomendacje dla polskiego systemu bezpieczeństwa narodowego”

W dobie postępującej cyfryzacji oraz rosnącego uzależnienia procesów państwowych od systemów teleinformatycznych ochrona infrastruktury krytycznej staje się jednym z fundamentów stabilności państwa. Celem referatu jest analiza ewolucji zagrożeń w cyberprzestrzeni skierowanych przeciwko kluczowym sektorom gospodarki, takim jak energetyka, zaopatrzenie w wodę oraz system finansowy.
W pierwszej części referatu analizie poddane zostaną wybrane przypadki z ostatnich lat, w tym ataki na ukraiński system energetyczny oraz incydenty związane z wykorzystaniem oprogramowania typu ransomware w sektorach usług publicznych na świecie. Analiza ta służyć będzie identyfikacji głównych kierunków ataków oraz metod działania sprawców.
Druga część referatu koncentrować się będzie na kondycji polskiego systemu bezpieczeństwa narodowego w kontekście wdrażania dyrektywy NIS2 oraz roli Wojsk Obrony Cyberprzestrzeni. Ocenione zostaną aktualne procedury reagowania kryzysowego oraz poziom współpracy sektora publicznego z prywatnymi operatorami infrastruktury krytycznej.
W opracowaniu wskazano, że jednym z największych wyzwań dla Polski pozostaje ochrona systemów sterowania przemysłowego. Analiza przypadków sugeruje, że skuteczna obrona wymaga nie tylko zaawansowanych technologii, lecz także zintegrowanego modelu współpracy cywilno-wojskowej oraz partnerstwa publiczno-prywatnego.

Adam Glinkowski
„Flipper Zero jako wyzwanie dla bezpieczeństwa infrastruktury”

W pracy poddano analizie podatność systemów kontroli dostępu na ataki z wykorzystaniem urządzenia Flipper Zero. Jest to urządzenie klasy SDR, łączące funkcje przechwytywania, emulowania i kopiowania wybranych sygnałów radiowych oraz kart zbliżeniowych stosowanych w systemach kontroli dostępu.

Celem pracy jest ocena wpływu tego typu narzędzi na bezpieczeństwo infrastruktury opartej na starszych standardach komunikacji.
Systemy wykorzystujące rozwiązania pozbawione odpowiedniego szyfrowania, takie jak RFID 125 kHz czy MIFARE Classic, mogą być podatne na techniki ataku z użyciem tego typu urządzeń. W sprzyjających warunkach Flipper Zero może umożliwiać sklonowanie wybranych kart dostępu, zwłaszcza tam, gdzie transmisja między kartą a czytnikiem nie jest właściwie zabezpieczona. Może to prowadzić do ryzyka nieautoryzowanego dostępu do stref chronionych.
Sytuację dodatkowo komplikuje dostępność nieoficjalnego oprogramowania, które rozszerza funkcjonalności urządzenia i zwiększa możliwości jego wykorzystania. Tego rodzaju modyfikacje mogą wzmacniać poszczególne moduły, znosić wybrane ograniczenia częstotliwościowe oraz umożliwiać testowanie podatności systemów radiowych, w tym także tych opartych na kodach zmiennych. Powszechna dostępność takich narzędzi znacząco obniża próg wejścia, umożliwiając osobom bez specjalistycznej wiedzy technicznej podejmowanie prób naruszenia zabezpieczeń.
W pracy przeanalizowane zostaną wybrane potencjalne scenariusze ataków na systemy kontroli dostępu, a także możliwość wykorzystania technik USB HID, które — w zależności od konfiguracji systemu — mogą omijać część mechanizmów ochronnych. Analiza wskazuje, że skuteczność takich działań zależy przede wszystkim od sposobu implementacji zabezpieczeń. Pojawienie się urządzeń takich jak Flipper Zero unaocznia słabości modelu security by obscurity, czyli podejścia zakładającego bezpieczeństwo wynikające głównie z ograniczonej dostępności wiedzy lub narzędzi.
Wnioski wskazują, że model bezpieczeństwa oparty na rzadkości specjalistycznych urządzeń traci skuteczność. Systemową odpowiedzią powinna być modernizacja infrastruktury, wdrażanie silnego szyfrowania, w tym standardu AES, oraz regularna aktualizacja systemów. Kluczowe znaczenie mają nie tylko siła zastosowanego szyfrowania, lecz także jakość jego implementacji, właściwa konfiguracja systemów oraz bieżące monitorowanie ich podatności.

