dr hab. inż. Mariusz FRĄCZEK
Katedra Zarządzania
Wydział Zarządzania i Przywództwa
Akademia Wojsk Lądowych
imienia generała Tadeusza Kościuszki

Wrocław, 29.02.2024 r.

OCENA

istotnej aktywności naukowej, dydaktycznej, publicystycznej i monografii wskazanej jako osiągnięcie naukowe dr. Roberta Adama JANCZEWSKIEGO pt.: *CYBERWALKA. Militarny wymiar działań*, Wydawnictwo Naukowe PWN SA, Warszawa 2023, ISBN: 978-83-01-23028-9.

1. PRZEDSTAWIENIE PODSTAWOWYCH DANYCH O KANDYDACIE

1.1. Data uzyskania stopnia doktora oraz nazwa jednostki organizacyjnej, w której stopień był nadany:

Dyplom uzyskania stopnia naukowego:	*doktor nauk o obronności (obecnie doktor nauk społecznych)*
Dyscyplina:	*Nauki o obronności (obecnie dyscyplina Nauki o Bezpieczeństwie)*
Specjalność:	*Zarządzanie w środowisku informacyjnym*
Miejsce i rok nadania:	*Wydział Zarządzania i Dowodzenia Akademii Obrony Narodowej, Warszawa, 2016*
Tytuł rozprawy doktorskiej:	*Procesy informacyjne w rozpoznaniu elektronicznym Wojsk Lądowych Sił Zbrojnych Rzeczypospolitej Polskiej.*

1.2. Informacja, czy kandydat ubiegał się uprzednio o nadanie stopnia doktora habilitowanego w tym – o ile wynika to z dokumentacji sprawy - informacja o przebiegu i zakończeniu wcześniejszego postepowania:

Kandydat nie ubiegał się uprzednio o nadanie o nadanie stopnia doktora habilitowanego.

1.3. Przebieg pracy naukowo-zawodowej (miejsce pracy, zajmowane stanowiska):

Przebieg zawodowej służby wojskowej Pana dr Roberta JANCZEWSKIEGO nie został zaprezentowany w części wstępnej dotyczącej ogólnej charakterystyki sylwetki kandydata do stopnia naukowego doktora habilitowanego, co wynika z zajmowanych przez ww. stanowisk oraz funkcji w SZ RP. W ocenie Recenzenta podkreślenia wymaga, iż jest on ścisłe powiązany z późniejszymi dokonaniami Habilitanta, gdyż stanowił fundament jego zainteresowań naukowych. Z kolei przebieg pracy naukowo-zawodowej Habilitanta prezentuje się następująco:

1. Wyższa Szkoła Biznesu i Zarządzania w Ciechanowie - 2002-2005 - umowa zlecenie na prowadzenie zajęć z zakresu informatyki w każdym roku akademickim.
2. Uniwersytet Warmińsko-Mazurski w Olsztynie - 2018-2021 - umowa zlecenie na prowadzenie zajęć w ramach przedmiotu informatyczne systemy bezpieczeństwa w Wydziale Nauk Społecznych Instytutu Nauk Politycznych.
3. Akademia Sztuki Wojennej w Warszawie - 2018-2019 - Adiunkt w Zakładzie Cyberbezpieczeństwa w Instytucie Działań Informacyjnych w Wydziale Wojskowym.

4. Wyższa Szkoła Policji w Szczytnie - 2019 - umowa zlecenie na prowadzenie zajęć w zakresie informatyki w Wydziale Bezpieczeństwa i Nauk Prawnych.
5. Państwowa Uczelnia Zawodowa im. Ignacego Mościckiego w Ciechanowie - 2020-2023 - Adiunkt w Zakładzie Informatyki na Wydziale Inżynierii i Ekonomii.
6. Państwowa Akademia Nauk Stosowanych im. Ignacego Mościckiego w Ciechanowie od 2023 - Adiunkt w Zakładzie Informatyki na Wydziale Inżynierii i Ekonomii.
7. Akademia Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni - 2020-2022 - główny specjalista w Morskim Centrum Cyberbezpieczeństwa w Wydziale Dowodzenia i Operacji Morskich:
   a) od 2019 – umowa zlecenie na prowadzenie zajęć w zakresie cyberbezpieczeństwa na Wydziale Dowodzenia i Operacji Morskich;
   b) 2019-2022 – umowa zlecenie na prowadzenie zajęć w zakresie cyberbezpieczeństwa na Wydziale Nauk Humanistycznych i Społecznych;
   c) 2019-2022 - umowa zlecenie na prowadzenie zajęć na studiach podyplomowych w zakresie cyberbezpieczeństwa na Wydziale Dowodzenia i Operacji Morskich;
   d) 2019-2022 - umowa zlecenie na prowadzenie zajęć na studiach MBA w zakresie cyberbezpieczeństwa na Wydziale Dowodzenia i Operacji Morskich.
8. Uniwersytet Pomorski w Słupsku - od 2023 - umowa zlecenie na prowadzenie zajęć na studiach podyplomowych w zakresie cyberbezpieczeństwa w Instytucie Bezpieczeństwa i Zarządzania w Katedrze Bezpieczeństwa Narodowego.

Recenzent ocenia, iż istotnym elementem świadczącym o dużym zaangażowaniu Kandydata do stopnia naukowego doktora habilitowanego we własny rozwój była jego działalność publicystyczna co zostało wyszczególnione w Autoreferacie oraz Wykazie dorobku naukowego habilitanta.

Powyższe, wraz z podstawowymi informacjami o kandydacie do stopnia naukowego doktora habilitowanego, świadczy o bardzo dużym zaangażowaniu Habilitanta w realizowanie zadań służbowych oraz dydaktykę.

2. PRZEDSTAWIENIE INFORMACJI O OBOWIĄZUJĄCYCH PRZEPISACH PRAWA NA DZIEŃ WSZCZĘCIA OCENIANEGO POSTĘPOWANIA HABILITACYJNEGO, W TYM OBOWIĄZUJĄCYCH KRYTERIACH OCENY

Ustawa z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2022 r., poz. 574 z późn. zm.). Artykuł 219 ust 1. Pkt.2:

1. Stopień doktora habilitowanego nadaje się osobie, która:

2) posiada w dorobku osiągnięcia naukowe albo artystyczne, stanowiące znaczny wkład w rozwój określonej dyscypliny, w tym co najmniej:

a) 1 monografię naukową wydaną przez wydawnictwo, które w roku opublikowania monografii w ostatecznej formie było ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit. a, lub

b) 1 cykl powiązanych tematycznie artykułów naukowych opublikowanych w czasopismach naukowych lub w recenzowanych materiałach z konferencji międzynarodowych, które w roku opublikowania artykułu w ostatecznej formie były ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit. b, lub

c) 1 zrealizowane oryginalne osiągnięcie projektowe, konstrukcyjne, technologiczne lub artystyczne.

3. PRZEDSTAWIENIE INFORMACJI O OCENIANYCH OSIĄGNIĘCIACH NAUKOWYCH

3.1. Tytuł osiągnięcia naukowego stanowiącego podstawę ubiegania się w aktualnym postępowaniu o nadanie stopnia doktora habilitowanego:

CYBERWALKA. Militarny wymiar działań, Wydawnictwo Naukowe PWN SA, Warszawa 2023, ISBN: 978-83-01-23028-9. 431 stron monografii (80 pkt.).

3.2. Informacja o danych naukometrycznych, jak sumaryczny współczynnik Impact Factor, sumaryczna punktacja ministerialna, liczba cytowań oraz indeks Hirscha, którymi legitymuje się kandydat na dzień wszczęcia postępowania w sprawie nadania stopnia doktora habilitowanego, z podaniem również danych współczynników po uzyskaniu awansu naukowego:

3.2.1. Informacja o punktacji Impact Factor (w dziedzinach i dyscyplinach, w których parametr ten jest powszechnie używany jako wskaźnik naukometryczny).

Kandydat do stopnia doktora habilitowanego posiada punktację Impact Factor. Według Recenzenta wynosi ona: Impact Factor = 0,00. (WoS, Scopus)

3.2.2. Informacja o liczbie punktów MNiSW:

Na podstawie przedstawionych w *Wykazie osiągnięć naukowych albo artystycznych, stanowiących znaczny wkład w rozwój określonej dyscypliny* informacji naukometrycznych Recenzent ocenia, iż Pan dr Robert Janczewski zgromadził następującą ilość punktów wynikającą z publikacji:

a) monografie (razem 3) - **240 pkt;**
b) rozdziały w monografiach (razem 9 rozdziałów) - **150 pkt** (wynikających z udziału procentowego Autora w danej monografii);
c) artykuły (razem 4) - łącznie punktów - **30** pkt.

Według Recenzenta łącznie jest to: **razem 420 pkt**.

3.2.3. Informacja o liczbie cytowań publikacji wnioskodawcy, z oddzielnym uwzględnieniem autocytowań:

Kandydat do stopnia doktora habilitowanego występuje w bazie Google Scholar, według której Habilitant posiada niżej wskazaną liczbę cytowań:

Cytowania = 1, autocytowania = 0 (z bazy Google Scholar:
https://scholar.google.pl/citations?hl=pl&user=bOpaUvoAAAAJ)

3.2.4. Informacja o posiadanym indeksie Hirscha:

Recenzent znalazł informację, że Kandydat do stopnia doktora habilitowanego posiada indeks Hirscha, który wynosi:

Index Hirscha = 1. (indeks Hirscha z bazy Google Scholar,
https://scholar.google.pl/citations?hl=pl&user=bOpaUvoAAAAJ).

3.3. Informacja o liczbie publikacji naukowych, monografii, rozdziałów w monografiach autorstwa oraz współautorstwa kandydata, z podaniem również danych informacji po uzyskaniu awansu naukowego:

Liczba publikacji, rodzaj/ czas publikacji	Razem w dorobku	Łącznie ilość pkt
Monografie	3	240 pkt
Rozdziały w monografiach	9	150 pkt
Artykuły	4	30 pkt
Prace naukowo-badawcze/ projekty badawcze	2	brak danych
Redakcje naukowe monografii	3	35 pkt
Razem:		**455**

Sumaryczna liczba punktów z publikacji według listy MEN – 455.

3.4. Informacja o najważniejszych czasopismach oraz konferencjach, w ramach których kandydat publikował swoje prace naukowe:

W opinii Recenzenta, do najważniejszych czasopism oraz konferencji, w ramach których Kandydat publikował swoje prace naukowe należą:

1) Przegląd Sił Zbrojnych - 2 artykuły
2) European Security - 1 artykuł.
3) Special Ops - 1 artykuł.
4) Security Ops - 1 artykuł.
5) Przegląd Policyjny, ISSN 0867-5708 - 1 artykuł.
6) Academic and Applied Research in Military and Public Management Science, the National University of Public Service, Budapest, Hungary 2018, ISSN 2498-5392 – 1 artykuł.
7) *New Trends in Signal Processing (NTSP)*, IEEE, 2018, ISBN 978-1-5386-0519-6 – 1 artykuł.
8) The Knowledge-Based Organization, XXV/3, DOI: https://doi.org/10.2478/kbo-2019-0113 - 1 artykuł.
9) 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, ISBN 978-83-65763-12-9. – 1 publikacja.
10) 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, ISSN 1843-6722DOI: https://doi.org/10.2478/kbo-2019-0113. (1 pkt.) (Czasopismo spoza wykazu) – 1 artykuł.
11) III Konferencja naukowa pt. „Bezpieczeństwo informacyjne w obszarze cyberprzestrzeni" Akademii Marynarki Wojennej w Gdyni, 23-24.11.2017 r.
12) Konferencja naukowa pt. „Udział Policji oraz innych służb i instytucji w ochronie infrastruktury krytycznej państwa w dobie niesymetrycznych zagrożeń. Diagnoza i perspektywy", Wyższa Szkoła Policji w Szczytnie, 27-28.02.2018 r.
13) Krajowa konferencja naukowa pt. „Scenariusz przebiegu konfliktu hybrydowego", Akademii Sztuki Wojennej w Warszawie, 07.05.2018 r.
14) XXII Konferencja naukowa pt. Techniczne aspekty przestępczości teleinformatycznej, Wyższa Szkoła Policji w Szczytnie, 03-04.06.2019 r.

