RAMY PROGRAMOWE
KBP TOTAL SECURITY WARSZAWA 2025

ŁĄCZNOŚĆ I INFRASTRUKTURA CYFROWA - STRATEGICZNE WYZWANIA DLA PAŃSTWA

- Strategia cyfryzacji i cyberobrony RP – jak budować długofalową odporność państwa na zakłócenia i ataki?
- System bezpiecznej łączności państwowej
- Zastosowanie satelitów w systemach łączności wojskowej i cywilnej - dual-use
    - Monitorowanie zagrożeń i sytuacji kryzysowych dzięki obserwacji satelitarnej
- Bezpieczeństwo i suwerenność technologiczna – jak państwo powinno inwestować w budowę własnej infrastruktury łączności krytycznej?
- Standardy, interoperacyjność i rekomendacje - jaka powinna być rola Państwa w tworzeniu standardów komunikacji i łączności w miastach?
- Odporność infrastruktury na cyberzagrożenia – blackouty, zakłócenia łączności, ataki hybrydowe – jak przygotować się na scenariusze wysokiego ryzyka?

SATELITY - ROZPOZNANIE OBRAZOWE

- Rozwój technologii satelitarnych jako współczesny kluczowy element bezpieczeństwa narodowego i obronności państwa
- Local content: rozwój rodzimych systemów satelitarnych i zwiększenie niezależności technologicznej
    - Wsparcie projektów satelitarnych i rozwijanie kompetencji w zakresie projektowania, produkcji i eksploatacji satelit.
- Znaczenie satelit optoelektronicznych i SAR w monitoringu granic, komunikacji i wczesnym ostrzeganiu
- Technologiczne wyzwania integracji danych z satelitów z informacjami z dronów, radarów i systemów lądowych
- Sojusznicze projekty satelitarne i możliwości włączenia do nich Polski
- Ochrona satelit przed zakłóceniami, cyberatakami oraz fizycznymi zagrożeniami
- Technologie satelitarne podwójnego zastosowania (synergia technologiczna AI, drony, systemy komunikacji)

KIERUNKI NA 2025+
PRZEMYSŁ ZBROJENIOWY JAKO FILAR BEZPIECZEŃSTWA

- Równoważenie zakupów zagranicznych z rozwojem własnych kompetencji i technologii w celu budowania niezależności przemysłowej
- Kluczowe kierunki i wyzwania dla inwestycji państwowych oraz strategii rozwoju przemysłu zbrojeniowego w Polsce
- Priorytety państwowych inwestycji i reform – co zrobić, żeby polska zbrojeniówka stała się globalnym graczem?
- Analiza wpływu konfliktu na Ukrainie na tempo modernizacji i oczekiwania wobec krajowego sektora zbrojeniowego
- Rola sektora prywatnego i start-upów w modernizacji i elastyczności produkcji wojskowej
- Konsolidacja i współpraca sektora publicznego i prywatnego (PPP)

FINANSOWANIE ZEWNĘTRZNE, PPP A SUWERENNOŚĆ TECHNOLOGICZNA PAŃSTWA POLSKIEGO

- Strategiczne inwestowanie w rozwój suwerennych technologii przez państwo jako fundament bezpieczeństwa narodowego
- Tworzenie nowych programów inwestycyjnych w technologie cyfrowe, militarne, przemysłowe
- Repolonizacji przemysłu zbrojeniowego
    - budowa suwerenności technologicznej jako konieczność w obliczu globalnych zagrożeń i zależności
- Problemy zakupowe i wymagania PZP w kontekście szybkiego wdrażania rozwiązań z zakresu cyberbezpieczeństwa
- Dostępność i pozyskiwanie środków na rozwój bezpieczeństwa. Jak informować firmy o możliwościach finansowania?
- Budowanie synergii publiczno-prywatnej. Współpraca PPP
- Rekordowy budżet MON i Funduszu Wsparcia Sił Zbrojnych - pierwsze podsumowanie

