Dr hab. Ireneusz T. DZIUBEK, prof. Akademii Kaliskiej
Instytut Nauk o Bezpieczeństwie
Akademia Kaliska
im. Prezydenta Stanisława Wojciechowskiego
ul. Nowy Świat 4, 62-800 Kalisz

Kalisz, dnia 14.07.2023 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

Pana mgr. Grzegorza MĄKOSY
pt. *Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej*
zrealizowanej pod kierownictwem naukowym Pana prof. dr. hab. Bogusława JAGUSIAKA

1. Wstęp

Podstawą prawną przeprowadzonych czynności i ostatecznego wydania niniejszej opinii stała się Uchwała Rady Dyscypliny *Nauki o Bezpieczeństwie* Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie Nr 24/RDN No/2023 z dnia 24.05.2023 roku – w sprawie powołania recenzentów w przewodzie doktorskim Pana mgr. Grzegorza MĄKOSY.

W konsekwencji powyższego, uwzględniając ustawowe kryteria i wymogi stawiane rozprawom doktorskim, w kolejnych częściach recenzji odniesiono się do następujących aspektów: określenie trafności wyboru i oryginalności problemu badawczego podjętego w rozprawie wraz z odniesieniem się do wiedzy teoretycznej Kandydata w danej dyscyplinie naukowej; ocena metodologiczna i merytoryczna dysertacji w kontekście umiejętności samodzielnego prowadzenia pracy naukowej; osiągnięcie określonych wyników badań i praktyczne ich zastosowanie; ocena od strony formalnej oraz wniosek końcowy.

2. Określenie trafności wyboru i oryginalności problemu badawczego podjętego w rozprawie

Stosując podstawowe odniesienie do problematyki pracy określonej tytułem: *Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej* należy stwierdzić, że trzeba ją lokalizować w dziedzinie *nauk społecznych*, w dyscyplinie *nauki o bezpieczeństwie*, a w węższym ujęciu, w obszarze *zarządzania bezpieczeństwem*.

Tytułowo wyróżnione zagadnienia dotyczące *cyberbezpieczeństwa* dotyczą nieprzeciętnej przestrzeni poznania powiązanej z wykształceniem się *społeczeństwa informacyjnego*, w której praktyczna penetracja wyprzedziła teoretyczną i ma tradycje zaledwie kilku dekad.

Warto zatem zauważyć, że o specyficznym obszarze, w którym zaczął funkcjonować nowoczesny człowiek, tworzonym przez technologie cyfrowe i ich możliwościach informacyjno-komunikacyjnych, usłyszano w Europie dopiero w roku 1978, zapoznając się z eksperckim protokółem opracowanym na potrzeby Prezydenta Francji przez S. Nora i A. Minca. Od tego momentu aż do początku lat 90. XX wieku, termin *społeczeństwo informacyjne* funkcjonował jedynie w środowisku uczonych, by w odniesieniu empirycznym zająć ponownie poczesne miejsce w 1994 roku – za sprawą, powołanej na zlecenie Komisji Europejskiej, specjalnej grupy roboczej pod przewodnictwem M. Bagnemanna. Ogłoszony w następstwie jej prac raport: upowszechnił na gruncie europejskim pojęcie społeczeństwa informacyjnego, uczynił powyższą problematykę przedmiotem poważnego zainteresowania, a także wskazał na wyzwania, które stanęły przed Europą w związku z gwałtownym rozwojem technologii informacyjnych.

W konsekwencji powyższego kraje Unii Europejskiej w 2000 roku, na szczycie w Lizbonie przyjęły dokument, określony jako *e-Europe-Information Society for All*, zobowiązujący państwa członkowskie do wprowadzenia obywateli Europy w erę *cywilizacji informacyjnej*. Wyszczególnione końcowo pojęcie przyjęto jednocześnie stosować do opisu przemian technologizacji, gdzie zarządzanie informacją, jej jakość, szybkość przepływu decyduje o konkurencyjności zarówno w przemyśle jak i w usługach, a stopień rozwoju wymaga stosowania nowych technik gromadzenia, przetwarzania, przekazywania i użytkowania danych.