15) Konferencja naukowa pt. „Przestępczość Teleinformatyczna XXI wieku", Akademia Marynarki Wojennej w Gdyni, 17-19.06.2019 r., wygłoszenie referatu nt.: *Planowanie interoperacyjności na rzecz cyberbezpieczeństwa.*
16) VI Ogólnopolska konferencja naukowa pt. „Współczesny człowiek wobec zagrożeń w cyberprzestrzeni. Aspekty techniczne, Innowacyjne narzędzia IT kreacji rzeczywistości społecznej", Akademia Pomorska w Słupsku, 23-24.11.2021 r.
17) Konferencja naukowa „Organizacja systemu rozpoznania zagrożeń państwa – priorytetowe potrzeby informacyjne w systemie bezpieczeństwa państwa", Akademia Sztuki Wojennej 14.04.2022 r.
18) VII Ogólnopolska konferencja naukowa z cyklu „Bezpieczeństwo informacyjne" nt. „Cyberprzestrzeń i ochrona informacji jako pole zmagań o bezpieczeństwo informacyjne", Uniwersytet Przyrodniczo-Humanistycznego w Siedlcach, 12.05. 2022 r.
19) I Krajowa konferencja naukowa „Współczesne uwarunkowania maskowania", Akademia Sztuki Wojennej w Warszawie, 18.05.2022 r.
20) VIII Ogólnopolska konferencja naukowa z cyklu „Bezpieczeństwo informacyjne" pt. „Współczesne zagrożenia informacyjne", Uniwersytet Przyrodniczo-Humanistycznego w Siedlcach, 18.05.2023 r.
21) Konferencja naukowa pt. „Dezinformacja. Walka. Wojna. Bezpieczeństwo", Akademia Marynarki Wojennej, 22.05.2023 r.
22) I Konferencja naukowa Łużyckiej Szkoły Wyższej w Żarach, pt.: „Interdyscyplinarność nauk o bezpieczeństwie w kontekście współczesnych zagrożeń', 30.09.2023 r., wygłoszenie referatu nt. *Teoretyczne aspekty Cyberwalki jako militarnego wymiaru działań.*
23) Międzynarodowa Konferencja naukowa pt. Knowledge-Based Organization, „Nicolae Balcescu" Land Forces Academy, Sibiu, Bułgaria, 10-14.06.2019.
24) Międzynarodowa konferencja pt. „Trends in Signal Processing (NTSP)", IEEE, Demanovska Dolina, Slovakia, 10-12.10.2019.
25) Międzynarodowa konferencja naukowe pt. "Capability Enhancement Regional Symposium - Northeast with Maritime Domain/Security Awareness (MDA/MSA & MCM) and C4/Cyber Focus Area", USEUCOM, Baltic Defence College w Tallinie, 29-31.10.2019.
26) XV Międzynarodowa konferencja pt. „Nowoczesne technologie dla bezpieczeństwa kraju i jego granic", Hotel Hilton w Warszawie, 20.11.2019 r.
27) Baltic Defence College 12 Riia St, Tartu, Estonia, 09.12.2019, Workshop on Cyber Defence: How to incorporate cyber in planning our defence and security.
28) Konferencja naukowa pt. „Mobile Deployment Communications", SMI Group Hotel Mariott w Warszawie, 30-31.01.2020 r.
29) XII Międzynarodowa konferencja naukowa pt. „Bezpieczeństwo w Internecie - Cyberpandemia", Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie.
30) Międzynarodowa konferencja naukowa pt. „Edukacja w pandemii. Nowe zjawiska, zagrożenia i szanse. Perspektywa edukacji (nie tylko) służb państwowych", Wyższa Szkoła Policji w Szczytnie.
31) IX Międzynarodowa konferencja naukowo-techniczna NATCON organizowana przez OBR Centrum Techniki Morskiej S.A., Akademię Marynarki Wojennej oraz Międzynarodowe Targi Gdańskie S.A, 20-22.04.2021 r.
32) Międzynarodowa konferencja Security&Forecasting 2021 SEC4 pt. „Wyzwania bezpieczeństwa Polski i bezpieczeństwa międzynarodowego – stan obecny i prognozy na przyszłość", Akademia Sztuki Wojennej w Warszawie, 11-12.05.2021 r.

W ocenie Recenzenta, Habilitant przekazał swoje publikacje do 10 czasopism oraz 22 materiałów pokonferencyjnych.

Razem 32 publikacje.

3.5. Informacja, czy kandydat odgrywał wiodącą rolę w ramach powstawania współautorskich prac naukowych:

Zdaniem Recenzenta, dotychczasowy dorobek kandydata do stopnia doktora habilitowanego pozwala sądzić, iż wkład Pana dr inż. Roberta Janczewskiego w ramach powstawania poszczególnych prac naukowych był istotny. Świadczy o tym udział w pracach 10 zespołów realizujących projekty naukowo-badawcze, a w tym samodzielne kierowanie 4 zadaniami badawczymi. Oceniam, że Habilitant opracował wyniki czterech projektów badawczych. Jest także autorem 4 punktowanych artykułów do czasopism naukowych. Należy zauważyć, że Habilitant wskazał na opracowanie 9 rozdziałów do sprawozdań badawczych.

3.6. Ocena wskazanego przez kandydata osiągnięcia naukowego, w tym, czy stanowi ono znaczący wkład w rozwój określonej dyscypliny naukowej:

Recenzowana monografia habilitacyjna dr. Roberta Adama JANCZEWSKIEGO pt.: *CYBERWALKA. Militarny wymiar działań*, Wydawnictwo Naukowe PWN SA, Warszawa 2023, ISBN: 978-83-01-23028-9, liczy 431 stron.

Monografia uwagę czytelnika skupia wokół problematyki ścisłe związanej z znaczeniem cyberwalki we współczesnych działaniach militarnych na wszystkich poziomach dowodzenia.

Według Kandydata do stopnia doktora habilitowanego stanowi istotny obszar problematyki bezpieczeństwa w kontekście sprawnego funkcjonowania organizacji zhierarchizowanej, jaką bez wątpienia są Siły Zbrojne Rzeczypospolitej Polskiej. Wyniki rozważań zawarte w jej treści są również odzwierciedleniem osobistych zainteresowań i doświadczeń Autora. Zdaniem Recenzenta dr Robert Janczewski prawidłowo określił aspekt poznawczy monografii, zidentyfikował oraz wskazał główne elementy cyberwalki oraz ustalił czynniki determinujące cyberwalkę jako militarny wymiar działań. Niemniej ważnym czynnikiem wpływającym na wybór obszaru badawczego była potrzeba zbadania teoretycznych aspektów cyberwalki jako militarnego wymiaru działań oraz zabezpieczenie potrzeb dydaktycznych, czyli opracowanie treści, które w trakcie kształcenia i doskonalenia specjalistów od cyberwalki (ale także innych specjalności) mogą służyć do poszerzania oraz uporządkowania wiedzy na ten temat.

Oceniam, iż jest to aktualny oraz bardzo ważny obszar badawczy, a dotychczasowe publikacje Habilitanta, a także innych autorów wskazywały na potrzebę całościowego naukowego ujęcia podjętej problematyki. Recenzowana rozprawa spełnia to zapotrzebowanie i stanowi kompleksowe opracowanie przyjętego przedmiotu badań, którym jest „*cyberwalka jako militarny wymiar działań* (s. 12)".

Monografia dr Roberta Janczewskiego składa się z wstępu, sześciu rozdziałów, zakończenia i bibliografii zawierającej według Recenzenta 446 pozycji, z tego 114 są to „*Publikacje zwarte (książki)*". „*Publikacje ciągłe (artykuły)*", to 67 pozycji. „*Słowniki*", to 15 pozycji. „*Źródła (Decyzje, Doktryny, Raporty, Regulaminy, Ustawy, Rozporządzenia, Zarządzenia)*", to 63 pozycji, a 187 publikacji stanowi „*Netografia*". Rozdziały od 1 do 6 zawierają wnioski Habilitanta także jako podrozdziały, co ułatwiło opis wyników procesu badawczego. Ostatnim elementem spisu treści jest „*Spis rysunków i tabel*".

We wstępie Autor podkreślił, że sytuację problemową, przedmioty i podmiot badań, cele badań, problemy badawcze oraz hipotezy badawcze. Wskazano również na zastosowane

metody badawcze, zaprezentowano założenia oraz procedurę badawczą, strukturę i charakterystykę monografii oraz ocenę literatury, a także materiałów źródłowych przedmiotu badań.

W ocenie Recenzenta warto zauważyć, iż literatura przedmiotu dotychczas nie zawierała kompleksowego opracowania dotyczącego tej problematyki w ujęciu zaproponowanym przez Autora w recenzowanej monografii, zatem jej struktura wyniknęła z potrzeby wieloaspektowej prezentacji przedmiotu badań.

W rozdziale pierwszym nt.: „*Uwarunkowania cyberwalki jako militarnego wymiaru działań*", Habilitant przedstawił uwarunkowania oraz wyniki dociekań naukowych dotyczących cyberwalki jako militarnego wymiaru działań. Na podstawie wyników badań zaprezentował rozwiązanie szczegółowego problemu badawczego sformułowanego w postaci pytania: *Jakie są uwarunkowania cyberwalki jako militarnego wymiaru działań?* Uzyskane wyniki badań pozwoliły autorowi na sformułowanie wniosku, że siły zbrojne są organizacją wojskową i poprzez realizację różnorodnych zadań w obszarze zapewnienia bezpieczeństwa w cyberprzestrzeni prowadzą cyberwalkę. Zatem posiada ona militarny wymiar działań. Recenzent podziela pogląd Habilitanta, że rozwój nowoczesnych technologii oraz ich wdrożenie spowodowało wzrost znaczenia teleinformatyki we współczesnej przestrzeni walki oraz przyczyniło się do zwiększenia skuteczności walki, co spowodowało konieczność zbudowania przez siły zbrojne zdolności do prowadzenia cyberwalki. Powyższe stało się fundamentem wielu zmian prawnych, organizacyjno-technicznych, edukacyjnych oraz dydaktycznych, które aktualnie oddziaływują na SZ RP w zakresie konieczności dokonywania przeobrażeń ich struktury organizacyjnej, wyposażenia, zdolności do identyfikacji zagrożeń, w aspekcie przygotowywania specjalistów, wzrostu świadomości operacyjnej, jak również sposobie prowadzenia działań militarnych w nowej, sztucznie wykreowanej przestrzeni walki. Doktor Robert Janczewski słusznie zauważył, iż powstała nowa przestrzeń prowadzenia dezinformacji, oddziaływania i rażenia obranych celów. Szczególną rolę w uwarunkowaniach cyberwalki jako militarnego wymiaru działań należy przypisać wrogim cyberdziałaniom, czyli działaniom prowadzonym z wykorzystaniem cyberprzestrzeni, które prowadzone pod dowództwem wojskowym stanowią militarny wymiar działań. To one uzasadniają konieczność budowania przez siły zbrojne zdolności do cyberwalki. Zidentyfikowano również formalny czynnik będący konsekwencją poprzedniej przyczyny, czyli wymagania stawiane siłom zbrojnym przez państwo wobec już zidentyfikowanych oraz pojawiających się zagrożeń świadczących o celowym prowadzeniu ataków i prób destabilizacji funkcjonowania wojska oraz państw (przykłady to: Estonia w 2007, Gruzja w 2008 oraz Ukraina od 2014 roku).

