CYBERSEC EXPO & FORUM 2026
15-16 czerwca 2026
Międzyrodowe Centrum Kongresowe
Katowice

AGENDA

15 CZERWCA 2026 r.		
08.00-09.00 rejestracja gości		
09.00-10:30 **Sala Balowa C** **Sesja Inauguracyjna** **Geopolityka cyberbezpieczeństwa a suwerenność technologiczna**		
10.30-11.00 przerwa		
11.00-12.00 **Sala Balowa C** **Praktyczne podejście do budowania cyberobronności. Oczekiwania kontra rzeczywistość**	11.00-12.00 **Sala Balowa B** **Cyberbezpieczeństwo państwa i administracji samorządowej**	11.00-12.00 **Scena Hol Dolny** **Cyberportret polskiego biznesu 2026**
12.00-12.30 przerwa		
12.30-13.30 **Sala Balowa C** **Partnerstwo dla cyfrowej obronności**	12.30-13.30 **Sala Balowa B** **KSC i NIS2 w praktyce**	12.30-13.30 **Scena Hol Dolny** **Pieniądze na cyber: od regulacji po szanse dla biznesu**
13.30-14.30 przerwa		
14.30-15.30 **Sala Balowa C** **AI w praktyce: 2026 - rok implementacji**	14.30-15.30 **Sala Balowa B** **Ochrona infrastruktury krytycznej. Lekcje na przyszłość**	14.30-15.30 **Scena Hol Dolny** **Dezinformacja i odporność społeczna**
15:30-16:00 – przerwa		
16:00-17:00 **Sala Balowa C** **Technologie przyszłości. Na co stawiać, aby wygrać?**	16:00-17:00 **Sala Balowa B** **Kompetencje jutra i edukacja przyszłości**	16:00-17:00 **Scena Hol Dolny** **Między specjalizacją a powszechnością. Jak zorganizować państwo do walki z cyberprzestępczością?**
18.30 Sala Balowa C **WYDARZENIE TOWARZYSZĄCE** **Gala**		
19.15 Sala Balowa A **WYDARZENIE TOWARZYSZĄCE** Bankiet		

16 CZERWCA 2026 r.		
08.00-09.30 - rejestracja gości		
09.30-10.30 **Sala Balowa C** **Państwo, wojsko, biznes - partnerstwo czy rywalizacja o talenty?**	09.30-10.30 **Sala Balowa B** **CISO i CIO pod presją. Wyzwania menadżerów**	09.30-10.30 **Scena Hol Dolny** **Cyberbezpieczeństwo w finansach**
10.30-11.00 – przerwa		
11.00-12.00 **Sala Balowa C** **Cyber Resilience Act i certyfikacja: nowe obowiązki, nowe standardy bezpieczeństwa produktów**	11.00-12.00 **Sala Balowa B** **Cyberbezpieczeństwo a technologie podwójnego zastosowania: jak wzmocnić polski ekosystem?**	11.00-12.00 **Scena Hol Dolny** **Cyberbezpieczeństwo sektora energetycznego**
12.00-12.30 - przerwa		
12.30-13.30 **Sala Balowa C** **Edukacja jako tarcza. Sektor naukowy w dobie zmian**	12.30-13.30 **Sala Balowa B** **Cyberdyplomacja a polska odwaga. Czy Polska może eksportować cyberbezpieczeństwo?**	12.30-13.30 **Scena Hol Dolny** **Cyberbezpieczeństwo ochrony zdrowia**
13:30-14:30 – przerwa		
14:30-15:30 **Sala Balowa C** **Smart city. Jak technologie zmienią miasta?**	14:30-15:30 **Sala Balowa B** **Cyberbezpieczeństwo przemysłu**	

15 czerwca 2026 | 1 dzień Cybersec

15 czerwca 2026 r. | 09.00-10.30 | Sala Balowa C | transmisja on-line | tłumaczenie [PL/EN]
Sesja inauguracyjna
Geopolityka cyberbezpieczeństwa a suwerenność technologiczna
Europa funkcjonuje między globalnymi potęgami technologicznymi, które narzucają standardy bezpieczeństwa, modele regulacyjne i architekturę cyfrową. Czy UE jest skazana na zależność, czy buduje własną podmiotowość w cyberprzestrzeni? Debata o suwerenności technologicznej, konkurencyjności przemysłu i ochronie wartości demokratycznych w warunkach rosnącej presji geopolitycznej. Perspektywa instytucji europejskich, biznesu i ekspertów.

