Autoreferat

1. **Robert Adam Janczewski**
2. **Posiadane dyplomy, stopnie naukowe lub artystyczne – z podaniem podmiotu nadającego stopień, roku ich uzyskania oraz tytułu rozprawy doktorskiej.**
   1. Dyplom inżyniera telekomunikacji, Wyższa Szkoła Łączności i Informatyki, 1996.
   2. Dyplom magistra inżyniera telekomunikacji, Politechnika Warszawska, 2001.
   3. Dyplom doktora nauk o obronności, Wydział Zarządzania i Dowodzenia Akademii Obrony Narodowej, 2016.

      Tytuł rozprawy: *Procesy informacyjne w rozpoznaniu elektronicznym Wojsk Lądowych Sił Zbrojnych Rzeczypospolitej Polskiej.*

Promotor:	prof. dr hab. inż. Marek Wrzosek
Recenzenci:	prof. dr hab. inż. Leopold Ciborowski
	prof. dr hab. inż. Józef Janczak

3. **Informacja o dotychczasowym zatrudnieniu w jednostkach naukowych lub artystycznych.**

   Wyższa Szkoła Biznesu i Zarządzania w Ciechanowie
   2002-2005 – umowa zlecenie na prowadzenie zajęć z zakresu informatyki w każdym roku akademickim.

   Uniwersytet Warmińsko-Mazurski w Olsztynie
   2018-2021 – umowa zlecenie na prowadzenie zajęć w ramach przedmiotu informatyczne systemy bezpieczeństwa na Wydziale Nauk Społecznych Instytutu Nauk Politycznych.

   Akademia Sztuki Wojennej w Warszawie
   2018-2019 – Adiunkt w Zakładzie Cyberbezpieczeństwa w Instytucie Działań Informacyjnych na Wydziale Wojskowym.

   Wyższa Szkoła Policji w Szczytnie
   2019 – umowa zlecenie na prowadzenie zajęć w zakresie informatyki na Wydziale Bezpieczeństwa i Nauk Prawnych.

   Państwowa Uczelnia Zawodowa im. Ignacego Mościckiego w Ciechanowie
   2020-2023 – Adiunkt w Zakładzie Informatyki na Wydziale Inżynierii i Ekonomii.

   Państwowa Akademia Nauk Stosowanych im. Ignacego Mościckiego w Ciechanowie
   od 2023 – Adiunkt w Zakładzie Informatyki na Wydziale Inżynierii i Ekonomii.

   Akademia Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni
   2020-2022 – główny specjalista w Morskim Centrum Cyberbezpieczeństwa na Wydziale Dowodzenia i Operacji Morskich.

   od 2019 – umowa zlecenie na prowadzenie zajęć w zakresie cyberbezpieczeństwa na Wydziale Dowodzenia i Operacji Morskich.

   2019-2022 – umowa zlecenie na prowadzenie zajęć w zakresie cyberbezpieczeństwa na Wydziale Nauk Humanistycznych i Społecznych.

2019-2022 – umowa zlecenie na prowadzenie zajęć na studiach podyplomowych w zakresie cyberbezpieczeństwa na Wydziale Dowodzenia i Operacji Morskich.

2019-2022 – umowa zlecenie na prowadzenie zajęć na studiach MBA w zakresie cyberbezpieczeństwa na Wydziale Dowodzenia i Operacji Morskich.

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.

4. **Omówienie osiągnięć, o których mowa w art. 219 ust. 1 pkt. 2 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2021 r. poz. 478 z późn. zm.). Omówienie to winno dotyczyć merytorycznego ujęcia przedmiotowych osiągnieć, jak i w sposób precyzyjny określać indywidualny wkład w ich powstanie, w przypadku, gdy dane osiągnięcie jest dziełem współautorskim, z uwzględnieniem możliwości wskazywania dorobku z okresu całej kariery zawodowej.**

Wieloletnie doświadczenie w prowadzeniu badań naukowych oraz osobiste zainteresowania zaowocowały osiągnięciem naukowym zatytułowanym: *Cyberwalka. Militarny wymiar działań.* Opis osiągnięcia zawarto w monografii stanowiącej podstawę ubiegania się o stopień naukowy doktora habilitowanego:

R. Janczewski. *Cyberwalka. Militarny wymiar działań*, Wydawnictwo Naukowe PWN, Warszawa 2023, ISBN: 978-83-01-23085-2, ISBN druku: 978-83-01-23028-9.

Recenzenci wydawniczy: prof. dr hab. inż. Piotr Dela,
prof. zw. dr hab. inż. Krzysztof Ficoń.

Zasadniczą przyczyną wyboru obszaru badawczego było znaczenie cyberwalki we współczesnych działaniach militarnych. Dociekania badawcze w zakresie cyberwalki jako militarnego wymiaru działań wynikały także z moich osobistych zainteresowań i doświadczeń. Kolejnym powodem był aspekt poznawczy, czyli zidentyfikowanie i wskazanie tak samej cyberwalki, jak i jej głównych elementów. Ustalenie czynników determinujących cyberwalkę jako militarnego wymiaru działań. Niemniej ważnym czynnikiem wpływającym na wybór obszaru badawczego była potrzeba zbadania teoretycznych aspektów cyberwalki jako militarnego wymiaru działań. Potrzeba badawcza zdeterminowana była również koniecznością przedstawienia rozwiązania problemu badawczego w postaci hipotezy naukowej. Kolejnym, ale niemniej ważnym powodem, była potrzeba dydaktyczna, czyli opracowanie treści, które w trakcie kształcenia i doskonalenia wojskowych lub cywilnych specjalistów od cyberwalki (ale także innych specjalności) mogą służyć do poszerzania oraz porządkowania wiedzy w sferze teorii i praktyki badanego problemu. U podstaw podjęcia przeze mnie badań było także oddziaływanie środowiska pracy. Prowadzone obserwacje, wywiady oraz zdobywane doświadczenie uwidoczniły, iż w ramach realizacji zadań mających na celu ochronę i obronę cyberśrodowiska resortu obrony narodowej (RON) wojskowi codziennie pozostają w kontakcie z napastnikiem próbującym przełamać militarne zabezpieczenia sieci i systemów teleinformatycznych. Wpływ środowiska naukowego również miał znaczenie dla podjęcia badań naukowych. Liczne konferencje i sympozja naukowe wykazały niedostatek i brak zgodności badaczy co do podstaw teoretycznych cyberwalki jako militarnego wymiaru działań.

Cyberwalka jako militarny wymiar działań nie została dotychczas zbadana i nie ma na ten temat kompleksowych opracowań naukowych, co za tym idzie 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.

W oparciu o przekonanie, że teoretyk walki tworzy i bada modele abstrakcyjne rzeczywistości zawierające pewne istotne analogie do tej rzeczywistości podjąłem wysiłek badawczy nad cyberwalką jako militarnym wymiarem działań, a wyniki badań syntetycznie przedstawiłem w formie monografii.

Celem zasadniczym dociekań naukowych było *zidentyfikowanie cyberwalki jako militarnego wymiaru działań.* Dla osiągniecia tego celu:

1. *Zidentyfikowałem uwarunkowania cyberwalki jako militarnego wymiaru działań.*
2. *Zbadałem przestrzeń determinującą prowadzenie cyberwalki przez siły zbrojne.*
3. *Określiłem podstawy teoretyczne cyberwalki jako militarnego wymiaru działań.*
4. *Zidentyfikowałem uwarunkowania skuteczności cyberwalki jako militarnego wymiaru działań.*
5. *Zidentyfikowałem zasadnicze działania sił zbrojnych w cyberwalce.*
6. *Przeprowadziłem analizę wpływu otoczenia na zdolności sił zbrojnych do prowadzenia cyberwalki.*

Fragment rzeczywistości, fakty, procesy stanowiące sytuację problemową oraz przyjęty cel badań naukowych pozwoliły mi wyodrębnić przedmiot badań naukowych, którym była *cyberwalka jako militarny wymiar działań.*

Przedmiot badań, ze względu na swoją złożoność, narzucił potrzebę nakreślenia jednolitego obszaru badawczego. Poszczególne składowe tematu, czyli cyberwalka oraz działania w kontekście militarnym, to pojęcia i zakresy tematyczne należące do różnych dziedzin wiedzy. Składniki tematu monografii tworzą desygnat wieloczłonowego pojęcia cyberwalki jako militarnego wymiaru działań. Obszar badań to część wspólna wyodrębnionych obszarów wiedzy.

Zidentyfikowanie cyberwalki jako militarnego wymiaru działań zdeterminował główny problem badawczy. W celu wypełnienia luki w teorii cyberwalki będącej militarnym wymiarem działań wyodrębniłem, a także aby był on empirycznie uzasadniony, sformułowałem go jako zasadnicze, domagające się narracji, pytanie otwarte: *Jakie cechy charakteryzują cyberwalkę jako militarny wymiar działań?*

Po zidentyfikowaniu głównego problemu badawczego i ujęciu go w formie pytania, ze względu na brak wiedzy naukowej, która posłużyłaby do identyfikacji cyberwalki jako militarnego wymiaru działań na podstawie przyjętego celu, dotychczasowej wiedzy wynikającej z badań wstępnych i analizy literatury przedmiotu, doświadczenia oraz wieloletniej praktyki zawodowej, pracy naukowej i dydaktycznej oraz założenia, że hipoteza:

- etymologicznie pochodzi od greckiego słowa hypóthesis, co znaczy tymczasowe przypuszczenie, mające ułatwić naukowe wyjaśnienie zjawiska; domysł oraz założenie oparte na prawdopodobieństwie a wymagające sprawdzenia;
- jest zdaniem nie w pełni uzasadnionym, tłumaczącym pewne stwierdzone fakty;
- w nauce jest domysłem (przypuszczeniem), będącym zdaniem tylko częściowo uzasadnionym, tłumaczącym pewne zaistniałe fakty (zdarzenia);
- w procesie badań naukowych ma być poddana weryfikacji, czyli potwierdzona lub obalona;
- jest ukierunkowaniem toku myślenia (rozumowania) badacza o podjętym w badaniach problemie
- nie może być wartościująca, czyli wartości wyznawane przez badacza, jego stronniczość czy subiektywne preferencje nie powinny w żadnym wypadku wpływać na proces badawczy

sformułowałem główną hipotezę badawczą, czyli prawdopodobną odpowiedź będącą rozwiązaniem postawionego, głównego problemu badawczego. Przedstawiała się ona następująco: przypuszcza się, że cyberwalka jako militarny wymiar działań jest cyberdziałaniami wojsk mającymi na celu uzyskanie przewagi nad przeciwnikiem lub

pokonanie go. Jej istotną cechą jest to, że determinowana jest zmianami dokonującymi się pod wpływem najnowszych rozwiązań technicznych i technologicznych w dziedzinie teleinformatyki. Zmian te wpływają zarówno na metody, taktyki, techniki, procedury i narzędzia prowadzenia działań we współczesnej przestrzeni walki jak i na samą przestrzeń. Przez to posiada cechy właściwe zarówno działaniom konwencjonalnym jak i te niespotykane w działaniach o takim charakterze, które wyróżniają ją z innych rodzajów walki.