W rozdziale pierwszym Autor odzwierciedlił, że wrogie działania wykorzystujące cyberprzestrzeń stanowią przyczynę do budowania przez siły zbrojne zdolności do cyberwalki. W oparciu o analizę i krytykę literatury oraz krytyczną analizę polskich oraz innych wybranych państw dokumentów normatywnych w kontekście działań militarnych zidentyfikowano desygnaty istotne z punktu widzenia rozwiązania pierwszego problemu szczegółowego.

Recenzent ocenia, że istotną treścią rozdziału pierwszego jest także identyfikacja konwencji terminologicznej warunkującej aparat pojęciowy w teorii i praktyce cyberwalki jako militarnego wymiaru działań, której skrupulatnie dokonał Autor monografii. Przytoczone wyniki badań w tym rozdziale stanowią uzupełnienie wiedzy na temat czynnika warunkującego budowanie zdolności sił zbrojnych do cyberwalki, czyli zmian zachodzących w cyberdziałaniach wrogich podmiotów. W podsumowaniu rozdziału sformułowano wnioski.

Rozdział drugi zatytułowany „*Przestrzeń cyberwalki*" jest odpowiedzią na sformułowany w postaci pytania szczegółowy problem badawczy: *Jaka przestrzeń determinuje prowadzenie cyberwalki przez siły zbrojne?* Rozdział ten poświęcony jest

identyfikacji oraz charakterystyce przestrzeni cyberwalki prowadzonej przez siły zbrojne. W tym kontekście Habilitant wskazał teatr wojny, teatr działań wojennych oraz teatr operacji. Następnie szczegółowo opisał desygnat cyberprzestrzeni oraz cyberśrodowiska, jak również znaczenie we współczesnej przestrzeni walki zwirtualizowanej rzeczywistości, pozornej inteligencji oraz uczenia maszynowego. W interesujący sposób scharakteryzowano cyberprzestrzeń w odniesieniu do przestrzeni walki. W oparciu o analizę dokumentów doktrynalnych i strategicznych innych państw zaprezentowano wybrane poglądy na temat cyberprzestrzeni. W rozdziale określono teoretyczne aspekty cyberzagrożeń w świetle funkcjonowania sił zbrojnych w cyberprzestrzeni oraz zaprezentowano ich taksonomię. w kontekście sieci i systemów teleinformatycznych resortu obrony narodowej, w tym sił zbrojnych.

W rozdziale tym Habilitant, opierając się na wynikach badań, sformułował wniosek, że siły zbrojne poszerzyły spektrum swoich działań, dostosowując je do nowej, nieznanej dotychczas w teorii wojskowości przestrzeni walki. Autor uwypuklił, że z punktu widzenia szeroko rozumianej w naukach o bezpieczeństwie teorii cyberwalki jako militarnego wymiaru działań są wyniki badań, które wyeksponowały obecność we współczesnej przestrzeni walki rozwiązań programowych i sprzętowych opartych o najnowsze rozwiązania technologiczne związane z teleinformatyką, mechatroniką oraz sztuczną inteligencją służące do przekazywania informacji oraz jej wirtualności. Ustalono, że cyberprzestrzeń stwarza warunki do prowadzenia cyberdziałań, a będąc nową przestrzenią prowadzenia działań militarnych posiada wyjątkowe cechy, m.in. zależność od niej wielu zdolności w pozostałych domenach, warunkujące nowy, unikatowy model podejmowania decyzji. W ocenie Recenzenta, trudno jest go bezpośrednio odnieść do znanego każdemu żołnierzowi wojsk lądowych procesu decyzyjnego.

W rozdziale drugim Autor monografii opisał oraz scharakteryzował także cyberśrodowisko. Jest to zbiór wszelkich elementów i czynników, będących w ścisłej współzależności, który wpływa na procesy informacyjne oraz sygnały danego układu w cyberprzestrzeni poprzez umacnianie stanów pożądanych i przeciwdziałanie stanom niepożądanym. W oparciu o powyższe Habilitant zbudował model systemu C-T-O, czyli człowiek-technika-otoczenie. Ustalił, 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, z kolei technika (T) to wszystko to, co służy żołnierzowi do wykonania powierzonego mu zadania. Bezpieczeństwo takiego systemu zależna jest od jego niezawodności. Zatem ustalono czynniki i elementy cyberśrodowiska. Mając na uwadze znaczenie informacji we współczesnej przestrzeni walki opisano proces informacyjny w cyberśrodowisku, który realizowany jest za pomocą działalności na danych i informacjach.

Rozwiązanie drugiego problemu szczegółowego umożliwiło Habilitantowi wskazanie zagrożeń właściwych dla cyberprzestrzeni, czyli cyberzagrożeń niewystępujących w innych domenach fizycznych. Wyniki badań pozwoliły na sformułowanie wniosku, że warunkiem stworzenia cyberzagrożenia przez wrogi podmiot, jest zaistnienie połączenia trzech czynników. Te trzy czynniki to: zamiar (czyli chęć złośliwego podmiotu do przeprowadzenia cyberataku na wybrany system); zdolność (posiadanie umiejętności zasobów niezbędnych do przeprowadzenia cyberataku - np. specjalistycznego oprogramowania) oraz możliwość (sposobność do przeprowadzenia cyberataku). Wnioski z badań wskazują rownież, że cyberrozpoznanie można postrzegać jako cyberzagrożenie. Autor ustalił, że powszechnie stosowany anglojęzyczny skrótowiec IT (ang. *information technology*) należy rozumieć jako informatykę. Z kolei charakterystykę cyberwalki jako militarnego wymiaru działań anglojęzyczny akronim ICT, czyli *Information and Communications Technology* należy odnieść do technologii informacyjnych i telekomunikacyjnych, w tym informatyki,

elektroniki i telekomunikacji oraz elektrotechniki, automatyki i robotyki, a nie komunikacji (aktu wysyłania i odbierania informacji przez mówienie, pisanie, dzwonienie, wysyłanie e-maili itp. lub wiadomości zawierających takie informacje). W procesie poznawczym zidentyfikowano atrybucję techniczną, którą zdefiniowano jako zdolność do powiązania cyberataku z odpowiedzialną stroną za pomocą środków technicznych w oparciu o informacje udostępnione w czasie cyberdziałań.

W kontekście przestrzeni prowadzenia cyberwalki jako działań militarnych uporządkowano definicje terminów: teatr, teatr wojny, teatr działań wojennych oraz teatr operacji. Badania Habilitanta jednoznacznie wskazały, że cyberprzestrzeń była pomijana w specyfikacji przestrzeni walki. W oparciu o nie ustalono, że współczesna przestrzeń walki obok domeny lądowej, morskiej, powietrznej, kosmicznej obejmuje także cyberprzestrzeń. Dlatego cyberwojska, aby sprostać dynamicznie zmieniającemu się otoczeniu, powinny być zdolne do prowadzenia obronnych i zaczepnych cyberdziałań. W podsumowaniu rozdziału sformułowano wnioski.

Rozdział trzeci nt.: „*Podstawy teoretyczne cyberwalki*" prezentuje wyniki badań skupionych na określeniu podstaw teoretycznych cyberwalki w wymiarze militarnym. W oparciu o nie wskazano na jej wielopoziomowość i wieloaspektowość. Autor opisał wybrane ramy analityczne przydatne w procesach informacyjnych cyberwalki jako militarnego wymiaru działań, zidentyfikował desygnat przeciwnika, wskazał operacyjne kierunki użycia robotów we współczesnej przestrzeni walki oraz zdefiniował cyberinformacyjne przygotowanie przestrzeni walki. Habilitant zaprezentował cyberwalkę w świetle Międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych, co dotychczas nie miało miejsca w literaturze przedmiotu.

Rozdział ten poszukuje odpowiedzi na problem szczegółowy będący pytaniem: *Jakie są podstawy teoretyczne cyberwalki jako militarnego wymiaru działań?* Wyniki rozważań badawczych pozwoliły Habilitantowi na sformułowanie wniosku, że cyberwalka jako militarny wymiar działań nie posiada jednoznacznej, uporządkowanej teorii. Punktem wyjścia terminologicznego dla przedmiotu badawczego niniejszej monografii jest anglojęzyczny termin *cyberwarfare*. Podstawami teoretycznymi cyberwalki prowadzonej przez siły zbrojne są podstawy teoretyczne sztuki wojennej oraz teorii działań militarnych. Ustalono, że ze względu na techniczny wymiar również podstawy teoretyczne informatyki i telekomunikacji stanowią założenia dla cyberwalki oraz, że charakterystyczne dla cyberwalki jako militarnego wymiaru działań jest to, iż podstawy prawne zarówno krajowe jak międzynarodowe nie są jednoznaczne w obszarze cyberwalki i tylko częściowo ją regulują, ponieważ w wielu przypadkach podstawą prawną pozostaje prawo karne. Istotnym wkładem do nauk o bezpieczeństwie jest ustalenie, że cyberwalka jako militarny wymiar działań to zorganizowane cyberdziałania wojsk mające na celu uzyskanie przewagi nad przeciwnikiem lub pokonanie go. Ze względu na brak desygnatu zdefiniowano przeciwnika jako indywidualny lub grupowy podmiot, którego celowe działania dążą do wywołania niepożądanego skutku. Natomiast, uzyskanie przewagi lub pokonanie przeciwnika można rozumieć jako osiągnięcie cyberefektu rozumianego jako manipulacje, zakłócenie, odmowę, degradację lub zniszczenie komputerów, systemów informacyjnych lub komunikacyjnych, sieci, infrastruktury fizycznej lub wirtualnej kontrolowanej przez komputery lub systemy informacyjne lub informacje w nich zawarte.

Recenzent podziela pogląd Habilitanta, że cyberwalka posiada strukturę przestrzenną, informacyjną, organizacyjną, proceduralną i techniczną, a w jej ramach mogą być prowadzone działania śmiercionośne, nieśmiercionośne, kinetyczne lub niekinetyczne. Warto również podkreślić, że cyberkonflikt ze względu na swoją charakterystykę jest istotnym pojęciem dla budowania teoretycznych podstaw cyberwalki prowadzonej przez siły zbrojne.

W podsumowaniu rozdziału sformułowano wnioski.

