

## Stanowisko Rady do Spraw Cyfryzacji w sprawie rozwoju technologii przełomowych.

W ostatnim czasie jesteśmy świadkami przyspieszenia w zakresie wyścigu technologicznego wykorzystującego technologie przełomowe, takie jak sztuczna inteligencja i rozwiązania komputerów kwantowych. Wyścig ten dotyczy nie tylko gospodarki cywilnej, ale również wiąże się z intensyfikacją wyścigu zbrojeń z wykorzystaniem technologii przełomowych w sferze militarnej, co ma kolosalne znaczenie w zakresie zwiększania zdolności obronnych i bezpieczeństwa narodowego. Trend ten będzie w jeszcze większym stopniu zwiększać globalne zapotrzebowanie na rozwiązania oparte o technologię sztucznej inteligencji, jak i popyt na komponenty niezbędne do jej rozwoju, w tym mikroprocesory. Zatem, technologie takie jak sztuczna inteligencja mają krytyczne znaczenie dla zwiększenia zdolności militarnych państw, w tym w operacjach wielodomenowych, które charakteryzować będą współczesne konflikty zbrojne. Umożliwiają one bowiem nie tylko lepszą analitykę danych kluczową dla funkcjonowania nowoczesnych systemów dowodzenia i kierowania oraz stanowiącą podstawę świadomości sytuacyjnej w czasie rzeczywistym, usprawnienie procesów decyzyjnych na poziomie strategicznym, czy też integrację systemów, w tym w ramach platform obsługujących samoloty F35, ale również zwiększenie autonomii działań bojowych. Sztuczna inteligencja jest także kluczową technologią, która w coraz większym zakresie wspierać będzie działania defensywne w cyberprzestrzeni. Dzięki zastosowaniu zaawansowanych algorytmów AI możliwe jest wykrywanie i neutralizowanie cyberzagrożeń w czasie rzeczywistym. AI może wspierać tworzenie i realizację strategii ofensywnych w cyberprzestrzeni, co w nowoczesnych konfliktach jest równie istotne. Z tego względu Polska powinna jasno wyartykułować swoje ambicje w zakresie modernizacji sił zbrojnych RP i integracji technologii sztucznej inteligencji, obejmujących zarówno tradycyjne rodzaje sił zbrojnych, jak i nowopowstałe wojska obrony cyberprzestrzeni czy wojska dronowe.

W opinii Rady ds. Cyfryzacji Polska powinna zabiegać o status kraju partnerskiego Stanów Zjednoczonych w zakresie rozwoju innowacji technologicznych, co byłoby zgodne z założeniami strategii rozwoju Departamentu Innowacji (DIU 3.0) w Departamencie Obrony Stanów Zjednoczonych, która zakłada wsparcie krajów sojuszników w ramach partnerstw technologicznych.

Niestety z niepokojem obserwujemy odpływ polskich naukowców, ekspertów i managerów technologii przełomowych, którzy nie znajdują w naszym kraju wystarczająco atrakcyjnych warunków dla zatrudnienia oraz warunków dla twórczej pracy. Rekomendujemy uruchomienie projektów publiczno-prywatnych wykorzystujących przełomowe technologie dla rozwiązania konkretnych problemów społecznych i gospodarczych.

Z uwagi na ograniczone zasoby kompetencyjne, infrastrukturalne i finansowe, rekomendujemy budowanie ekosystemu wokół najmocniejszych wybranych ośrodków naukowo-badawczych, które mają potencjał tworzenia synergii i skalowania.

Mając na względzie tworzenie optymalnych warunków dla długotrwałego i stabilnego rozwoju oraz wzrostu konkurencyjności polskiej gospodarki w oparciu o najbardziej zaawansowaną myśl ekspercką, naukową i techniczną, za szczególnie ważne uznajemy stworzenie warunków dla rozwoju polskich kadr technologicznych i tworzenie warunków dla rozwoju naukowego, a także udziału w projektach, które dają dostęp do najnowocześniejszej wiedzy i bazy materialnej z najnowszymi wielkoskalowymi superkomputerami (HPC), w tym dostępem do danych. Z tego względu konieczne jest rozwijanie strategicznej współpracy cywilno-militarnej z zaangażowaniem krajowych uniwersytetów technologicznych posiadających odpowiednią infrastrukturę naukowo-badawczą. Należy także zwiększyć zdolność do pozyskiwania danych o polu walki, ich gromadzenia, przetwarzania w ramach bezpiecznego środowiska danych (data lab), a także ich analizy i przekształcania za pomocą technik anonimizacji i "maskowania" danych w odpowiednio zabezpieczone i "zaufane" zbiory danych do trenowania algorytmów sztucznej inteligencji. Tego typu działania pozwolą udostępniać takie bazy danych w sposób szybki, skalowalny i bezpieczny dla innowatorów (zespołów naukowo-badawczych, start-upów) w celu zwiększenia wydajności i szybkości procesu akceleracji rozwiązań technologicznych opartych na algorytmach sztucznej inteligencji w celu wsparcia procesu rozwoju innowacyjnych technologii dla bezpieczeństwa i obronności, w tym technologii podwójnego-zastosowania.