Określony główny problem badawczy wskazał jedynie dalszy kierunek badań, ponieważ odpowiadał na pytanie *Czego nie wiem?* Był jednak zbyt ogólny i niejasny, żeby stać się podstawą projektowania badań. Jego rozwiązanie wymagało rozważenia problemów szczegółowych. Dlatego w celu uszczegółowienia głównego problemu badawczego, w postaci również pytań otwartych, domagających się narracji, sformułowałem następujące problemy szczegółowe:

1. *Jakie są uwarunkowania cyberwalki jako militarnego wymiaru działań?*
2. *Jaka przestrzeń determinuje prowadzenie cyberwalki przez siły zbrojne?*
3. *Jakie są podstawy teoretyczne cyberwalki jako militarnego wymiaru działań?*
4. *Jakie są uwarunkowania skuteczności cyberwalki jako militarnego wymiaru działań?*
5. *Jakie są zasadnicze rodzaje działań sił zbrojnych w cyberwalce?*
6. *Jak na zdolności sił zbrojnych do prowadzenia cyberwalki wpływa otoczenie?*

Wyodrębnienie przedmiotu badań znacząco wpłynęło na dobór terminologii. Przyjąłem, że terminologia, którą posługują się siły zbrojne w czasie prowadzenia działań w cyberprzestrzeni pochodzi nie tylko z aktów prawnych, dokumentów normatywnych czy doktrynalnych, regulaminów lub instrukcji, ale również z beletrystyki, literatury naukowej, popularnonaukowej oraz żargonu. Uwzględniając, że „wiedza i system pojęć ewoluują wraz ze zmianami zachodzącymi we współczesnym świecie" i „każda dziedzina nauki posiada swój specyficzny system pojęć, który sytuowany jest w układzie nadrzędnym i wpływa na aparat pojęciowy w danych dyscyplinach i specjalnościach naukowych" podjąłem się identyfikacji i ustalenia aparatu pojęciowego związanego z cyberwalką. Biorąc pod uwagę, że „system pojęć, podobnie jak otaczająca nas rzeczywistość, ulega ewolucji odpowiednio do przedmiotu, który jest definiowany" przeprowadziłem analizę używanej w piśmiennictwie terminologii związanej z cyberwalką. Jeżeli pojęcia nie były sprzeczne z wnioskowaniem wynikającym z dociekań naukowych, posłużyłem się nimi w monografii. Jednak, gdy mnogość, niespójność i niejednoznaczność niektórych terminów nie pozwoliła na uchwycenie jednoznaczności i spójności nazewnictwa oraz nadanemu mu znaczeniu, redefiniowano je lub wprowadzono nowe i podano ich definicje. Podczas tworzenia nowej definicji założyłem, że powinna: być zrozumiała dla osób spoza dziedziny; stanowić punkt odniesienia dla ludzi zajmujących się przedmiotową dziedziną; być jednoznaczna.

Rozwiązanie głównego problemu badawczego miało charakter jakościowy i wymagało specyficznego podejścia. Badania wykonane były na ograniczonej ilości danych. Ze względu na fakt, iż nauki o bezpieczeństwie należą do dziedziny nauk społecznych skorzystałem z dorobku metodologicznego nauk społecznych, posłużyłem się aparaturą metodologiczną, stosowaną właśnie w naukach społecznych. Heterogeniczność zarówno przedmiotu badań, jak i obszaru spowodowała, że aby rozwiązać problem badawczy i zachować wysoką jakość prowadzonych badań i ograniczyć błąd pomiaru, badania przeprowadziłem metodą triangulacji. Główny problem badawczy zdeterminował zastosowanie triangulacji danych, teorii oraz metod.

Triangulacja danych polegała na zgromadzeniu danych z różnych źródeł. Zakres źródeł dostępnych do rozważań nad cyberwalką jest zróżnicowany. Obejmują one naukową literaturę przedmiotu, publikacje medialne, dokumenty urzędowe, instytucje edukacyjne i organizacje non-profit. Wiele treści zamieszonych było w Internecie, na rządowych stronach internetowych, stronach akademickich i innych serwisach. Dlatego też wiele materiałów wykorzystanych w badaniach pochodzi z zasobów Internetowych. Triangulacja teorii zastosowałem ze względu na niespójność terminologiczną w obszarze badawczym. W procesie

badań, spośród wielu nieraz różnych definicji, wybrałem najodpowiedniejsze rozwiązanie dla problemu badawczego. Triangulacja metod polegała na wybraniu i połączeniu najlepszych, najprzydatniejszych metod badawczych dla postawionego problemu badawczego, w celu maksymalizacji wyników badań.

Weryfikację głównej hipotezy badawczej dokonałem w oparciu o analizę i krytykę piśmiennictwa oraz krytyczną analizę literatury w szczególności prac naukowo-badawczych, zarówno krajowych jak zagranicznych, jak również obserwacje ćwiczeń dowódczo-sztabowych, szkieletowych i z wojskami. W ich wyniku zaobserwowałem istotną lukę związana z brakiem opracowań teoretycznych dotyczących cyberwalki jako militarnego wymiaru działań. Do rozwiązania głównego problemu badawczego wykorzystałem również wyniki uzyskane z obserwacji, wywiadów skategoryzowanych oraz debaty przeprowadzonej w czasie Wojskowego Forum Cyberbezpieczeństwa (którego byłem organizatorem). Krytyczna analizy literatury przedmiotu posłużyła zarówno do zweryfikowania wiedzy zastanej (ang. *background knowledge*) na temat cyberwalki jako militarnego wymiaru działań, jak i rozwiązania wygenerowanych, nowych problemów badawczych. Dzięki temu wyodrębniłem związki, różnice oraz zależności badanego przedmiotu z istniejącym stanem wiedzy. Analiza i krytyka piśmiennictwa pozwoliły na wypełnienie luk informacyjnych i pogłębienie wiedzy w obszarze badań. W badaniach stosowałem syntezę, która posłużyła do scalenia w nową całość zebranego i przeanalizowanego materiału badawczego. Metoda ta jako proces myślowy pozwoliła na złączenie uzyskanych z analizy wniosków i określenie, czym jest cyberwalka jako militarny wymiar działań oraz jakie czynniki ją warunkują. W badaniach posłużyłem się również wnioskowaniem (zawodnym) indukcyjnym, polegającym na zbieraniu skończonej, niezupełnej liczby obserwacji i na ich podstawie formułowałem nowe twierdzenia, będące ogólną prawidłowością. Dzięki tej metodzie na podstawie wyników badań sformułowałem nieznane do tej pory twierdzenia. Abstrahowanie, będące operacją myślową, pozwoliło wyodrębnić i pominąć określone elementy przedmiotu badań, które uznałem za wprawdzie istotne, ale drugorzędne, oraz uwzględnić inne elementy uznane za istotne. Znacząca, w celu identyfikacji cyberwalki jako militarnego wymiaru działań, była analogia bliska, polegająca na ustaleniu podobieństw i różnic między opisami cyberwalki w ogóle i jej elementów przedstawionymi przez innych badaczy. W celu zrozumienia wyjątkowości cyberdziałań (szczególnych przypadków), prowadzonych we współczesnych konfliktach, ich kontekstu i interakcji z innymi elementami (zakresu oddziaływania), a także cech charakterystycznych dla cyberprzestrzeni oraz wybranych rodzajów cyberdziałań w procesie poznawczym posłużyłem się studium przypadku. W trakcie badań posłużyłem się także klasyfikowaniem jako operacją myślową oraz czynnością porządkującą materiał badawczy.

Ze względu na niedostatek literatury naukowej prezentującej tematykę poświęconą stricte cyberwalce jako militarnemu wymiarowi działań oraz potrzebę zidentyfikowania aparatu pojęciowego, desygnatów wybranych, istotnych terminów funkcjonujących w środowisku wojskowych, a także formalnych wytycznych i założeń warunkujących przedmiot badawczy, jako uzupełniające źródło w badaniach naukowych wykorzystałem także dokumenty urzędowe takie jak: ustawy, strategie, doktryny, programy czy regulaminy. Treści owych dokumentów dostarczyły materiał badawczy, który w dążeniu do jak najdokładniejszego zrozumienia ich treści został poddany analizie i krytyce. Te zaś, pozwoliły na sformułowanie wniosków na temat spójności i jednoznaczności aparatu pojęciowego zawartego w formalnych dokumentach oraz formalnych uwarunkowań przedmiotu badawczego. Dokumenty urzędowe posłużyły do pośredniej obserwacji cyberwalki jako militarnego wymiaru działań. Stanowiły materiał dostarczający danych do badania procesów zmian zachodzących w siłach zbrojnych mających na celu zbudowanie zdolności do cyberdziałań w wymiarze militarnym. Analiza i krytyka wybranych dokumentów urzędowych pozwoliły na opis normatywnych ram warunkujących cyberwalką jako militarny wymiar działań. W czasie badań przyjęto, że cyberwalka prowadzona jest na trzech poziomach dowodzenia: taktycznym, operacyjnym i strategicznym.

Mając na uwadze, że cyberwalka posiada także społeczny charakter, podczas badań założono, że przedmiot badań posiada cechy dyspozycyjne, czyli takie, które nie są dostępne bezpośredniej obserwacji. Charakter diagnostyczny badań niejako wymusił opisową prezentację wyników badań w postaci monografii.

W Akademii Marynarki Wojennej w Gdyni w październiku 2022 roku zorganizowałem Wojskowe Forum Cyberbezpieczeństwa w trakcie, którego za pomocą wywiadu skategoryzowanego weryfikowano wyniki badań nad cyberwalką. Uczestnicy spotkania (specjaliści kluczowych podmiotów SZ RP zajmujący się cyberbezpieczeństwem) omawiali w czasie debaty stan aktualny, wyzwania oraz perspektywy w zakresie zdolności sił zbrojnych do prowadzenia cyberwalki. Dyskusje, rozważania, wypowiedzi oraz wymiana zdań lub poglądów potwierdziły zasadność podjęcia wysiłku dociekań naukowych nad cyberwalką jako militarnym wymiarem działań.

Podejście systemowe do badań pozwoliło na ograniczenie badań do uznanych za interesujące elementów cyberwalki jako militarnego wymiaru działań. Abstrahowano od innych elementów, skupiając się jedynie na wyodrębnionych składowych. W czasie badań ograniczeniem było także piśmiennictwo. Zapoznawanie się na bieżąco z całą literaturą przedmiotu, w odniesieniu do każdego zagadnienia w obszarze badań, którym jest cyberwalka, było wręcz niewykonalne. Literatura przedmiotu była w badaniach naukowych tylko częściowo dostępna.

Istotnym założeniem badań naukowych było przeprowadzenie ich na takim poziomie szczegółowości, aby zakres nie dotyczył informacji niejawnych czy operacyjnych. Ze względu na jawność przeprowadzonych badań podstawowym wymogiem, który stanowił jednocześnie podstawowe ograniczenie w dostępie do wielu wartościowych informacji, było przestrzeganie Ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182, poz. 1228). Ze względu na niejawność niektórych aspektów cyberdziałań wyniki takich badań nie zostały zaprezentowane, a jawny charakter niniejszej monografii wymusił prezentację wyników badań niestanowiących ujawnienia danych i informacji niejawnych.

Układ monografii odzwierciedla przyjęte szczegółowe problemy badawcze. W poszczególnych rozdziałach zaprezentowałem treści stanowiące ich rozwiązanie. Każdy z rozdziałów przedmiot badań przedstawia z innej perspektywy. Monografia składa się ze wstępu, sześciu spójnych logicznie i pojęciowo, jednak różnych w swej istocie rozdziałów, zakończenia i bibliografii. Rozdziały zakończone są wnioskami.

W pierwszym rozdziale – Uwarunkowania cyberwalki jako militarnego wymiaru działań – zaprezentowałem wyniki dociekań naukowych na temat uwarunkowań cyberwalki jako militarnego wymiaru działań. Na podstawie wyników badań przedstawiłem rozwiązanie szczegółowego problemu badawczego sformułowanego w postaci pytania: Jakie są uwarunkowania cyberwalki jako militarnego wymiaru działań? Zgromadzone wyniki badań dały podstawę do sformułowania wniosku, że siły zbrojne są organizacją wojskową i z powodzeniem wpisują się w systemową interpretację organizacji, co pozwala działania sił zbrojnych postrzegać jako działania organizacji wojskowej i w konsekwencji cyberwalkę postrzegać jako militarny wymiar działań. Badania wykazały, że rozwój techniczny i technologiczny społeczeństw oraz wzrost znaczenia teleinformatyki we współczesnej przestrzeni walki przyczynił się do zwiększenia skuteczności walki, co spowodowało konieczność zbudowania przez siły zbrojne zdolności do prowadzenia cyberwalki. Otoczenie państwa wymusiło zmiany w ich strukturze organizacyjnej, wyposażeniu, identyfikacji zagrożeń, zakresie przygotowywania specjalistów, świadomości operacyjnej, sposobie prowadzenia działań militarnych. 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 stanowią przyczynę do budowania przez siły zbrojne zdolności do cyberwalki. Zidentyfikowano również formalny czynnik,

będący konsekwencją poprzedniej przyczyny, czyli wymagania stawiane siłom zbrojnym przez państwo.