W **rozdziale czwartym** pt.: „*Uwarunkowania skuteczności cyberwalki jako militarnego wymiaru działań*" zaprezentowano efekty poznawcze uwarunkowań właściwych skuteczności cyberwalki jako militarnego wymiaru działań. Na ich podstawie Autor scharakteryzował cyberwalkę jako militarny wymiar działań. Opisał podstawy teoretyczne skuteczności cyberwalki, cyberrozpoznania, przeciwdziałania, obrony elektronicznej oraz znaczenie logistyki w cyberwalce. Przedstawił teorię zakłóceń radiowych mających wpływ na bezprzewodową transmisję danych. Zaprezentował także czynniki cyberwalki jako militarnego wymiaru działań z podziałem na czynniki pierwotne i wtórne. Scharakteryzował cyberwojska oraz podstawowe zasady ich użycia. Przedstawił taksonomie zdarzeń, ataków i incydentów.

Recenzent podziela wniosek Habilitanta, że cyberwalka prowadzona może być na każdym poziomie dowodzenia oraz szczeblu organizacyjnym sił zbrojnych. Powodzenie cyberwalki zabezpieczone logistycznie determinowane jest jej skutecznością mierzoną stopniem osiągnięcia zamierzonego celu. Autor przyjął, że cele sił zbrojnych w cyberwalce: dostarczają wskazówek i pozwalają nadać jednolity kierunek działań, sprzyjają dobremu planowaniu działań, a ono z kolei sprzyja ustalaniu kolejnych celów na przyszłość, mogą być źródłem motywacji do działań, stanowią skuteczny mechanizm oceny i kontroli. Istotnym wynikiem badań jest zilustrowanie, że cyberwalka prowadzona może być przez wojska właściwe do tego rodzaju walki jednak w ograniczonym zakresie, w zależności od rodzaju działań, także przez każdy inny rodzaj wojsk czy sił zbrojnych, a także przez każdego żołnierza indywidualnie w przestrzeni walki. Istotnym wkładem do teorii cyberwalki, jako militarnego wymiaru działań jest zidentyfikowanie unikalnych, determinujących ją czynników pierwotnego oraz wtórnego. Według Recenzenta, Autor właściwe wskazał, że pierwotną przyczyną (czynnikiem pierwotnym) podjęcia przez siły zbrojne cyberwalki jest jej cel, który określają różnorodne czynniki techniczne, infrastruktura teleinformatyczna, taktyczno-operacyjne, organizacyjne, proceduralne, czas oraz dane i informacje. Współczesna przestrzeń walki wymusza, aby traktować ją jako czynnik zwiększający wiedzę człowieka o otaczającej go rzeczywistości, obok rażenia i ruchu, kształtujący walkę zbrojną oraz zmniejszający stopień niewiedzy o otoczeniu, umożliwiający polepszenie jego znajomości i w sprawniejszy sposób przeprowadzenie celowego działania.

Wyniki rozważań Autora wskazują, że charakterystyczne dla cyberwalki jako militarnego wymiaru działań jest to, że jest ona czymś więcej niż jedynie działaniami skierowanymi przeciwko sieciom lub systemom teleinformatycznym w celu zakłócenia ich działania, uszkodzeniu danych lub informacji albo unieruchomieniu komputerów za pomocą szkodliwego pliku wykonawczego. Cyberefekt może wpływać nie tylko na militarne cyberdziałania, ale także na zdolności sił zbrojnych we wszystkich domenach walki.

W podsumowaniu rozdziału sformułowano wnioski.

W rozdziale piątym nt.: „*Zasadnicze rodzaje działań sił zbrojnych w cyberwalce*" Habilitant dokonał przedstawienia swoich badań dotyczących identyfikacji zasadniczych działań sił zbrojnych w cyberwalce. Wskazał na różnice między cyberrozpoznaniem a rozpoznaniem cyberzagrożeń. Przybliżył cykl rozpoznawczy, zadania cyberrozpoznania oraz podstawy teoretyczne źródeł danych i informacji rozpoznawczych. Zwrócił uwagę na znaczenie eksploracji danych w cyberrozpoznaniu. Zebrany materiał badawczy pozwolił na sformułowanie wniosku, że rola cyberzagrożeń w cyberrozpoznaniu powoduje różnicę w zakresie znaczeniowym między cyberrozpoznaniem a rozpoznaniem cyberzagrożeń. Mimo, iż cyberzagrożenia stanowią dużą część zainteresowania cyberrozpoznania, które obejmuje również analizę obszarów, takich jak technika i technologie, geopolityka i zdolności do cyberdziałania, infrastruktura i status sieci, gotowość sprzętu i personelu przeciwnika oraz unikalne identyfikatory sygnatur w cyberprzestrzeni, takie jak wersje sprzętu czy oprogramowania. Cyberrozpoznanie jest pojęciem szerszym niż rozpoznanie cyberzagrożeń

i obejmuje rozpoznanie cyberzagrożeń, jednak dane i informacje pochodzące z rozpoznania cyberzagrożeń to tylko część materiału rozpoznawczego pozostającego w zainteresowaniu cyberrozpoznania.

Stosowane w rozpoznaniu wojskowym skale ocen znajdują zastosowanie w ocenie wiarygodności danych i informacji pochodzących z cyberrozpoznania oraz pewności ich źródła. Poprzez analogię do rozpoznania radioelektronicznego - cyberrozpoznanie Autor uznał za składową (podsystemem) systemu rozpoznania wojskowego sił zbrojnych. Stwierdził, iż stanowi ona układ organizacyjnie i funkcjonalnie powiązanych elementów, które zbierają informacje o obiektach przeciwnika w cyberprzestrzeni oraz funkcjonujących, w oparciu o nią, poprzez poszukiwanie, przechwytywanie, śledzenie, namierzanie oraz analizę informacji, przetwarzają je do postaci zrozumiałej przez użytkownika, a w ostateczności udostępniają i dostarczają odbiorcy. Kolejnym istotnym ustaleniem w procesie badań naukowych jest to, że wykorzystując cyberbroń, siły zbrojne mogą prowadzić działania zarówno obronne jak i zaczepne, w tym przeprowadzać cyberataki. Na podstawie teorii taktyki określono także, że w cyberwalce jako militarnym wymiarze działań cyberobrona, obok cybernatarcia i wycofania, stanowi jeden z podstawowych rodzajów działań. Ze względu na przestrzeń, w czasie prowadzenia cyberwalki żołnierze nie mogą skorzystać z relatywnie komfortowej, a w określonych warunkach korzystnej formy działań militarnych, jaką jest rozumiane w tradycyjny sposób wycofanie. Jednak możliwe jest wycofanie się (uchylenie) z prowadzenia cyberdziałań. Warto zauważyć, że w okresie pokoju codzienną rutyną sił zbrojnych jest cyberochrona własnych zasobów. Dla zwiększenia przewagi nad przeciwnikiem stosowane jest cyberodstraszanie.

Wybór celów, nadanie im priorytetów oraz dobór i realizacja odpowiedniego sposobu oddziaływania na te cele siły zbrojne dokonuje się w ramach procesu targetingu. Cyberdziałania nie ograniczają się jedynie do stacjonarnych sieci oraz systemów teleinformatycznych. Dla zachowania mobilności mogą być prowadzone w oparciu o spektrum elektromagnetyczne. Takie działania nazywane są przez Autora cyberelektromagnetycznymi. Zwiększenie anonimowości oraz anonimizacji własnych cyberdziałań zapewnia cybermaskowanie. Ważnym z punktu widzenia rozwoju teorii cyberwalki jako militarnego wymiaru działań są zidentyfikowane i zdefiniowane terminy: cyberobrona, cyberbroń, cyberatak, cyberodstraszanie militarne i cyberelektromagnetyczne działania militarne.

W podsumowaniu rozdziału sformułowano wnioski.

Rozdział szósty nt.: „*Wpływ otoczenia na zdolność sił zbrojnych do prowadzenia cyberwalki*" poświęcony jest rozwiązaniu szczegółowego problemu badawczego sformułowanego w postaci pytania: *Jak na zdolności sił zbrojnych do prowadzenia cyberwalki wpływa otoczenie*? Rozdział prezentuje badania nad ewolucją zdolności SZ RP od cyberochrony po zdolność do cyberdziałań ofensywnych.

Autor wykazał, że na przestrzeni lat SZ RP dostosowywały się do cyberzagrożeń w otoczeniu. Zmieniając swoje struktury organizacyjne, przygotowały się do cyberochrony własnych sieci i systemów teleinformatycznych. Utworzony został system reagowania na incydenty komputerowe. Sformowano struktury właściwe do działań zarówno defensywnych oraz ofensywnych. Powołano do życia ośrodki szkoleniowe doskonalenia specjalistycznego. Zreformowano wyższe wojskowe szkolnictwo w kierunku przygotowania stosownych kadr. W rozdziale tym zidentyfikowano również rosyjski punkt widzenia na cyberdziałania, który ma odzwierciedlenie w kontekście osiągania zdolności SZ RP do cyberwalki jako militarnego wymiaru działań. Zwrócono uwagę na wpływ cyberdziałań prowadzonych przez Federację Rosyjską na obszarze europejskim, który nie jest ograniczony jedynie do Polski. Habilitant słusznie zauważył, że działalność wrogich podmiotów, pojawiające się nowsze zagrożenia i wyzwania prowadzą do powstawania sojuszy, koalicji oraz zawierania dwu- lub

wielostronnych porozumień w zakresie cyberwalki. Zatem polskie siły zbrojne, aby być równoważnym partnerem w NATO, muszą rozwijać zdolność do zdefiniowanych przez Autora interoperacyjnych cyberdziałań, a rozwijanie cyberrozpoznania ukierunkowanego na potencjalnego oponenta staje się koniecznością. Z kolei zapewnienie cyberwojskom ochrony prawnej wymaga zmian legislacyjnych. Na koniec tego rozdziału zaprezentowano wyniki rozważań naukowych nad interoperacyjnością w cyberwalce jako militarnym rodzaju działań.

W podsumowaniu rozdziału sformułowano wnioski.

W **zakończeniu** Autor zawarł wnioski z całości badań oraz treści zaprezentowanych w monografii.

Recenzent pragnie podkreślić, iż jest pod dużym wrażeniem pracy wykonanej przez Habilitanta w zakresie dokonania badań w tak rozległym obszarze związanym z cyberwalką. Uwaga Pana dr Roberta JANCZEWSKIEGO skupiona była przede wszystkim na funkcjonowaniu cyberwojsk w odniesieniu do realizacji zadań na rzecz wojsk lądowych, jako największego komponentu SZ RP w okresie pokoju, kryzysu oraz wojny. Oceniam, że jego monografia prezentuje szereg cennych konkluzji badawczych wnosząc do rozwoju nauk o bezpieczeństwie liczne wartości poznawcze.

