prof. dr hab. Grzegorz SOBOLEWSKI
Akademia Pożarnicza w Warszawie

Warszawa, dnia 21.02.2024 r.

RECENZJA

osiągnięć naukowych Pana dr. inż. Roberta Adama JANCZEWSKIEGO
w postępowaniu o nadanie stopnia naukowego doktora habilitowanego w dziedzinie nauk społecznych w dyscyplinie nauki o bezpieczeństwie

1. Podstawowe dane o Kandydacie

Pan dr inż. Robert Adam Janczewski jest absolwentem Wyższej Szkoły Łączności i Informatyki, którą ukończył w 1996 r., uzyskując stopień inżyniera telekomunikacji. Następnie studiował w Politechnice Warszawskiej, gdzie w 2001 r. uzyskał stopień magistra inżyniera telekomunikacji. W toku pracy zawodowej Kandydat stale podnosi kwalifikacje i rozwija swoje zainteresowania naukowe przez uczestnictwo w wielu kursach specjalistycznych. Stopień doktora nauk społecznych w dyscyplinie nauki o obronności uzyskał na Wydziale Zarządzania i Dowodzenia Akademii Obrony Narodowej w 2016 r., na podstawie rozprawy doktorskiej: *Procesy informacyjne w rozpoznaniu elektronicznym Wojsk Lądowych Sił Zbrojnych Rzeczypospolitej Polskiej*.

Kariera naukowo-dydaktyczna Pana dr. inż. Roberta Adama Janczewskiego związana jest z wieloma uczelniami, które prowadziły badania i studia w zakresie szeroko pojętego cyberbezpieczeństwa. Jako nauczyciel akademicki uzyskiwał doświadczenie, współpracując między innymi z:

- Wyższą Szkołą Biznesu i Zarządzania w Ciechanowie, w latach 2002–2005 prowadził zajęcia z zakresu informatyki w każdym roku akademickim, na podstawie umowy zlecenia;
- Uniwersytetem Warmińsko-Mazurskim w Olsztynie, w latach 2018–2021 prowadził zajęcia z przedmiotu informatyczne systemy bezpieczeństwa na Wydziale Nauk Społecznych Instytutu Nauk Politycznych, na podstawie umowy zlecenia;
- Akademią Sztuki Wojennej w Warszawie, w latach 2018–2019 na stanowisku adiunkta w Zakładzie Cyberbezpieczeństwa w Instytucie Działań Informacyjnych na Wydziale Wojskowym;
- Wyższą Szkołą Policji w Szczytnie, od 2019 r. prowadzi zajęcia w zakresie informatyki na Wydziale Bezpieczeństwa i Nauk Prawnych;

– Państwową Uczelnią Zawodową im. Ignacego Mościckiego w Ciechanowie, w latach 2020–2023 na stanowisku adiunkta w Zakładzie Informatyki na Wydziale Inżynierii i Ekonomii;
– Państwową Akademią Nauk Stosowanych im. Ignacego Mościckiego w Ciechanowie, od 2023 r. na stanowisku adiunkta w Zakładzie Informatyki Wydziału Inżynierii i Ekonomii;
– Akademią Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni, w latach 2020–2022 jako główny specjalista w Morskim Centrum Cyberbezpieczeństwa na Wydziale Dowodzenia i Operacji Morskich; prowadził zajęcia m.in. na studiach MBA, podyplomowych w zakresie cyberbezpieczeństwa.

2. Ocena osiągnięć naukowych

Habilitant wskazał jako osiągnięcie naukowe monografię: R. Janczewski, *Cyberwalka. Militarny wymiar działań,* Warszawa 2023, ISBN: 978-83-01-23085-2. Przedstawiona do oceny publikacja jest monografią naukową, liczy 431 stron i została opublikowana przez Wydawnictwo Naukowe PWN w Warszawie.