Otwarcie:
- **Wojciech Kuśpik,** prezes zarządu, PTWP
- **Leszek Pietraszek,** przewodniczący zarządu, Górnośląsko-Zagłębiowska Metropolia
- **Wojciech Saługa,** marszałek województwa śląskiego
- **Bogumił Sobula,** wiceprezydent Miasta Katowice

Wystąpienie (10')
- **Dariusz Standerski,** sekretarz stanu, Ministerstwo Cyfryzacji

Wystąpienie (10')
- **Borys Budka,** Poseł do Parlamentu Europejskiego, Przewodniczący Komisji PE ITRE

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):
- **Andy Garth,** Director of Government Affairs, ESET
- **Radosław Nielek,** dyrektor, NASK
- **[online] Jacek Siewiera,** ppłk. Wojska Polskiego, ekspert Atlantic Council, szef Biura Bezpieczeństwa Narodowego w latach 2022-2025
- **Dariusz Standerski,** sekretarz stanu, Ministerstwo Cyfryzacji
- **Tomasz Zdzikot,** wiceprzewodniczący Rady ds. Bezpieczeństwa i Obronności przy Prezydencie RP

Moderacja
- **Nikola Bochyńska,** dziennikarka, WNP.pl

15 czerwca 2026 r. | 11.00-12.00 | Scena Hol Dolny | transmisja on-line
Cyberportret polskiego biznesu 2026
Rośnie liczba, skala i różnorodność cyberataków. Z czym zmagają się polskie firmy? Czy nadal to pracownik jest najsłabszym ogniwem systemu cyberbezpieczeństwa? Jak często polskie podmioty walczą ze skutkami ataków ransomware?
Najnowsze informacje o sytuacji w polskiej cyberprzestrzeni, uwzględniając biznes i kadrę zarządzającą przedstawi raport „Cyberportret polskiego biznesu 2026", przygotowany przez ESET i DAGMA Bezpieczeństwo IT. Dyskusja skupi się nie tylko na rozmowie o stanie technologii i procedur, ale także postrzeganiu zagrożeń przez organizacje i ich gotowości na stale zmieniający się krajobraz cyberzagrożeń. To właśnie w czasie Cybersec EXPO & Forum odbędzie się premiera publikacji raportu.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):
- **Marcin Dudek**, kierownik CERT Polska, NASK
- **Andrzej Dulka,** prezes, Polska Izba Informatyki i Telekomunikacji
- **Paweł Jurek,** dyrektor rozwoju biznesu, DAGMA Bezpieczeństwo IT
- **Agnieszka Ulanowska**, dyrektorka, Dział Nadzoru Wewnętrznego i Bezpieczeństwa IT, VeloFunds TFI SA, ISACA Warsaw Chapter
- **Mirosław Wróblewski**, prezes, Urząd Ochrony Danych Osobowych

Moderacja
- **Nikola Bochyńska,** dziennikarka, WNP.pl

15 czerwca 2026 r. | 11.00-12.00 | Sala Balowa B | transmisja on-line | tłumaczenie [PL/EN]
Cyberbezpieczeństwo państwa i administracji samorządowej
Administracja centralna i JST stoją przed wspólnym wyzwaniem: wdrożeniem NIS2, rosnącą presją regulacyjną oraz eskalacją zagrożeń dla usług publicznych i infrastruktury krytycznej. Jak budować spójny system cyberodporności państwa - od strategii i legislacji po wspólne SOC, ochronę smart city i współpracę sektorową? Debata o cyfrowych fundamentach bezpiecznego

państwa działającego w warunkach permanentnej presji. Państwo i JST w jednym systemie: SOC, Zero Trust i nowe modele współpracy.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Michał Gramatyka,** sekretarz stanu, Ministerstwo Cyfryzacji
- **Monika Ingram,** dyrektorka, Centrum Badawcze Cyberbezpieczeństwa, Łukasiewicz-AI
- **Stanisław Korman,** członek zarządu, Górnośląsko-Zagłębiowska Metropolia
- **Jakub Olszowiec,** dyrektor, Biuro Strategii, Rozwoju i Zarządzania Projektami, Polska Wytwórnia Papierów Wartościowych
- **Jacek Orłowski,** kierownik, Dział Współpracy z Podmiotami Otoczenia EZD, NASK

Moderacja

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

15 czerwca 2026 r. | 11.00-12.00 | Sala Balowa C | transmisja on-line | tłumaczenie [PL/EN]
Praktyczne podejście do budowania cyberobronności. Oczekiwania kontra rzeczywistość

Jak w praktyce wygląda budowa SOC i CSIRT, wdrażanie procedur oraz testowanie planów ciągłości działania? Debata o różnicy między strategiami a realiami organizacyjnymi: brakach kadrowych, ograniczeniach budżetowych i oporze wobec zmian. Co rzeczywiście działa w podnoszeniu cyberodporności i jak uniknąć najczęstszych pułapek? Po pierwsze zaufanie. Kierunki rozwoju i współpracy dla cyberbezpieczeństwa

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Miroslav Čačík**, Filed CISO Advisor, ESET
- **Agnieszka Jankowska,** przewodnicząca Rady ds. Cyfryzacji, Ministerstwo Cyfryzacji, dyrektor ds. Korporacyjnych i Public Affairs, T-Mobile Polska
- **Filip Kupiński,** Security Services Lead for Poland, Accenture
- **Piotr Potejko,** dyrektor ds. bezpieczeństwa, Grupa Veolia w Polsce
- **Agata Ślusarek,** CTI Expert

Moderacja

- **Michał Duszczyk**, dziennikarz, Rzeczpospolita

15 czerwca 2026 r. | 12.30-13.30 | Sala Balowa C | transmisja on-line | tłumaczenie [PL/EN]
Partnerstwo dla cyfrowej obronności

Cyberprzestrzeń stała się jednym z kluczowych obszarów działania Sojuszu. Jak NATO buduje wspólne zdolności w zakresie cyberobrony i mechanizmy reagowania na poważne incydenty? Dyskusja o współdzieleniu informacji o zagrożeniach, wspólnych ćwiczeniach oraz roli państw członkowskich. Jaką pozycję w kształtowaniu agendy cyber w NATO zajmuje Polska i region Europy Środkowo-Wschodniej?