Monografia zawiera teorię cyberwalki, która stanowi istotny wkład wiedzy o niej jako militarnym wymiarze działań do teorii nauk o bezpieczeństwie, a szczególnie w obszarze szeroko rozumianej sztuki wojennej. Prezentuje zwięźle dociekania naukowe na temat cyberwalki jako militarnego wymiaru działań. W syntetyczny sposób opisuje zagadnienia z nią związane i zawiera tylko te pojęcia, które są rzeczywiście niezbędne. Terminy i pojęcia ujęte w monografii dają możliwość tworzenia teorii szczegółowych, zgodnych ze znanymi faktami. Recenzowana monografia oferuje uporządkowaną teorię, która może być stosowana w działaniach zarówno żołnierzy, którzy rozumieją specyfikę cyberwalki, jak i tych, którzy nie rozumieją istoty działań militarnych prowadzonych w cyberprzestrzeni, ale poszukują źródeł wiedzy z tego obszaru. Recenzent podziela pogląd Habilitanta, iż treści zawarte w monografii mogą posłużyć poszerzaniu i porządkowaniu wiedzy dotyczącej teorii i praktyki w odniesieniu do profesjonalnego przygotowania specjalistów, nie tylko na potrzeby sił zbrojnych, ale również takich, które chcą poznać ten wycinek rzeczywistości. Zbudowana oraz przedstawiona teoria cyberwalki jako militarnego wymiaru działań może i powinna być wykorzystana do rozwiązań praktycznych. Uzyskane wyniki badań redukują bariery wynikające z niejednoznaczności desygnatów zarówno cyberwalki, jak i składowych ją tworzących.

W ocenie Recenzenta, układ rozprawy habilitacyjnej jest poprawny, a jej wielowątkowość znajduje odzwierciedlenie w treści poszczególnych rozdziałów oraz jest podporządkowana prezentacji wszystkich celów badawczych i zagadnień zawartych w spisie treści. Przedstawiona do oceny monografia, została napisana zrozumiałym i precyzyjnym językiem.

Recenzent nie znalazł mankamentów w ocenianej monografii, natomiast zdecydował się podkreślić, że aby w pełni zrozumieć ogrom wysiłku dokonanego przez Habilitanta nie wystarczy tylko zapoznać się z ogólnodostępnymi przykładami zagrożeń pochodzącymi z cyberprzestrzeni. W tym przypadku potrzebna jest również szeroka wiedza o zakresu telekomunikacji, informatyki, a także bezpiecznego zastosowania nowoczesnych technologii dla potrzeb SZ RP. Oceniam, iż Habilitant dokonał czegoś więcej - postarał się dodatkowo uporządkować dotychczasową wiedzę na ten temat oraz niewątpliwie wniósł znaczny wkład do teorii nauk o bezpieczeństwie prezentując wyniki swoich rozważań badawczych.

Według Recenzenta, monografia przeznaczona jest dla teoretyków i praktyków z obszaru szeroko rozumianego bezpieczeństwa teleinformatycznego z szczególnym uwzględnieniem cyberprzestrzeni, która aktualnie jest istotnym obszarem zainteresowania nauk o bezpieczeństwie. Na podkreślenie zasługuje fakt, że choć niniejsze opracowanie

dotyczy wycinka obszaru bezpieczeństwa, to stanowić może punkt wyjściowy do poszerzonych badań rzutujących na funkcjonowanie całych sił zbrojnych w kontekście cyberbezpieczeństwa w aspekcie konieczności prowadzenia działań kinetycznych oraz niekinetycznych.

Monografia stanowi cenny materiał do dogłębnej analizy. Osiągnięcie naukowe powinno spotkać się z zainteresowaniem decydentów, przedstawicieli sił zbrojnych oraz ekspertów zajmujących się problematyką cyberbezpieczeństwa, nie tylko związanych z szeroko rozumianą teleinformatyką. Oceniam, że może stanowić płaszczyznę do realizacji procesu dydaktycznego na kierunkach studiów związanych z bezpieczeństwem w obszarze cyberprzestrzeni, teleinformatycznym oraz nowoczesnych technologii. Niewątpliwie recenzowana rozprawa zawiera syntezę wieloletnich prac badawczych oraz doświadczeń zawodowych Autora.

Propozycje rozwiązań zaprezentowane przez Habilitanta stanowią oryginalne inicjatywy w kontekście posiadanych zdolności w obszarze cyberbezpieczeństwa ukierunkowanych na prowadzenie cyberwalki. Pozwala to na stwierdzenie o znaczącym wkładzie Habilitanta w rozwój nauki, szczególnie dla dyscypliny nauki o bezpieczeństwie.

Reasumując oceniam, że rozprawa habilitacyjna dr Roberta JANCZEWSKIEGO w pełni odpowiada wymogom aktualnie obowiązujących przepisów w zakresie prezentacji dorobku naukowego.

Na podstawie powyższych faktów można wnioskować, że opracowanie recenzowanej monografii wymagało od Habilitanta rzetelnego przygotowania, systematyczności oraz wytrwałości w pracy badawczej, jak również szerokiej wiedzy o funkcjonowaniu tego obszaru systemów i sieci teleinformatycznych w SZ RP.

Rozprawa stanowi zwartą, logiczną całość, w głównej mierze opartą na oryginalnych koncepcjach Autora, znajdujących swe odbicie w jego publikacjach.

3.6. Informacja o spełnieniu przez kandydata kryterium dotyczącego wykazania się istotną aktywnością naukową:

Działalność naukową dr Roberta JANCZEWSKIEGO można podzielić na dwa główne obszary tematyczne. Są one pochodną jego awansów naukowych, pełnionych funkcji i osobistych zainteresowań naukowych.

Pierwszy obszar badawczy związany był z procesami informacyjnymi, rozpoznaniem elektronicznym i w efekcie procesami informacyjnymi w rozpoznaniu elektronicznym.

Drugi obszar dociekań naukowych dotyczył cyberbezpieczeństwa układu militarnego w powiązaniu z układem pozamilitarnym, identyfikacji przestrzeni prowadzenia cyberwalki, cyberzagrożeń, zależności zachodzących między rozpoznaniem elektronicznym a cyberrozpoznaniem i w efekcie cyberwalki jako militarnego wymiaru działań.

W pierwszym obszarze badawczym, który został zapoczątkowany w 2001 roku po uzyskaniu tytułu magistra inżyniera telekomunikacji, swoje rozważania naukowe Habilitant skupił na procesach informacyjnych w rozpoznaniu elektronicznym. Wynikały z obserwacji, że przestrzeń walki uzależniła się od urządzeń elektronicznych. Dzięki zaawansowanej elektronice operacje wojskowe zaczęły być prowadzone precyzyjnie i znacząco wzrosły działania przy użyciu fal elektromagnetycznych, które decydują o mobilności wojsk. Potwierdza to fakt, że wszystkie rodzaje sił zbrojnych oraz wojsk posługiwały się oraz zwiększyły zakres eksploatacji radiowego sprzętu elektronicznego. To samo miało miejsce oraz aktualnie dotyczy dedykowanych systemów radiokomunikacyjnych dla potrzeb cywilnych oraz innych formacji mundurowych. W ślad za Autorem wypada zauważyć, iż powyższe odzwierciedla powszechne trendy stosowania fal EM dla potrzeb wojskowych, jak

i pozamilitarnych, w relacjach sojuszniczych w ramach NATO, jak i potencjalnego przeciwnika. Natomiast wraz z rozwojem technologicznym są one coraz bardziej wyspecjalizowane.

Dociekania naukowe nad rozpoznaniem elektronicznym zaowocowały identyfikacją konieczności implementacji eksploracji danych do standardowych procedur przetwarzania danych, co pozwala na otrzymywanie zależności oraz podsumowania zwane modelami i wzorcami. Wyniki badań zaprezentowano w publikacji: R. Janczewski, *Eksploracja danych w rozpoznaniu elektronicznym*, [w:] W. Scheffs (red.), *Nowe kierunki w rozpoznaniu Sił Zbrojnych RP*, AON, Warszawa 2013, ISBN 978-83-7523-225-7.

Aktywność naukowa Habilitanta w Akademii Obrony Narodowej w obszarze nauk o obronności zaowocowała opracowaniem i wprowadzeniem do tych nauk nowej metody badawczej – *triangulacji*. O wynikach pracy poinformowano społeczność naukową podczas III Konferencji Doktorantów Wydziału Zarządzania i Dowodzenia AON pt. „Wybrane metody, techniki i narzędzia badawcze stosowane w obszarze nauk społecznych w Akademii Obrony Narodowej w Warszawie", w dniu 8 marca 2013 r. poprzez wygłoszenie referatu nt. *Triangulacja jako metoda badawcza w naukach o obronności.* Wyniki badań zawarto w artykule: R. Janczewski, *Triangulacja jako metoda badawcza w naukach o obronności*, Obronność Zeszyty Naukowe, Nr 2(6)/2013, ISSN 2084-7297.

Dociekania naukowe przyczyniły się do ustalenia, że proces informacyjny w rozpoznaniu elektronicznym wojsk lądowych spełnia kryteria właściwe dla systemu działania. Wyniki badań wraz z wnioskami przedstawiono w artykule naukowym. Wnioski z analizy i krytyki literatury dotyczącej walki elektronicznej, uwidoczniły lukę w wiedzy na temat procesów informacyjnych w rozpoznaniu elektronicznym. W wyniku badań ustaliłem, że bariery informacyjne w rozpoznaniu elektronicznym WL SZ RP nie są opisane w literaturze przedmiotu.

Istotnym wkładem do nauk o obronności było uzyskanie odpowiedzi na sformułowany w postaci pytania główny problem badawczy: *Jakie czynniki warunkują przebieg i strukturę procesu informacyjnego?* Uzyskane wyniki badań zamieszczono w publikacji: R. Janczewski, *Systemowy charakter procesu informacyjnego w rozpoznaniu elektronicznym Wojsk Lądowych Sił Zbrojnych Rzeczypospolitej Polskiej*, AON, Wydział Zarządzania i Dowodzenia, Zeszyty Naukowe Obronność, Nr 2/2015, ISSN 2084-7297.

Istotnym dla nauk o obronności było ustalenie, że proces informacyjny w RE WL SZ RP posiada strukturę zależną od przyjętego kryterium, czyli przestrzenną, informacyjną, organizacyjną, proceduralną i techniczną. Dekomponuje się na etapy: zbierania, przetwarzania, przechowywania i udostępniania danych i informacji rozpoznawczych. Każdy z tych etapów dekomponuje się na fazy, a każda z faz składa się z czynności realizowanych przez wyspecjalizowany personel. Proces informacyjny jest systemem niematerialnym. Realizowany jest za pomocą zasobów technicznych, ludzkich i proceduralnych systemu informacyjnego rozpoznania elektronicznego. Wynikiem dociekań naukowych nad procesami informacyjnymi w rozpoznaniu elektronicznym Wojsk Lądowych Sił Zbrojnych Rzeczypospolitej Polskiej jest monografia naukowa: R. Janczewski, *Procesy informacyjne w rozpoznaniu elektronicznym Wojsk Lądowych Sił Zbrojnych Rzeczypospolitej Polskiej*, Akademia Sztuki Wojennej, Warszawa 2019, ISBN 978-83-7523-851-8.