Wraz z dynamicznym rozwojem nowych technologii zmieniło się też postrzeganie cyberprzestrzeni. Obecnie to nieograniczona wirtualna przestrzeń, w której połączone siecią komputery i inne media cyfrowe (telefony, tablety, radio, telewizja) pozwalają nam lepiej funkcjonować. Nowe technologie codziennie wykorzystujemy w komunikacji między sobą, w funkcjonowaniu wielu elementów infrastruktury krytycznej państwa, zarządzaniu i kierowaniu wieloma organizacjami i przedsiębiorstwami. Skala potencjalnych form działań wymierzonych w bezpieczeństwo państwa jest tak szeroka, że zasadne jest postrzeganie bezpieczeństwa cybernetycznego jako transsektorowego obszaru bezpieczeństwa, a ochrona cyberprzestrzeni stała się ważnym prorytetem wielu państw i organizacji międzynarodowych. Państwa, organizacje międzynarodowe i inne podmioty bezpieczeństwa zrozumiały, że stabilność funkcjonowania i rozwój globalnego społeczeństwa uzależniona jest od skutecznego przeciwdziałania i reagowania na zagrożenia cybernetyczne.

Cyberprzestrzeń stała się też przestrzenią walki zbrojnej we współczesnych konfliktach. Współczesne siły zbrojne powinny posiadać zdolność do prowadzenia cyberwalki, jako formy działań militarnych, które mogą przyczyniać się do wygrywania wojen bez zbędnego narażania życia własnych żołnierzy i sprzętu. Cyberwalka jako militarny wymiar działań może oznaczać też zagrożenia z dowolnego miejsca na świecie ze strony państw lub podmiotów niepaństwowych, które unikają otwartego konfliktu lub nie są w stanie przeprowadzić konwencjonalnego ataku.

Habilitant odniósł się do bardzo ważnego obecnie problemu, jakim jest znaczenie cyberwalki we współczesnych działaniach militarnych oraz zidentyfikowanie uwarunkowania skutecznych działań sił zbrojnych w wirtualnym wymiarze. Podzielam motywację Habilitanta, że cyberwalka jako militarny wymiar działań, w narodowym ujęciu, nie posiada jednoznacznego desygnatu oraz jego charakterystyki. Źródła poruszające tematykę cyberwalki w znaczeniu ogólnym nie są zgodne w opisie cyberwalki jako militarnego wymiaru działań. Obecnie w piśmiennictwie istnieje tendencja do utożsamiania cyberwalki

z istniejącymi aspektami studiów nad bezpieczeństwem, bez podejmowania nad nią dociekań naukowych i formułowania kompleksowej teorii.

Dlatego, mając na uwadze przywołane wcześniej fakty oraz aktualne potrzeby poszukiwania skutecznej koncepcji prowadzenia działań militarnych w cyberprzestrzeni, z osobistą satysfakcją (przez kilkanaście lat naukowo i dydaktycznie zajmowałem się problematyką działań militarnych sił zbrojnych), przyjąłem wyzwanie zrecenzowania osiągnięcia naukowego Pana dr. inż. Roberta Adama Janczewskiego, *Cyberwalka. Militarny wymiar działań.*

Przyjęte założenia badawcze, których konsekwencją są uzyskane wyniki badań i treść ocenianej monografii, zawarto we wstępie, w części dotyczącej metodologii badań. Przedstawiając uzasadnienie wyboru tematu (sytuację problemową), Habilitant w sposób czytelny uzasadnił potrzebę podjęcia badań na temat przyjęty w tytule monografii, wskazał przedmiot i cel badań, przedstawił problemy i hipotezy badawcze. Tu na uwagę zasługuje przemawiająca do czytelnika sytuacja problemowa, związek poprawnie sformułowanych celów badawczych z tą sytuacją, tematem monografii, określonymi problemami i hipotezami badawczymi.

W ujęciu ogólnym przedmiotem badań uczyniono cyberwalkę jako militarny wymiar działań. Autor słusznie dostrzega złożoność zjawiska i potrzebę nakreślenia jednolitego obszaru badawczego. Składniki tematu monografii tworzą desygnat wieloczłonowego pojęcia cyberwalki jako militarnego wymiaru działań. Celem zasadniczym dociekań naukowych było *zidentyfikowanie cyberwalki jako militarnego wymiaru działań.* Do osiągniecia tego celu Habilitant ambitnie sformułował aż sześć celów szczegółowych:

- *zidentyfikowanie uwarunkowań cyberwalki jako militarnego wymiaru działań;*
- *zbadanie przestrzeni determinującej prowadzenie cyberwalki przez siły zbrojne;*
- *określenie podstaw teoretycznych cyberwalki jako militarnego wymiaru działań;*
- *zidentyfikowania uwarunkowań skuteczności cyberwalki jako militarnego wymiaru działań;*
- *zidentyfikowanie zasadniczych działań sił zbrojnych w cyberwalce;*
- *dokonanie analizy i oceny wpływu otoczenia na zdolności sił zbrojnych do prowadzenia cyberwalki.*