Aleksander Kotlarz
„Chińskie megakonstelacje satelitów jako wyzwanie dla dominacji amerykańskiej na niskiej orbicie okołoziemskiej”

W XXI wieku niska orbita okołoziemska stanowi nieodłączny element globalnej infrastruktury bezpieczeństwa. Znajdujące się na niej satelity są podstawą funkcjonowania współczesnego świata, zapewniając dostęp do internetu, komunikacji radiowej oraz łączności w sytuacjach kryzysowych. Wraz z rozwojem sektora kosmicznego oraz globalnego rynku usług satelitarnych rośnie rywalizacja między przedsiębiorstwami i państwami o dominację na orbicie.
W ostatnich latach niska orbita okołoziemska była zdominowana przez megakonstelację satelitów Starlink, należącą do amerykańskiej firmy SpaceX. Rozwój chińskiego potencjału kosmicznego przyniósł jednak odpowiedź na dominację Stanów Zjednoczonych w postaci megakonstelacji Guowang oraz Qianfan. Ambicje Chińskiej Republiki Ludowej, zakładające rozbudowę tych systemów do ponad 20 000 obiektów, coraz częściej skłaniają do pytania o dalszą bezkonkurencyjność amerykańskich podmiotów w sektorze satelitarnym.
W trakcie wystąpienia Aleksander Kotlarz podejmie próbę odpowiedzi na pytanie, czy prognozy dotyczące rozwoju chińskiego potencjału satelitarnego stanowią podstawę do coraz poważniejszego kwestionowania przewagi amerykańskich dostawców technologii. Analizie poddane zostanie również to, czy megakonstelacje Guowang oraz Qianfan mogą w przyszłości zagrozić dominującej pozycji systemu Starlink.

Jozef Huljak
„Drone Diplomacy as a Key Instrument of Polish-Taiwanese Security Partnership”

The aim of this paper is to examine the theoretical and empirical foundations of drone diplomacy as an emerging instrument of security cooperation between Poland and Taiwan. Drone diplomacy is understood as the strategic use of unmanned aerial vehicle technology transfers, joint development programmes, and defence-industrial partnerships as tools of foreign policy. This form of cooperation differs from conventional diplomatic channels rooted in formal alliance structures or multilateral frameworks.
The main research question concerns the principal mechanisms through which drone-related cooperation has become embedded in Polish-Taiwanese bilateral relations, as well as its significance within the broader dynamics of Indo-Pacific security and Central European defence transformation. The paper proceeds from the assumption that drone diplomacy constitutes a key instrument through which Taiwan develops security partnerships with like-minded states despite the formal constraints resulting from its limited international recognition.
Drawing on an analysis of recent cooperative initiatives and policy documents, the paper demonstrates the growing importance of technology-driven informal diplomacy in shaping security alignments in the contemporary international order.

Izabela Kucharzyk
„Migracja nieregularna, a bezpieczeństwo granic UE: rola Frontexu w erze dezinformacji”

W 2025 r. liczba nielegalnych przekroczeń granic Unii Europejskiej spadła o 26%, do poziomu 178 tys., co może świadczyć o skuteczności działań podejmowanych przez Frontex. Jednocześnie rosnące zagrożenia hybrydowe, takie jak dezinformacja, zaawansowany przemyt, cyberzagrożenia czy wykorzystanie dronów, wymagają wypracowania nowej strategii ochrony granic zewnętrznych UE. Celem wystąpienia jest ocena roli Europejskiej Agencji Straży Granicznej i Przybrzeżnej w koordynacji ochrony granic zewnętrznych, wspieraniu państw członkowskich oraz monitorowaniu nowych zagrożeń. Szczególna uwaga zostanie poświęcona atakom z użyciem dronów oraz kampaniom dezinformacyjnym, w tym fake newsom destabilizującym politykę migracyjną.
Analiza opiera się na danych zawartych w dokumentach Frontexu, w tym Annual Risk Analysis 2025/2026, wskazujących na pojawienie się nowych tras migracyjnych z Afryki oraz wzrost znaczenia cyberzagrożeń. Uwzględnione zostaną również propozycje reform Komisji Europejskiej z 2026 r., obejmujące m.in. potrojenie personelu Agencji do 30 tys. funkcjonariuszy, wzmocnienie systemów IT oraz rozwój technologii antydronowych.
Sukcesy Frontexu, widoczne m.in. w spadku liczby nielegalnych przekroczeń granic oraz rozwoju współpracy międzynarodowej, kontrastują z istotnymi wyzwaniami. Należą do nich normalizacja „kryzysu” migracyjnego, ograniczona odporność na hybrydowe operacje państw trzecich oraz konieczność dostosowania narzędzi ochrony granic do realiów cyfrowego środowiska bezpieczeństwa.
Perspektywy reform po 2026 r. zakładają integrację Paktu o Migracji i Azylu z elementami koncepcji „Bezpieczeństwa 2.0”, w tym wykorzystaniem sztucznej inteligencji, cyberobrony oraz technologii antydronowych. Rekomendacje obejmują pogłębienie współpracy z NATO, zapewnienie etycznego nadzoru nad nowymi technologiami oraz wdrażanie pilotażowych działań antydezinformacyjnych w Polsce.
Wystąpienie wpisuje się w debatę nad bezpieczeństwem wewnętrznym Unii Europejskiej, podkreślając potrzebę holistycznego podejścia do zagrożeń hybrydowych w erze cyfrowej.

