



KONGRES BEZPIECZEŃSTWO POLSKI

Rzeszów 2025

11-12 CZERWCA 2025
ZEN.COM EXPO Rzeszów-Jasionka

W kontekście dynamicznie zmieniającego się otoczenia geopolitycznego i technologicznego, kluczowym aspektem staje się także zapewnienie bezpieczeństwa.

Ten projekt tworzy platformę dialogu, wymiany wiedzy i doświadczeń, sprzyjających analizie oraz opracowaniu skutecznych strategii w tej dziedzinie. Integrujemy różne branże - rozmawiamy o bezpieczeństwie cross-sektorowo.

Na kanwie sukcesu pierwszej edycji Kongresu Bezpieczeństwo Polski - Total Security organizujemy drugą, dużo większą edycję w Rzeszowie.

W jednym miejscu spotkają się przedstawiciele świata polityki, gospodarki, wojskowości, samorządów, eksperci z branży IT i cyberbezpieczeństwa, a także energetyki, przemysłu i telekomunikacji. Takie szerokie grono pozwoli na kompleksowe spojrzenie na szeroko pojęte wyzwania związane z bezpieczeństwem.

Podczas Kongresu odbędzie się jubileuszowa 20. edycja Smart City Forum, Komitet CISOs i CSOs działający przy Radzie Programowej KBP, dodatkowe zamknięte sesje tematyczne i Wielka Gala.



KBP RZESZÓW 2025 w liczbach



3000 gości



ponad 20 bloków
tematycznych



prawie 200
prelegentów



dziesiątki prezentacji,
raportów i case-studies



Dzień 1

BLOK INAUGURACYJNY



KONGRES
BEZPIECZEŃSTWO
POLSKI
Rzeszów 2025



MAIN STAGE



KONGRES
BEZPIECZEŃSTWO
POLSKI
Rzeszów 2025

SALA KONGRESOWA



SESJE
ZAMKNIĘTE

WARSZTATY

SPOTKANIE
KOMITETU
CSOs CISOs

SALA GŁÓWNA

WIELKA GALA

Dzień 2

MAIN STAGE



KONGRES
BEZPIECZEŃSTWO
POLSKI
Rzeszów 2025

SALA AUDYTORyjNA



WARSZTATY

SESJE
ZAMKNIĘTE

ZAKRES TEMATYCZNY

1. SIŁY I ŚRODKI WPŁYWAJĄCE NA BEZPIECZEŃSTWO NARODOWE

- Rola Polski w kształtowaniu nowego ładu geopolitycznego w Europie Środkowo-Wschodniej
- Geopolityka a zagrożenia hybrydowe – jak zmieniające się realia wpływają na bezpieczeństwo narodowe?
- Potencjał współpracy gospodarczej pomiędzy Polską a Stanami Zjednoczonymi
- Zarządzaniu kryzysowe podczas powodzi i klęsk żywiołowych PKB na siły zbrojne. Czy bezpieczeństwo kraju zależy od finansowania?
- Kompetencje i zasoby samorządów w zarządzaniu kryzysowym - czy polskie samorządy mają wystarczające zasoby finansowe, technologiczne i ludzkie, aby skutecznie zarządzać sytuacjami kryzysowymi?

2. ROLA SAMORZĄDÓW W ZARZĄDZANIU SYTUACJAMI KRYZYSOWYMI I REAGOWANIU NA NAGŁE ZDARZENIA

- Jakie wyzwania stoją przed polskimi miastami w kontekście bezpieczeństwa w kolejnych latach?
- Cyberzagrożenia w infrastrukturze miejskiej – od zakłóceń transportu po blackoutu
- Lekcje z przeszłości - czy obecne mechanizmy współpracy są wystarczające? Koordynacja działań wojskowych i samorządowych w obliczu zagrożeń militarnych i klimatycznych
- Decentralizacja, a koordynacja z poziomu centralnego - w jakich obszarach samorządy powinny mieć większą autonomię, a gdzie potrzebna jest silna koordynacja centralna?
- Rola społeczności lokalnych i organizacji pozarządowych w zarządzaniu kryzysowym