Istotną częścią tego rozdziału jest, w oparciu o studium przypadku, uwidocznienie ewolucji cyberdziałań na przykładzie przeprowadzonych przez Rosję przeciwko Estonii w 2007, Gruzji w 2008 oraz Ukrainie w 2014 roku, jawne źródła informacji ukształtowały przedstawione treści.

Badania wykazały, że w przypadku Estońskim wykorzystanie cyberprzestrzeni w czasie działań hybrydowych służyło, obok zamieszek i sankcji, do wywołania i pogłębiania sytuacji kryzysowej w państwie. Cyberdziałania skierowane były nie tylko przeciwko Estonii, ale poddały prośbie także Sojusz Północnoatlantycki. Skutki tych działań powodowały nie tylko uciążliwości czy niedogodności w państwie, lecz sparaliżowały jego funkcjonowanie.

Wyniki dociekań naukowych uwidoczniły, że w przypadku Gruzińskim cyberdziałania były uzupełnieniem bombardowania rosyjskich sił powietrznych oraz ostrzałów wojsk lądowych. Korzystne warunki dla takiego scenariusza działań hybrydowych wynikały z infrastruktury teleinformatycznej Gruzji. Prawie połowa z trzynastu połączeń do Internetu przebiegała przez Rosję. Badania wykazały także, że mimo, iż Gruzja prześledziła drogę skierowanych przeciwko niej cyberdziałań i nie miała wątpliwości, że cyberataki na nią przeprowadziła Rosja niestety wykorzystując cechę cyberprzestrzeni, jaką jest anonimizacja działań, nie mogła jednoznacznie przypisać wrogich cyberdziałań zidentyfikowanemu napastnikowi.

Natomiast w przypadku Ukraińskim studium przypadku pozwoliło zauważyć, że cyberdziałania skierowane były nie tylko na serwisy internetowe podmiotów państwowych, ale także elementy infrastruktury krytycznej państwa oraz przeciwko żołnierzom sił zbrojnych Ukrainy. Również w tym przypadku państwo nie było w stanie rozwiązać problemu atrybucji, co w konsekwencji doprowadziło do tego, że nie było w stanie jednoznacznie udowodnić, że to właśnie Rosja jest odpowiedzialna za skierowane przeciwko niemu cyberataków.

W rozdziale tym uwidoczniłem, 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 urzędowych w kontekście działań militarnych zidentyfikowałem desygnaty istotne z punktu widzenia rozwiązania pierwszego problemu szczegółowego. Rozdział pierwszy jest także identyfikacją konwencji terminologicznej warunkującej aparat pojęciowy w teorii i praktyce cyberwalki jako militarnego wymiaru działań. W tym miejscu monografii zaprezentowałem zidentyfikowane gramatyczne zasady pisowni wyrazów zawierających przedrostek cyber-, wskazałem jego jednoznaczne znaczenie oraz rolę konwencji terminologicznej dla sprawności interoperacyjnych działań militarnych wykorzystujących cyberprzestrzeń.

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. Kolejnym, w niniejszym rozdziale, uzupełnieniem nauk o bezpieczeństwie jest identyfikacja desygnatów charakterystycznych i istotnych z punktu widzenia rozwiązania pierwszego szczegółowego problemu badawczego. W tym miejscu określiłem, że *incydentem* jest bezprawne, nieautoryzowane lub niespodziewane zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Zidentyfikowałem gramatyczne zasady pisowni wyrazów zawierających przedrostek cyber- oraz wskazałem jego jednoznaczne znaczenia dla cyberwalki prowadzonej przez siły zbrojne. Dociekania naukowe wykazały, że złożoność współczesnej przestrzeni walki oraz znaczenie informacji, energii, informatyki, telekomunikacji, robotyki i automatyki w działaniach militarnych XXI wieku pozwalają jednoznacznie przyjąć, że w języku polskim cząstka cyber- jest pierwszym członem wyrazów złożonych wskazującym na ich związek ze sterowaniem, elektronicznymi procesami wymiany lub przetwarzania sygnałów oraz procesami pozyskiwania, przetwarzania lub transmisji danych lub informacji w systemach technicznych,

biologicznych lub społecznych. W trakcie badań ustaliłem, że jednoznacznie w języku polskim wszystkie rzeczowniki złożone, których człony są wyrazami pospolitymi, z prefiksem cyber- pisze się łącznie. Wykorzystując syntezę przeanalizowanego materiału badawczego, ujednoliciłem zakres znaczeniowy podstawowych terminów związanych z cyberwalką jako militarnym wymiarem działań oraz określiłem rolę konwencji terminologicznej dla sprawności interoperacyjnych cyberdziałań militarnych.

Rozdział drugi – Przestrzeń cyberwalki – jest odpowiedzią na sformułowany w postaci pytania szczegółowy problem badawczy: Jaka przestrzeń determinuje prowadzenie cyberwalki przez siły zbrojne? Rozdział ten poświęcony jest wynikom identyfikacji przestrzeni cyberwalki prowadzonej przez siły zbrojne. Wskazałem w nim cechy charakterystyczne przestrzeni determinującej prowadzenie cyberwalki przez siły zbrojne. W kontekście przestrzeni prowadzenia cyberwalki jako działań militarnych w pierwszej kolejności zidentyfikowałem teatr, teatr wojny, teatr działań wojennych oraz teatr operacji. Następnie szczegółowo omówiłem i wskazałem desygnat cyberprzestrzeni oraz cyberśrodowiska. Uwidoczniłem znaczenie we współczesnej przestrzeni walki zwirtualizowanej rzeczywistości, pozornej inteligencji oraz uczenia maszynowego. Omówiłem charakterystykę cyberprzestrzeni jako przestrzeni walki. W oparciu o analizę dokumentów doktrynalnych i strategicznych innych państw jako uzupełnienie zaprezentowałem wybrane poglądy na temat cyberprzestrzeni. Znaczną część tego rozdziału poświęciłem na teoretyczne aspekty cyberzagrożeń w świetle funkcjonowania sił zbrojnych w cyberprzestrzeni. W tym miejscu monografii zaprezentowałem taksonomie cyberzagrożeń. Omówiłem wewnętrzne i zewnętrzne cyberzagrożenia dla sieci i systemów teleinformatycznych resortu obrony narodowej, w tym sił zbrojnych.

W rozdziale tym w oparciu o wyniki badań sformułowałem wniosek, że siły zbrojne poszerzyły spektrum swoich działań, dostosowując je do nowej, nieznanej dotychczas w teorii wojskowości przestrzeni walki. Niezwykle ważne z punktu widzenia szeroko rozumianej w naukach o bezpieczeństwie teorii cyberwalki jako militarnego wymiaru działań są wyniki badania, które uwidoczniły, że ze względu na obecność we współczesnej przestrzeni walki rozwiązań opartych o informatykę, telekomunikację, robotykę, automatykę oraz pozorną inteligencję jako desygnat przestrzeni prowadzenia cyberwalki jako militarnego wymiaru działań (cyberprzestrzeni), należy rozumieć zbiór wszystkich urządzeń z dziedziny telekomunikacji lub informatyki (ang. *hardware*) wraz z oprogramowaniem (ang. software); kanałów komunikacyjnych tworzący nieskończony cybergraf ($\mathbb{V}$, $\mathbb{E}$) z wagami wektorowymi, c-węzłami, c-krawędziami lub c-łukami o zasięgu ogólnoświatowym utworzony do realizacji procesów wymiany lub przetwarzania sygnałów; procesów pozyskiwania, przetwarzania lub dystrybucji danych lub informacji; wirtualizacji przedmiotów wirtualności. Ustalono, że cyberprzestrzeń stwarza warunki do prowadzenia cyberdziałań. A jako przestrzeń walki posiada wyjątkowe, atrakcyjne z punktu widzenia prowadzenia działań militarnych cechy, m.in. zależność od niej wielu zdolności militarnych w pozostałych domenach, warunkujące nowy, specyficzny, oparty o istniejącą rutynę model podejmowania decyzji.

Stwierdziłem, że podzbiór cyberprzestrzeni, czyli 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 stanowi cyberśrodowisko. Charakterystyka cyberśrodowiska pozwala na zbudowanie dla cyberwalki jako militarnego wymiaru działań modelu systemu C-T-O, czyli człowiek-technika-otoczenie. Ustaliłem, 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. Bezpieczeństwo takiego systemu zależna jest od jego niezawodności, którą zdefiniowano jako zdolność do prawidłowego funkcjonowania, w określonym czasie bez niesprawności. Ustaliłem czynniki i elementy cyberśrodowiska. Mając na uwadze znaczenie informacji we współczesnej przestrzeni walki wyizolowałem proces informacyjny

w cyberśrodowisku, który zdefiniowałem jako oparty o wypracowaną metodologię, realizowany za pomocą określonych zasobów systemu informacyjnego cyberśrodowiska system działalności na danych i informacjach.

Rozwiązanie drugiego problemu szczegółowego umożliwiło mi wskazanie klasy zagrożeń właściwych dla cyberprzestrzeni, czyli cyberzagrożeń niewystępujących w innych domenach fizycznych. Cyberzagrożenia, zdefiniowałem jako potencjalny czynnik mogący za pośrednictwem cyberprzestrzeni naruszyć bezpieczeństwo człowieka, elementów cyberprzestrzeni, ich zasobów lub infrastruktury fizycznej. Wyniki badań pozwoliły na sformułowanie wniosku, że warunkiem stworzenia cyberzagrożenia przez wrogi podmiot, jest zaistnienie połączenia trzech czynników. Bez tego warunku zagrożenie nie istnieje. Te trzy czynniki to: zamiar, czyli chęć złośliwego podmiotu do przeprowadzenia cyberataku na wybrany system; 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). Wnioski z badań wskazują, że cyberrozpoznanie można postrzegać jako cyberzagrożenie. Ustaliłem, że powszechnie stosowany anglojęzyczny skrótowiec IT (ang. *information technilogy*) należy rozumieć jako informatykę. Natomiast ze względu na 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 (w sensie metody, techniki, lub systemu odbierania, przetwarzania i wysyłania informacji, czyli linii telefonicznych, komputerów, urządzeń czy sieci), a nie komunikacji (aktu wysyłania i odbierania informacji przez mówienie, pisanie, dzwonienie, wysyłanie e-maili itp. lub wiadomości zawierających takie informacje). W procesie poznawczym zidentyfikowałem atrybucję techniczną, którą zdefiniowałem 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 uporządkowałem definicje terminów: teatr, teatr wojny, teatr działań wojennych oraz teatr operacji. Badania jednoznacznie wskazały, że cyberprzestrzeń była pomijana w specyfikacji przestrzeni walki. W oparciu o wyniki badań ustaliłem, 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 procesie badawczym zidentyfikowałem także relacje między ochroną (ang. *security*) a bezpieczeństwem (ang. *safety*).

W rozdziale trzecim – Podstawy teoretyczne cyberwalki – zaprezentowałem wyniki badań skupionych na określeniu podstaw teoretycznych cyberwalki jako militarnego wymiaru działań. W oparciu o wyniki badań własnych przedstawiłem podstawy teoretyczne cyberwalki jako militarnego wymiaru działań. Uwypukliłem jej wielopoziomowość i wieloaspektowość. Opisałem wybrane ramy analityczne przydatne w procesach informacyjnych cyberwalki jako militarnego wymiaru działań. Zidentyfikowałem desygnat przeciwnika. Pokazałem operacyjne kierunki wykorzystywania robotów we współczesnej przestrzeni walki. Zdefiniowałem cyberinformacyjne przygotowanie przestrzeni walki. W kontekście uwarunkowań i ograniczeń zarówno przepisów prawa krajowego, jak i międzynarodowego zaprezentowałem cyberwalkę w świetle Międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych.