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Tomasz Florczak,** CEO, ChallengeRocket
- **gen. bryg. rez. Włodzimierz Nowak,** ekspert w dziedzinie cyberbezpieczeństwa
- **Joanna Pawełek-Mendez,** radca-minister ds. cyberbezpieczeństwa, Departament Polityki Bezpieczeństwa, Ministerstwo Spraw Zagranicznych
- **Tomasz Zdzikot,** wiceprzewodniczący Rady ds. Bezpieczeństwa i Obronności przy Prezydencie RP

Moderacja

- **Marcin Piasecki,** redaktor zarządzający, Rzeczpospolita

15 czerwca 2026 r. | 12.30-13.30 | Sala Balowa B | transmisja on-line | tłumaczenie [PL/EN]
KSC i NIS2 w praktyce

Aktualny stan wdrażania KSC i dyrektywy NIS2 – czego przedsiębiorcy mogą spodziewać się w najbliższym czasie. Jak przygotować organizację już dziś: identyfikacja obowiązków, analiza ryzyka i pierwsze kroki do zgodności z nowymi regulacjami. Wyzwania wdrożeniowe dla firm – interpretacja przepisów, przygotowanie procedur, współpraca z dostawcami i zarządzanie łańcuchem dostaw. Rola zarządu i kadry menedżerskiej w procesie przygotowania firmy do nowych wymogów cyberbezpieczeństwa.

Prezentacja (15')

Wiedza i świadomość jako klucz do spełnienia wymagań UoKSC i NIS2

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

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Przemysław Frąk,** Senior Presales Engineer, Axence
- **Jarosław Homa**, pełnomocnik rektora ds. cyberbezpieczeństwa, wicedyrektor, Centrum Cyberbezpieczeństwa, Politechnika Śląska
- **Joanna Karczewska,** audytor SI, ekspert ds. cyberbezpieczeństwa i ochrony danych osobowych
- **Karol Skupień,** prezes, KIKE
- **Dariusz Szostek**, sędzia Trybunału Konstytucyjnego, dyrektor, Centrum Cyber Science, Uniwersytet Śląski

Moderacja

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

15 czerwca 2026 r. | 12.30-13.30 | Scena Hol Dolny | transmisja on-line
Pieniądze na cyber: od regulacji po szanse dla biznesu

Rosnąca skala zagrożeń oznacza większe nakłady na cyberbezpieczeństwo - w administracji, MŚP i sektorze nauki. Jak zbudować skuteczny system finansowania: od mechanizmów publicznych i regulacji po mobilizowanie kapitału prywatnego? Debata o dostępnych instrumentach wsparcia oraz o tym, jak przekuwać presję regulacyjną i ryzyka w impuls do rozwoju krajowych technologii i usług.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Marietta Gieroń,** prezes zarządu, Instytut Kościuszki
- **Adrian Kapczyński**, koordynator, podobszar badawczy „Cyberbezpieczeństwo", Politechnika Śląska
- **Marianna Sidoroff**, dyrektorka, Departament Gospodarki Cyfrowej, Ministerstwo Rozwoju i Technologii
- **Krzysztof Szubert,** pełnomocnik dyrektora ds. komercjalizacji i współpracy międzynarodowej, Instytut Łączności – PIB, Senior Associate Member, Centre of Excellence in Cyber Security, Uniwersytet Oxfordzki
- **Piotr W. Zawadzki**, ekspert, Dział Zarządzania Strategicznego, Narodowe Centrum Badań i Rozwoju

Moderacja

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

15 czerwca 2026 r. | 14.30-15.30 | Scena Hol Dolny | transmisja on-line
Dezinformacja i odporność społeczna

Operacje informacyjne stały się narzędziem presji politycznej i gospodarczej. Propaganda i kampanie dezinformacyjne wpływają na decyzje konsumentów, stabilność rynków, zdrowie publiczne i nastroje społeczne. Jak budować odporność komunikacyjną państwa, biznesu i obywateli? Debata o mechanizmach reagowania, edukacji oraz współpracy instytucji publicznych i sektora prywatnego. Komunikacja strategiczna a rola państwa. Jak odpowiadać na kryzysy?