3. STRAŻNICY BEZPIECZEŃSTWA – KLUCZOWA ROLA SŁUŻB MUNDUROWYCH W OCHRONIE KRAJU

- Służby mundurowe na rzecz bezpieczeństwa Polski. W jakim kierunku zmierzają służby mundurowe, by skutecznie chronić bezpieczeństwo Polski?
- Komunikacja kryzysowa z obywatelami. Jak przekazywać wiarygodne informacje?
- Dezinformacyjny front. Relacja z wojny w mediach społecznościowych
- Obowiązkowa służba wojskowa jako potencjalny czynnik wzmacniający zdolności obronne Państwa?
- "Pod Przykryciem" W cieniu tajnych operacji – misja Służb Specjalnych w walce z zagrożeniami
- Kooperacja działań Straży Pożarnej ze służbami mundurowymi. Współpraca jako czynnik podnoszący bezpieczeństwo obywateli
- Bezpieczeństwo antyterrorystyczne w czasach podwyższonego zagrożenia - stopień BRAVO i jego wyzwania

4. INFRASTRUKTURA KRYTYCZNA JAKO IMPERATYW BEZPIECZEŃSTWA NARODOWEGO

- Wpływ infrastruktury krytycznej na stabilność państwa i jego zdolność do obrony
- Jaki obszar infrastruktury krytycznej wymaga większego zaangażowania wobec współczesnych zagrożeń?
- Ochrona infrastruktury krytycznej w kontekście rosnących zagrożeń cybernetycznych
- Finansowanie infrastruktury bezpieczeństwa i cyberbezpieczeństwa. Jaką rolę w finansowaniu odgrywają środki z programów europejskich, takich jak Digital Europe?

5. GOSPODARKA, PRZEMYSŁ, ŁAŃCUCH DOSTAW

- Polska w ramach UE a globalna konkurencyjność przemysłu
- Rezerwy strategiczne jako fundament realizacji zadań bezpieczeństwa narodowego
- Local content w przemyśle. Jakie kroki powinny zostać podjęte, aby zwiększyć lokalną produkcję w Polsce? Wzmacnianie polskiego przemysłu obronnego poprzez innowacyjne projekty wojskowe
- Współpraca międzynarodowa i ekspansja zagraniczna polskich firm
- Zagrożenia wynikające z ograniczeń eksportowych i sankcji: Jak chronić kluczowe sektory?

6. CYBERBEZPIECZEŃSTWO W ERZE GLOBALNYCH WYZWAŃ

- Cyberbezpieczeństwo w obliczu globalnych napięć ekonomicznych i geopolitycznych
- Bezpieczeństwo i suwerenność danych. Zastosowanie koncepcji Zero Trust i architektury SASE
- Liderzy cyberbezpieczeństwa i zwiększenie finansowania Funduszu Cyberbezpieczeństwa. Czy zwiększone finansowanie przyczyni się do zatrzymania specjalistów ds. cyberbezpieczeństwa w kraju?
- Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) i jej wpływ na sektor w Polsce
- Rozwój autonomicznych systemów cyberobrony - cyberbroń, cyberwojsko

7. SEKTOR BANKOWY NA RZECZ ROZWOJU SEKTORA WOJSKOWEGO

- Rola liderów sektora bankowego w promocji inicjatyw finansowania dla obronności
- Tworzenie funduszu bankowego – jak skonstruować mechanizm udzielania preferencyjnych kredytów dla sektora zbrojeniowego?
- Warunki kredytowe dla banków – jakie wymagania muszą spełniać wnioskodawcy, aby uzyskać finansowanie?
- Kto powinien finansować kosztowny rozwój zbrojeniówki w Polsce?