Habilitant podjął się rozwiązania istotnego współcześnie problemu badawczego, wyrażonego w pytaniu: *jakie cechy charakteryzują cyberwalkę jako militarny wymiar działań?* Następnie Habilitant dokonał poprawnej dekompozycji problemu głównego i w konsekwencji sformułował sześć problemów szczegółowych oraz odpowiednio sprecyzował hipotezy robocze, które stanowiły logiczną podstawę przeprowadzenia badań będących w obszarze jego dociekań naukowych. Rozwiązanie polegające na formułowaniu hipotez w odniesieniu do problemu głównego, jak i do przyjętych szczegółowych problemów badawczych, należy uznać za bardzo dojrzałe metodologicznie i sprawia, że założenia badawcze przyjęte przez Habilitanta stają się bardziej czytelne. Korelacje sformułowanych problemów badawczych i przyjętych hipotez są klarowne i na ogół trafne.

Dokonując podsumowania założeń metodologicznych, należy ocenić, że tytuł recenzowanej monografii, założone cele badań, sformułowane problemy badawcze i założenia hipotetyczne oraz przyjęte do ich rozwiązania metody łączą przejrzyste

i spójne relacje logicznego wynikania, a jednocześnie pozostają ze sobą w jasnym, nienagannym związku przyczynowo-skutkowym. Przedłożona do oceny praca jest niewątpliwie dziełem naukowym odpowiadającym pod względem sformułowanych założeń badawczych i zastosowanych metod badawczych wymogom stawianym monografiom naukowym. Przyjęte założenia metodologiczne pozwoliły uzyskać udokumentowany materiał teoretyczny o cennych walorach poznawczych.

Podsumowując ocenę metodologiczną przyjętych założeń badawczych, mogę z pełnym przekonaniem stwierdzić, że wysoko oceniam wartość sprecyzowanych założeń badawczych, co świadczy o dużej wiedzy i dobrym warsztacie metodologicznym Habilitanta.

Struktura pracy obejmuje wstęp wraz z elementami metodologii badań, sześć logicznie powiązanych rozdziałów merytorycznych, zakończenie i bibliografia. Na podkreślenie zasługuje bogaty zasób literatury, w tym obcojęzycznej oraz wartościowe wnioski podsumowujące każdy rozdział.

W pierwszym rozdziale Habilitant przedstawił wyniki badań w zakresie uwarunkowań cyberwalki jako militarnego wymiaru działań. Badania wykazały, że rozwój techniczny i technologiczny społeczeństw oraz wzrost znaczenia teleinformatyki we współczesnej przestrzeni walki przyczynia się do jej skuteczności, co spowodowało konieczność zbudowania przez siły zbrojne zdolności do prowadzenia cyberwalki. Na przykładzie przeprowadzonych przez Rosję działań militarnych przeciwko Estonii, Gruzji i Ukrainie w 2014 r. została przedstawiona ewolucja cyberdziałań. Szczególną rolę w uwarunkowaniach cyberwalki jako militarnego wymiaru działań Autor słusznie przypisuje wrogim cyberdziałaniom, czyli działaniom prowadzonym z wykorzystaniem cyberprzestrzeni, które prowadzone pod dowództwem wojskowym stanowią militarny wymiar działań.