Za szczególnie ważne uznajemy zarówno wykorzystywanie tego co już jest w polskich zasobach, tu należy podkreślić przykładowo dorobek NCBR IDEAS. Koniecznym jest stworzenie tego typu podmiotom optymalnych warunków rozwoju.

Wraz z powstaniem społeczeństwa informacyjnego i dążeniem do zapewnienia cyberbezpieczeństwa widać konieczność rozwoju technologii, który zostanie ukierunkowany intensywnie na obszar badań w zakresie cyberbezpieczeństwa. Kluczowe w tym przypadku są prawa niematerialne, które stają się coraz cenniejsze – tak w środowisku cywilnym, jak i militarnym. Uczelnie, z uwagi na swoje potrzeby powinny dążyć do zabezpieczenia praw autorskich i praw własności przemysłowej swoich pracowników i studentów, tak aby wszystkie wymienione strony uzyskały wymierne korzyści dla Państwa, ale także ekonomiczne dla samych twórców.

Celem komercjalizacji wyników badań i prac rozwojowych jest identyfikacja ich aspektów komercyjnych, czyli określenie stopnia zapotrzebowania, obszaru zainteresowania, grup docelowych, bezpośredniego odbiorcy. Ustalona organizacja współpracy międzyresortowej z organizacjami akademickimi i uniwersyteckimi powinna umożliwić bezpośrednie wykorzystywanie wyników badań i prac rozwojowych w życiu społecznym na rzecz cyberbezpieczeństwa i obronności w cyberprzestrzeni.

Dla zagranicznych uczelni, szczególnie amerykańskich i zachodnioeuropejskich współpraca z administracją publiczną jest podstawowym (obok kształcenia i badań) elementem ich działalności. Od lat angażowane są w strategiczne działania państwa w zakresie budowy innowacyjnego potencjału gospodarczego, w tym sektora bezpieczeństwa i obronności. Podstawowym warunkiem takiej współpracy jest zadbanie o ochronę własnej wiedzy, która w

wymianie nauka-gospodarka jest formą towaru. Dlatego też systemy ochrony własności intelektualnej rozwijane i doskonalone są od wielu lat. Odwołując się do analizy stanu aktualnej sytuacji należy podkreślić potrzebę usprawnienia poprzez wdrożenie najbardziej skutecznych mechanizmów na poziomie centralnym i regionalnym. Zdolność do tworzenia i absorbowania innowacji jest największym wyzwaniem obecnego wieku. Tak więc podstawy współczesnej konkurencji budowane są przez firmy zdolne do realizacji, nabywania i wdrażania innowacji. Podaż innowacji wymaga sprawnego systemu wsparcia za pośrednictwem instytucji okołobiznesowych, w tym profesjonalnych inkubatorów i akceleratorów, których powstanie na uczelniach wyższych powinno być wspierane przez państwo. Dla ośrodków działających w sferze innowacji i nowych technologii niezwykle ważna jest współpraca ze wszystkimi aktorami ekosystemu innowacji, w tym instytucjami publicznymi. Lista znaczących aktorów wciąż się poszerza, gdyż komercjalizacja i transfer technologii coraz częściej postrzegane są jako wielopłaszczyznowe i wielokierunkowe działania przy współudziale sektora publicznego, prywatnego, społeczeństwa, brokerów (takich jak parki, inkubatory) oraz jednostek samorządu terytorialnego.

Wobec powyższego, rekomendujemy opracowanie uwarunkowań organizacyjnych i biznesowych do tworzenia CyberParku technologicznego, który ma stanowić platformę współpracy nauki, przemysłu (rynku), administracji publicznej i sfery militarnej, wykorzystującą potencjał intelektualny w zakresie współpracy zmierzającej do wytwarzania narzędzi dla pełnego spektrum działania w zapewnieniu cyberbezpieczeństwa oraz rozwoju innowacji w Polsce. Kluczowym elementem CyberParku byłby transfer wiedzy i technologii między uczestniczącymi w nim podmiotami, prowadzący do tworzenia, pozyskiwania i wdrażania nowych technologii z zakresu cyberbezpieczeństwa. Należy przy tym podkreślić, iż CyberParki technologiczne są formułą i celem zapewnienia przepływu wiedzy i technologii także podwójnego zastosowania pomiędzy jednostkami naukowymi a przedsiębiorcami. Najistotniejszą wartością CyberParku technologicznego jest szeroko pojęta współpraca międzyresortowa i międzysektorowa, która stanowi podstawę dla rozwoju systemu bezpieczeństwa Państwa w cyberprzestrzeni.