PANEL III A
BEZPIECZEŃSTWO SPOŁECZNE WOBEC NOWYCH ZAGROŻEŃ

MODERACJA: OLIWIA RADKIEWICZ

Przemysław Merklinger
„Współczesne wyzwania i zagrożenia środowiska bezpieczeństwa społecznego seniorów w kontekście miejskim i wiejskim”

Starzenie się społeczeństwa stanowi jedno z kluczowych wyzwań współczesnych państw, wpływając bezpośrednio na kształt systemów bezpieczeństwa społecznego. Celem prezentacji jest analiza wyzwań i zagrożeń związanych z bezpieczeństwem społecznym seniorów w zróżnicowanym kontekście środowiskowym — miejskim i wiejskim. W opracowaniu przyjęto podejście interdyscyplinarne, uwzględniające perspektywę socjologiczną, ekonomiczną oraz zdrowotną.
W prezentacji wskazano, że seniorzy zamieszkujący obszary miejskie i wiejskie doświadczają odmiennych, choć częściowo nakładających się problemów. W środowisku miejskim dominują zagrożenia związane z anonimowością społeczną, osłabieniem więzi międzyludzkich, przestępczością oraz rosnącymi kosztami życia. Z kolei na obszarach wiejskich szczególnego znaczenia nabierają ograniczony dostęp do usług zdrowotnych, infrastruktury społecznej i transportu publicznego, a także zjawiska wykluczenia komunikacyjnego i cyfrowego. W obu środowiskach istotnymi problemami pozostają samotność, marginalizacja społeczna oraz rosnące ryzyko ubóstwa wśród osób starszych.
Analiza wskazuje również na znaczenie lokalnych polityk społecznych oraz inicjatyw wspólnotowych w budowaniu poczucia bezpieczeństwa seniorów. Podkreślona zostanie rola działań ukierunkowanych na integrację społeczną, rozwój usług opiekuńczych oraz zwiększanie dostępności przestrzeni publicznej i cyfrowej. Wnioski płynące z badań wskazują na konieczność różnicowania strategii wsparcia seniorów w zależności od specyfiki środowiska zamieszkania oraz wzmacniania współpracy międzyinstytucjonalnej.
Prezentacja stanowi próbę identyfikacji kluczowych obszarów ryzyka oraz kierunków działań, które mogą przyczynić się do poprawy jakości życia i poziomu bezpieczeństwa społecznego osób starszych zarówno w miastach, jak i na obszarach wiejskich.

Małgorzata Kulawska
„Analiza zagrożeń wobec nieletnich w Internecie - pedofilia i grooming”

Celem pracy jest przedstawienie problematyki pedofilii i groomingu oraz ukazanie wielowymiarowości trudności, z jakimi mierzy się skrzywdzone dziecko. Uszczerbek na zdrowiu fizycznym, psychicznym i seksualnym, będący konsekwencją wykorzystania, znacząco utrudnia małoletniemu prawidłowe funkcjonowanie w społeczeństwie. W pracy omówiono formy pomocy ofiarom pedofilii i groomingu, wskazując kluczowe obszary, na których powinny koncentrować się organy państwowe oraz organizacje pozarządowe w procesie wspierania dziecka.

Julia Kobak
„Między religią a polityką – prawa kobiet w Afganistanie w XXI wieku jako wyzwanie dla bezpieczeństwa społecznego”

Celem wystąpienia jest analiza sytuacji kobiet w Afganistanie w XXI wieku w kontekście napięcia między religią a polityką, a także ocena wpływu ograniczania ich praw na bezpieczeństwo społeczne. Po przejęciu władzy przez talibów w 2021 r. doszło do znaczącego regresu w zakresie praw kobiet, obejmującego m.in. dostęp do edukacji, rynku pracy oraz życia publicznego.
Wystąpienie podejmuje próbę odpowiedzi na pytanie, czy działania te stanowią wyłącznie element ideologii religijnej, czy także narzędzie kontroli społecznej. W analizie wskazano, że systemowe wykluczenie kobiet prowadzi do pogłębiania nierówności społecznych, osłabienia rozwoju państwa oraz wzrostu ryzyka destabilizacji.
Wnioski sugerują, że ograniczanie praw kobiet w Afganistanie należy postrzegać nie tylko jako problem z zakresu praw człowieka, lecz również jako istotne wyzwanie dla bezpieczeństwa społecznego.