Odnośnie do trzeciego problemu szczegółowego będącego pytaniem: Jakie są podstawy teoretyczne cyberwalki jako militarnego wymiaru działań? Wyniki badań pozwoliły 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. Ustaliłem, że ze względu na techniczny wymiar

również podstawy teoretyczne informatyki i telekomunikacji stanowią założenia dla cyberwalki. Zidentyfikowałem, 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. W wielu przypadkach regulacją 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 zdefiniowałem 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 (ang. *cybereffect*) 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. Cyberwalka jako militarny wymiar działań posiada 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. Ustalono, że przy interpretacji i stosowaniu istniejącego prawa międzynarodowego do cyberwalki, należy zwrócić należytą uwagę na specyficzne cechy cyberprzestrzeni. Przede wszystkim to, że cyberprzestrzeń jest domeną całkowicie stworzoną przez człowieka. Jest tworzona, utrzymywana, posiadana i zarządzana wspólnie przez interesariuszy publicznych i prywatnych na całym świecie. Jej fenomen polega na tym, że stanowi obszar działań tworzony i utrzymywany przez każdą z walczących ze sobą stron. Stwarza jednocześnie obszar zwycięstwa lub przegranej. Stale się zmienia w odpowiedzi na techniczne i technologiczne innowacje. Jest przestrzenią walki niepodlegającą granicom geopolitycznym lub naturalnym. Proces badawczy uwidocznił, że przeniesienie zasad międzynarodowego prawa humanitarnego na wykorzystanie cyberataków jest nie tylko możliwe, ale i właściwe. Wymaga to przyjrzenia się zasadom wywodzącym się z tradycyjnego schematu użycia *in bello* w odniesieniu do prowadzenia cyberwalki w czasie działań militarnych: konieczności wojskowej, rozróżnienia, proporcjonalności, perfidii, neutralności i niepotrzebnego cierpienia.

Wyniki badań pozwoliły sformułować wniosek, że cyberkonflikt ze względu na swoją charakterystyką jest istotnym pojęciem dla budowania teoretycznych podstaw cyberwalki prowadzonej przez siły zbrojne. Zidentyfikowałem go jako proces oparty o wypracowaną metodologię, realizowany za pomocą określonych zasobów systemu działań. Ma swój początek i koniec oraz trwa nieprzerwanie w czasie. Strukturę cyberkonfliktu tworzą podprocesy składające się z etapów, faz i czynności. Jest procesem niematerialnym, czyli nie posiada zasobów materialnych, w związku z tym wykorzystuje zasoby techniczne sieci i systemów teleinformatycznych, którymi dysponują strony konfliktu. Czynniki pierwotne i czynniki wtórne warunkują strukturę oraz przebieg cyberkonfliktu. Cyberkonflikt może być zakłócony przez bariery organizacyjne, proceduralne i techniczne. Mają one negatywny wpływ na przebieg cyberkonfliktu. Cyberkonflikt jako proces posiada strukturę zależną od przyjętego kryterium, czyli przestrzenną, informacyjną, organizacyjną, proceduralną i techniczną.

W czwartym rozdziale – Uwarunkowania skuteczności cyberwalki jako militarnego wymiaru działań – zaprezentowałem efekty poznawcze uwarunkowań właściwych skuteczności cyberwalki jako militarnego wymiaru działań. Na podstawie wyników własnych badań naukowych, scharakteryzowałem cyberwalkę jako militarny wymiar działań. Opisałem podstawy teoretyczne skuteczności cyberwalki, cyberrozpoznania, przeciwdziałania, obrony elektronicznej oraz znaczenie logistyki w cyberwalce. Przedstawiłem teorię zakłóceń radiowych, mających wpływ na bezprzewodową transmisję danych. Zaprezentowałem także czynniki cyberwalki jako militarnego wymiaru działań z podziałem na czynniki pierwotny

i wtórne. Scharakteryzowałem cyberwojska oraz podstawowe zasady ich użycia. Przedstawiłem taksonomie zdarzeń, ataków i incydentów.

Obserwacje wykazały, że cyberwalka prowadzona może być na każdym poziomie dowodzenia i szczeblu organizacyjnym sił zbrojnych. Powodzenie cyberwalki zabezpieczanej logistycznie, prowadzonej przez siły zbrojne we współczesnej przestrzeni walki determinowane jest jej skutecznością. Natomiast skuteczność mierzona jest stopniem osiągnięcia zamierzonego celu. Uwidoczniłem, że można uznać, iż 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 uwidocznienie, że cyberwalka prowadzona może być przez wojska właściwe do tego rodzaju walki, jednak w ograniczonym zakresie, w zależności od rodzaju działań, także przez każdy 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 ważnej i unikalnej cechy cyberwalki jako militarnego wymiaru działań, czyli czynników ją determinujących: pierwotnego i wtórnego. Pierwotną przyczyną (czynnikiem pierwotnym) podjęcia przez siły zbrojne cyberwalki jest jej cel. Wtórnie determinują je czynniki: techniczne, czyli cyberbroń, infrastruktura teleinformatyczna (urządzenia, oprogramowanie, kanały transmisyjne, źródła danych i informacji); taktyczno-operacyjne, czyli rażenie, ruch, obszar (rejonu) działań, oddziaływanie otoczenia; organizacyjne, czyli zasoby ludzkie (siły), struktury organizacyjne, otoczenie państwa; Proceduralne, czyli uwarunkowania prawne, doktryny, regulaminy, instrukcje; dane i informacje, czyli dane i informacje rozpoznawcze, dane i informacje pochodzące z monitorowania własnych sieci i systemów teleinformatycznych; czas, czyli przeszłość, teraźniejszość, przyszłość oraz dane i informacje, które są odrębną kategorią czynników wtórnych. Informacja jest niematerialnym czynnikiem walki. Współczesna przestrzeń walki wymusza, aby traktować ją jako czynnik zwiększający wiedzę człowieka o otaczającej go rzeczywistości, sterujący strumieniami zasileń (materii i energii), obok rażenia i ruchu, kształtujący walkę zbrojną oraz zmniejszający stopień niewiedzy (nieokreśloności) o otoczeniu, umożliwiający polepszenie znajomości otoczenia i w sprawniejszy sposób przeprowadzenie celowego działania. W procesie badawczym ustaliłem, 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 funkcji, uszkodzeniu danych lub informacji, lub unieruchomieniu urządzeń komputerowych za pomocą szkodliwego pliku wykonawczego. Cyberefekt może wpływać nie tylko na militarne cyberdziałania, ale także na zdolności sił zbrojny we wszystkich domenach walki.

Kolejnym osiągnięciem badawczym jest przedstawiona w rozdziale piątym – Zasadnicze rodzaje działań sił zbrojnych w cyberwalce – identyfikacja zasadniczych działań sił zbrojnych w cyberwalce. W tym miejscu monografii uwidoczniłem różnice między cyberrozpoznaniem a rozpoznaniem cyberzagrożeń. Przybliżyłem cykl rozpoznawczy, zadania cyberrozpoznania oraz podstawy teoretyczne źródeł danych i informacji rozpoznawczych. Zwróciłem 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, to cyberrozpoznanie 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, np. firmware lub pliki konfiguracyjne. Cyberrozpoznanie jest pojęciem szerszym niż rozpoznanie cyberzagrożeń i obejmuje rozpoznanie cyberzagrożeń, jednak dane i informacje pochodzące z rozpoznania

cyberzagrożeń nie stanowią całości 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 można uznać za składową (podsystemem) systemu rozpoznania wojskowego sił zbrojnych. 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 przez receptory człowieka, przetwarzają je do postaci zrozumiałej przez użytkownika, a w ostateczności udostępniają i dostarczają odbiorcy. Kolejnym osiągnięciem badawczym jest ustalenie, iż zidentyfikowany w czasie badań desygnat cyberprzestrzeni umożliwia uznanie, że cyberrozpoznanie czynnościowo w istocie polega na przeszukiwaniu grafu lub inaczej przechodzeniu grafu, czyli czynności polegającej na przechodzeniu w usystematyzowany sposób, pozostających w operacyjnym zainteresowaniu wierzchołków grafu w celu zebrania potrzebnych danych i informacji rozpoznawczych.

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 określiłem, 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. W czasie pokoju codzienną rutyną sił zbrojnych jest cyberochrona zasobów własnych. Dla zwiększenia przewagi nad przeciwnikiem stosowane jest cyberodstraszanie. Wyboru celów, nadania im priorytetów oraz doboru i realizacji odpowiedniego sposobu oddziaływania na te cele siły zbrojne dokonują w ramach procesu targetingu. Cyberdziałania nie ograniczają się jedynie do stacjonarnych sieci i systemów teleinformatycznych. Dla zachowania mobilności mogą być prowadzone w oparciu o spektrum elektromagnetyczne. Takie działania są działaniami cyberelektromagnetycznymi. Zwiększenie anonimowości i anonimizacji własnych cyberdziałań zapewnia cybermaskowanie. Ważnym z punktu widzenia rozwoju teorii cyberwalki jako militarnego wymiaru działań są zidentyfikowane i zdefiniowane przeze mnie terminy: cyberobrona, cyberbroń, cyberatak, cyberodstraszanie militarne, cyberelektromagnetyczne działania militarne. W czasie pokoju codzienną rutyną sił zbrojnych jest cyberochrona zasobów własnych. Dla zwiększenia przewagi nad przeciwnikiem stosowane jest cyberodstraszanie. Analiza i krytyka piśmiennictwa umożliwiła mi usystematyzowanie rozwiązań w zakresie maskowania cyberdziałań. Identyfikując szereg zagadnień związanych z samą cyberprzestrzenią wyodrębniłem jedenaście wymagań dotyczących cyberodstraszania. Opisałem teoretyczne aspekty cyberbroni, podstawy cyberataku w kontekście ataku zbrojnego oraz proces targetingu w cyberwalce. Zaprezentowałem także teorię działań cyberelektromagnetycznych. Rozdział zakończyłem prezentacją wyników badań nad cybermaskowaniem.

W rozdziale szóstym – Wpływ otoczenia na zdolność sił zbrojnych do prowadzenia cyberwalki – w procesie badań zidentyfikowałem wpływ otoczenia na zdolności sił zbrojnych do prowadzenia cyberwalki i na podstawie wyników badań przedstawiłem rozwiązanie szczegółowego problemu badawczego sformułowanego w postaci pytania: Jak na zdolności sił zbrojnych do prowadzenia cyberwalki wpływa otoczenie? Rozdział ten poświęcony został także prezentacji wyników badań nad ewolucją zdolności SZ RP od cyberochrony po zdolność do cyberdziałań ofensywnych. Badania wykazały, że na przestrzeni lat SZ RP dostosowywały się do cyberzagrożeń w otoczeniu. Zmieniając swoje struktury organizacyjne, dostosowywały się do cyberochrony własnych sieci i systemów teleinformatycznych. Utworzony został system reagowania na incydenty komputerowe. Sformowano struktury właściwe do działań zarówno defensywnych jak i ofensywnych. Powołano do życia ośrodki szkoleniowe doskonalenia

specjalistycznego. Zreformowano wojskowe szkolnictwo wyższe w kierunku przygotowania stosownych kadr. W rozdziale tym opisałem zidentyfikowany w czasie badań rosyjski punkt widzenia na cyberdziałania, który ma niebagatelne znaczenie w kontekście osiągania zdolności SZ RP do cyberwalki jako militarnego wymiaru działań. Na zdolności SZ RP do cyberwalki ma również wpływ cyberdziałań prowadzonych przez Federację Rosyjską w regionie. Zakres tych działań nie jest ograniczony jedynie do Polski. Działalność podmiotów wrogich, pojawiające się coraz nowsze zagrożenia i wyzwania wymuszają zawiązywanie sojuszy, koalicji oraz zawierania dwu lub wielostronnych porozumień w zakresie cyberwalki. Siły zbrojne, aby być równoważnym partnerem dla sojuszników czy koalicjantów (wojsk sprzymierzonych) muszą rozwijać zdolność do interoperacyjnych cyberdziałań. W celu pozyskiwania jak największej ilości wartościowych danych i informacji rozpoznawczych o przeciwniku rozwijanie cyberrozpoznania staje się koniecznością. Zapewnienie cyberwojskom ochrony prawnej wymaga zmian w prawie (opracowanie kontratypów dla cyberwojsk). Teorię cyberwalki jako militarnego wymiaru działań uzupełniono również o definicję interoperacyjności cyberwalki, która określa, że jest to zdolność synergicznego, wspólnego, spójnego, skutecznego i wydajnego działania wojsk w cyberprzestrzeni podczas realizacji powierzonych zadań w celu osiągnięcia taktycznych, operacyjnych lub strategicznych celów w ramach sojuszy, koalicji lub porozumień na poziomie krajowym lub wielonarodowym. rozwoju zdolności SZ RP do cyberwalki (temu zagadnieniu poświęcono dużą część rozdziału). Na koniec tego rozdziału zaprezentowano wyniki dociekań naukowych nad interoperacyjnością w cyberwalce jako militarnym rodzajem działań.