W kolejnym, drugim rozdziale, Autor przedstawia wyniki badań w zakresie rozwiązania drugiego problemu badawczego. Odpowiada na pytanie: *jaka przestrzeń determinuje prowadzenie cyberwalki przez siły zbrojne?* W rezultacie rozdział ten poświęcony jest identyfikacji przestrzeni cyberwalki prowadzonej przez siły zbrojne. Habilitant z powodzeniem dowodzi, że cyberprzestrzeń stwarza warunki do prowadzenia cyberdziałań militarnych. Charakterystyka cyberśrodowiska pozwala na zbudowanie dla cyberwalki jako militarnego wymiaru działań modelu systemu C-T-O, czyli człowiek-technika-otoczenie. Habilitant określa, że system ten tworzą trzy elementy oraz istniejące między nimi zależności. W cyberwalce rolę otoczenia (O) człowieka (C), czyli żołnierza ją prowadzącego, spełnia właśnie jego cyberśrodowisko. Natomiast technika (T) to wszystko to, co służy żołnierzowi do wykonania powierzonego mu zadania. Rozdział dopełniają wyniki badań poświęcone cyberzagrożeniom w kontekście funkcjonowania resortu obrony narodowej i sił zbrojnych w cyberprzestrzeni. Zaprezentowano także podział takich zagrożeń i scharakteryzowano główne ich rodzaje. Habilitant przedstawia autorskie podejście do formułowania cyberzagrożeń przez wrogi podmiot, jako zdolność do połączenia trzech czynników. Pierwszy to zamiar, czyli chęć złośliwego podmiotu do przeprowadzenia cyberataku na wybrany system; drugi, to zdolność, czyli posiadanie umiejętności zasobów niezbędnych do przeprowadzenia cyberataku (np. specjalistycznego oprogramowania) oraz możliwość, czyli sposobność do przeprowadzenia cyberataku (np. podatności oprogramowania, sprzętu lub personelu atakowanego systemu).

Rozdział trzeci i czwarty poświęcony został przedstawieniu podstaw teoretycznych cyberwalki jako militarnego wymiaru działań oraz określeniu jej uwarunkowań skuteczności. Opierając się na uzyskanych wynikach badań Habilitant prezentuje podstawy teoretyczne cyberwalki jako militarnego wymiaru działań. Cyberwalka posiada swoją strukturę zależną od przyjętego kryterium, czyli przestrzenną, informacyjną, organizacyjną, proceduralną i techniczną. W ramach cyberwalki mogą być prowadzone działania śmiercionośne, nieśmiercionośne, kinetyczne lub niekinetyczne. Istotną część tego rozdziału stanowią wyniki dociekań naukowych nad cyberwalką w świetle Międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych oraz rozważania na temat cyberkonfliktu. Autor z powodzeniem identyfikuje główne uwarunkowania skuteczności cyberwalki, cyberrozpoznania, przeciwdziałania, obrony elektronicznej oraz znaczenie logistyki w cyberwalce. Prezentuje interesujące podejście do czynników cyberwalki jako militarnego wymiaru działań z podziałem na czynniki pierwotne i wtórne. Scharakteryzowano cyberwojska i podstawowe zasady ich użycia oraz przedstawiono taksonomie zdarzeń, ataków i incydentów.

W rozdziale piątym scharakteryzowane zostały zasadnicze rodzaje działań sił zbrojnych w cyberwalce. Autor definiuje i przedstawia istotę cyberrozpoznania oraz charakteryzuje działania defensywne i ofensywne. Ważnym z punktu widzenia rozwoju teorii cyberwalki jako militarnego wymiaru działań sił zbrojnych jest zidentyfikowanie i omówienie przez Habilitanta takich pojęć, jak: cyberobrona, cyberbroń, cyberatak, cyberodstraszanie militarne, cyberelektromagnetyczne działania militarne, czy też cybermaskowanie. W efekcie mamy pełen obraz możliwych działań sił zbrojnych w ramach cyberwalki.

Doskonałym uzupełnieniem analizowanych aspektów cyberwalki jest rozdział szósty, poświęcony wpływowi otoczenia na zdolność sił zbrojnych do prowadzenia cyberdziałań militarnych. Badania wykazały, że na przestrzeni lat Siły Zbrojne RP dostosowywały się do cyberzagrożeń w otoczeniu. Zmieniając swoje struktury organizacyjne, dostosowywały się do cyberochrony własnych sieci i systemów teleinformatycznych. Sformowano struktury i uzyskano zdolności do działań zarówno defensywnych jak i ofensywnych. Ze względu na złożoność i interdyscyplinarność przedmiotu badań (zjawisko cyberwalki), uzyskane wyniki badań, które stanowią treść recenzowanej monografii w przyszłości mogą stanowić wartościowy materiał do kolejnych badań naukowych z uwzględnieniem nowych, dynamicznie zmieniających się perspektyw.