Natalia Krokocka
„Bezpieczeństwo w epoce Silver Economy: Nowy model finansowania opieki i stabilności państwa”

Niniejszy referat podejmuje kluczową problematykę bezpieczeństwa ekonomicznego, społecznego i zdrowotnego państwa w obliczu starzenia się społeczeństwa oraz dynamicznego rozwoju srebrnej gospodarki, określanej także jako silver economy. Celem pracy jest analiza niewydolności dotychczasowych systemów finansowania opieki senioralnej i emerytalnej oraz zaproponowanie nowego, wielowymiarowego modelu, który mógłby zapewnić długofalową stabilność państwa.
W pierwszej części referatu zdefiniowana zostanie koncepcja srebrnej gospodarki. Wskazane zostanie, że osoby po 50. roku życia stanowią nie tylko grupę wymagającą wsparcia, lecz także istotny rynek konsumencki oraz niewykorzystany potencjał kadrowy. Następnie przeanalizowane zostaną ograniczenia tradycyjnych, repartycyjnych modeli finansowania, określanych jako PAYG. W obliczu kurczącej się bazy osób w wieku produkcyjnym oraz wyjątkowo niskich nakładów na opiekę długoterminową, wynoszących w Polsce ok. 0,6% PKB, modele te stają się trwale niezrównoważone. Wskazano również, że system opierający się w znacznym stopniu na nieformalnej opiece rodzinnej prowadzi do pogłębiania nierówności i wymaga pilnej transformacji strukturalnej.
W odpowiedzi na te wyzwania referat postuluje konieczność radykalnej dywersyfikacji źródeł finansowania opieki poprzez integrację środków publicznych i prywatnych. Równocześnie, w oparciu o dane OECD i WHO, wykazano, że racjonalizacja wydatków wymaga przesunięcia ciężaru z opieki instytucjonalnej na szeroko rozumianą profilaktykę zdrowotną oraz promowanie aktywnego starzenia się. Szczególną uwagę zwrócono na rolę nowoczesnych technologii, takich jak telemedycyna, teleopieka, systemy smart home czy robotyka usługowa. Odpowiednie wdrożenie zintegrowanych narzędzi e-zdrowia może znacząco obniżyć koszty systemowe, a zarazem ułatwić dostęp do usług medycznych.
Ostatnia część pracy koncentruje się na krytycznych aspektach zarządczych, prawnych i etycznych proponowanego modelu. Podkreślono konieczność ujednolicenia definicji opieki długoterminowej w prawie, zagwarantowania autonomii pacjenta, przeciwdziałania wykluczeniu cyfrowemu oraz zapewnienia bezpieczeństwa wrażliwych danych medycznych.
W podsumowaniu stwierdzono, że skuteczna odpowiedź na wyzwania demograficzne wymaga wdrożenia spójnej, centralnie koordynowanej strategii. Synergia innowacyjnego finansowania, profilaktyki i rozwoju technologicznego stanowi fundament utrzymania wydolności oraz spójności państwa w epoce srebrnej gospodarki.

Gustaw Krakowiak
„Wpływ algorytmów mediów społecznościowych: czy platformy faworyzują jedną stronę konfliktu?”

Algorytmy rekomendacyjne platform społecznościowych stanowią kluczowy mechanizm selekcji i dystrybucji informacji w środowisku cyfrowym. Wpływają one zarówno na ekspozycję użytkowników na treści polityczne, jak i na dynamikę percepcji konfliktów społecznych oraz informacyjnych.

W literaturze przedmiotu wskazuje się, że systemy oparte na optymalizacji zaangażowania i uwagi użytkowników mogą nieintencjonalnie wzmacniać treści polaryzujące, emocjonalne, konfliktogenne, a niekiedy także radykalne.Jednocześnie nadal pozostaje nierozstrzygnięte, czy obserwowane asymetrie w widoczności treści wynikają z systemowej stronniczości algorytmicznej, czy raczej z endogenicznych preferencji użytkowników oraz struktury sieci społecznych. Problem badawczy został sformułowany w postaci pytania: czy algorytmy rekomendacyjne mediów społecznościowych systematycznie faworyzują jedną stronę konfliktu informacyjnego, czy też obserwowane dysproporcje w widoczności treści są funkcją zachowań użytkowników i właściwości sieciowych?
Przyjęto hipotezę, że algorytmy rekomendacyjne nie wykazują intencjonalnej stronniczości względem konkretnej strony konfliktu, lecz amplifikują treści o wysokim ładunku emocjonalnym i polaryzacyjnym. Prowadzi to do asymetrii widoczności, która może być interpretowana jako przejaw stronniczości algorytmicznej.