Monografia zawiera teorię cyberwalki, która stanowi wkład wiedzy o cyberwalce jako militarnym wymiarze działań do teorii nauk o bezpieczeństwie, a szczególnie w obszarze sztuki wojennej. Jest syntetyczną prezentacją dociekań naukowych na temat cyberwalki jako militarnego wymiaru działań. W jak najprostszy sposób opisuje zagadnienia z nią związane i zawiera tylko te pojęcia, które są rzeczywiście niezbędne. Terminy i pojęcia zaprezentowane w monografii dają możliwość tworzenia teorii szczegółowych, zgodnych ze znanymi faktami. Jednocześnie dzięki swojemu utylitarnemu charakterowi niniejsza monografia oferuje uporządkowaną teorię, która może być wykorzystana w działaniach zarówno tych żołnierzy, którzy rozumieją specyfikę cyberwalki, jak i tych, którzy nie rozumieją istoty działań militarnych, wykorzystujących cyberprzestrzeń, ale poszukują źródeł wiedzy. Treści zawarte w monografii mogą posłużyć poszerzaniu i porządkowaniu wiedzy dotyczącej teorii i praktyki badanego problemu do procesu profesjonalnego przygotowania personelu sił zbrojnych. Mogą być wykorzystane również przez osoby, które nie są związane z wojskowością, a zajmują się cyberwalką jako militarnym wymiarem działań, lub te, które chcą poznać ten wycinek rzeczywistości. Zbudowana teoria cyberwalki jako militarnego wymiaru działań może być wykorzystana do rozwiązań praktycznych. Można będzie ją wykorzystać w zbudowaniu zwirtualizowanej przestrzeni walki, która umożliwi prowadzenie symulowanej cyberwalki jako działań militarnych. Uzyskane wyniki badań redukują bariery wynikające z niejednoznaczności desygnatów zarówno cyberwalki, jak i składowych ją tworzących.

Ze względu na rozległość, interdyscyplinarność oraz dynamiczną zmienność obszar badań przedstawiony we wskazanej jako główne osiągnięcie naukowe monografii będzie w przyszłości poddany kolejnym badaniom naukowym z uwzględnieniem różnych perspektyw problemu badawczego, a teoria cyberwalki jako militarnego wymiaru działań rozwijana w dalszych dociekaniach naukowych. Żywię nadzieję, że wyodrębniony przeze mnie przedmiot badań znajdzie się w obszarze zainteresowań badawczych innych naukowców, którzy podejmą wysiłek badawczy rozwijający teorię cyberwalki jako militarnego wymiaru działań.

5. **Informacja o wykazywaniu się istotną aktywnością naukową albo artystyczną realizowaną w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej.**

Moją działalność naukową można podzielić na dwa główne obszary tematyczne. Są one pochodną awansów naukowych, pełnionych funkcji i osobistych zainteresowań naukowych.

Pierwszy obszar badawczy związany był z procesami informacyjnymi, rozpoznaniem elektronicznym i w efekcie procesami informacyjnymi w rozpoznanie 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 dociekania naukowe skupiłem na procesach informacyjnych w rozpoznaniu elektronicznym. Moje dociekania naukowe wynikały z obserwacji, że przestrzeń walki uzależniła się od urządzeń elektronicznych. Dzięki zaawansowanej elektronice operacje wojskowe zaczęły być prowadzone z wręcz chirurgiczną dokładnością. Znaczenie fal elektromagnetycznymi (EM) na teatrze znacząco wzrosła. Wszystkie rodzaje sił zbrojnych oraz wojsk posługiwały się sprzętem elektronicznym nadającym lub odbierającym fale EM. Radiostacje, radiolinie, środki naprowadzania lotnictwa, środki kierowania ogniem, radary radiolokacyjne oraz wiele innych elementów, takich jak choćby telefonia komórkowa, wykorzystywały promieniowanie elektromagnetyczne. Z powyższych faktów wynikało zatem, że zarówno struktury militarne jak i pozamilitarne, sojusznicze jaki potencjalnego przeciwnika wykorzystywały i nadal wykorzystują w swoich działaniach coraz bardziej wyspecjalizowane systemy elektroniczne emitujące fale EM.

Moje dociekania naukowe nad rozpoznaniem elektronicznym zaowocowały identyfikacją konieczności implementacji eksploracji danych do standardowych procedur przetwarzania danych w rozpoznaniu elektronicznym. Ustaliłem, że za pomocą eksploracji danych w rozpoznaniu elektronicznym otrzymuje się zależności i podsumowania zwane modelami i wzorcami.

Za pomocą modelowania możliwe jest w RE opisanie zmiennej, np. okręg wojskowy o n wartościach. Oprócz modelu opisowego możliwe jest tworzenie modelu indukcyjnego, umożliwiającego formułowanie wniosków o populacji, z której pochodzą dane. Podstawowymi formami modeli są: modele regresji liniowej, modele mieszane lub modele Markowa. Modele są abstrakcyjnym odzwierciedleniem procesów realnego otoczenia i nie służą do wykrywania zależności przyczynowych. Nawet jeżeli w danych istnieje pewna zależność, nie znaczy to, że jest między nimi faktyczna zależność przyczynowa.

Wzorzec w przeciwieństwie do modelu jest pojęciem lokalnym. Opisuje część danych w ograniczonej przestrzeni rozpiętej przez zmienne. Lokalny wzorzec jest opisem zjawisk, zachowań czy procesów normalnych, typowych. W odniesieniu do takiego opisu umożliwia określenie anomalii. Wzorzec pomaga wykryć nieprawidłowości. Odzwierciedla odchylenia od ogólnej partii danych, np. para zmiennych mająca szczególnie wysoką korelację, co w rozpoznaniu radioelektronicznym może oznaczać ścisłą zależność między dwoma obiektami o szczególnie istotnym znaczeniu operacyjnym. Tak jak w przypadku modeli można posłużyć się wzorcami opisowymi lub wzorcami indukcyjnymi.

Wyniki badań zaprezentowałem wygłoszeniem referatu nt. *Eksploracja danych w rozpoznaniu elektronicznym* na konferencji naukowej *Nowe kierunki w rozpoznaniu Sił Zbrojnych RP* w Akademii Obrony Narodowej w 2010 roku w Warszawie. Natomiast szczegółowy opis zawarłem w artykule naukowym:

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.

Moja aktywność naukowa w Akademii Obrony Narodowej w obszarze nauk o obronności zaowocowała opracowaniem i wprowadzeniem do nauk o obronności nowej metody badawczej

– *triangulacji*. O wynikach pracy poinformowałem społeczność naukową w czasie 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 zawarłem w artykule naukowym:

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 RE WL SZ RP spełnia kryteria właściwe dla systemu działania. Na tej podstawie określiłem desygnat procesu informacyjnego jako *system działania, czyli system rzeczywisty, w którym personel RE WL SZ RP za pomocą zasobów technicznych i proceduralnych systemu informacyjnego RE WL SZ RP realizuje zamierzony cel działania*. Szczegółowo wyniki badań opisałem w artykule naukowym:

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.

Wnioski z analizy i krytyki literatury dotyczącej Walki Elektronicznej, uwidoczniły lukę w wiedzy na temat procesów informacyjnych w rozpoznaniu elektronicznym WL SZ RP. Stan wiedzy nie precyzował, jak kształtuje się proces informacyjny w rozpoznaniu elektronicznym WL SZ RP.

W wyniku badań ustaliłem, że bariery informacyjne w rozpoznaniu elektronicznym WL SZ RP nie są opisane w przedmiotowej literaturze. Ponadto stwierdziłem, że przestarzałe zasoby techniczne wykorzystywane zarówno w pracy bojowej (komputery, komutatory, odbiorniki radiowe, okablowanie), jak i w szkoleniu (kasetowe nadajniki alfabetu Morse'a oraz radiogramów fonicznych czy słuchawki) negatywnie wpływają na rozpoznanie elektroniczne WL SZ RP. Ustaliłem, że personel biorący udział w procesie informacyjnym składa się z żołnierzy zawodowych i pracowników wojska. Ich wyszkolenie, motywacja i zaangażowanie różnią się od siebie. Dociekania naukowe pozwoliły wnioskować, że wskazane zróżnicowanie również wpływało negatywnie na procesy informacyjne. Argumentem wskazującym na słuszność powyższego wniosku okazał się fakt, że pracownicy wojska, jako grupa społeczna inaczej niż żołnierze zawodowi podchodzą do obowiązków służbowych. Zróżnicowane przyzwyczajenia i nawyki, a także uwarunkowania prawne odmiennie oddziaływały na procesy informacyjne.

Moim 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?* To pozwoliło na sformułowanie *hipotezy naukowej* w brzmieniu: *Proces informacyjny w RE WL SZ RP jest opartym o wypracowaną metodologię, realizowanym za pomocą określonych zasobów systemu informacyjnego RE WL SZ RP systemem działalności na danych i informacjach rozpoznawczych. Ma swój początek i koniec oraz trwa nieprzerwanie w czasie.*

Strukturę procesu informacyjnego w RE WL SZ RP tworzą podprocesy składające się z etapów, faz i czynności.

Czynniki pierwotne i czynniki wtórne warunkują strukturę oraz przebieg procesu informacyjnego w RE WL SZ RP.

Bariery organizacyjne, proceduralne i techniczne zakłócają proces informacyjny w RE WL SZ RP. Mają one negatywny wpływ na sprawność i organizację walki elektronicznej. Wyeliminowanie lub ograniczenie barier usprawni przebieg i strukturę procesu informacyjnego.

Istotnym ustaleniem 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 personel RE WL SZ RP. Proces informacyjny jest systemem niematerialnym. Realizowany jest za pomocą zasobów technicznych, ludzkich i proceduralnych systemu informacyjnego RE WL SZ RP. Odnośnie źródeł danych i informacji rozpoznawczych w procesie informacyjnym w RE WL SZ RP wyizolowałem ich kryteria: rodzaj źródła, miejsce pozyskiwania informacji, charakter informacji, format informacji, pewność źródła, poziom przetworzenia, geneza informacji, typ gromadzonych zasobów, dostępność źródeł informacji, rodzaj emitowanego sygnału, zasady zdobywania informacji, wpływ na istnienie źródła, wpływ na pracę źródła. Jednak podstawowym kryterium jest rodzaj źródła i według tego kryterium wyróżniłem źródła danych i informacji rozpoznawczych w RE WL SZ RP: pierwotne, wtórne i pochodne.