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Szymon Grabowski**, Pion Ochrony Informacyjnej Cyberprzestrzeni, NASK
- **Marcel Kiełtyka,** członek zarządu, dyrektor ds. komunikacji i PR, Stowarzyszenie Demagog, członek Rady konsultacyjnej ds. przeciwdziałania dezinformacji zewnętrznej przy MSZ
- **Michał Kowalczyk**, dyrektor ds. badań, członek zarządu, Instytut Badań Rynkowych i Społecznych
- **Marcin Piasecki,** redaktor zarządzający, Rzeczpospolita
- **Marta Zabłocka,** dział Fact-Checking, korespondentka, Polska Agencja Prasowa
- **Łukasz Zych**, rzecznik prasowy, Górnośląsko-Zagłębiowska Metropolia

Moderacja

- **Karolina Markowska,** redaktor naczelna, PulsHR.pl

15 czerwca 2026 r. | 14.30-15.30 | Sala Balowa B | transmisja on-line | tłumaczenie [PL/EN]
Ochrona infrastruktury krytycznej. Lekcje na przyszłość

Energetyka, woda, transport i łączność pozostają głównymi celami zaawansowanych ataków. Jakie wnioski płyną z najpoważniejszych incydentów ostatnich lat? Debata o nowych wymaganiach regulacyjnych i technicznych oraz o projektowaniu odporności w ujęciu systemowym - tak, by chronić nie tylko pojedyncze obiekty, lecz całe łańcuchy zależności. Sztuczna inteligencja. Energia, chmura, Gigafabryki AI: jak chronić infrastrukturę krytyczną w cyfrowym państwie.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Marcin Dudek,** kierownik CERT Polska, NASK
- **Krzysztof Dyl,** wiceprezes, Urząd Komunikacji Elektronicznej
- **Agnieszka Jankowska,** przewodnicząca Rady ds. Cyfryzacji, Ministerstwo Cyfryzacji, dyrektor ds. Korporacyjnych i Public Affairs, T-Mobile Polska
- **Dariusz Pałka,** kierownik, Dział Standardów i Architektury, Pion Cyberbezpieczeństwa, GAZ-SYSTEM
- **mjr rez. mgr inż. Artur Szachno,** Kierownik Działu Operacji Cyfrowych**,** Rządowa Agencja Rezerw Strategicznych
- **Grzegorz Wawryniuk**, dyrektor Biura Produktu i Marketingu, EXATEL
- **Dawid Zięcina**, Technical Department Director, DAGMA Bezpieczeństwo

Moderacja

- **Aleksandra Helbin,** redaktor naczelna, WNP.pl

15 czerwca 2026 r. | 14.30-15.30 | Sala Balowa C | transmisja on-line | tłumaczenie [PL/EN]
AI w praktyce: 2026 - rok implementacji

Rok 2026 oznacza przejście od deklaracji do realnych wdrożeń AI - także pod presją AI Act. Jakie systemy będą regulowane i jakie obowiązki spadną na firmy? Debata o przygotowaniu organizacji na audyty, odpowiedzialności za modele i bezpieczeństwie danych. Jak połączyć zgodność z regulacjami z efektywnością i budowaniem przewagi konkurencyjnej? Sztuczna inteligencja zmienia reguły gry - jest narzędziem zarówno ataku, jak i obrony. Jak wykorzystać AI w sektorach wrażliwych - od wojska po przemysł i zdrowie.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Gabriela Bar,** radczyni prawna, założycielka kancelarii, Gabriela Bar Law & AI
- **Karol Jędrasiak,** zastępca dyrektora, Centrum Transferu Technologii, Akademia WSB
- **Joanna Karczewska,** audytor SI, ekspert ds. cyberbezpieczeństwa i ochrony danych osobowych
- **Monika Karwacka**, adiunkt, kierownik zespołu Humanistyki Cyfrowej, Uniwersytet Śląski w Katowicach
- **Marcin Kowalski**, profesor badawczy, lider zespołu badawczego sztucznej inteligencji w Instytucie Optoelektroniki, Wojskowa Akademia Techniczna
- **Dariusz Szostek**, sędzia Trybunału Konstytucyjnego, dyrektor, Centrum Cyber Science, Uniwersytet Śląski

Moderacja

- **Marcin Mazur,** PR & Communication Officer, Dagma

15 czerwca 2026 r. | 16.00-17.00 | Scena Hol Dolny | transmisja on-line
Między specjalizacją a powszechnością. Jak zorganizować państwo do walki z cyberprzestępczością?