W obszarze badawczym dotyczącym wpływu teleinformatyki na działania militarne poszukiwania badawcze Habilitana ewoluowały w kierunku poszukiwań desygnatu cyberbezpieczeństwa i identyfikacji nowych zależności w tym obszarze. Korzystając z własnych dotychczasowych eksploracji naukowych zidentyfikował procesy informacyjne w systemie wspomagania dowodzenia w kontekście działania w środowisku cybernetycznym. Istotnym osiągnięciem naukowym tych dociekań było wyizolowanie środowiska działań militarnych w cyberprzestrzeni wraz z jego *czynnikami* i *elementami* nazwanego

środowiskiem cybernetycznym i zdefiniowanie go już w 2013 roku. Szczegółowy opis rozważań naukowych zawarto w publikacji: R. Janczewski, *Procesy informacyjne w systemie wspomagania dowodzenia w kontekście działania w środowisku cybernetycznym*, [w:] J. Wołejszo (red.), *Automatyzacja dowodzenia SZ RP w środowisku sieciocentrycznym, Monografia zbiorowa z konferencji naukowej*, Gdynia - Warszawa, Czerwiec 2013, ISBN 978-83-930150-3-0.

Procesy informacyjne oraz środowisko cybernetyczne stały się podstawą badań zmierzających do identyfikacji cyberzagrożeń. Ustalono, że każdy proces informacyjny jest jednocześnie procesem semiotycznym, technicznym, proceduralnym, organizacyjnym oraz ekonomicznym, w których mogą występować podatności sieci i systemów teleinformatycznych na cyberzagrożenia. Potwierdza to publikacja Habilitanta: R. Janczewski, *Identyfikacja cyberzagrożeń* [w:] M. Frączek, M. Marczyk (red.), *Wybrane aspekty bezpieczeństwa cybernetycznego Sił Zbrojnych Rzeczypospolitej Polskiej*, AON, Warszawa 2014, ISBN 978-83-7523-372-8.

Pan Doktor ustalił, że istota cyberzagrożeń powoduje, że zarówno użytkownicy jak i właściciele systemów oraz sieci teleinformatycznych nie mają wpływu na istnienie cyberzagrożeń, które są jedynie potencjalnym czynnikiem wywołującym szkodę. Może być przyczyną niepożądanych wyników w rezultacie, których może nastąpić zakłócenie procesu informacyjnego bądź jego przerwanie. Cyberzagrożenie, zatem może wywołać niepożądany skutek. Skutki niepożądane nie zawsze są szkodliwe, ale szkodliwe zawsze są niepożądane. Wyniki badań prowadzonych w Akademii Obrony Narodowej zawarto w opracowaniu: R. Janczewski, *Bezpieczeństwo procesów informacyjnych w środowisku cybernetycznym*, [w:] M. Marczyk, B. Biernacik (red.), *Wybrane aspekty bezpieczeństwa cybernetycznego Sił Zbrojnych Rzeczypospolitej Polskiej*, Akademia Sztuki Wojennej, Warszawa 2015, ISBN 978-83-7523-422-0.

Aktywność badawcza Habilitanta w Akademii Obrony Narodowej zaowocowała uczestnictwem w latach 2015-2016 w międzynarodowym projekcie badawczym na rzecz rozwoju rozwiązań - Multinational Capabilities Development Campaign (MCDC) 15-16, której celem było wspólne opracowywanie koncepcji i możliwości, które można wykorzystać do sprostania wyzwaniom związanym z prowadzeniem międzynarodowych operacji. Projekt badawczy rozwoju zdolności międzynarodowych miał na celu identyfikację i ocenę potencjalnych luk w zdolnościach międzynarodowych (w tym koalicyjnych). Uczestniczył w roli członka projektu w obszarze Multinational Defensive Cyber Operations (MDCO), którego celem było stworzenie zasad i wskazówek do planowania Wielonarodowych Operacji Obronnych w Cyberprzestrzeni (MDCO), które powtarzalne procesy wesprą Dowódcę Wielonarodowych Sił w opracowaniu szybszych sposobów skutecznej integracji sił wielonarodowych w celu prowadzenia defensywnych cyberoperacji.

Drugi obszar badawczy, przypadający na okres po uzyskaniu stopnia doktora nauk o obronności związany jest militarnymi aspektami działań w cyberprzestrzeni. Aktywność naukowa w tym obszarze wynikała potrzeby uzupełnieni luki poznawczej. Brak opracowań naukowych w tym zakresie stanowił istotną przyczynę podjęcia badań i uzyskania wyników, które mogą stanowić podstawę zarówno do dalszych naukowych eksploracji przedmiotowego obszaru jak i realizacji praktycznych rozwiązań związanych z osiąganiem przez SZ RP zdolności do skutecznych działań w cyberprzestrzeni. Wyniki aktywności naukowej zawarto w opracowaniach krajowych i zagranicznych w postaci polskich i anglojęzycznych artykułów i rozdziałów monografii naukowych. Szczegóły dotyczące aktywności naukowej zostały zaprezentowane przez dr Roberta JANCZEWSKIEGO w jego Autoreferacie i stały się fundamentem powstania recenzowanej monografii oraz dorobku naukowo-badawczego.

3.7. Wykaz osiągnięć projektowych, konstrukcyjnych, technologicznych:

Oceniam, że Kandydat do stopnia doktora habilitowanego wskazał w swoim dorobku na osiągnięcia technologiczne w aspekcie wdrażania w Siłach Zbrojnych RP nowej metody badawczej w naukach o obronności.

Habilitant opracował propozycję 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 pt.: *Nowe technologie w obszarze bezpieczeństwa i obronności państwa* o kryptonimie PERUN. Projekt przewidziany do realizacji na IX poziomie gotowości technologii.

W ramach recenzowanego dorobku naukowego, a w szczególności wskazanej monografii, Autor wykazał się istotną aktywnością naukową badając szereg zjawisk, powiązań, zależności oraz zawiłości terminologicznych związanych przede wszystkim z obszarem cyberwalki, który wcześniej nie znalazł swego odzwierciedlenia w jednym, kompleksowym oraz wieloaspektowym opracowaniu naukowym.

3.8. Informacja o osiągnięciach dydaktycznych, organizacyjnych i popularyzujących naukę kandydata do stopnia doktora habilitowanego:

W opinii Recenzenta, warto podkreślić, iż Pan dr Robert JANCZEWSKI jest wykładowcą akademickim od 2002 roku, z przerwami na realizację zadań służbowych w ramach SZ RP. Posiada bogate doświadczenie dydaktyczne o czym świadczy lista uczelni ujęta w punkcie 1.3. niniejszej recenzji, które chętnie współpracowały oraz nadal korzystają z wiedzy oraz doświadczenia Habilitanta. Nie mniej istotnym elementem dydaktyki, która była realizowana przez Pana Doktora był udział w charakterze eksperta w licznych ćwiczeniach z wojskami oraz w szkoleniach specjalistycznych dedykowanych dla żołnierzy zajmujących się obszarem cyberbezpieczeństwa (posiada 7 certyfikatów potwierdzających kwalifikacje). W ramach realizacji zajęć dydaktycznych prowadził przedmioty oraz wykłady takie jak:

1. Wyższa Szkole Biznesu i Zarządzania w Ciechanowie:
   - Systemy operacyjne,
   - Bazy danych,
   - Metody i narzędzia modelowania systemów informacyjnych.
2. Wyższa Szkoła Policji w Szczytnie:
   - Inżynieria wiedzy - wstęp do sztucznej inteligencji.
3. Uniwersytet Warmińsko-Mazurski w Olsztynie:
   - Informatyczne systemy bezpieczeństwa.
4. Akademia Marynarki Wojennej w Gdyni:
   - Cyberbezpieczeństwo,
   - Zarządzanie systemami bezpieczeństwa wewnętrznego,
   - Planowanie operacji w cyberprzestrzeni,
   - Audyt bezpieczeństwa systemów teleinformatycznych.
5. Wykłady w ramach Letniej Szkoły Cyberbezpieczeństwa.
6. Wykłady w ramach Zimowej Szkoły Cyberbezpieczeństwa.
7. Wykłady w Centrum Doskonalenia Zawodowego Oficerów AON.
8. Wykłady i ćwiczeń w ramach wyższego kursu operacyjno-strategicznego na Wydziale Wojskowym ASzWoj w ramach przedmiotu bezpieczeństwo w cyberprzestrzeni.

9. Wykłady i ćwiczeń w ramach wyższego kursu operacyjno-strategicznego na Wydziale Wojskowym ASzWoj w ramach przedmiotu bezpieczeństwo w cyberprzestrzeni.
10. Cykl wykładów z cyberbezpieczeństwa w The Vasil Levski National Military University, Veliko Tarnovo, Bulgaria, 27-31.05.2019 r.
11. Wykłady w dniach 10-14.06.2019 roku w języku angielskim, w „Nicolae Balcescu" Land Forces Academy, Sibiu, Bułgaria, nt. Terminology as a barrier of NATO's interoperability in cyberspace operations.
12. Prelekcje w Centrum Doktryn i Szkolenia Sił Zbrojnych.
13. Wykłady w Centrum Doskonalenia Zawodowego Oficerów AON.
14. Wykłady i ćwiczeń w ramach wyższego kursu operacyjno-strategicznego na Wydziale Wojskowym ASzWoj w ramach przedmiotu bezpieczeństwo w cyberprzestrzeni.
15. Wykłady i ćwiczeń w ramach wyższego kursu operacyjno-strategicznego na Wydziale Wojskowym ASzWoj w obszarze bezpieczeństwa w cyberprzestrzeni.
16. Wykłady w ramach szkolenia administratorów i inspektorów bezpieczeństwa w 3 Warszawskiej Brygadzie Rakietowej Obrony Powietrznej nt.:
    - Działania w cyberprzestrzeni,
    - Cyberzagrożenia.
17. Wykłady w ramach szkolenia administratorów i inspektorów bezpieczeństwa w 9 Brygadzie Wsparcia Dowodzenia nt.:
    - Działania w cyberprzestrzeni,
    - Cyberzagrożenia.
18. Wykłady w czasie warsztatów SZ RP pk. OPERATOR-15 nt. Planowanie operacyjne realizowane przez Siły Zbrojne RP w zakresie działań w cyberprzestrzeni – integralny element polityczno-strategicznego planowania obronnego RP.
19. Wykłady w ramach program MON "Cyber.mil z klasą" w:
    - I Liceum Ogólnokształcące im. Jana Kasprowicza w Inowrocławiu,
    - I Liceum Ogólnokształcące im. Władysława Broniewskiego w Świdniku,
    - I Liceum Ogólnokształcące im. Stefana Żeromskiego w Lęborku.
20. Szkolenia w języku angielskim ukraińskich podchorążych z Military Institute of Telecommunications and Information Technologies named after Heroes of Kruty w ramach „Officer training academic program in the specialty cybersecurity" w zakresie „Fundamentals of information security management".
21. Wykład nt. *Planowanie interoperacyjności cyberdziałań* podczas webinarium nt.: „Specyfika, zachodzące zmiany i wpływ środowiska elektromagnetycznego oraz cyberprzestrzeni na środowisko bezpieczeństwa z uwzględnieniem perspektywy długoterminowej" organizowanego przez CDiS w ramach kampanii analiz środowiska bezpieczeństwa pk. „Nowe Urządzenia Polskie – NUP 2X35, 26.05.2021 r.
22. Wykłady i ćwiczeń w Państwowej Uczelni Zawodowej im, Ignacego Mościckiego w Ciechanowie w ramach przedmiotów:
    - Programowanie obiektowe I (C++),
    - Systemy operacyjne,
    - Programowanie obiektowe II (JAVA&J2EE),
    - Aplikacje Microsoft .NET,
    - Aplikacje WWW,
    - Grafika, multimedia i komunikacja człowiek – komputer,
    - Bezpieczeństwo systemów komputerowych,

- Metody programowania,
- Inżynieria oprogramowania (Wykłady),
- Inżynieria oprogramowania (Laboraorium),
- WebGL i grafika 3D,
- Wstęp do programowania,
- Wprowadzenie do sztucznej inteligencji,
- Przedmiot ogólnouczelniany - Grafika komputerowa,
- Seminarium dyplomowe.