Posiłkując się zobrazowanym powyżej stanem rzeczy, poszczególne zbiorowości, a w tym praktycy zarządzający i środowiska naukowe, stanęły przed koniecznością odnalezienia się w nowo wyodrębnionym wymiarze funkcjonowania, który szybko określono mianem *cyberprzestrzeni*. Wśród wielu aspektów tej rzeczywistości szybko dostrzeżono nieuchronność weryfikowania dotychczasowych poglądów na poszczególne sfery bezpieczeństwa, zarówno w wymiarze narodowym jak i międzynarodowym. Odnotowano nie tylko wpływ *cyfryzacji* na poziom obecnych zagrożeń, ale także pojawianie się nowych, dotąd mniej znaczących lub w ogóle nie zauważalnych. Idąc dalej tropem takich obserwacji wyprowadzono, że zagrożenia te mogą powstawać między innymi w newralgicznych punktach infrastruktury informacyjnej państwa, a także w związku z celowo wprowadzanymi zaburzeniami, w postępującym uzależnieniu społeczeństwa od natychmiastowego i niezakłóconego przepływu danych. W logicznym łańcuchu takiego rozumowania już niejako automatycznie wyłonił się dodatkowy *sektor bezpieczeństwa*, któremu nadano miano *cyberbezpieczeństwa*.

W optyce powyższego pochylenie się Autora nad wyodrębnionym obszarem organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej, znajduje swoje głębokie uzasadnienie zarówno za sprawą względów teoretycznych jak i utylitarnych.

W pierwszej płaszczyźnie tych starań – trafność wyboru wynika przede wszystkim ze złożoności nowej, transsektorowej, a jednocześnie wielowymiarowej, powikłanej i niepewnej formuły bezpieczeństwa – dotyczącej środowiska informacyjnego państwa w cyberprzestrzeni. Wnosząc swoimi badaniami znaczący wkład w rozpoznanie tak złożonej materii Doktorant przyczynił się moim zdaniem nie tylko do naukowego identyfikowania groźnych zmiennych, ale i do racjonalnego uporządkowania wybranych kwestii natury ogólnej.

Od strony praktycznej Doktorant – w zgodzie ze swoimi badawczo uzasadnionymi stwierdzeniami – udowodnił, że bezpieczeństwo państwa: *wymaga nowych rozwiązań w zakresie bezpieczeństwa, w tym efektywnego systemu cyberbezpieczeństwa. Wyniki badań prowadzonych i zaprezentowanych w ramach niniejszej dysertacji mogą stanowić wkład i propozycję rozwiązań koncepcyjnych, których zastosowanie może przyczynić się do poprawy efektywności polskiego systemu cyberbezpieczeństwa i tym samym zwiększenia bezpieczeństwa państwa* (strona *15.* dysertacji).

Odnotowując powyższe, należy jednocześnie zwrócić uwagę na oryginalność problemu badawczego podjętego w recenzowanej rozprawie – co w sposób bezsprzeczny wynika nie tylko z penetracji standardów cyberbezpieczeństwa, ale i rekapitulacji treści dotąd ogłoszonych opracowań, monografii bądź artykułów naukowych. Ten ostatni aspekt Autor niezwykle szeroko i dogłębnie wykazał w przeprowadzonej *krytycznej analizie literatury* (strony od *28.* do *41.* dysertacji) udowodniając, że wyodrębniona problemowo materia nie była wcześniej badawczo penetrowana i naukowo objaśniana, nie tylko na płaszczyznach zbieżnych, ale nawet zbliżonych.