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.

Recenzenci: prof. dr. hab. Ryszard Jakubczak,
dr. hab. inż. Waldemar Scheffs.

Moja aktywność naukowa wraz z rozwojem wpływu teleinformatyki na działania militarne ewoluowała w kierunku poszukiwań desygnatu cyberbezpieczeństwa i identyfikacji nowych zależności w tym obszarze. Korzystając z własnych dotychczasowych eksploracji naukowych zidentyfikowałem 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 przeze mnie *środowiskiem cybernetycznym* i zdefiniowanie go jako zespół wszelkich elementów i czynników, będących w ścisłej współzależności, który wpływa na procesy informacyjne danego układu poprzez umacnianie stanów pożądanych i przeciwdziałanie stanom niepożądanym. O osiągnięciu tym poinformowałem społeczność naukową na Konferencji naukowej pt. „Automatyzacja dowodzenia SZ RP w środowisku sieciocentrycznym" w Akademii Obrony Narodowej w dniach 17-19 czerwca 2013 roku poprzez wygłoszenie referatu nt. *Procesy informacyjne w systemie wspomagania dowodzenia w kontekście działania w środowisku cybernetycznym.* Natomiast szczegółowy opis zawarłem w artykule naukowym:

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.

Badania procesów informacyjnych, środowiska cybernetycznego dały podwaliny pod badania zmierzające do identyfikacji cyberzagrożeń. W wyniku dociekań naukowych ustaliłem, że każdy proces informacyjny jest jednocześnie procesem semiotycznym, technicznym, proceduralnym, organizacyjnym i ekonomicznym, pozwoliło mi to wyizolować właśnie te obszary, jako obszary, w których mogą występować podatności sieci i systemów teleinformatycznych na cyberzagrożenia. Osiągnięcie to ogłosiłem na konferencji naukowej pt. „Wybrane aspekty bezpieczeństwa cybernetycznego Sił Zbrojnych Rzeczypospolitej Polskiej"

w Akademii Obrony Narodowej w grudniu 2013 roku poprzez wygłoszenie referatu nt. *Identyfikacja cyberzagrożeń.* Szczegóły opisałem w artykule naukowym:

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.

Identyfikując zagrożenia procesów informacyjnych w środowisku cybernetycznym ustaliłem, że istota cyberzagrożeń powoduje, że zarówno użytkownicy jak i właściciele systemów oraz sieci teleinformatycznych nie mają wpływu na istnienie cyberzagrożeń. Pewne czynniki mogą stanowić zagrożenie lub nie. Cyberzagrożenie jest w swej istocie jedynie potencjalnym czynnikiem wywołującym szkodę. Może być przyczyną niepożądanych wyników w rezultacie, których może nastąpić zakłócenie procesu informacyjnego bądź jego przerwanie. Cyberzagrożenie jest jedynie potencjalnym źródłem szkody. Czynnik należy naturalnie rozumieć jako przyczynę wywołującą skutek. Cyberzagrożenie, zatem może wywołać niepożądany skutek. Skutki niepożądane nie zawsze są szkodliwe, ale szkodliwe zawsze są niepożądane. Nie dostrzeganie zagrożeń, czyli czynników, które powodują lub mogą powodować szkody może być pojmowane jako poczucie bezpieczeństwa. Określone czynniki stanowią zagrożenia i mogą wywołać szkodliwy skutek jednak tylko wówczas, gdy chroniony przedmiot (czyli sieć lub system teleinformatyczny bądź jego elementy) posiada podatność i znajduje się w zasięgu oddziaływania zagrożenia. Zagrożenie musi, zatem mieć możliwość oddziaływania na przedmiot, wykorzystując jego podatność. Wyniki dociekań ogłosiłem na sympozjum naukowym pt. „Wybrane aspekty bezpieczeństwa cybernetycznego Sił Zbrojnych Rzeczypospolitej Polskiej" w Akademii Obrony Narodowej w 2014 roku poprzez wygłoszenie referatu nt. *Bezpieczeństwo procesów informacyjnych w środowisku cybernetycznym.* Wyniki badań prowadzonych w Akademii Obrony Narodowej zawarłem w:

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.

Moja aktywność badawcza 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). Uczestniczyłem w charakterze 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. Moja 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 mojej aktywności naukowej zawarłem w opracowaniach krajowych i zagranicznych w postaci polsko i anglojęzycznych artykułów i rozdziałów monografii naukowych.

Do najważniejszych opracowań w tym obszarze zaliczam:

R. Janczewski, *Procesy informacyjne w działaniach militarnych w cyberprzestrzeni*, [w:] B. Biernacik, L. Kalman (red.), *Systemy i sieci teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polskiej – wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2016, ISBN 978-83-7523-534-0.

W tym opracowaniu naukowym zawarłem efekt moich badań. Dotychczasowe dociekania naukowe nad procesami informacyjnymi umożliwiły mi w oparciu o kryterium złożoności zidentyfikować, iż o wielkości procesu informacyjnego w działaniach militarnych w cyberprzestrzeni nie decyduje ilość elementów go tworzących, a ich morfologia. To pozwoliło na sklasyfikowanie procesów informacyjnych w działaniach militarnych w cyberprzestrzeni jako procesy: małe, średnie i wielkie oraz zidentyfikowanie czynników je warunkujących.

R. Janczewski, *Charakterystyka i struktura procesu informacyjnego*, [w:] M. Wrzosek (red.) *Procesy informacyjne w obronności i bezpieczeństwie. Teoria i praktyka*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2017, ISBN 978-83-7523-571-5.

W tym opracowaniu naukowym zawarłem teorię procesów informacyjnych skupioną na jego charakterystyce i strukturze. Podkreślenia wymaga to, że istotnym ustaleniem badawczym jest to, że proces informacyjny jest systemem niematerialnym. Nie posiada zatem materialnych elementów. Realizowany jest wobec tego za pomocą zasobów technicznych, ludzkich i proceduralnych systemu informacyjnego organizacji.

R. Janczewski, G. Pilarski, *Autonomiczny symulator działań taktycznych w warunkach cyberzagrożeń*, [w:] B. Biernacik, L. Kalman, G. Pilarski (red.), *Wsparcie teleinformatyczne i bezpieczeństwo cyberprzestrzeni w SZ RP*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2018, ISBN 978-83-7523-653-8.

W tym artykule naukowym jako istotny wynik badań naukowych zaprezentowane zostały warianty konfiguracji systemu symulacyjnego działań militarnych w cyberprzestrzeni. Zaprezentowano koncepcję systemów zależnych od kryterium przeznaczenia oraz kryterium dostarczenia danych do platformy symulatora. Przedstawiono założenia architektury autonomicznego symulatora bazującego na heterogenicznym środowisku symulacyjnym.

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.

W tym opracowaniu naukowym w oparciu o wyniki badań naukowych, zaproponowałem definicje wybranych terminów takich jak: działania militarne w cyberprzestrzeni czy cyberobrona. Opracowanie zawiera wyniki badań prowadzonych w ramach projektu naukowego: *Zdolność sił zbrojnych do interoperacyjnego działania w cyberprzestrzeni*. Projekt ten jako *kierownik projektu* realizowałem w *Akademii Sztuki* we współpracy z Wydziałem Studiów Międzynarodowych i Politycznych *Uniwersytetu Jagiellońskiego*, który w czasie badań był ośrodkiem naukowym o *najwyższym krajowym potencjale naukowym*. Podczas ostatniej oceny parametrycznej uzyskał *kategorię naukową A*. Projekt ten finansowany był 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 7.11.2018 r. Wyniki badań zaprezentowałem także na:

> Międzynarodowej Konferencji pt. Knowledge-Based Organization w „Nicolae Balcescu" Land Forces Academy, w Sibiu, w Bułgarii, w dniach 10-14.06.2019 r. poprzez wygłoszenie referatu nt. *Terminology as a barrier of NATO'S interoperability in cyberspace operations*.

A następnie opublikowałem je w:

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.

R. Janczewski, *Znaczenie cyberprzestrzeni w działaniach hybrydowych*, [w:] L. Elak i in. (red.), Zagrożenia hybrydowe, Bellona, Warszawa 2019, ISBN 978-83-11-15650-0.

W ramach tej monografii naukowej przedstawiłem w postaci rozdziału wyniki badań nad rolą cyberprzestrzeni w wykorzystaniu potencjału militarnego w czasie działań militarnych. W oparciu o studium przypadku zidentyfikowałem i przedstawiłem metodologię działań w cyberprzestrzeni Rosji przeciwko Ukrainie w 2014 roku. Przedstawiłem także wyniki identyfikacji zastosowania cyberprzestrzeni w scenariuszu działań w cyberprzestrzeni. Istotne jest to, że badania wykazały zależność skuteczności wykorzystania cyberprzestrzeni w działaniach hybrydowych od stopnia uzależnienia społeczeństwa od najnowszych rozwiązań technicznych i technologii.

R. Janczewski, *Cyberbezpieczeństwo – ponadsektorowa kategoria bezpieczeństwa narodowego*, [w:] R. Jakubczak (red.) *Współczesna obrona narodowa*, Fundacja Historia i Kultura, Warszawa 2020, ISBN 978-83-952490-5-1.

W monografii naukowej poświęconej dostarczeniu podstawowej wiedzy o organizacji i funkcjonowaniu obrony narodowej Polski w tworzeniu bezpieczeństwa narodowego oraz międzynarodowego przedstawiłem wyniki badań nad wielowymiarowością cyberbezpieczeństwa i miejsca sił zbrojnych w systemie obrony państwa. Wyniki badań pozwoliły na sformułowanie wniosku, że dość powszechne postrzeganie cyberbezpieczeństwa państwa w sposób holistyczny nie jest podejściem gwarantującym cyberbezpieczeństwo. Dla osiągnięcia i utrzymania cyberbezpieczeństwa Polski potrzebne jest bardziej szczegółowe i kompleksowe podejście. Jednowymiarowy, terytorialny obraz konfliktu zmienił się w wielowymiarowy, wielopoziomowy kompleks działań militarnych i niemilitarnych, służących do osiągania niejednokrotnie zróżnicowanych celów.

R. Janczewski, *Cyberprzestrzeń: źródło zagrożeń bezpieczeństwa państwa*, [w:] M. Wrzosek, *Organizacja systemu rozpoznania zagrożeń państwa*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2020, ISBN 978-83-7523-770-2.

W monografii naukowej poświęconej organizacji systemu rozpoznania zagrożeń państwa w formie rozdziału zaprezentowałem rodzaje cyberzagrożeń cyberbezpieczeństwa państwa. Analiza i krytyka piśmiennictwa oraz analiza wybranych. cyberataków przeprowadzonych przeciwko strukturom państwowym oraz siłom zbrojnym pozwoliła mi scharakteryzować cyberprzestrzeń jako źródło zagrożenia państwa. W rozdziale tym na podstawie badań wykazałem, że jednym z negatywnych skutków informatyzacji funkcjonowania państwa jest jego zagrożenie bezpieczeństwa.

R. Janczewski, *Cyberbezpieczeństwo w życiu społecznym*, [w:] J. Stala, M. Butrymowicz (red.), *W służbie społeczeństwu. Polska w obronie praw człowieka na świecie i w kraju*, Wydawnictwo naukowe Uniwersytetu Papieskiego Jana Pawła II w Krakowie, Kraków 2022, ISBN 978-83-7438-988-4, DOI: https://doi.org/10.15633/9788374389891.09.

W monografii naukowej wydanej przez Wydawnictwo naukowe Uniwersytetu Papieskiego Jana Pawła II poświęconej wieloaspektowości i współczesnym warunkom funkcjonowania społeczeństw przedstawiłem rozwiązanie problemu badawczego sformułowanego w postaci pytania *Jaka jest charakterystyka cyberbezpieczeństwa w społeczeństwie?* Badania wykazały jednoznaczny obraz współczesnego świata. Charakter przeprowadzanych cyberataków jednowymiarowy i terytorialny obraz konfliktu zmienił się w wielowymiarowy, wielopoziomowy kompleks działań militarnych i niemilitarnych służących niejednokrotnie osiąganie zróżnicowanych celów.