W CENTRUM ODPORNOŚCI – ZARZĄDZANIE I KOMUNIKACJA W SYTUACJACH KRYZYSOWYCH

- Lessos learn - Komunikacja kryzysowa - wnioski z doświadczeń
- Gotowość instytucji na czas wojny. Testowanie i standaryzacja procedur reagowania na incydenty wysokiego ryzyka i ciągłości działania (wojna, cyberataki, sabotaż, dezinformacja)
- Zagrożenia hybrydowe, dezinformacja i zespoły zarządzania kryzysowego
- Współpraca z cyberwojskiem i budowa narodowego cyberlegionu i cyberpoligonu
- CISO jako kluczowy element odporności organizacyjnej. Integracja z BCP, zarządami i strategią cyber

- Wzmocnienie współpracy cywilno-wojskowej (CIMIC) i planów ciągłości działania (BCP)

OD INNOWACJI DO WDROŻENIA. SKALOWANIE TECHNOLOGII OBRONNYCH

- Od prototypu do seryjnej produkcji. Wyzwania procesu integracji innowacji dla potrzeb Sił Zbrojnych RP
- Ekosystem innowacji dla obronności. Jak poprawić współpracę pomiędzy startupami, uczelniami, przemysłem i instytucjami państwowymi?
- Współpraca międzynarodowa w rozwoju technologii obronnych
- Rola programów pilotażowych i testów operacyjnych w ocenie przydatności rozwiązań defence tech
- Technologie podwójnego zastosowania - jednoczesne zastosowanie cywilnie i militarnie (AI, drony, systemy komunikacji)

CYBERBEZPIECZEŃSTWO W CZASACH AI. NOWE ATAKI I ŚWIADOMOŚĆ SPOŁECZNA

- AI a cyberbezpieczeństwo - wyzwania techniczne i wpływ na kluczowe sektory gospodarki
- Jak rozwój AI zmienia sektor cyberbezpieczeństwa i cyberzagrożenia?
- Nowe zagrożenia cyfrowe i jak się na nie przygotować - deepfake i cyberoszustwa napędzane AI - jak skutecznie zarządzać ryzykiem?
- Jak bezpiecznie podchodzić do wdrożeń AI? Budowanie świadomości społecznej
- Multidyscyplinarność – łączenie wiedzy technicznej, biznesowej i społecznej w walce z cyberzagrożeniami
- AI w technologiach podwójnego zastosowania

OD POTRZEB PRODUKCYJNYCH DO GOTOWOŚCI BOJOWEJ - ZBROJENIÓWKA W DZIAŁANIU

- Przemysł zbrojeniowy wobec rosnących potrzeb operacyjnych Sił Zbrojnych - gotowość produkcyjna i logistyka dostaw
- Eksport polskiego uzbrojenia. Szanse, ograniczenia i strategie wejścia na rynki zagraniczne
- Dialog: wojsko - nauka - przemysł
- Transparentny i efektywny proces zakupowy jako fundament szybkiego wyposażenia Sił Zbrojnych RP – realizacja zamówień, wsparcie krajowego przemysłu obronnego oraz zapewnienie zgodności technologicznej i jakościowej z wymaganiami operacyjnymi
- Zdolność przemysłu do działania w sytuacjach kryzysowych - bezpieczeństwo dostaw, rezerwy produkcyjne, elastyczność

TECHNOLOGIE PRZYSZŁOŚCI

- Technologie dual use (synergia technologiczna drony, AI, systemy komunikacji)
- Jak nowe technologie zmieniają podejście do ochrony organizacji? Zastosowania AI, automatyzacji i analizy danych w systemach bezpieczeństwa
- Dywersyfikacja ryzyka technologicznego i ograniczanie zależności od zewnętrznych dostawców
- Jak zagwarantować dostęp do kluczowych technologii w czasie zagrożeń, kryzysów i wojny?
- Outsourcing cyberbezpieczeństwa
- Testowanie odporności organizacji w praktyce - red teaming, symulacje ataków i automatyczne sprawdzanie gotowości na kryzysy
- Bezpieczeństwo w procesie tworzenia i wdrażania systemów IT. Jak pomóc ograniczać błędy i luki?