Bazując na powyżej zaprezentowanych konstatacjach można zaryzykować twierdzenie o charakterze ostatecznie podsumowującym, że Pan mgr Grzegorz MĄKOSA wykazał się samodzielnym wyróżnieniem – niezwykle interesującego i współcześnie determinującego przemiany w bezpieczeństwie – obszaru badawczego. Przedstawiony teoretyczny i praktyczny wymiar autorsko wyartykułowanego wycinka niewiedzy czyni tym samym zadość potrzebom dyscypliny *nauki o bezpieczeństwie* i odpowiednio ją wzbogaca.

3. Ocena metodologiczna dysertacji

Zakres zastosowanych procedur badawczych został przez Autora wyartykułowany w wyrazisty sposób, w *Rozdziale 1.* (strony od *13.* do *41.* dysertacji) – rozpoczęto go nie budzącymi żadnych wątpliwości rozważaniami stanowiącymi *uzasadnienie podjęcia badań* (strony od *13.* do *16.* dysertacji).

Po wcześniejszym zapoznaniu się z prawidłowo opracowaną treścią *Streszczenia rozprawy* (strona *3.* dysertacji) i nieco chaotycznie skonstruowanym *Wstępem* (szczególnie: strona *9.* dysertacji) należałoby oczekiwać ponownie prawidłowo realizowanego przekazu na rzecz zobrazowania całości postępowania badawczego. Zachowanie takie stanowi przecież pewien uporządkowany proces. Składa się na niego, co najmniej kilka etapów (faz), a pierwszym z nich jest wyróżnienie *przedmiotu badań*. Należy bowiem najpierw sobie uzmysłowić, o jakim zakresie zjawisk chciałoby się *coś orzekać*. Tymczasem Autor rozpoczął dalsze swoje rozważania, od prezentacji *celu badań* (strony od *16.* do *17.* dysertacji), wyróżniając: *cel główny* i *cele szczegółowe*.

Rozpatrując treść: *Celem głównym prowadzonych badań jest opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia poziomu bezpieczeństwa państwa*, a następnie kolejno wyróżnionych pięciu *celów szczegółowych* – nie sposób pominąć kolejnej uwagi dotyczącej powtarzającego się tam wyrażenia *opracowanie koncepcji*, a w tym szczególnie w moim przekonaniu rażącego zwrotu w postaci: *Opracowanie koncepcji wykazu (...)*. Uważam, że podczas formułowania *głównego celu badań* i *celów szczegółowych* używane określenia powinny bardziej korespondować z takimi pojęciami jak: *identyfikacja*, *klasyfikacja*, *ustalenie*, *ocena* czy *analiza*, a zarazem z zakładaną autorsko realizacją funkcji poznawczych i praktyczno-użytecznych.

Podobnego charakteru jest dalsza uwaga, powiązana z treścią *głównego problemu badawczego*, zawartego w pytaniu: *Czy organizacja systemu cyberbezpieczeństwa RP zapewnia odpowiedni poziom bezpieczeństwa państwa i jakie są możliwości usprawnienia organizacji tego systemu dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa?* – gdzie podwójne wykorzystanie słowa *organizacja* (także *systemu)* wydaje się być zbędne.

Drobne te uwagi nie deprecjonują wykazanych w kolejnych częściach pracy cech poprawności metodologicznej, ale powinny być w pełni przestrzegane i uwzględniane, podobnie jak ograniczenia w interpretacji zastosowanych metod, technik i narzędzi badawczych.

Zauważyć zatem należy, że stały proces myślowy jakim jest *wnioskowanie,* Autor zaliczył do *teoretycznych metod badawczych* (strona *22.* dysertacji), a pozyskanie informacji drogą *empirycznej metody badawczej* w postaci *wywiadu eksperckiego* – sprowadził nie do *osobistej rozmowy* – lecz procesu powiązanego z przekazaniem i zwrotnym odbiorem wypełnionych *arkuszy*, czyli po prostu do *rozszerzonych badań o charakterze ankietowym* (opis realizacji: strony od *23.* do *26.* dysertacji).