8. BEZPIECZEŃSTWO TECHNOLOGICZNE

- Czy technologie bezpieczeństwa nadążają za szybko zmieniającymi się zagrożeniami?
- Suwerenność technologiczna Polski. Jak Polska może rozwijać krajowe rozwiązania technologiczne, by uniezależnić się od dostawców zagranicznych?
- Zastosowanie blockchain w bezpieczeństwie systemów rozproszonych - bezpieczne zarządzanie tożsamością, śledzenie łańcuchów dostaw oraz bezpieczeństwo IoT
- Rozwój technologii dual-use dla bezpieczeństwa i rozwoju sektora obronnego

9. BEZPIECZEŃSTWO TELEKOMUNIKACJI I ENERGETYKI

- Łączność i energetyka – synergiczne podejście do ochrony i rozwoju infrastruktury krytycznej
- Telekomunikacja kablowa - działanie sieci mobilnych i stałych - modernizacja infrastruktury w kontekście wdrażania sieci 5G i przyszłych standardów 6G
- Łączność krytyczna - budowa nowoczesnych sieci światłowodowych MCC
- Jak zwiększyć odporność infrastruktury energetycznej na cyberataki?
- Stabilność dostaw gazu w obliczu regionalnych i globalnych napięć politycznych

OSOBISTOŚCI ZAANGAŻOWANE W PROJEKT W RAMACH PREZYDIUM, RADY PROGRAMOWEJ ORAZ KOMITETU CISO I CSO



Konrad Fijołek

Współprzewodniczący Rady Programowej KBP,
Prezydent Miasta Rzeszowa



Radosław Maćkiewicz

Współprzewodniczący Rady Programowej KBP,
Dyrektor Centralny Ośrodek Informatyki



Krzysztof Dyki

Współprzewodniczący Rady Programowej KBP,
Prezes Zarządu ComCERT



Władysław Kosiniak-Kamysz

Wiceprezes Rady Ministrów,
Minister Obrony Narodowej



Michał Szczerba

Posel Parlamentu Europejskiego, Członek Komisji Spraw Zagranicznych i Komisji Bezpieczeństwa i Obrony



Mariusz Chmielewski

Zastępca Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni DKWOC



Krzysztof Żuk

Prezydent Miasta Lublin



Wojciech Bakun

Prezydent Miasta Przemysła



Tadeusz Białek

Prezes Zarządu,
Związek Banków Polskich



Jarosław Kraszewski

Członek Zarządu
RBL Defence Polska



Dorota Zawadzka-Stepniak

Prezes Zarządu
Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej



Mariusz Lenartowicz

Dyrektor Biura Ochrony Ludności
Komenda Główna Państwowej Straży Pożarnej



Robert Piec

Dyrektor Instytutu Bezpieczeństwa Wewnętrznego
Akademia Pożarnicza



Paweł Boruszewski

Dowódca 18. Stołecznej Brygady Obrony Terytorialnej
Wojska Obrony Terytorialnej



Zbigniew Tarapata

Dziekan Wydziału Cybernetyki
Wojskowa Akademia Techniczna



Andrzej Szewiński

Posel na Sejm RP,
Zastępca Przewodniczącego Sejmowej Komisji Obrony Narodowej



Maciej Kluczyński

Prezes
Polskie Towarzystwo Bezpieczeństwa Narodowego



Joanna Kopczyńska

Prezes
PCW Wody Polskie



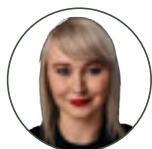
Andrzej Abramczuk

Prezes Zarządu
Netia



Piotr Ciepela

Globalny Lider Bezpieczeństwa Architektury i Nowoczesnych Technologii, Partner EY Polska



Paula Januszkiewicz

CEO
CQURE & CQURE Academy



Andrzej Karpiński

Dyrektor Bezpieczeństwa
Biuro Informacji Kredytowej S.A.