Zuzanna Jaksender
„Bezpieczne hasła w erze cyfrowej: jak chronić swoje dane przed cyberzagrożeniami”

W obliczu dynamicznego rozwoju technologii informacyjnych oraz eskalacji zagrożeń w cyberprzestrzeni, problematyka bezpieczeństwa haseł nabiera kluczowego znaczenia zarówno w kontekście indywidualnym, jak i organizacyjnym. Celem niniejszego artykułu jest analiza współczesnych praktyk związanych z tworzeniem i zarządzaniem hasłami oraz identyfikacja najczęstszych podatności wynikających z niewłaściwych zachowań użytkowników. W opracowaniu omówiono mechanizmy ataków ukierunkowanych na uwierzytelnianie, w tym techniki phishingowe, ataki typu brute force oraz wykorzystanie wycieków danych. Szczególną uwagę poświęcono znaczeniu stosowania silnych, unikalnych haseł, implementacji menedżerów haseł oraz zastosowaniu uwierzytelniania wieloskładnikowego jako efektywnych metod minimalizacji ryzyka naruszeń bezpieczeństwa. Artykuł podejmuje również próbę oceny skuteczności aktualnych standardów ochrony danych oraz wskazuje rekomendacje mające na celu podniesienie poziomu świadomości użytkowników w zakresie cyberbezpieczeństwa.

PANEL III B
OD WOJNY KOLONIALNEJ DO WOJNY INFORMACYJNEJ: BEZPIECZEŃSTWO W PERSPEKTYWIE HISTORYCZNEJ I CYFROWEJ

MODERACJA: NIKOLA KRÓLAK

Jan Szałankiewicz
„Zarządzanie populacją w czasie wojny: kultura, przestrzeń i kontrola społeczna podczas konfliktu w Algierii (1954-1962)”

Referat analizuje francuskie strategie zarządzania ludnością cywilną podczas wojny algierskiej w latach 1954-1962, ujmując je w perspektywie kultury, przestrzeni i kontroli społecznej. Pierwszy wątek dotyczy polityki wobec kobiet, obejmującej kampanie „emancypacyjne”, działania opiekuńcze i medyczne oraz sposób, w jaki Front Wyzwolenia Narodowego – FLN – interpretował je jako ingerencję w normy społeczne, honor i tożsamość wspólnotową.
Druga część referatu poświęcona jest propagandzie i wojnie psychologicznej. Omówione zostaną cele przekazu oraz jego formy, takie jak radio, kino, wydarzenia publiczne, plakaty i ulotki, a także ich rola w legitymizowaniu projektu Algérie française.
Następnie przedstawiona zostanie infrastruktura instytucjonalna wpływu i socjalizacji, obejmująca Sections Administratives Spécialisées – SAS, Équipes Médico-Sociales Itinérantes – EMSI, Centres Sociaux oraz Service de Formation des Jeunes en Algérie – SFJ. Instytucje te ukazane zostaną jako narzędzia łączące świadczenie usług publicznych z selektywną kontrolą, dystrybucją zasobów oraz pozyskiwaniem informacji.
Wątek przestrzenny obejmuje reformy administracyjne, Plan Konstantyny oraz system wiosek przesiedleńczych jako instrumenty reorganizacji życia społecznego i ograniczania autonomii lokalnych wspólnot. Zakończenie syntetyzuje reakcje społeczeństwa, obejmujące adaptację, opór i ambiwalencję, oraz zestawia je z perspektywą FLN, wskazując na rywalizację o „serca i umysły” poprzez praktyki codzienności.

Jan Boruta
„Niszczenie polskiej tożsamości na Białorusi przez reżim Łukaszenki jako element wojny hybrydowej”

Celem wystąpienia jest analiza systemowych działań reżimu Alaksandra Łukaszenki wymierzonych w mniejszość polską na Białorusi. Działania te zostaną ukazane jako element szeroko zakrojonej wojny hybrydowej prowadzonej przeciwko Rzeczypospolitej Polskiej. Choć początkowe relacje po 1989 r. opierały się m.in. na traktatach o dobrym sąsiedztwie, objęcie władzy przez Łukaszenkę w 1994 r. zapoczątkowało proces stopniowej izolacji Białorusi oraz narastającej wrogości wobec Polski i polskiej mniejszości zamieszkującej terytorium Białorusi.
Poprzez aresztowania liderów Związku Polaków na Białorusi, takich jak Andżelika Borys i Andrzej Poczobut, a także uznanie strony internetowej tej organizacji za ekstremistyczną, reżim dąży do ograniczenia, a w dalszej perspektywie eliminacji niezależnych struktur mniejszości polskiej. Szczególnym przykładem represji jest skazanie Andrzeja Poczobuta na osiem lat kolonii karnej o zaostrzonym rygorze.
Reżim Łukaszenki systemowo likwiduje polskie szkolnictwo, czego przykładem są działania wobec szkoły w Brześciu prowadzonej przez Annę Paniszewą. Równocześnie wykorzystuje propagandę do oskarżania Polaków o „rehabilitację nazizmu”, zwłaszcza w kontekście upamiętniania Żołnierzy Wyklętych. Władze białoruskie celowo dopuszczają się również destrukcji miejsc pamięci, w tym niszczenia cmentarzy żołnierzy Armii Krajowej, m.in. w Mikuliszkach, Wołkowysku i Kaczyczach, oraz dewastacji Krzyża Katyńskiego w Grodnie. Tego rodzaju akty wandalizmu służą zacieraniu historycznych śladów polskości oraz prowokowaniu polskiej opinii publicznej.
Celem wystąpienia jest wykazanie, że opisane działania nie stanowią wyłącznie elementu wewnętrznej polityki Mińska, lecz są częścią celowej strategii destabilizacji państwa polskiego. Wojna hybrydowa nie ogranicza się bowiem do wywołania kryzysu migracyjnego na granicy polsko-białoruskiej w 2021 r. Niszczenie fundamentów tożsamościowych Polaków na Białorusi należy postrzegać jako formę agresji kulturowej, której celem jest osłabienie pozycji Polski jako jednego z kluczowych aktorów polityki wschodniej.