Być może dyskusyjnie, ale nie do końca zgodziłbym się również ze stanowieniem Badacza (strona *27.* dysertacji), że *przedmiot i zakres rozprawy ograniczony jest czasowo w okresie od roku 2018 do czasu aktualnego (rok 2022)*, gdyż u podstaw swoich rozważań teoretycznych lokalizuje przykładowo z roku 2015: *Doktrynę cyberbezpieczeństwa RP* (s. *7.* dysertacji), podobnie jak z tego samego okresu dane statystyczne (strona *103.* dysertacji).

Zaprezentowane powyżej przygany są w moim przekonaniu znacznie zniwelowane za sprawą ostatniej części *Rozdziału 1.*, czyli wyróżnionej już powyżej, *krytycznej analizy literatury* (strony od *28.* do *41.* dysertacji).

Staranność tego opracowania i zbiór zawartych tam danych wystawiają Autorowi nie tylko wysoką ocenę na rzecz posiadanego warsztatu metodologicznego, ale stanowią możliwą kanwę dla innych odbiorców – skłaniających się ku pogłębionym badaniom na rzecz cyberprzestrzeni. Umiejętności analizowania oraz wyciągania wniosków zostały tam zaprezentowane wraz z wykorzystaniem pogłębionej argumentacji, a także odpowiednim osadzeniem tego materiału zarówno w formule analitycznej jak i porównawczej.

Skonkretyzowana w ten sposób dbałość Autora, by teoretyczne elementy recenzowanej rozprawy miały solidne fundamenty piśmiennicze, znajduje swoje odzwierciedlenie w *Bibliografii* (strony od *443.* do *461.* dysertacji).

Wyszczególniono tam 155 publikacji zwartych i artykułów, które w przeważającej liczbie powstały w ostatnim dziesięcioleciu XXI wieku, z pojedynczymi i trafnie dobranymi odniesieniami do opracowań wcześniejszych. Tylko w incydentalnych przypadkach trudno znaleźć uzasadnienie do przywołania pewnych dzieł – na przykład z roku 1978: autorstwa J.L. Kulikowskiego, *Informacja i świat, w którym żyjemy* (strona *447.* dysertacji), bądź z 1984: M. Dobroczyńskiego i J. Stefanowicza, *Polityka zagraniczna* (strona *445.* dysertacji).

Za niezwykle pogłębione należy przy tym uznać starania Autora w przedmiocie doboru i w konsekwencji zestawienia: analizowanych dokumentów o charakterze strategicznym (13); regulacji prawnych (19); raportów (16); norm i wytycznych (70) i źródeł *internetowych* (15) wyszczególnionych na stronach od *445.* do *461.* dysertacji).

W ocenie tego aspektu pracy wyeksponować również trzeba, że zgromadzone w ten sposób materiały wskazują, że jest to nie tylko zestawienie prawidłowe, dające możliwość rzetelnego opisania badanych zagadnień i zgodne z przyjętą przez Doktoranta tematyką, ale też możliwe do praktycznego wykorzystania przez teoretyków i praktyków zarządzających problematyką cyberbezpieczeństwa.

Podsumowując zatem zaprezentowane powyżej rozważania stwierdzam, że niezależnie od sformułowanych powyżej pewnych uwag natury krytycznej – recenzowaną rozprawę należy ocenić jako poprawną, a tym samym zgodną z ogólnie przyjętymi wymogami logicznymi i proceduralnymi. Wyłoniona autorsko konstrukcja metodologiczna rozprawy, sposób opracowania materiału empirycznego, a także forma przeprowadzonej analizy i przyjęta metodyka badań – pozwoliły Doktorantowi na przeprowadzenie uzasadnionych rozważań natury teoretycznej, a następnie wyprowadzenie praktycznych wniosków natury ogólnej. Poczyniono to wraz z równoczesną prezentacją wypracowanych rozwiązań – popartych wynikami badań własnych i wskazówkami natury eksperckiej.