Podsumowując ocenę, recenzowane osiągnięcie naukowe jest skonstruowane prawidłowo, stanowi zamkniętą i spójną tematycznie monografię naukową. Poszczególne rozdziały są logicznie ze sobą powiązane. Struktura opracowania w zdecydowanej części zaświadcza również o właściwym logicznie ułożonym toku postępowania badacza. Na szczególne podkreślenie zasługuje usystematyzowany tok wywodów Habilitanta, znajdujący odzwierciedlenie nie tylko w kolejności rozdziałów, ale także w ich wewnętrznym układzie. Takie podejście sprawiło, że w efekcie uzyskano materiał badawczy, jako całościowe ujęcie rozwiązywanych problemów badawczych. Treść opracowania została mocno osadzona w literaturze przedmiotu badań, co w połączeniu z wykorzystaniem własnej wiedzy i doświadczeń oraz uzyskanymi wynikami badań sprawia, że przedstawione przez Habilitanta rozwiązania i propozycje są przekonujące i nie wzbudzają wątpliwości. Monografia jest syntetyczną prezentacją dociekań naukowych na temat cyberwalki jako militarnego wymiaru działań, tym samym stanowi wkład do rozwoju wiedzy w zakresie teorii nauk

o bezpieczeństwie, a szczególnie w obszarze sztuki wojennej. Treści zawarte w monografii mają też dużą wartość utylitarną, gdyż mogą posłużyć do profesjonalnego przygotowania personelu sił zbrojnych do prowadzenia działań militarnych w nowym, cybernetycznym wymiarze. Prowadzone przez Pana dr. inż. Roberta Adama Janczewskiego badania doskonale wpisują się w istniejące potrzeby naukowego poznania procesów zachodzących w cyberprzestrzeni w ujęciu działań militarnych, a oceniana monografia jest jednym z niewielu (zwłaszcza w wymiarze krajowym), całościowych opracowań poświęconemu cyberwalce. Pan dr inż. Robert Adam Janczewski przyczynił się do poszerzenia dotychczasowego obszaru eksploracji nauk o bezpieczeństwie, opublikował autorską monografię: *Cyberwalka. Militarny wymiar działań*, która posiada cechy osiągnięcia naukowego. Wobec powyższego stwierdzam, że Kandydat posiada wybitne osiągnięcie naukowe w dziedzinie społecznej, w dyscyplinie nauki o bezpieczeństwie, tym samym spełnia przesłanki, o której mowa w art. 219 ust. 1, pkt. 2, ustawy z dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce*.

3. Ocena aktywności naukowej

Przekazany do oceny dorobek naukowy Pana dr. inż. Roberta Adama Janczewskiego obejmuje aktywność naukową głownie po uzyskaniu stopnia naukowego doktora w obszarze teorii i praktyki nauk o bezpieczeństwie, w tym autorstwo i współautorstwo około 30 publikacji. W swoim dorobku naukowym Habilitant posiada między innymi:

- 3 monografie (autorskie);
- 6 monografii, w których był współautorem lub współredaktorem naukowym;
- 7 artykułów w czasopismach naukowych;
- 13 rozdziałów w monografiach naukowych;
- 33 referaty naukowe wygłoszone w kraju i za granicą;
- aktywny udział w 17 międzynarodowych i krajowych konferencjach naukowych;
- 51 recenzji artykułów naukowych, w tym 20 w czasopismach międzynarodowych;
- uczestniczył 23 razy w zespołach eksperckich lub konkursowych;

Oceniam, że wskazane publikacje jako wynik prowadzonych badań są źródłem wiedzy w obszarze cyberbezpieczeństwa, w szczególności w zakresie działań militarnych sił zbrojnych w cyberprzestrzeni. Wartość poznawcza analizowanego dorobku zawiera się w umiejętnym łączeniu teorii i praktyki. Habilitant podejmuje wysiłek empirycznego weryfikowania założonych tez badawczych, co niezwykle wzbogaca wartość poznawczą jego prac twórczych i świadczy o ich oryginalności. W ramach upowszechniania uzyskanych wyników badań Pan dr inż. Robert Adam Janczewski wygłosił 33 referaty w ramach konferencji krajowych i międzynarodowych oraz kilkadziesiąt prelekcji i wykładów poświęconych bezpieczeństwu w cyberprzestrzeni w różnych instytucjach (jednostki policji, sił zbrojnych, w uczelniach w kraju i za granicą oraz w ramach szkoleń dla administracji publicznej i przedsiębiorców). Jednak ta wysoka aktywność różnego rodzaju wystąpień, w ramach których Habilitant dzielił się uzyskanymi wynikami badań, nie przełożyła się na dorobek w postaci artykułów. Do najbardziej istotnych artykułów można m. in. zaliczyć:

- R. Janczewski, *Konwencja terminologiczna w cyberbezpieczeństwie* [w:] S. Topolewski, K. Karwacka, J. Sekuła, T. Sobczyński (red.), *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni wymiar teoretyczny i praktyczny*, AMW, Gdynia 2018.
- R. Janczewski, G. Pilarski, M. Marczyk, *Terminology as a barrier to NATO's interoperability in cyberspace operations*, International conference The Knowledge-Based Organization, XXV/3, 2019 „Nicolae Balcescu" Land Forces Academy, Sibiu 2019.
- R. Janczewski, *Współdziałanie Sił Zbrojnych RP i Policji dla zapewnienia cyberbezpieczeństwa infrastruktury krytycznej państwa w czasie działań hybrydowych prowadzonych na terenie RP*, „Przegląd Policyjny" 2018, nr 4(132).
- R. Janczewski and G. Pilarski, *The Information Processing in the Cybernetic Environment of Signals Intelligence* [w:] R. Berešík, M. Šostronek, M. Babjak (red.), *New Trends in Signal Processing (NTSP)*, IEEE, 2018.

W uznaniu dorobku naukowego i posiadanej wiedzy z zakresu cyberbezpieczeństwa Habilitant jest zapraszany do współpracy z różnymi wydawnictwami, recenzuje i redaguje publikacje zwarte i artykuły. Kandydat wchodzi w skład komitetu redakcyjnego „Cybersecurity&Cybercrime" wydawanego przez Akademię Marynarki Wojennej (ISSN 2720-4251) oraz jest redaktorem tematycznym działu cyberbezpieczeństwo w „Zeszytach Naukowych Pro Publico Bono" wydawanych przez Akademię Pożarniczą (ISSN 2719-3403).

Przywołana wysoka aktywność wystąpień na konferencjach, jak też uczestnictwo w komitetach naukowych i organizacyjnych wielu spotkań naukowych, wieloletnia współpraca z uczelniami, uzyskiwane systematycznie doświadczenie dydaktyczne i naukowe sprawiły, że Pan dr inż. Robert Adam Janczewski stał się rozpoznawalny w zakresie cyberbezpieczeństwa. Potwierdzeniem tego są liczne zaproszenia w roli eksperta, między innymi do recenzowania artykułów na potrzeby wydawnictw i prac doktorskich związanych z cyberbezpieczeństwem w konkursach narodowych i międzynarodowych, prowadzenia wielu szkoleń, udziału w projektach, uczestnictwa w konferencjach, udziału w zespołach autorskich ćwiczeń i regulaminów na potrzeby szkolenia sił zbrojnych oraz wielu jeszcze innych przedsięwzięć. Dlatego zaskakujący jest fakt, że Habilitant wykazuje bardzo znikome wartości wskaźników naukometrycznych: Index Hirscha – 1, Google Scholar – 1, Impact Factor – 0. Do słabości ocenianego dorobku naukowego zaliczyć też należy brak staży w instytucjach naukowych.

Istotnym elementem działalności naukowej Habilitanta jest też aktywność w obszarze realizacji projektów badawczych i badawczo-rozwojowych w środowisku narodowym i międzynarodowym. W swoim dorobku Pan dr inż. Robert Adam Janczewski może także odnotować udział i realizację projektów w drodze konkursów krajowych i zagranicznych.

- Udział w projekcie: *Identyfikacja zagrożeń cyberprzestrzeni w odniesieniu do funkcjonowania Systemu informacyjno-analitycznego wspomagającego zarządzanie ryzykiem podczas planowania i realizacji działań Policji.* Projekt realizowany w Akademii Marynarki Wojennej DOB-BIO7/02/01/2015 krypt. JANTAR.
- Kierownik projektu: *Zdolność sił zbrojnych do interoperacyjnego działania w cyberprzestrzeni,* Projekt finansowany ze środków finansowych w ramach środków Ministerstwa Obrony Narodowej z programu wsparcia badań podstawowych pn. „Grant

Badawczy", Umowa nr GB/4/2018/208/2018/DA, Decyzja nr 9/2018/GB z dnia 07.11.2018 r.