23. Cykl szkoleń z kierowniczą kadrą Agencji Rezerw Materiałowych w ramach zagadnienia: Współczesne zagrożenia bezpieczeństwa państwa, w szczególności zagrożenia cyberprzestrzeni dla systemów teleinformatycznych oraz usuwanie ich negatywnych skutków w sytuacji podwyższenia gotowości obronnej państwa i w czasie wojny.
24. Szkolenia dla Poczty Polskiej S.A. nt. „Audyt organizacji i funkcjonowania procesu zarządzania cyberbezpieczeństwem".
25. Szkolenia dla Ministerstwo Klimatu i Środowiska, „Krajowy system cyberbezpieczeństwa", 11.12.2020 r.
26. Wykłady w ramach studiów podyplomowych Executive MBA „Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi w Akademii Marynarki Wojennej".
27. Wykłady nt. *Cyberbezpieczeństwo – kategoria międzydyscyplinarna* w ramach konferencji pt. „Bezpieczeństwo jako przedmiot edukacji" organizowanej przez Mazowieckie Samorządowe Centrum Doskonalenia Nauczycieli w dniu 31.05.2023 roku.
28. Wykłady nt. *Po co nam cyberbezpieczeństwo* w czasie Wojskowego Dnia Otwartego inaugurującego projekt AKADEMIA_CYBER_MIL w Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie w dniu 24.09.203 r.

Praca nauczyciela akademickiego związana była również z prowadzeniem seminariów licencjackich, magisterskich i dyplomowych. Jest promotorem następującej ilości dyplomantów:

1. prac dyplomowych MBA – 11,
2. prac dyplomowych studiów podyplomowych – 2,
3. prac licencjackich – 12,
4. prac magisterskich – 3,
5. prac inżynierskich – 2,
6. prac doktorskich – 3.

Aktywność naukowa Habilitanta zaowocowała również opracowaniem „Założeń zmian w podstawie programowej kształcenia ogólnego w zakresie edukacji dla bezpieczeństwa i obszar cyberbezpieczeństwo w wymiarze wojskowym" na zlecenie Ministerstwa Edukacji.

Jest autorem, organizatorem i wykonawcą warsztatów cyberbezpieczeństwa dla uczestników ze szkół średnich z szesnastu województw Polski uczestniczących w programie Ministerstwa Obrony Narodowej „CYBER.MIL z klasą" organizowanych w Akademii Marynarki Wojennej w Gdyni.

W ramach popularyzacji nauki opublikował niżej wskazane artykuły:

1) R. Janczewski, *Walka w cyberprzestrzeni*, Przegląd Sił Zbrojnych, 2018, Nr 01.
2) R. Janczewski, *Cyberprzestrzeń – część teatru działań hybrydowych*, Przegląd Sił Zbrojnych, 2019, Nr 02.
3) R. Janczewski, *Facing the New Risks of Digitised Wars*, European Security, 6. November 2019.
4) R. Janczewski, *Wojska obrony cyberprzestrzeni – formacja do zadań specjalnych*, Special Ops, Nr 6(73) 2021. https://www.special-ops.pl/artykul/jednostki-

specjalne/83874,wojska-obrony-cyberprzestrzeni-formacja-do-zadan-specjalnych 2080-8771.

5) R. Janczewski, Cyberatak, cyber atak, a może cyber-atak – to jak jest z tą pisownią?, 10.10.2022 r., https://security-ops.pl/cyberbezpieczenstwo/cyberatak-cyber-atak-a-moze-cyber-atak-to-jak-jest-z-ta-pisownia/.
6) R. Janczewski, *Współdziałanie Sił Zbrojnych RP i Policji dla zapewnienia cyberbezpieczeństwa infrastruktury krytycznej państwa w czasie działań hybrydowych prowadzonych na terenie RP*, Przegląd Policyjny, 4(132)/2018, ISSN 0867-5708.
7) R. Janczewski, G. Pilarski, *Comprehending Gerasimov's Perception of a Contemporary Conflict – The Way to Prevent Cyber Conflicts*, Academic and Applied Research in Military and Public Management Science, the National University of Public Service, Budapest, Hungary 2018, ISSN 2498-5392.
8) 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, ISBN 978-1-5386-0519-6
9) R. Janczewski, G. Pilarski, M. Marczyk, *Terminology as a barrier to NATO's interoperability in cyberspace operations*, The Knowledge-Based Organization, XXV/3, DOI: https://doi.org/10.2478/kbo-2019-0113.
10) 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, ISBN 978-83-65763-12-9.
11) 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, ISSN 1843-6722DOI: https://doi.org/10.2478/kbo-2019-0113. (1 pkt.) (Czasopismo spoza wykazu)

Istotnym osiągnięciem Pana Doktora jest uczestnictwo jako Eksperta ds. cyberbezpieczeństwa w pracach zespołu, który opracował pierwszy w historii NATO pilotażowy plan ćwiczeń z zakresu cyberbezpieczeństwa „The Exercise Plan CYBER PHALANX 2018" w ramach *Multinational Capabilities Development Campaign (MCDC) 17-18 – International Cyberspace Operations Planning Curricula (ICOPC) Project*. 2017-2018 r.

W ramach swojej działalności naukowej i zawodowej 21 razy był Ekspertem ds. cyberbezpieczeństwa lub działań militarnych w cyberprzestrzeni w różnego rodzajach zespołach autorskich opracowujących doktryny na potrzeby SZ RP oraz ćwiczeniach.

Współpraca z otoczeniem społecznym i gospodarczym:

1. Prelekcja dotycząca cyberbezpieczeństwa w Agencji Rezerw Materiałowych.
2. Współpraca z GRAAL S.A. z siedzibą w Wejherowie, 84-200, ul. Zachodnia 22 w zakresie testów bezpieczeństwa, szczególnie testów penetracyjnych.
3. Udział w projekcie utworzenia CyberParku Technologicznego, stanowiącego platformę współpracy nauki, przemysłu i wojska.
4. Prelekcja na webinarium pt. „Dezinformacja i propaganda w sektorze bankowym" organizowanym przez Fundację Warszawski Instytut Bankowości nt. *Sposoby identyfikacji kampanii informacyjnych.*
5. Współpraca z Collegium Intermarium w zakresie *Bezpieczeństwa informacji* oraz *Analiza i śledzenie cyberzagrożeń.*

6. Współudział w opracowaniu pytań kompetencyjnych w obszarze bezpieczeństwa technicznego dla Poczty Polskiej S.A.
7. Wykładów w ramach program MON "Cyber.mil z klasą" w: I Liceum Ogólnokształcące im. Jana Kasprowicza w Inowrocławiu,
   - I Liceum Ogólnokształcące im. Władysława Broniewskiego w Świdniku,
   - I Liceum Ogólnokształcące im. Stefana Żeromskiego w Lęborku.

Współpraca z sektorem gospodarczym:

1. Przeprowadzenie cyklu szkoleń z kierowniczą kadrą Agencji Rezerw Materiałowych w ramach zagadnienia: *Współczesne zagrożenia bezpieczeństwa państwa, w szczególności zagrożenia cyberprzestrzeni dla systemów teleinformatycznych oraz usuwanie ich negatywnych skutków w sytuacji podwyższenia gotowości obronnej państwa i w czasie wojny.*
2. Przeprowadzenie szkolenia dla Poczty Polskiej S.A. nt. „Audyt organizacji i funkcjonowania procesu zarządzania cyberbezpieczeństwem", 21-22.12.2020 rok.
3. Forum ekonomiczne 2020, „Europa po pandemii: Solidarność, Wolność, Wspólnota?" Karpacz, 8-10.09.2020 r., panelista w panelu: „#Cyberbezpieczny Samorząd - jak zrobić to dobrze?".
4. Forum ekonomiczne 2020, „Europa po pandemii: Solidarność, Wolność, Wspólnota?" Karpacz, 8-10.09.2020 r. panelista w panelu: „Rosja, Chiny, Iran, Cyber. Największe wyzwania dla utrzymania bezpieczeństwa w Europie".
5. Przeprowadzenie szkolenia dla Ministerstwa Klimatu i Środowiska, „Krajowy system cyberbezpieczeństwa", 11.12.2020 r.
6. Kierownik zadania badawczego nr 4400120192 nt. „Threat assessment for cyber threats assessment for Baltica 2 Offshore Windfarm in Polish exclusive economic zone (EEZ) EWB2_CIS" realizowanego na zamówienie PGE Baltica Sp. z o.o. oraz Ørsted.
7. Kierownik zadania badawczego nr 4400120186 nt. „Threat assessment for cyber threats assessment for Baltica 3 Offshore Windfarm in Polish exclusive economic zone (EEZ)EWB3_CYNIA" realizowanego na zamówienie PGE Baltica Sp. z o.o. oraz Ørsted.
8. Kierownik zadania badawczego nr 4400120193 nt. „Threat assessment for physical threats assessment for Baltica 2 Offshore Windfarm in Polish exclusive economic zone (EEZ) EWB2_ FLOKS" realizowanego na zamówienie PGE Baltica Sp. z o.o. oraz Ørsted.
9. Kierownik zadania badawczego nr 4400120191 nt. „Threat assessment for physical threats assessment for Baltica 3 Offshore Windfarm in Polish exclusive economic zone (EEZ) EWB3_ FIKUS" realizowanego na zamówienie PGE Baltica Sp. z o.o. oraz Ørsted.

Wykonanie 4 ekspertyz:

1. Opinia ekspercka „*Wspólnego komunikatu do parlamentu europejskiego i rady. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę JOIN(202)18*" w ramach przygotowania stanowiska Rządu do dokumentu.
2. Wywiad ekspercki w ramach badań doktoranckich prowadzonych w NATO CCDCOE in Tallinne, Estonia przez doktorantów z Australian Defence Force Academy.
3. Opracowanie eksperckie „Założeń zmian w podstawie programowej kształcenia ogólnego w zakresie edukacji dla bezpieczeństwa i obszar cyberbezpieczeństwo w wymiarze wojskowym" na zlecenie Ministerstwa Edukacji, 2022 r.
4. Raport z postępowania „Dezinformacja i propaganda w sektorze bankowym" opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski

Instytut Bankowości. Autor rozdziału 5 *Propozycja narzędzi do zwalczania kampanii informacyjnych* i współautor rozdziału 3 *Modele dezinformacji i propagandy w sektorze bankowym.*

Informacja o wystąpieniach na krajowych lub międzynarodowych konferencjach naukowych lub artystycznych, z wyszczególnieniem przedstawionych wykładów na zaproszenie i wykładów plenarnych:

a. krajowe konferencje naukowe:

Według oceny Recenzenta, Habilitant uczestniczył w 13 konferencjach oraz 5 sympozjach naukowych krajowych.

b. międzynarodowe konferencje naukowe:

W opinii Recenzenta, Habilitant uczestniczył w 10 międzynarodowych konferencjach naukowych.