4. Ocena merytoryczna dysertacji

Posiłkując się powinnościami warunkującymi merytoryczną ocenę dysertacji Pana mgr. Grzegorza MĄKOSY, uznać na wstępie trzeba, że tytuł rozprawy został skonstruowany w sposób wzbudzający zainteresowanie, a jednocześnie jasno i przekonująco określony.

Głównym częściom rozważań nadano przejrzystą strukturę składającą się ze wstępu, sześciu rozdziałów, zakończenia i zestawień natury dodatkowej (bibliografii i wykazów, na które składają się tabele, rysunki i załączniki). Zachowuje ona określone proporcje, a ponadto tworzy spójną i przemyślanie zredagowaną całość.

Każdy z rozdziałów wyróżnia przy tym rozbudowana *preambuła* zapowiadająca zakres i charakter sprawozdawczych czynności Autora, uzasadnianych pochyleniem się nad kolejno artykułowanymi zagadnieniami badawczymi. Zawarte z kolei w każdej części końcowej specjalnie wyróżnione – *Podsumowanie i wnioski* – w syntetyczny sposób zamykają dany człon zaprezentowanych wcześniej treści i prezentują autorsko wypracowane rezultaty.

Nie wnikając następnie w zawartość treściową owych głównych członów recenzowanego dzieła – późniejszym zakłóceniem dla tak logicznej struktury – jest w moim przekonaniu mało komunikatywnie przyjęcie nazewnictwa dla dalszych podrozdziałów. Kanon schematycznej sekwencyjności sugeruje, żeby ich tytuły były nie tylko krótkie, ale redakcyjnie pozwalające na szybką orientację, co do zawartości. O ile zatem przyjęte rozwiązania do podziału zastosowanego dla rozdziałów *1.* i *2.* nie budzą wątpliwości to w kolejnych – bez zapoznania się z ich zawartością – trudno wyprowadzić *o co chodzi* i zrozumieć nadanie, dla wszystkich tam istniejących podrozdziałów, z oznaczeniem *3.* tytułu: *Wyniki przeprowadzonych badań*; dla zawartości *4.*: *Podsumowanie wyników badania*, a dla *6.*: *Podsumowanie i wnioski*. Równie niezręcznie plasuje się prezentacja części końcowej *Spisu treści* z kolejno następującą po sobie zawartością o tytułach: *Podsumowanie i wnioski*; *Podsumowanie*; *Zakończenie* (strona *6.* dysertacji).

Uwaga ta jest o tyle zasadna, że zawartość *Podsumowania* (strony od *399.* do *428.* dysertacji), gdzie Autor ponownie przywołuje założenia metodologiczne rozprawy i prezentuje w skondensowanej formie przeprowadzone działania procesu badawczego w ramach rozdziałów od drugiego do szóstego wraz z prezentacją opracowanych rozwiązań koncepcyjnych jest – wobec wcześniejszych *podsumowań* – zbędnie powielana.

Przy tak zaprezentowanym układzie pracy – *Wstęp* (strony od *7.* do *12.* dysertacji) – zawiera krótkie wprowadzenie w problematykę dotyczącą *cyberprzestrzeni* i *cyberbezpieczeństwa.*

Po ogólnym zdefiniowaniu przedmiotu badań Autor uniknął następnie treściowego określenia *głównego problemu badawczego*, przywołując w to miejsce *hipotezę główną* i *cel główny*. Całość rozważań zamknięto charakterystyką poszczególnych rozdziałów pracy, którą powiązano z uwzględnieniem *problemów szczegółowych* i *hipotez pomocniczych.*

Rozdział 1. (strony od *13.* do *41.* dysertacji) został klasycznie poświęcony zakresowi metodologicznemu badań – o czym w niniejszej recenzji napisano już powyżej.

Rozdział 2. (strony od *43.* do *169.* dysertacji), któremu nadano tytuł: *Cyberbezpieczeństwo w bezpieczeństwie narodowym RP* , ma charakter introdukcyjny.