Czy skuteczniejszy jest model wyspecjalizowanych struktur, takich jak CBZC, czy budowanie kompetencji cyber w całym systemie służb i administracji? Debata o roli jednostek centralnych i terenowych, współpracy z SOC i CSIRT oraz o lukach organizacyjnych. Czy zwalczanie cyberprzestępczości jest dziś właściwie osadzone w KSC i systemie bezpieczeństwa państwa? Od wycieku do aktu oskarżenia. Kiedy i jak włączać organy ścigania w obsługę incydentów? Nowe oblicza cyberprzestępczości: AI, deepfake'i, cyberprzestępczość as a service. Cyberprzestępczość bez granic. Europol, współpraca międzynarodowa i wpływ nowych regulacji

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Maciej Jan Broniarz,** Cyber Incident Response Expert
- **Agnieszka Gryszczyńska,** Wydział Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
- **mł. insp. Wojciech Olszowy,** komendant, Centralne Biuro Zwalczania Cyberprzestępczości
- **Dominik Rozdziałowski,** ekspert w zakresie cyberbezpieczeństwa, cyberprzestępczości oraz bezpieczeństwa systemów informatycznych
- **Agata Ślusarek,** CTI Expert

Moderacja

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

15 czerwca 2026 r. | 16.00-17.00 | Sala Balowa B | transmisja on-line | tłumaczenie [PL/EN]
Kompetencje jutra i edukacja przyszłości

Dynamiczny rozwój technologii wymaga nowych kompetencji i ścisłej współpracy nauki z biznesem. Jak odpowiadać na rosnące zapotrzebowanie na ekspertów w obszarze cyber, AI i technologii przełomowych? Debata o rynku pracy, systemie szkoleń i certyfikacji oraz o tym, jak dostosować edukację do realnych potrzeb gospodarki i bezpieczeństwa państwa. Edukacja cyberbezpieczeństwa jako kompetencja przyszłości. Od higieny cyfrowej w domu po realne kompetencje rynku pracy

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Michał Gramatyka,** sekretarz stanu, Ministerstwo Cyfryzacji
- **Adrian Kapczyński**, koordynator, podobszar badawczy „Cyberbezpieczeństwo", Politechnika Śląska
- **Michał Maurycy Mazur,** fundator, Our Future Foundation
- **Monika Rosa,** posłanka na Sejm RP
- **Iryna Volnytska,** prezes, SET University, założycielka, IronCyber
- **Rafał Żelazny,** prezes zarządu, Katowicka Specjalna Strefa Ekonomiczna

Moderacja

- **Karolina Markowska,** redaktor naczelna, PulsHR.pl

15 czerwca 2026 r. | 16.00-17.00 | Sala Balowa C | transmisja on-line | tłumaczenie [PL/EN]
Technologie przyszłości. Na co stawiać, aby wygrać?

Świat cyberbezpieczeństwa ewoluuje szybciej niż kiedykolwiek. Sztuczna inteligencja, komputery kwantowe, rozwój chmury obliczeniowej i rynek półprzewodników redefiniują możliwości oraz granice cyfrowej odporności. Od post-kwantowego szyfrowania po automatyzację reakcji na incydenty - nowe technologie przynoszą przełomowe szanse, jak i nieznane ryzyka. Czy wygrani przyszłości to ci, którzy zainwestują w AI i suwerenne chmury, czy ci, którzy postawią na bezpieczeństwo łańcuchów dostaw półprzewodników? Eksperci zastanowią się, które kierunki rozwoju i inwestycji będą kluczowe, by utrzymać lub zyskać przewagę w najbliższej dekadzie.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Rafał Duczmal,** przewodniczący zarządu, EuroHPC Joint Undertaking
- **Filip Kupiński,** Security Services Lead for Poland, Accenture
- **Marek Niezgódka,** dyrektor, Centrum Technologii i Nauk Obliczeniowych, Politechnika Śląska
- **Jan Kozak,** dyrektor, Sieć Badawcza Łukasiewicz – Instytut Sztucznej Inteligencji i Cyberbezpieczeństwa, Łukasiewicz – AI
- **Bianka Siwińska,** prezes, Fundacja Edukacyjna Perspektywy, członek, Rada Cyfryzacji MC, członek, Rada Nadzorcza Creotech Quantum

Moderacja

- **Marcin Piasecki,** redaktor zarządzający, Rzeczpospolita

16 czerwca 2026 | 2 dzień Cybersec

16 czerwca 2026 r. | 09.30-10.30 | Sala Balowa C | transmisja on-line | tłumaczenie [PL/EN]
Państwo, wojsko, biznes - partnerstwo czy rywalizacja o talenty?

Cyberbezpieczeństwo i technologie obronne wymagają najwyższych kompetencji, o które konkurują administracja, siły zbrojne i sektor prywatny. Jak stworzyć model współpracy zamiast rywalizacji o specjalistów? Debata o programach dual career, wspólnych projektach B+R oraz roli uczelni w budowaniu kadr dla bezpieczeństwa państwa i gospodarki.

[video] Rozmowa 1:1 (20')

- **gen. Karol Molenda**, były dowódca, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Adam Dzwonkowski**, Defense & Intelligence Technology Lead, Microsoft
- **mjr rez. Robert Gałązka,** kierownik projektu, Biuro Projektów Polsko-Ukraińskich, Departament Rozwoju, Polska Grupa Zbrojeniowa
- **płk Michał Majewski,** zastępca dyrektora**,** Eksperckie Centrum Szkolenia Cyberbezpieczeństwa
- **Marcin Starzyk**, manager ds. rekrutacji i HR, Rekrut 24
- **Anna Timofiejczuk,** Katedra Podstaw Konstrukcji Maszyn – RMT6 , Politechnika Śląska
- **płk. Jarosław Wacko,** główny specjalista, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni

Moderacja

- **Paweł Szygulski,** zastępca redaktorki naczelnej, WNP.pl

16 czerwca 2026 r. | 09.30-10.30 | Sala Balowa B | transmisja on-line | tłumaczenie [PL/EN]
CISO i CIO pod presją. Wyzwania menadżerow.