Wojciech Twaróg

CISO
Nationale-Nederlanden Polska



Grzegorz Jasiulewicz

Dyrektor Departamentu Cyberbezpieczeństwa
Bank Gospodarstwa Krajowego

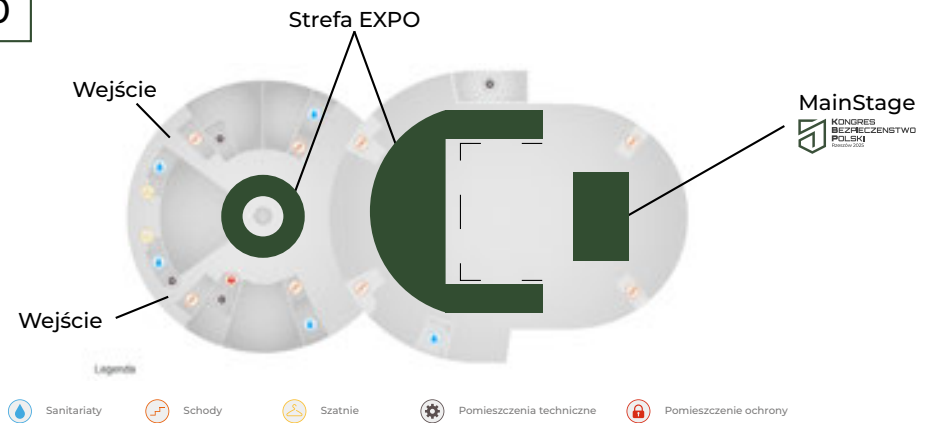


Krzysztof Słotwiński

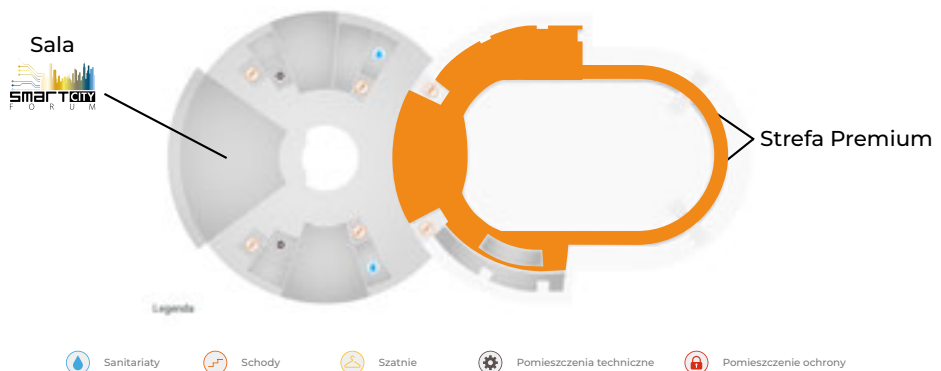
Dyrektor Zarządzający Pionem Bezpieczeństwa i Zarządzania Ciągłością Działania,
BNP Paribas Bank Polska

PLAN OBIEKTU

POZIOM 0



POZIOM 1



Dostęp do merytoryki jest bezpłatny.

Bezwzględnie wymagana jest rejestracja. Organizator zastrzega sobie odmowę przyjęcia zgłoszenia.

Dostęp do zamkniętych stref premium jest płatny.

PAKIET GOLD

dostęp do strefy Premium

PAKIET PLATINIUM

dostęp do strefy Premium i Gali

WIELKA GALA

udział w wieczornej kolacji i wręczeniu nagród

Zeskanuj kod QR i przejdź na stronę wydarzenia



Kontakt:

Merytoryka:

Monika Nowak

Flagship Events

Department Director

e-mail: m.nowak@mmcpolska.pl

kom: +48 530 662 013

Uczestnictwo:

Ewa Gućik

Marketing Manager

Marketing Department

e-mail: e.gucik@mmcpolska.pl

kom: +48 535 200 840

Współpraca:

Tomasz Petruk

Vice Director of Business

Development Department

Senior Project Manager

e-mail: t.petruk@mmcpolska.pl

kom: +48 883 784 084