Autor trafnie w nim wyłożył, że państwo *jego struktury i organy administracyjne i instytucjonalne, podmioty sfery gospodarczej, społecznej i politycznej funkcjonują w pewnym kontekście, w pewnych warunkach i środowisku prawnym, strategicznym, funkcjonalnym, społecznym, technologicznym i normatywno-standaryzacyjnym, tak wewnętrznym, jak międzynarodowym – regionalnym i globalnym, kształtującym i definiującym jego system bezpieczeństwa.* Odnotowując powyższe stwierdził jednocześnie, że konieczny wówczas system bezpieczeństwa *powinien być kompletny, spójny, funkcjonalny oraz wydolny, sprawny, skuteczny i efektywny, a jego komponenty powinny być wewnętrznie wzajemnie powiązane, skoordynowane i zsynchronizowane w celu działania na rzecz zapewnienia trwałego i niezakłóconego rozwoju kraju i społeczeństwa oraz odpowiedniego poziomu bezpieczeństwa.* (strona *42.* dysertacji).

Bazując na tak wyartykułowanych założeniach, następnie w stopniu niezbędnym do prowadzonych badań – w podrozdziale *2.1.* (strony od *44.* do *56.* dysertacji) – dokonano analizy odnoszenia się do problematyki bezpieczeństwa narodowego. Istotnym walorem tej części rozważań jest autorskie uporządkowanie budzącej szereg wątpliwości, a jednak powszechnie stosowanej zróżnicowanej terminologii jak również zajęcie stanowiska w sprawie zależności pomiędzy pojęciami *bezpieczeństwo państwa* i *bezpieczeństwo narodowe.*

Trudno przy tym nie zgodzić się z przywołanymi wnioskami, że *niektóre definicje bezpieczeństwa narodowego w istocie rzeczy definiują bezpieczeństwo państwa. Należy przyjąć, że dzieje się tak z powodu powszechnego przyjęcia kategorii pojęciowej bezpieczeństwa narodowego, jako kategorii najwyższej i najszerszej, zawierającej w sobie inne kategorie bezpieczeństwa* (strona *56.* dysertacji).

W kolejnych częściach wyspecyfikowanego rozdziału, Autor w sposób solidnie syntetyzujący podnoszoną materię – zaprezentował problematykę cyberbezpieczeństwa w różnych ujęciach: zarówno definicyjnych jak i praktyczno-funkcjonalnych.

Istotne i ważne dla oceny realizowanego w ten sposób procesu badawczego Doktoranta jest przy tym to, że odwołując się dokonanych ustaleń od strony teoretycznej, nie wahał się wprowadzać definicji przez siebie komponowanych, czego przykładem może być fraza ze strony *61.* dysertacji: *Autor definiuje cyberbezpieczeństwo jako bezpieczeństwo systemu teleinformatycznego, realizowanych przez niego procesów przetwarzania i przetwarzanych danych oraz systemów od nich zależnych.*

Opisane powyżej wartości dodatkowo mnożono poprzez wprowadzanie charakterystyk dotyczących *cyberzagrożeń*, *cyberataków*, *cyberwalki* i *cyberwojny* (strony od *67.* do *79.* dysertacji), by przejść następnie z odniesień o charakterze ogólnym do statystyk zgłoszeń i incydentów odnotowanych w skali kraju, a dalej do poziomowania tego w dokumentach strategicznych, regulacjach i normach prawnych (strony *79.* do *166.* dysertacji).

Rozdział 3. (strony od *169.* do *207.* dysertacji) zatytułowano: *Organizacja zarządzania cyberbezpieczeństwem na poziomie krajowym.* Jest to pierwsza z dalszych części dysertacji, w której Autor bazując na zwięzłej ekspozycji i eksplanacji istniejącego stanu rzeczy, wyprowadził esencjonalne wnioski, uzasadniające następnie proponowane przez siebie zmiany i mające walory końcowej syntezy o charakterze koncepcyjnym.