Bartłomiej Kielesiński
„Smartfon jako świadek” przeciwko samemu sobie. Konstytucyjne i procesowe granice przymuszania podejrzanego do odblokowania urządzenia w polskim procesie karnym

Współczesne postępowanie karne coraz częściej opiera się na dowodach cyfrowych, a smartfon pełni funkcję nośnika szczegółowych informacji o użytkowniku, takich jak dane lokalizacyjne, kontakty czy historia aktywności. W tym ujęciu może on działać jako swoisty „świadek” w procesie karnym.
Celem wystąpienia jest analiza granic przymuszania podejrzanego do odblokowania urządzenia mobilnego w świetle Konstytucji RP oraz Kodeksu postępowania karnego, ze szczególnym uwzględnieniem prawa do obrony i zakazu samooskarżenia. Omówione zostanie rozróżnienie między zabezpieczeniami opartymi na wiedzy, takimi jak PIN lub hasło, a metodami biometrycznymi, np. odciskiem palca czy rozpoznawaniem twarzy. Podjęty zostanie również problem dopuszczalności stosowania przymusu fizycznego w celu odblokowania urządzenia.
Analiza ma charakter dogmatyczny i została uzupełniona o przegląd orzecznictwa oraz obserwacje praktyki postępowania przygotowawczego. Wnioski wskazują na niedopuszczalność zmuszania podejrzanego do ujawnienia informacji o charakterze mentalnym, a jednocześnie na możliwość zabezpieczenia urządzenia oraz pozyskiwania określonych danych w granicach obowiązujących przepisów.

Aleksandra Antoszewska-Kielesińska
„Różnice demograficzne między regionami Polski a skuteczność polityk lokalnych. Wpływ samorządów na procesy ludnościowe”

Zmiany demograficzne w Polsce stanowią jedno z najważniejszych wyzwań dla samorządów lokalnych, szczególnie w kontekście starzenia się społeczeństwa oraz silnego zróżnicowania przestrzennego procesów ludnościowych. Celem wystąpienia jest określenie roli polityk lokalnych w kształtowaniu tych procesów na tle uwarunkowań regionalnych oraz odpowiedź na pytanie, w jakim stopniu obserwowane różnice demograficzne wynikają z działań samorządów, a w jakim z takich czynników jak rynek pracy, dostępność mieszkań, infrastruktura, urbanizacja oraz położenie względem dużych miast.
Przedstawiono zróżnicowanie przestrzenne procesów demograficznych w układzie gmin i powiatów. Korzystne trendy populacyjne wynikające z dodatniego salda migracji oraz napływu ludności w młodszym wieku obserwuje się w gminach położonych wokół dużych miast (tj. Warszawa, Kraków, Wrocław, Poznań, Gdańsk etc.). Analogicznie, obszary oddalone od głównych ośrodków miejskich charakteryzują się ujemnym saldem migracji oraz ubytkiem naturalnym, a w efekcie trwałym spadkiem liczby ludności.

W drugiej części wystąpienia omówiono działania podejmowane przez samorządy na rzecz poprawy sytuacji demograficznej na obszarze danej jednostki terytorialnej. Zwrócono również uwagę na znaczenie czynników społeczno-kulturowych, takich jak model życia rodzinnego, opóźnianie decyzji o posiadaniu dzieci oraz zmiany stylu życia, które ograniczają poziom przyrostu naturalnego niezależnie od działań samorządów.
Wnioski wskazują, że polityki lokalne mogą wpływać na procesy demograficzne głównie poprzez poprawę warunków życia i ograniczanie barier osiedleńczych, jednak ich skuteczność jest przestrzennie zróżnicowana i silnie uzależniona od lokalnych uwarunkowań. Polityki lokalne powinny również obejmować działania integracyjne wzmacniające więzi społeczne i kapitał społeczny, gdyż mogą one pośrednio sprzyjać stabilizacji związków oraz podejmowaniu decyzji o zakładaniu rodzin, zwłaszcza w warunkach niskiego przyrostu naturalnego w Polsce.