Panel poświęcony roli CISO, CIO w organizacji - między odpowiedzialnością operacyjną a oczekiwaniami zarządu. Uczestnicy omówią typowe bolączki komunikacji: jak przekładać ryzyka techniczne na język biznesu, jak budować zaufanie i mandat do działania oraz jak reagować na sytuacje, w których to manager ds. cyberbezpieczeństwa staje się celem ataków (personalnych, wizerunkowych, prawnych). Cyberbezpieczeństwo jako przewaga konkurencyjna, nie koszt.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Andrzej Bartosiewicz,** założyciel, prezes zarządu, Fundacja CISO #Poland
- **Przemysław Dęba,** CISO, Orange Polska
- **Andrzej Jarosz**, dyrektor, Departament ds. IT i Cyberbezpieczeństwa, Koleje Małopolskie
- **Iwona Prószyńska**, kierownik, Zespół ds. Strategicznej Komunikacji Cyberbezpieczeństwa, NASK-PIB
- **Kajetan Przybysz**, CISO, Public Transport Service

Moderacja

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

16 czerwca 2026 r. | 09.30-10.30 | Scena Hol Dolny | transmisja on-line
Cyberbezpieczeństwo w finansach

Bankowość i e-commerce należą do najczęstszych celów cyberprzestępców. Jak chronić transakcje online, wykrywać fraud i reagować na wycieki danych? Debata o nowych trendach w cyberprzestępczości finansowej, ochronie klientów przed scamem oraz o rosnących wymaganiach regulacyjnych, w tym DORA, które redefiniują standardy odporności sektora finansowego. Bezpieczeństwo finansowe. Od wewnętrznych wycieków po walkę ze scamem

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Jarosław Biegański,** Director of the Banking Security Department, Związek Banków Polskich
- **Adam Cieślak,** komendant, Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) w latach 2022-2026
- **Patryk Gęborys,** dyrektor biura cyberbezpieczeństwa, PZU SA
- **Ireneusz Jazownik**, Chief Information Security Officer, IBK Bank Polska
- **Magdalena Korona,** ekspertka ds. cyberbezpieczeństwa, mBank
- **Łukasz Miedziński**, dyrektor obszaru cyberbezpieczeństwa, ING Hubs Poland

Moderacja

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

16 czerwca 2026 r. | 11.00-12.00 | Sala Balowa B | transmisja on-line | tłumaczenie [PL/EN]
Cyberbezpieczeństwo a technologie podwójnego zastosowania: jak wzmocnić polski ekosystem?

Cyber to obszar naturalnie „dual use" - rozwiązania dla wojska szybko trafiają do biznesu i odwrotnie. Jak projektować granty, regulacje i programy wsparcia, by budować silny, konkurencyjny ekosystem cyber w Polsce? Debata o roli państwa, funduszy i partnerstw publiczno-prywatnych oraz o tym, jak skutecznie komercjalizować rodzące się technologie.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Adam Dzwonkowski**, Defense & Intelligence Technology Lead, Microsoft
- **Wojciech Górecki,** ekspert dual-use, Centrum Cyberbezpieczeństwa, Akademia Górniczo-Hutnicza
- **płk Jan Kelner,** dziekan, Wydział Elektroniki, Wojskowa Akademia Techniczna
- **Mariusz Kujawski,** prezes zarządu, ComCERT, Grupa Asseco
- **gen. bryg. rez. Włodzimierz Nowak,** ekspert w dziedzinie cyberbezpieczeństwa

Moderacja

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

16 czerwca 2026 r. | 11.00-12.00 | Sala Balowa C | transmisja on-line | tłumaczenie [PL/EN]
Cyber Resilience Act i certyfikacja: nowe obowiązki, nowe standardy bezpieczeństwa produktów

Cyber Resilience Act przenosi odpowiedzialność za bezpieczeństwo także na producentów i dostawców rozwiązań cyfrowych. Co w praktyce zmienia dla projektowania produktów, zarządzania podatnościami i cyklu życia aktualizacji? Debata o nowych obowiązkach, roli certyfikacji oraz o tym, jak wykorzystać zgodność z regulacjami jako element przewagi konkurencyjnej.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Andrzej Bartosiewicz,** założyciel, prezes zarządu, Fundacja CISO #Poland
- **Andrzej Dulka**, prezes zarządu, Polska Izba Informatyki i Telekomunikacji