Treści poszczególnych podrozdziałów podporządkowano zatem stanowieniu Doktoranta, że ujednolicenie i zharmonizowanie tytułowo wyróżnionego zarządzania *zapewni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa* (strona *170.* dysertacji).

Część wprowadzająca, zagadnieniowo ma postać kompleksowego przeglądu dotąd funkcjonujących rozwiązań organizacyjnych, które zlokalizowano w *systemie zarządzania kryzysowego* i *krajowym systemie cyberbezpieczeństwa*, gdzie stworzono dla nich pewną strukturę procesów, planów oraz dokumentów wykonawczych (strony od *170.* do *178.* dysertacji).

Rekapitulując ten fragment swoich badań Autor przyjął, że *system zarządzania kryzysowego* posiada kompleksowe rozwiązania planistyczne i zarządcze w zakresie dbałości o bezpieczeństwo w cyberprzestrzeni, a zbudowana na te potrzeby architektura odpowiedzialności nie budzi zastrzeżeń. Inaczej rzecz ma się z ustanowionym *krajowym systemem cyberbezpieczeństwa*, który paradoksalnie – mimo, że jego zadaniem jest zapewnienie spokojnego bytu dla usług realizowanych przy zastosowaniu systemów teleinformatycznych – nie posiada w swojej strukturze *rozwiązania organizacyjnego* wyrażonego w procesach i dokumentach zarządzania. Koncentruje się natomiast na zapewnieniu operacyjnego, funkcjonalnego bezpieczeństwa systemów teleinformatycznych, podmiotów tego systemu oraz na ustanowieniu rozwiązań *zarządzania incydentami cyberbezpieczeństwa.*

Potwierdzeniem dla rozpoznanej w ten sposób sytuacji stały się wyniki badań empirycznych z wykorzystaniem stanowisk respondentów – wspierających wcześniejsze wnioskowanie i pozwalające na dalsze wykorzystanie w końcowej części charakteryzowanego rozdziału – na rzecz autorskiej *koncepcji rozwiązań udoskonalenia zorganizowania zarządzania cyberbezpieczeństwem.* Jest to moim zdaniem materiał niezwykle wartościowy, a przy tym na tyle dobrze syntetyzowany, że pozwala na jego dalsze – teoretyczne i praktyczne wykorzystanie, nie tylko przez *badaczy* tytułowo wyróżnionego obszaru, ale przede wszystkim przez *praktyków zarządzających.*

Niestety zapowiadana przez Doktoranta w *Podrozdziale 3.5.* pisemna esencja powyższych rozważań nie została przedstawiona już tak czytelnie. Na stronach od *199.* do *200.* dysertacji odnosi się wrażenie, że została ona sporządzona niejako w dwóch wersjach i bez rozsądzenia, która ma postać ostateczną. W moim przekonaniu efekt taki nastąpił za sprawą mało przekonywującego rozróżnienia w proponowanej koncepcji, istniejących tam relacji *zarządczych* i *systemowo-funkcjonalnych.*

Przy takim komentarzu – pierwszy obraz stanowiący o proponowanych zmianach – ma postać następującą (z moimi podkreśleniami): *Koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, adresująca wyniki i wnioski z badania, oparta na hipotezie badawczej przedstawia się następująco: Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego (ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania*

kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej, i powinna funkcjonować równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo być z nim połączona – co może zostać zrealizowane poprzez ustanowienie dedykowanej, tożsamej struktury procesów i dokumentów zarządczych dla systemu cyberbezpieczeństwa RP, jak w systemie zarządzania kryzysowego, punktowo/problemowo wzajemnie powiązanych i odwołujących się do siebie.