R. Janczewski, *Cyberdziałania w aspekcie maskowania*, [w:] K. Wysocki, W. Kuchta (red.), *Techniczne aspekty współczesnego maskowania*, Akademia Sztuki Wojennej, Warszawa 2022, ISBN 978-83-8263-254-5.

W tej monografii w postaci rozdziału zaprezentowałem swoje wyniki badań nad kamuflowaniem działań militarnych w cyberprzestrzeni. Zaprezentowałem rozwiązania w zakresie maskowania działań w cyberprzestrzeni oraz scharakteryzowałem metody podstępów w cyberprzestrzeni, do których zaliczyłem zwodzenie, wykrywanie, zakłócanie oraz zakłócanie. Badania wykazały, że kamuflowanie się w cyberprzestrzeni ma szanse powodzenia zarówno na poziomie taktycznym, operacyjnym jak i strategicznym. A korzyści płynące z podstępu można osiągnąć defensywnie i ofensywnie.

Mój wysiłek badawczy zaowocował autorstwem ośmiu haseł (przetwarzanie informacji, *wiarygodność informacji, informacja rozpoznawcza, cykl Deminga, dane szczególnej kategorii, system informacyjny, cykl rozpoznawczy, kanał telekomunikacyjny*) w R. Janczewski, [w:] W. Fehler, Leksykon bezpieczeństwa informacyjnego, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce, 2023, ISBN 978-83-67162-78-4.

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.

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.

Jako istotny wynik mojej aktywności naukowej uważam artykuł naukowy indeksowany w bazie publikacji naukowych Web of Science:

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

W niniejszym artykule naukowym zaprezentowane zostały wyniki dociekań naukowych nad zrozumieniem postrzegania współczesnego konfliktu przez Gierasimowa, jako sposobem na zapobieganie cyberkonfliktom.

Moja aktywność naukowa zaowocowała uczestnictwem w redakcjach naukowych monografii:

1. R. Janczewski, M. Marczyk, B. Terebiński (red.), *Militarne aspekty cyberbezpieczeństwa państwa w czasie działań hybrydowych przeciwko RP*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2020, ISBN 978-83-7523-761-0.
2. R. Janczewski, J. Kosiński (red.), *Przestępczość Teleinformatyczna 2021*, Wydawnictwo BP, Gdynia 2021, ISSN 1898-3189.
3. R. Janczewski, J. Kosiński (red.), *Przestępczość Teleinformatyczna 2022*, Wydawnictwo BP, Gdynia 2022, ISSN 1898-3189.
4. Indywidualnie wydałem jako redaktor naukowy monografie:
5. R. Janczewski (red.), *Cyberbezpieczeństwo teoretycznie i empirycznie w naukach o bezpieczeństwie*, Wydawnictwo PB, Gdynia 2021, ISBN 978-83-65763-50-1.
6. R. Janczewski (red.), *Cyberbezpieczeństwo teoretycznie i empirycznie w naukach o bezpieczeństwie 2022*, Wydawnictwo PB, Gdynia 2022, ISBN 978-83-65763-54-9.

7. R. Janczewski (red.), *Cyberbezpieczeństwo. Punkty widzenia*, Wydawnictwo BP., Gdynia 2023, ISBN 978-83-65763-55-6 - w procedowaniu.

W ramach mojej aktywności naukowej wykonałem opracowanie: „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.

Zrealizowałem w dniach 01.04.2019 r. do 19.12.2019 r. zadanie badawcze: „Cyberbezpieczeństwo w organizacji" w ramach projektu naukowego ROTOR realizowanego przez WAT, NCK oraz ABW. Przygotowałem moduły kursu e-learningowego dla pracowników administracji państwowej, którzy nie są przełożonymi i którzy są przełożonym najniższego szczebla.

Jestem członkiem zespołu badawczego pt. *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.

Jestem współautorem wniosku w ramach konkursu NCN - Konkurs nr 4/SZAFIR/2021 na projekt pt. „Szerokopasmowy, wielosensorowy system elektroniczno-obrazowego rozpoznania morskiego klasy ELINT/IMINT/AIS dla bezzałogowych statków powietrznych". Składanego przez Morskie Centrum Cyberbezpieczeństwa w ramach konsorcjum.

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

Moja aktywność zawodowa pozwoliła na uczestniczenie jako członek projektu w międzynarodowych projektach:

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).

Jako reprezentant Polski w międzynarodowym programie *DEEP Ukraine 2022* w zakresie *Cyber Security Curriculum Development for the Odesa Naval Institute.*

Byłe także członek zespołu badawczego „Diagnoza kompetencji IT pracowników Poczty Polskiej, ze szczególnym uwzględnieniem obszaru cyberbezpieczeństwa" przeprowadzonego przez Morskie Centrum Cyberbezpieczeństwa w Akademii Marynarki Wojennej 2020 roku.

Jako istotne osiągnięci uważam pełnienie roli kierownika w zadaniach badawczych:

1. 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.
2. 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.

3. 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.
4. 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.

Moje zaangażowanie naukowe przyczyniło się do uczestniczenia jako członek projektu w projekcie badawczym realizowanym przez Morskie Centrum Cyberbezpieczeństwa na zlecenie Warszawskiego Instytutu Bankowości w 2022 r. *Dezinformacja i propaganda w sektorze bankowym.* W ramach tego projektu byłem autorem rozdziału 5: *Propozycja narzędzi do zwalczania kampanii* informacyjnych i współautorem rozdziału 3: Modele dezinformacji i propagandy w sektorze bankowym w Raporcie *„Dezinformacja i propaganda w sektorze bankowym".*

Moje zaangażowanie naukowe pożytkowałem także uczestnicząc w radach i komitetach naukowych krajowych i międzynarodowych konferencji i sympozjów naukowych:

1. III Konferencja naukowa pt. „Bezpieczeństwo informacyjne w obszarze cyberprzestrzeni", Akademia Marynarki Wojennej w Gdyni, 25-26.06.2017 r., 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., członek kierownictwa naukowego oraz prowadzący II sesję pt. „Bezpieczeństwo cyberprzestrzeni".
3. Sympozjum naukowe nt. „Znaczenie cyberprzestrzeni w procesie targetingu, Systemy i sieci teleinformatyczne SZ RP – Wielorakie aspekty bezpieczeństwa cyberprzestrzeni", Akademia Sztuki Wojennej w Warszawie, 05.12.2017 r., prowadzący sesję *bezpieczeństwo cyberprzestrzeni.*
4. 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.
5. 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.
6. Konferencja naukowa pt. „Techniczne Aspekty Przestępczości Teleinformatycznej", Wyższa Szkoła Policji w Szczytnie, 3-4.06.2019 r., członek komitetu naukowego konferencji.
7. Konferencja naukowa pt. Przestępczość Teleinformatyczna XXI wieku, Akademia Marynarki Wojennej, 17-19.06.2019 r., członek rady naukowej.
8. Sympozjum naukowe pt. „Cyberbezpieczeństwo obszaru militarnego i niemilitarnego", Akademia Sztuki Wojennej, 28-29.11.2022, Członek komitetu naukowego, członek komitetu organizacyjnego.
9. 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.

10. Konferencja PWNing Security Conference, Państwowe Wydawnictwo Naukowe, 17-19.11.2021 r., członek rady programowej konferencji.
11. 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.
12. I Krajowa konferencja naukowa „Współczesne uwarunkowania maskowania", Akademia Sztuki Wojennej 18.05.2022 r., członek komitetu naukowego konferencji.
13. 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.
14. 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.
15. Konferencja naukowa pt. Przestępczość Teleinformatyczna XXI wieku, Akademia Marynarki Wojennej, 13-15.06.2022 r., członek rady naukowej.
16. 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.
17. 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.
18. Konferencja naukowa pt. „Dezinformacja. Walka. Wojna. Bezpieczeństwo", Akademia Marynarki Wojennej, 22.05.2023 r., wygłoszenie referatu nt. członek komitetu naukowego.

Moją aktywność naukowa skupiła się także na redagowaniu opracowań naukowych. W ramach tego rodzaju działalności naukowej jestem:

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

Istotnym osiągnięciem naukowym w moim dorobku było wykonanie recenzji:

1. Artykułu naukowego pt. „Unity of Russian society. Importance of building social cohesion for the security of Russia" dla kwartalnika „Security and Defence Quarterly".
2. Pracy doktorskiej pt. „Efektywne metody skrytej synchronizacji akustycznych kanałów steganograficznych" w ramach Konkursu DNiSZW MON o Nagrodę im. Mariana Rejewskiego za najlepszą pracę inżynierską, licencjacką, magisterską i rozprawę doktorską poświęconą cyberbezpieczeństwu i kryptologii.
3. Pracy doktorskiej pt. „Clustering-based method for botnet detection" w ramach Konkursu DNiSZW MON o Nagrodę im. Mariana Rejewskiego za

najlepszą pracę inżynierską, licencjacką, magisterską i rozprawę doktorską poświęconą cyberbezpieczeństwa i kryptologii.

4. Pracy doktorskiej pt. „Orkiestracja narzędzi bezpieczeństwa w sieci operatora telekomunikacyjnego z wykorzystaniem technik uczenia maszynowego oraz metod przetwarzania języka naturalnego" w ramach Konkursu DNiSZW MON o Nagrodę im. Mariana Rejewskiego za najlepszą pracę inżynierską, licencjacką, magisterską i rozprawę doktorską poświęconą cyberbezpieczeństwu i kryptologii.
5. Skryptu pt. *Podstawy administracji SAP BASIS (ABAP)* dla Wydawnictwa PUZ im. Ignacego Mościckiego w Ciechanowie, 2023 r.

W ramach mojej aktywności naukowej jestem także członkiem Polskiego Towarzystwa Nauk o Bezpieczeństwie, na Uniwersytecie Przyrodniczo-Humanistyczny w Siedlcach.

Wydałem opinię „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.

Moją aktywność naukowa 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.

Za moje istotne i ważne osiągnięcia wynikające z aktywności naukowej uważam:

1. Uczetnictwo na zaproszenie w OSCE-wide Cyber/ICT Security Conference w dniach 20-2110.2022 w Łodzi nt. Building societal resilience by raising public awareness of cyber threats and enhancing the role of cyber education jako panelista w panelu *Enhancing the role of cyber education.*
2. Uczestnictwo na zaproszenie jako panelista w RoundTable discussion nt. Perceptions of the cyber threat, attribution and interoperability - view from Poland w Baltic Defence College, w Tartu, w Estonii, 09.12.2019 r.,
3. Uczestnictwo na zaproszenie w Forum ekonomicznym 2020, „Europa po pandemii: Solidarność, Wolność, Wspólnota?" Karpacz, 8-10.09.2020, panelista w panelu: „#CyberbezpiecznySamorząd – jak zrobić to dobrze?".
4. Uczestnictwo na zaproszenie jako panelissta w Forum ekonomicznum 2020, „Europa po pandemii: Solidarność, Wolność, Wspólnota?" Karpacz, 8-10.09.2020 panelista w panelu: „Rosja, Chiny, Iran, Cyber. Największe wyzwania dla utrzymania bezpieczeństwa w Europie".

6. Informacja o osiągnięciach dydaktycznych, organizacyjnych oraz popularyzujących naukę lub sztukę.

Za osiągnięcie dydaktyczne uważam przeprowadzenie:

1. Wykładów w Wyższej Szkole Biznesu i Zarządzania w Ciechanowie w ramach przedmiotów:
   - Systemy operacyjne,
   - Bazy danych,
   - Metody i narzędzia modelowania systemów informacyjnych.
2. Wykładów w Wyższej Szkole Policji w Szczytnie w ramach przedmiotu:
   - Inżynieria wiedzy - wstęp do sztucznej inteligencji.
3. Wykładów na Uniwersytecie Warmińsko-Mazurskim w Olsztynie. Prowadzone przedmioty:

- Informatyczne systemy bezpieczeństwa.