- Realizacja zadania badawczego: „Cyberbezpieczeństwo w organizacji" w ramach projektu ROTOR realizowanego przez WAT, NCK oraz ABW, Warszawa 2019 r.
- Projekt badawczy: *Wykorzystanie algorytmów hybrydowych wspieranych infrastrukturą komputera kwantowego do bezpiecznego przetwarzania danych z satelitów i BSP w zakresie działań militarnych lub pozamilitarnych*, nr rejestr. DOB-SZAFIR/03/A/021/04/2021.
- Opracowanie propozycji zmian technologicznych, organizacyjnych i prawnych, pozwalających ograniczać i zwalczać spoofing w środowisku elektronicznym, a także ustalić jego sprawców do Projektu Cyber Scourge: Nowe możliwości informatyczno-technologiczne w podniesieniu poziomu bezpieczeństwa w cyberprzestrzeni w ramach konkursu Narodowego Centrum Badań i Rozwoju na rok 2023: Program pn. *Nowe technologie w obszarze bezpieczeństwa i obronności państwa o kr. PERUN.* Projekt przewidziany do realizacji na IX poziomie gotowości technologii.

Poza aktywnym udziałem w konferencjach naukowych i innych typowo naukowych przedsięwzięciach mających na celu popularyzację nauki Kandydat skutecznie realizował się w innych formach. W swoim dorobku może wskazać aktywną współpracę z sektorem społecznym i gospodarczym, występując w roli eksperta podczas bardzo licznych szkoleń i prelekcji oraz realizując zadania zlecone (zadania badawcze) na rzecz cyberbezpieczeństwa przedsiębiorstw. Uczestniczył też jako ekspert w zakresie cyberbezpieczeństwa w międzynarodowych programach: Multinational Capabilities Development Campaign (MCDC) 17-18 – International Cyberspace Operations Planning Curricula (ICOPC) Project, Multinational Capabilities Development Campaign (MCDC) 17-18 – Countering Hybrid Warfare (CHW2), program DEEP Ukraine 2022 w zakresie Cyber Security Curriculum Development for the Odesa Naval Institute. Dlatego też mimo uwag w zakresie wskaźników naukometrycznych i staży naukowych, Habilitant wykazuje istotną aktywność naukową realizowaną w więcej niż jednej uczelni lub instytucji.

W ramach oceny osiągnięć dydaktycznych Kandydat posiada doświadczenie udziału w opracowaniu i aktualizacji programów kształcenia studiów związanych z dyscypliną nauki o bezpieczeństwie. Ponadto Habilitant opracował *Założenia zmian w podstawie programowej kształcenia ogólnego w zakresie edukacji dla bezpieczeństwa i obszar cyberbezpieczeństwo w wymiarze wojskowym* na zlecenie Ministerstwa Edukacji, prowadzenia wielu przedmiotów kształcenia z obszaru bezpieczeństwa. Jako nauczyciel sprawuje opiekę nad pracami licencjackimi, magisterskimi i podyplomowymi oraz je recenzuje.

W toku swojej działalności na rzecz bezpieczeństwa, nauki i dydaktyki oraz popularyzacji wyników badań Pan dr inż. Robert Adam Janczewski był wielokrotnie uhonorowany odznaczeniami państwowymi i resortowymi oraz wyróżnieniami ze strony współpracujących instytucji.

4. Wniosek końcowy

Pozytywnie oceniony dorobek naukowy i dydaktyczny oraz przede wszystkim recenzowane osiągnięcie naukowe, które w dużej części stanowi oryginalny i twórczy wkład Habilitanta do rozwoju nauk o bezpieczeństwie, upoważnia mnie do stwierdzenia, że spełnione zostały wymagania w art. 219 ust. 1 pkt 2 ustawy z dnia 20 lipca 2018 r. — *Prawo o szkolnictwie wyższym i nauce*, tekst jednolity Dz. U. z 2023 r., poz. 742. Wobec tego, wnioskuję o dalsze etapy postępowania habilitacyjnego i nadanie Panu dr. inż. Robertowi Adamowi Janczewskiemu stopnia doktora habilitowanego w dziedzinie nauk społecznych, w dyscyplinie nauki o bezpieczeństwie.

.....

/ prof. dr hab. Grzegorz SOBOLEWSKI/