- **Jarosław Homa**, pełnomocnik rektora ds. cyberbezpieczeństwa, wicedyrektor, Centrum Cyberbezpieczeństwa, Politechnika Śląska
- **Kinga Pawłowska-Nojszewska,** radca prawny, Kancelaria Prawna MEDIA
- **Wojciech Piszewski,** partner, Sterberg
- **Krzysztof Silicki**, dyrektor ds. Strategicznego Rozwoju Cyberbezpieczeństwa, NASK, Rada Zarządzająca i Rada Wykonawcza ENISA
- **Mikołaj Śniatała,** partner, Andersen
- **Aleksandra Wójtowicz,** analityczka ds. nowych technologii i cyfryzacji, Polski Instytut Spraw Międzynarodowych

Moderacja

- **Karol Tokarczyk**, starszy analityk ds. gospodarki cyfrowej, Polityka Insight

16 czerwca 2026 r. | 11.00-12.00 | Scena Hol Dolny | transmisja on-line
Cyberbezpieczeństwo sektora energetycznego

Energetyka to kręgosłup gospodarki i jeden z głównych celów cyberataków. Jak chronić infrastrukturę krytyczną w dobie transformacji energetycznej, rozwoju OZE i rosnącej cyfryzacji sieci? Debata o nowych technologiach, wykorzystaniu AI, odporności systemów OT/IT oraz o budowie bezpieczeństwa sektora w warunkach presji geopolitycznej i regulacyjnej. AI w energetyce: od predykcji awarii po cyberobronę

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Radosław Dumański,** Ekspert w CERT PSE, Polskie Sieci Elektroenergetyczne SA
- **Mariusz Jurczyk,** prezes zarządu, TAURON Dystrybucja Pomiary, doradca zarządu ds. Inteligentnego Opomiarowania, TAURON Dystrybucja
- **Dariusz Kluska**, dyrektor wykonawczy ds. Bezpieczeństwa, TAURON Polska Energia
- **Tomasz Małecki**, wiceprezes zarządu ds. Strategii, PGE Dystrybucja
- **Aleksandra Walter**, dyrektor, Departament Cyfryzacji i Bezpieczeństwa, Ministerstwo Energii
- **Marek Pisarczyk,** kierownik, Dział Telekomunikacji, Victor Energy

Moderacja

- **Aleksandra Helbin,** redaktor naczelna, WNP.pl

16 czerwca 2026 r. | 12.30-13.30 | Sala Balowa C | transmisja on-line | tłumaczenie [PL/EN]
Edukacja jako tarcza. Sektor naukowy w dobie zmian

Uczelnie stają się elementem krajowego systemu cyberbezpieczeństwa. Jak wdrażać wytyczne KSC w środowisku akademickim - od zabezpieczenia systemów po kształcenie kadr? Debata o programach studiów, szkoleniach wewnętrznych i standardach wdrożeniowych oraz o tym, jak pogodzić wymagania regulacyjne z realnymi możliwościami organizacyjnymi szkół wyższych. Wdrażanie KSC w praktyce. Jak wygląda rola CISO w dużej organizacji akademickiej? Nauka i kompetencje dla cyfrowej autonomii. Od badań do technologii. Cybersuwerenność zaczyna się od silnego zaplecza naukowego i odpowiednich kompetencji.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Krystian Mączka,** inspektor ochrony danych osobowych, Audytor Wewnętrzny SZBI, Dział Bezpieczeństwa Informacji i Ochrony Danych Osobowych, Akademia WSB
- **Tomasz Miłkowski,** generał brygady Służby Ochrony Państwa w stanie spoczynku, dyrektor, Instytut Nauk o Bezpieczeństwie, Akademia Humanitas
- **Marek Pawełczyk,** rektor, Politechnika Śląska
- **Paweł Słoń,** ekspert ds. współpracy, Centrum Cyberbezpieczeństwa, Akademia Górniczo-Hutnicza
- **Michał Szczerbowski**, inspektor ochrony danych, Uniwersytet Ekonomiczny w Katowicach

Moderacja

- **Karolina Markowska,** redaktor naczelna, PulsHR.pl

16 czerwca 2026 r. | 12.30-13.30 | Sala Balowa B | transmisja on-line | tłumaczenie [PL/EN]
Cyberdyplomacja a polska odwaga. Czy Polska może eksportować cyberbezpieczeństwo?

Czy Polska ma potencjał, by stać się eksporterem technologii i usług cyberbezpieczeństwa? Funduszy i instytucje wsparcia, rola kapitału, kompetencje menedżerskich. Jak budować globalne ambicje polskich firm i tworzyć nowe sektory oparte na wysokich technologiach?
Polska branża cybersec - szansa dla inwestorów, biznesu i startupów. Cyberbezpieczeństwo to jeden z najszybciej rosnących segmentów rynku technologii. Gdzie są dziś nisze dla startupów, czego oczekują inwestorzy i jakie bariery hamują skalowanie polskich firm? Debata o wykorzystaniu programów publicznych i unijnych, ekspansji zagranicznej oraz budowie silnej, rozpoznawalnej marki polskiego cyber na świecie.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **[online] Michał Baranowski,** podsekretarz stanu, Ministerstwo Rozwoju i Technologii
- **Artur Bicki,** prezes, Energy Logserver
- **Łukasz Gawron**, prezes zarządu, Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland
- **Paweł Hansdorfer**, dyrektor rynków zagranicznych, Asseco Data Systems
- **dr Joanna Pawełek-Mendez,** radca-minister ds. cyberbezpieczeństwa, Departament Polityki Bezpieczeństwa, Ministerstwo Spraw Zagranicznych