Daria Węgrzyn
„Wojna informacyjna w mediach społecznościowych”

Wojna informacyjna w mediach społecznościowych stanowi istotny element współczesnych konfliktów w przestrzeni cyfrowej, oddziałując na procesy społeczne, polityczne oraz bezpieczeństwo informacyjne. Dynamiczny rozwój platform komunikacyjnych umożliwił szybkie rozpowszechnianie treści, w tym również dezinformacji, która bywa wykorzystywana do manipulowania opinią publiczną oraz kształtowania określonych narracji.
Szczególną rolę odgrywają mechanizmy algorytmiczne wzmacniające przekazy o wysokim ładunku emocjonalnym, co sprzyja polaryzacji użytkowników. Istotnym narzędziem pozostają także zautomatyzowane konta oraz skoordynowane działania informacyjne, które zwiększają zasięg i pozorną wiarygodność fałszywych przekazów.
Skala i skuteczność tych działań wynikają z szybkości dystrybucji informacji oraz ograniczonej weryfikacji treści przez odbiorców. Zjawisko to generuje poważne konsekwencje dla jakości debaty publicznej oraz stabilności systemów demokratycznych, wskazując na potrzebę wzmacniania kompetencji medialnych i rozwijania mechanizmów przeciwdziałania dezinformacji.

Sebastian Skop
„Pokolenie w ciągłym stresie. Jak doomscrolling wpływa na wartości młodzieży i bezpieczeństwo wewnętrzne państwa”

W swoim wystąpieniu chciałbym poruszyć problem, który na co dzień dotyka większość z nas – zjawisko ciągłego i bezwiednego przeglądania negatywnych informacji w sieci, czyli tak zwanego doomscrollingu. Algorytmy mediów społecznościowych bez przerwy bombardują młodych ludzi wiadomościami o kryzysach, konfliktach i zagrożeniach. Chcę pokazać, że to zjawisko to coś znacznie więcej niż tylko problem psychologiczny czy chwilowy spadek nastroju. To realne wyzwanie dla bezpieczeństwa kulturowego i stabilności całego państwa.Opierając się na analizie współczesnych trendów społecznych i specyfiki mediów cyfrowych, opowiem o tym, jak życie w permanentnym, informacyjnym stresie rzutuje na system wartości i poczucie tożsamości młodego pokolenia. Ciągła ekspozycja na negatywne treści sprawia, że młodzi ludzie coraz częściej stają się wyobcowani, tracą poczucie przynależności do wspólnoty i przestają ufać instytucjom państwowym oraz tradycyjnym autorytetom.Dlaczego to zjawisko jest kluczowe z punktu widzenia bezpieczeństwa wewnętrznego? Ponieważ podzielone społeczeństwo, które żyje w lęku i nie ufa własnemu państwu, staje się niezwykle łatwym celem dla dezinformacji i różnego rodzaju działań hybrydowych. Zmniejsza się nasza naturalna odporność na kryzysy. W podsumowaniu referatu chciałbym zaproponować wnioski i zastanowić się, jak państwo oraz system edukacji powinny na to zareagować, by skuteczniej budować odporność informacyjną młodzieży i chronić jej bezpieczeństwo kulturowe w cyfrowym świecie.

Podsumowanie

Wystąpienia prezentowane podczas I Ogólnopolskiej Studencko-Doktoranckiej Konferencji Naukowej „Bezpieczeństwo 2.0” ukazują bezpieczeństwo jako kategorię wielowymiarową, dynamiczną i coraz silniej powiązaną z przemianami technologicznymi, społecznymi oraz informacyjnymi. Poruszana problematyka dowodzi, że współczesne zagrożenia nie ograniczają się już wyłącznie do tradycyjnie rozumianych konfliktów zbrojnych, ochrony granic czy stabilności instytucji państwowych. Coraz częściej dotyczą one cyberprzestrzeni, infrastruktury krytycznej, mediów społecznościowych, sztucznej inteligencji, procesów poznawczych, bezpieczeństwa użytkowników technologii cyfrowych, a także odporności społecznej wobec manipulacji i dezinformacji.

Wystąpienia poświęcone sztucznej inteligencji i cyberbezpieczeństwu wskazują na dualny charakter nowych technologii. Z jednej strony AI może wspierać wykrywanie zagrożeń, automatyzować analizę incydentów i wzmacniać systemy ochrony. Z drugiej jednak strony umożliwia tworzenie bardziej zaawansowanych cyberataków, treści deepfake, fałszywych przekazów, kampanii dezinformacyjnych oraz narzędzi manipulacji poznawczej. Szczególne znaczenie zyskuje tu pytanie o bezpieczeństwo informacyjne i poznawcze jednostek, zwłaszcza młodych użytkowników mediów cyfrowych, którzy funkcjonują w środowisku nieustannego przepływu danych, emocjonalnych narracji i algorytmicznie wzmacnianych komunikatów.