Informacja o udziale w komitetach organizacyjnych i naukowych konferencji krajowych lub międzynarodowych, a także sympozjów, z podaniem pełnionej funkcji:

1) III Konferencja naukowa pt. „Bezpieczeństwo informacyjne w obszarze cyberprzestrzeni", Akademia Marynarki Wojennej w Gdyni, 25-26.06.2017, członek rady naukowej.
2) Sympozjum naukowe nt. „Systemy i sieci teleinformatyczne SZ RP – Wielorakie aspekty bezpieczeństwa cyberprzestrzeni", Akademia Sztuki Wojennej w Warszawie, 05.12.2017 r., prowadzący II sesję pt. „Bezpieczeństwo cyberprzestrzeni". Członek kierownictwa naukowego, prowadzący sesję *bezpieczeństwo cyberprzestrzeni.*
3) Ogólnopolska konferencja naukowa nt. „Bezpieczeństwo danych osobowych w cyberprzestrzeni – szanse, wyzwania, zagrożenia", Akademia Marynarki Wojennej w Gdyni, 04-05.12.2018 r., członek komitetu organizacyjnego, członek rady naukowej.
4) Sympozjum naukowe pt. „Rola i zadania sił zbrojnych dla zapewnienia cyberbezpieczeństwa w czasie działań hybrydowych przeciwko RP", Akademia Sztuki Wojennej, 18.12.2018 r., zastępca przewodniczącego komitetu organizacyjnego, członek komitetu naukowego.
5) Konferencja naukowa pt. „Techniczne Aspekty Przestępczości Teleinformatycznej", Wyższa Szkoła Policji w Szczytnie, 3-4.06.2019 r., członek komitetu naukowego konferencji.
6) Konferencja naukowa pt. Przestępczość Teleinformatyczna XXI wieku, Akademia Marynarki Wojennej, 17-19.06.2019 r., członek rady naukowej.
7) Sympozjum naukowe pt. „Cyberbezpieczeństwo obszaru militarnego i niemilitarnego", Akademia Sztuki Wojennej, 28-29.11.2022, członek komitetu naukowego, członek komitetu organizacyjnego.
8) Międzynarodowa konferencja naukowa pt. „Mathematical Cryptology and Cybersecurity (MC&C 2020)", Wojskowa Akademia Techniczna w Warszawie, 16-17.01.2020 r., Chairman sesji II w dniu 17.01.2020 r.
9) Konferencja PWNing Security Conference, Państwowe Wydawnictwo Naukowe, 17-19.11.2021 r., członek rady programowej konferencji.
10) VI Ogólnopolska konferencja naukowa pt. „Współczesny człowiek wobec zagrożeń w cyberprzestrzeni. Aspekty techniczne, Innowacyjne narzędzia IT kreacji rzeczywistości społecznej", Akademia Pomorska w Słupsku, 23-24.11.2021 r., członek komitetu naukowego konferencji.

11) Konferencja naukowa „Organizacja systemu rozpoznania zagrożeń państwa – priorytetowe potrzeby informacyjne w systemie bezpieczeństwa państwa", Akademia Sztuki Wojennej 14.04.2022 r., członek komitetu naukowego konferencji.
12) I Krajowa konferencja naukowa „Współczesne uwarunkowania maskowania", Akademia Sztuki Wojennej 18.05.2022 r., członek komitetu naukowego konferencji.
13) VII Ogólnopolska konferencja naukowa z cyklu „Bezpieczeństwo informacyjne" nt.: „Cyberprzestrzeń i ochrona informacji jako pole zmagań o bezpieczeństwo informacyjne", Uniwersytet Przyrodniczo-Humanistycznego w Siedlcach, 12.05.2022 r., członek komitetu naukowego.
14) Konferencja naukowa pt. Przestępczość Teleinformatyczna XXI wieku, Akademia Marynarki Wojennej, 13-15.06.2022 r., członek rady naukowej.
15) VIII Ogólnopolska konferencja naukowa z cyklu „Bezpieczeństwo informacyjne" pt.: „Współczesne zagrożenia informacyjne", Uniwersytet Przyrodniczo-Humanistycznego w Siedlcach, 18.05.2023 r., członek komitetu naukowego konferencji.
16) Międzynarodowa interdyscyplinarna konferencja naukowa pt. „Nauki społeczne wobec kryzysów XXI wieku", Państwowa Uczelnia Zawodowa im. Ignacego Mościckiego w Ciechanowie, 27.09.2023 r., członek rady naukowej konferencji.
17) Konferencja naukowa pt. „Dezinformacja. Walka. Wojna. Bezpieczeństwo", Akademia Marynarki Wojennej, 22.05.2023 r., wygłoszenie referatu nt. członek komitetu naukowego.

Informacja o uczestnictwie w pracach zespołów badawczych realizujących projekty finansowane w drodze konkursów krajowych lub zagranicznych, z podziałem na projekty zrealizowane i będące w toku realizacji oraz z uwzględnieniem informacji o pełnionej funkcji w ramach prac zespołów.

1. Wykonanie części projektu: „Identyfikacja zagrożeń cyberprzestrzeni w odniesieniu do funkcjonowania Systemu informacyjno-analitycznego wspomagającego zarządzanie ryzykiem podczas planowania i realizacji działań Policji". W ramach projektu Akademii Marynarki Wojennej DOB-BIO7/02/01/2015 krypt. JANTAR, Etap V, zad. 1.
2. 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, Decyzji Nr 9/2018/GB z dnia 07.11.2018 r.
3. Realizacja w dniach od 01.04.2019 r. do 19.12.2019 r. zadania badawczego: „Cyberbezpieczeństwo w organizacji" w ramach projektu ROTOR realizowanego przez WAT, NCK oraz ABW.
4. 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.
5. Wniosek w ramach konkursu NCN - Konkurs nr KONKURS NR 4/SZAFIR/2021 na projekt „Szerokopasmowy, wielosensorowy system elektroniczno-obrazowego rozpoznania morskiego klasy ELINT/IMINT/AIS dla bezzałogowych statków powietrznych". Współautor wniosku składanego przez Morskie Centrum Cyberbezpieczeństwa w ramach konsorcjum.

6. 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 pn. Nowe technologie w obszarze bezpieczeństwa i obronności państwa o kryptonimie PERUN. Projekt przewidziany do realizacji na IX poziomie gotowości technologii.

Członkostwo w międzynarodowych lub krajowych organizacjach i towarzystwach naukowych wraz z informacją o pełnionych funkcjach:

1. Polskie Towarzystwo Nauk o Bezpieczeństwie, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, ul. Żytnia 39, 08-110 Siedlce, członek zwyczajny.

Członkostwo w komitetach redakcyjnych i radach naukowych czasopism wraz z informacją o pełnionych funkcjach (np. redaktora naczelnego, przewodniczącego rady naukowej, itp.):

1. Członek rady programowej w Roczniku „Cybersecurity&Cybercrime" wydawanym przez Akademię Marynarki Wojennej, ISSN 2720-4251.
2. Redaktor tematyczny działu cyberbezpieczeństwo w „Zeszytach Naukowych Pro Publico Bono" wydawanych przez Szkołę Główną Służby Pożarniczej. ISSN 2719-3403.

Cykl powiązanych tematycznie artykułów naukowych, zgodnie z art. 219 ust. 1. pkt. 2b Ustawy:

Według oceny Recenzenta, cykl powiązanych tematycznie artykułów naukowych po uzyskaniu stopnia doktora stanowią niżej wskazane opracowania:

1. 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, ISBN 978-83-65763-12-9. (20 pkt.)
2. 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, ISSN 1843-6722DOI: https://doi.org/10.2478/kbo-2019-0113. (1 pkt.) (Czasopismo spoza wykazu).

Kandydat do stopnia doktora habilitowanego główne swoje zainteresowania naukowe związał z obszarem cyberbezpieczeństwa.

Z analizy dorobku dr Roberta JANCZEWSKIEGO podczas aktywności zawodowej i naukowej wynika, stale dążył on do poznania i poszerzenia swej wiedzy przede wszystkim z obszaru funkcjonowania bezpieczeństwa cyberprzestrzeni w odniesieniu do funkcjonowania SZ RP ze szczególnym uwzględnieniem jej roli w systemie bezpieczeństwa państwa.

Opublikowane pozycje należy uznać jako istotny dorobek, świadczący również o tym, że Pan dr Robert JANCZEWSKI jest specjalistą z zakresu nauk społecznych, w dyscyplinie nauki o bezpieczeństwie. Z analizy dorobku, który jest spójny i systematyczne rozwijany wynika, iż dysertacja przedstawiona do recenzji stanowi ukoronowanie wieloletnich badań, a Habilitant realizuje zadania badawcze w naukach o bezpieczeństwie w zakresie, który nadal może stanowić obszar dalszej eksploracji oraz wymaga kolejnych wnikliwych rozważań badawczych obejmujących wiele współzależnych zagadnień naukowych.

Dorobek naukowy Habilitanta świadczy o posiadaniu przez niego rozległej wiedzy z obszaru zaprezentowanego w monografii oraz dorobku publicystycznym. Jako Recenzent

oceniam, iż jest ona wystarczająca pod względem ilościowym oraz jakościowym aby ubiegać się o stopień doktora habilitowanego. Według mnie, recenzowany dorobek posiada wartość poznawczą i utylitarną, potwierdzające dojrzałość dr Roberta JANCZEWSKIEGO do samodzielnej pracy naukowej. Podkreśla to również wskazana ilość 19 wyróżnień ujętych w Autoreferacie.

4. KONSTATACJE OGÓLNE I WNIOSKI KOŃCOWE

W konkluzji poczynionych uwag i wskazanych wniosków stwierdzam, że Habilitanta cechuje odpowiednia/ wysoka dojrzałość naukowa i dydaktyczna. Jego wieloletnia działalność naukowo-dydaktyczna, znaczący dorobek naukowy i publicystyczny oraz rozprawa habilitacyjna pozwalają na stwierdzenie, że wniosła ona wiele wartości do teorii w dziedzinie nauk społecznych, a zwłaszcza w dyscyplinie nauki o bezpieczeństwie. Habilitant wykazał się głęboką wiedzą w przedmiocie badań (*„cyberwalka jako militarny wymiar działań"*) oraz wystarczającymi umiejętnościami metodologicznymi.

Wyrażam przekonanie, że przedstawiony dorobek jest wystarczająco oryginalny, twórczy oraz znaczący. Oceniam pozytywnie zarówno dotychczasowy dorobek naukowy, jak również rozprawę habilitacyjną.

Reasumując oceniam, że dorobek naukowy i rozprawa habilitacyjna dr Roberta Adama JANCZEWSKIEGO odpowiada wymogom określonym dla kandydata do stopnia naukowego doktora habilitowanego według obowiązujących przepisów prawa. Według mojej oceny, dorobek Habilitanta spełnia wymagania określone w Ustawie z dnia 20 lipca 2018 roku *Prawo o szkolnictwie wyższym i nauce* (Dz. U. z 2022 r., poz. 574 z późn. zm.). Artykuł 219 ust 1. Pkt.2 i oceniam go POZYTYWNIE. W tej sytuacji kieruję do Komisji Habilitacyjnej wniosek o dopuszczenie Pana dr Roberta Adama JANCZEWSKIEGO do dalszych etapów postępowania habilitacyjnego.

Mariusz Fryc