Moderacja

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

16 czerwca 2026 r. | 12.30-13.30 | Scena Hol Dolny | transmisja on-line
Cyberbezpieczeństwo ochrony zdrowia
Sektor zdrowia należy do najbardziej wrażliwych na cyberzagrożenia. Jak chronić dane medyczne, systemy szpitalne i urządzenia medyczne w erze telemedycyny i AI w diagnostyce? Debata o odporności placówek na cyberincydenty, ciągłości działania oraz o standardach bezpieczeństwa, które muszą nadążać za cyfryzacją ochrony zdrowia. Cyberkaretka. SOC sektora.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Krzysztof Brud,** współzałożyciel, doradca zarządu, ekspert w obszarze jakości oprogramowania, Soflab Technology
- **Janusz Cieszyński**, poseł na sejm RP, minister cyfryzacji w 2023 r., podsekretarz stanu w ministerstwie zdrowia w latach 2018-2020
- **Rafał Lityński,** ekspert sektorowego CSIRT CeZ
- **Klaudia Rogowska,** dyrektorka, Górnośląskie Centrum Medyczne im. prof. Leszka Gieca Śląskiego Uniwersytetu Medycznego w Katowicach
- **Anna Sibilska,** dyrektorka, Biuro Bezpieczeństwa Informacji i Ciągłości Działania, Narodowy Fundusz Zdrowia
- **Małgorzata Wywrot**, Project Managerka, NIL IN - Sieć Lekarzy Innowatorów, Naczelna Izba Lekarska, Szkoła Zdrowia Publicznego CMKP
- **Michał Zabojszcz,** dyrektor, Samodzielny Publiczny Zakład Opieki Zdrowotnej Ministerstwa Spraw Wewnętrznych i Administracji w Krakowie

Moderacja

- **Klara Klinger,** redaktorka naczelna, Rynek Zdrowia

16 czerwca 2026 r. | 14.30-15.30 | Sala Balowa C | transmisja on-line | tłumaczenie [PL/EN]
Smart city. Jak technologie zmienią miasta?
NIS2, IoT i krkry komunalna. Wodociągi, transport, energetyka i IoT miejskie stają się celem zaawansowanych ataków. Jak JST powinny wdrażać NIS2, zarządzać ryzykiem dostawców i aktualizacjami systemów? Debata o praktycznych scenariuszach reagowania, cyberhigienie i priorytetach inwestycyjnych w inteligentnych miastach.

Rozmowa 1:1 (15')

- **Jacek Woźnikowski**, dyrektor Departamentu Rozwoju Społeczno-Gospodarczego i Współpracy, Górnośląsko-Zagłębiowska Metropolia
- **Aneta Kaczmarek,** redaktor naczelna, Portalsamorzadowy.pl

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Agnieszka Olbrycht-Banach,** prezes zarządu, Śląska Sieć Metropolitalna
- **Marcin Staniek,** prorektor ds. współpracy z otoczeniem społeczno-gospodarczym, Politechnika Śląska
- **Ewelina Włoch**, Naczelnik Wydziału Cyfryzacji i Nowych Technologii, Urząd Miasta Rybnika
- **Łukasz Żółciak,** oficer ds. Smart City, Wydział Obsługi Inwestorów, Urząd Miasta Katowice
- **Katarzyna Żółkiewska–Malicka,** Chief Security Officer (CSO), Uniwersytet Marii Curie Skłodowskiej w Lublinie

Moderacja

- **Aneta Kaczmarek,** redaktor naczelna, Portalsamorzadowy.pl

16 czerwca 2026 r. | 14.30-15.30 | Sala Balowa B | transmisja on-line | tłumaczenie [PL/EN]
Cyberbezpieczeństwo przemysłu
Od Security by Design po reakcję na incidenty**.** Cyfryzacja produkcji sprawia, że bezpieczeństwo systemów OT staje się kluczowe dla ciągłości działania gospodarki. Jak chronić środowiska przemysłowe - od energetyki po logistykę - zgodnie z normą IEC 62443 i zasadą Security by Design? Debata o separacji IT/OT, budowie SOC/MDR, reagowaniu na incydenty oraz o tym, jak bezpieczeństwo może wzmacniać konkurencyjność firm.

Do udziału w debacie zostali zaproszeni (kolejność alfabetyczna):

- **Dawid Bazan,** Cybersecurity Lead Architect, Stellantis
- **Waldemar Chlebik,** Head of Cyber Security, Siemens
- **Mikołaj Śniatała**, partner, Andersen
- **Dawid Wachowiak**, dyrektor ds. transformacji cyfrowej i IT, TDJ
- **Zuzanna Wieczorek**, prezes zarządu, Tekniska Polska Przemysłowe Systemy Transmisji Danych Sp. z o. o.

Moderacja

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