4. Wykładów w Akademii Marynarki Wojennej w Gdyni w ramach przedmiotu:
   - Cyberbezpieczeństwo,
   - Zarządzanie systemami bezpieczeństwa wewnętrznego,
   - Planowanie operacji w cyberprzestrzeni,
   - Audyt bezpieczeństwa systemów teleinformatycznych.
5. Wykładów w ramach Letniej Szkoły Cyberbezpieczeństwa.
6. Wykładów w ramach Zimowej Szkoły Cyberbezpieczeństwa.
7. Wykładów w Centrum Doskonalenia Zawodowego Oficerów AON.
8. Wykładów i ćwiczeń w ramach wyższego kursu operacyjno-strategicznego na Wydziale Wojskowym ASzWoj w ramach przedmiotu bezpieczeństwo w cyberprzestrzeni.
9. Wykładów i ćwiczeń w ramach wyższego kursu operacyjno-strategicznego na Wydziale Wojskowym ASzWoj w ramach przedmiotu bezpieczeństwo w cyberprzestrzeni.
10. Cyklu wykładów z cyberbezpieczeństwa w The Vasil Levski National Military University, Veliko Tarnovo, Bulgaria, 27-31.05.2019 r.
11. Wykładów 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. Prelekcji w Centrum Doktryn i Szkolenia Sił Zbrojnych.
13. Wykładów w Centrum Doskonalenia Zawodowego Oficerów AON.
14. Wykładów i ćwiczeń w ramach wyższego kursu operacyjno-strategicznego na Wydziale Wojskowym ASzWoj w ramach przedmiotu bezpieczeństwo w cyberprzestrzeni.
15. Wykładów i ćwiczeń w ramach wyższego kursu operacyjno-strategicznego na Wydziale Wojskowym ASzWoj w obszarze bezpieczeństwa w cyberprzestrzeni.
16. Wykładów w ramach szkolenia administratorów i inspektorów bezpieczeństwa w 3 Warszawskiej Brygadzie Rakietowej Obrony Powietrznej nt.
    - Działania w cyberprzestrzeni,
    - Cyberzagrożenia.
17. Wykładów w ramach szkolenia administratorów i inspektorów bezpieczeństwa w 9 Brygadzie Wsparcia Dowodzenia nt.
    - Działania w cyberprzestrzeni,
    - Cyberzagrożenia.
18. Wykładu 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. 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.

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.

W ramach popularyzacji nauki opublikowałem artykuły:

1. R. Janczewski, *Efektywność a skuteczność w walce elektronicznej*, Przegląd Wojsk Lądowych, 2012, Nr 01 (055).
2. R. Janczewski, *Źródła informacji w rozpoznaniu radioelektronicznym*, Przegląd Wojsk Lądowych, 2012, Nr 02 (056).
3. R. Janczewski, *Walka w cyberprzestrzeni*, Przegląd Sił Zbrojnych, 2018, Nr 01.
4. R. Janczewski, *Cyberprzestrzeń – część teatru działań hybrydowych*, Przegląd Sił Zbrojnych, 2019, Nr 02.
5. R. Janczewski, *Facing the New Risks of Digitised Wars*, European Security, 6. November 2019.
6. 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.
7. 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/.

Moim istotnym osiągnięciem jest uczestniczenie jako Ekspert 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.

7. Oprócz kwestii wymienionych w pkt. 1-6, wnioskodawca może podać inne informacje, ważne z jego punktu widzenia, dotyczące jego kariery zawodowej.

W związku z moją aktywnością naukową i zawodową uczestniczyłwm w Cyber Security Curriculum Development Workshop for the Odesa Naval Institute 07-11.03.2022 (DEEP Ukraine 2022 - Event #2833) Hosted by Nikola Vaptsarov Naval Academy, Varna, Bulgaria.

W ramach działalności dydaktycznej w roku 2008 zostałem Mistrzem Metodyki na szczeblu jednostki wojskowej 5699.

W ramach mojej działalności naukowej i zawodowej uczestniczyłem jako:

1. Ekspert ds. cyberbezpieczeństwa w zespole opracowującym doktrynę Operacje informacyjne – DD-3.10(A).
2. Ekspert ds. cyberbezpieczeństwa w zespole opracowującym Doktrynę działań połączonych – D-01(E).
3. Ekspert ds. działań militarnych w cyberprzestrzeni w zespole autorskim ćwiczenia pk. JESION-15.
4. Ekspert ds. działań militarnych w cyberprzestrzeni w zespole autorskim ćwiczenia pk. ANAKONDA-16.

5. Ekspert ds. cyberbezpieczeństwa w zespole opracowującym Zasady użycia Wojsk Obrony Terytorialnej.
6. Ekspert ds. działań militarnych w cyberprzestrzeni, wygłoszenie wykładu w czasie warsztatów SZ RP pk. OPERATOR-15 nt. *Procesy informacyjne w działaniach militarnych w cyberprzestrzeni.*
7. Ekspert ds. działań militarnych w cyberprzestrzeni, zespół autorski ćwiczenia pk. ZIMA-17.
8. Ekspert ds. cyberbezpieczeństwa, udział w analizie „Organizacja i funkcjonowanie StratCom i InfoOps w RON", Miejsce: CO MON, Warszawa.
9. Ekspert ds. cyberbezpieczeństwa, zespół opracowujący doktrynę Działania w cyberprzestrzeni – DD-3.20(A).
10. Ekspert ds. cyberbezpieczeństwa w sympozjum nt. *Wyzwania związane z budową krajowego systemu cyberbezpieczeństwa*, Ministerstwo Nauki i Szkolnictwa Wyższego, 20.06.2018 roku.
11. Ekspert ds. cyberbezpieczeństwa w konferencja pt. „OH My H@ck 2020"organizowanym przez Zaufaną trzecią stronę, Pl oraz Proidea w dniach 27.11.2020 r. wygłaszając referat nt. *Cyberochrona żołnierzy we współczesnej przestrzeni walki.*
12. Ekspert ds. cyberbezpieczeństwa Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni w webinarium „Webinar on cyber threats – Polish, Danish and NATO perspectives" organizowanym przez Ambasadę RP w Danii (Kopenhaga), ISP PAN oraz OBA CBB ASzWoj w dniu 11.01.2021 r.
13. Ekspert ds. cyberbezpieczeństwa grupy „Enabling" dokonującej przegląd zdolności obronnych NATO w spotkanie dwustronnym w dniach 28-29.01.2020 r. w Akademii Sztuki Wojennej w Warszawie.
14. Ekspert ds. cyberbezpieczeństwa Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni w konferencji pt. „Navigating through a Sea of Data – Challenges for Secure and Efficient Reinforcement and Military Mobility in Europe/NATO", AFCEA Europe i the Joint Support and Enabling Command (JSEC), 29-30 September 2020, jako panelista w panelu: „Comprehensive Situational Awareness on Cyber Security in the Rear Area – the importance of gaining and maintaining".
15. Ekspert Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni w webinarium pt. „Technoautorytaryzm czy technodemokracja. Nowe technologie w służbie państwu w dobie pandemii: Singapur-Korea Południowa-Chiny", w dniu 07.01.2021 r., ISP PAN i Ośrodka Badań Azji Centrum Badań nad Bezpieczeństwem ASzWoj.
16. Ekspert ds. cyberbezpieczeństwa na konferencji pt. „Itechday" organizowanej przez Warszawską Grupę Użytkowników i Specjalistów Windows w dniu 29.09.2020 r., wygłoszony referat nt: *IT na współczesnym polu walki – nie tylko sprzymierzeniec.*
17. Ekspert ds. cyberbezpieczeństwa reprezentujący Polskę w Polsko-Estońskim dialogu strategicznym w Tallinie, w Estonii.
18. Ekspert ds. cyberbezpieczeństwa w zespole opracowującym pierwszy w SZ RP „Plan Zarządzania Kryzysowego Resortu Obrony Narodowej".
19. Koordynator działań militarnych w cyberprzestrzeni w ćwiczeniu Dragon-17.
20. Ekspert ds. cyberbezpieczeństwa w grupie roboczej zespołu ds. opracowania założeń i dokumentów zapewniających wzrost liczebności SZ RP (niepublikowane).

21. Ekspert ds. cyberbezpieczeństwa w 2019 roku w grupie roboczej zespołu ds. opracowania „Programu kształcenia na studiach wyższych" na kierunku Informatyka na poziomie studiów pierwszego stopnia (inżynierskich) o profilu praktycznym w dziedzinie nauk społecznych dla studiów stacjonarnych i niestacjonarnych w Wyższej Szkole Policji w Szczytnie.

Jestem współorganizatorem Wojskowego Forum Cyberbezpieczeństwa w dniu 14.10.2022 r. w Morskim Centrum Cyberbezpieczeństwa Akademii Marynarki Wojennej, organizatorem spotkania studentów informatyki z przedstawicielem Dowództwo komponentu wojsk obrony cyberprzestrzeni w ramach projektu „Jak zostać żołnierzem Wojsk Obrony Cyberprzestrzeni", organizatorem warsztatów dla studentów informatyki w zakresie pentestingu realizowanych przez specjalistów firmy „Securak".

Jestem 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 zainteresowań naukowych podnoszę kwalifikacje zawodowe, do najważniejszych zaliczam:

1. „Information Security Management Systems Auditor/Lead Auditor" – certyfikat nr PL151210-PL2010-12-10-1297.
2. „Auditor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg wymagań normy ISO/IEC 27001: 2005" – certyfikat nr 1652/06/11.
3. „Security Manager Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO/IEC 27001: 2005" – certyfikat nr 1642/06/11.
4. Ukończony kurs „Podstawowy kurs tworzenia materiałów i prowadzenia zajęć z wykorzystaniem technik i metod kształcenia zdalnego".
5. Ukończony kurs „PostgreSQL".
6. Ukończony akredytowany kurs ITIL® Foundation – otrzymanie 21 Professional Development Units (PDU).
7. Certyfikat: „ITIL® Foundation Certificate in IT Service Management". Ukończony kurs „Zarządzanie ryzykiem w Systemach Bezpieczeństwa Informacji zgodnie z ISO/IEC 27005: 2011" – BSI.

Wyróżnienia:

1. Mistrz Metodyki na szczeblu jednostki wojskowej.
2. Złota Wojskowa Odznaka Sprawności Fizycznej.
3. Brązowa Odznaka Sprawności Strzeleckiej.
4. Złoty medal „ZA ZASŁUGI DLA OBRONNOŚCI KRAJU".
5. Srebrny medal „SIŁY ZABROJNE W SŁUZBIE OJCZYZNY".
6. „Odznaka honorowa PCK" IV stopnia.
7. Brązowy medal za długoletnią służbę wojskową.
8. Medal Pamiątkowy Wielonarodowej Dywizji Centrum-Południe
9. Gwiazda Iraku.
10. Gwiazda Afganistanu.
11. Odznaka pamiątkowa 2 prel.
12. Odznaka pamiątkowa 2ORel.
13. List uznania dowódcy kontyngentu Rumunii za dobrą współpracą w ramach VII zmiany PKW w Republice Iraku.
14. Odznaka pamiątkowa CBC SZ.

15. Odznaka pamiątkowa COC.
16. Zasłużony Żołnierz RP III Stopnia.
17. Wojskowy Krzyż Zasługi.
18. List gratulacyjny od Dyrektora Narodowego Centrum Kryptologii.
19. List gratulacyjny od Komendanta Centrum Operacji Cybernetycznych.

Za ważne dla mnie wyróżnienie za szczególne zasługi dla oświaty i wychowania uważam „Medal Komisji Edukacji Narodowej", którym odznaczony zostałem w dniu 29 lipca 2019 r.

.....
(podpis wnioskodawcy)