Istotną część konferencji stanowi refleksja nad wojną informacyjną, dezinformacją i rolą mediów społecznościowych. Autorzy wystąpień zwracają uwagę, że współczesne platformy cyfrowe nie są jedynie neutralnymi kanałami komunikacji, lecz aktywnymi elementami ekosystemu informacyjnego. Algorytmy rekomendacyjne, ekonomia uwagi, boty, farmy kont, mikrotargetowanie oraz mechanizmy amplifikacji emocjonalnych treści wpływają na postrzeganie rzeczywistości, poziom zaufania społecznego, jakość debaty publicznej oraz stabilność procesów demokratycznych. W tym kontekście dezinformacja jawi się nie tylko jako problem komunikacyjny, ale również jako realne zagrożenie dla bezpieczeństwa państwa i społeczeństwa.

Ważnym obszarem rozważań jest także bezpieczeństwo użytkowników w społeczeństwie cyfrowym. Wystąpienia dotyczące phishingu, ochrony seniorów przed cyberoszustwami, bezpieczeństwa haseł, ciemnych wzorców projektowych, gier online czy doomscrollingu pokazują, że człowiek pozostaje jednym z najważniejszych punktów odniesienia we współczesnych badaniach nad bezpieczeństwem. Zagrożenia cyfrowe oddziałują nie tylko na dane i systemy techniczne, ale również na emocje, decyzje, prywatność, relacje społeczne, poczucie sprawczości oraz kondycję psychiczną użytkowników. Dlatego skuteczna ochrona wymaga łączenia rozwiązań technologicznych z edukacją cyfrową, rozwijaniem krytycznego myślenia i budowaniem odporności informacyjnej.

Kolejna grupa wystąpień koncentruje się na infrastrukturze krytycznej, bezpieczeństwie państwa oraz technologicznej rywalizacji międzynarodowej. Analizowane są zarówno zagrożenia dla systemów energetycznych, wodnych, finansowych i przemysłowych, jak i podatności starszych systemów kontroli dostępu czy znaczenie technologii satelitarnych, dronów oraz systemów ochrony granic. Referaty te pokazują, że bezpieczeństwo państwa coraz częściej zależy od odporności infrastruktury technicznej, jakości współpracy cywilno-wojskowej, partnerstwa publiczno-prywatnego oraz zdolności do szybkiego dostosowywania prawa i procedur do nowych form zagrożeń.

W poruszanej problematyce silnie obecny jest również społeczny wymiar bezpieczeństwa. Starzenie się społeczeństwa, sytuacja seniorów w miastach i na obszarach wiejskich, srebrna gospodarka, polityki lokalne wobec zmian demograficznych, prawa kobiet w Afganistanie czy bezpieczeństwo grup szczególnie wrażliwych pokazują, że stabilność państwa zależy nie tylko od technologii i instytucji, ale również od jakości więzi społecznych, dostępu do usług, poziomu zaufania, integracji wspólnotowej oraz zdolności systemów publicznych do reagowania na długofalowe przemiany demograficzne i kulturowe.

Zgromadzone wystąpienia dowodzą, że „Bezpieczeństwo 2.0” należy rozumieć jako próbę uchwycenia nowej logiki zagrożeń. Jej istotą jest przenikanie się wymiaru cyfrowego, społecznego, politycznego, psychologicznego, infrastrukturalnego i międzynarodowego. Współczesne bezpieczeństwo wymaga zatem nie tylko ochrony systemów i granic, lecz także ochrony zaufania, tożsamości, danych, procesów poznawczych, instytucji demokratycznych oraz zdolności społeczeństwa do odróżniania informacji wiarygodnych od manipulacyjnych.

Konferencja pokazuje jednocześnie, że odpowiedź na nowe zagrożenia musi mieć charakter interdyscyplinarny. Nie wystarczą rozwiązania techniczne, prawne ani edukacyjne stosowane osobno. Konieczne jest łączenie wiedzy z zakresu nauk o bezpieczeństwie, prawa, politologii, socjologii, komunikacji społecznej, informatyki, psychologii i stosunków międzynarodowych. Dopiero takie podejście pozwala zrozumieć, dlaczego współczesne zagrożenia są tak skuteczne oraz jak budować odporność państwa, społeczeństwa i jednostki.

Niniejszy zbiór abstraktów stanowi zatem nie tylko zapis programu konferencji, lecz także świadectwo kierunków, w jakich rozwijają się młode badania nad bezpieczeństwem. Prezentowane teksty pokazują wysoką wrażliwość autorek i autorów na aktualne problemy społeczne, technologiczne i polityczne. Wspólnym mianownikiem wszystkich wystąpień jest przekonanie, że bezpieczeństwo w XXI wieku nie jest stanem danym raz na zawsze, lecz procesem wymagającym ciągłej diagnozy, adaptacji, współpracy i odpowiedzialności.

Oliwia Radkiewicz
Juliusz Sikorski