Drugiej natomiast nadano brzmienie: *Koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym brzmi następująco: Organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowym powinna obejmować funkcjonującą równoległe, dedykowaną, tożsamą strukturę procesów i dokumentów zarządczych systemu cyberbezpieczeństwa RP (SCRP), jak w systemie zarządzania kryzysowego, punktowo/problemowo wzajemnie powiązanych i odwołujących się do siebie. System cyberbezpieczeństwa RP (SCRP) powinien obejmować dedykowane i skoncentrowane na kwestiach cyberbezpieczeństwa procesy oraz dokumenty zarządcze poziomu krajowego, jako odpowiedniki dokumentów systemu zarządzania kryzysowego, np.: Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC), ministerialne, sektorowe i regionalne Plany Zarządzania Cyberbezpieczeństwem (PZC), Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT) oraz dedykowany Raport o zagrożeniach cyberbezpieczeństwa.*

Rozdział 4. (strony od *208.* do *307.* dysertacji) zatytułowano: *Struktury i relacje operacyjne zarządzania w systemie cyberbezpieczeństwa.* Jest to kolejna część dysertacji, podporządkowana przez Autora schematowi opisywanemu już powyżej, ale w tym przypadku opierającemu się na hipotetycznym stanowieniu o konieczności ujednolicenia i zharmonizowania czynności *operacyjnych zarządzania.*

Doktorant w toku realizowanych czynności badawczych trafnie dowiódł, że w *krajowym systemie cyberbezpieczeństwa* skupiono się przede wszystkim na poziomie operacyjnym odpowiedzialnym za *zarządzanie incydentami cyberbezpieczeństwa* i tam tylko ustanowiono konieczną strukturę podmiotów – kompetentnych organów i instytucji. Weryfikując powyższe wyprowadził, że rozwiązania te są niespójne, nie powiązane i nie angażują struktur organizacyjnych w sposób zintegrowany z regulacjami istniejącymi z kolei w *zarządzaniu kryzysowym.* Tym samym nie mogą zapewnić odpowiedniego poziomu dla cyberbezpieczeństwa kraju.

Wyeksponowane w ten sposób wyniki badań zostały wartościowo umocowane za sprawą autorskich eksplikacji aktów prawnych i opracowanych na tych podstawach modelach istniejących relacji organizacyjnych. Przykładem takich dokonań Doktoranta może być opracowany materiał ze strony *212.* dysertacji i sygnowany jako *Rys. 17.*

Równie interesująco została zintegrowana z całością prowadzonych w ten sposób wywodów analiza porównawcza stosowanych praktycznie rozwiązań, ale niestety – zawierająca wielokrotnie dublowany i w oczywisty sposób zbędny zwrot – *na poziomie krajowym* (przykładowo: *s. 235.* dysertacji). Czynię to z uwagą, że przecież *ten obszar nie mógł być inny* – wobec wcześniejszego stanowienia Autora o przyjętych założeniach i ograniczeniach badawczych dysertacji (patrz: s. 27. dysertacji).

Dokonana następnie rzeczowa interpretacja wyników pozyskanych od respondentów przyczyniła się do wypracowania trzech koncepcyjnych kompozycji dla struktur i relacji: *operacyjnych systemu cyberbezpieczeństwa* (strony od *275.* do *285.* dysertacji); *zarządzania cyberbezpieczeństwem* (strony od *285.* do *292.* dysertacji); *zarządzania incydentami cyberbezpieczeństwa* (strony od *292.* do *304.* dysertacji).

Zestawienie to oceniam bardzo wysoko, gdyż w mojej opinii zawarte tam propozycje rozwiązań są na tyle racjonalnie przygotowane, że mogą pomóc w praktycznym optymalizowaniu wyróżnionego przez Badacza stanu rzeczy.

Rozdział 5. (strony od *308.* do *350.* dysertacji) poświęcono tytułowo określonym *sektorom i podmiotom systemu cyberbezpieczeństwa RP.* Przyjęty dla niego schemat konstrukcyjny nie odbiega od wcześniej charakteryzowanych założeń i postępowania badawczego Autora.

Wyróżnia go moje wcześniej już podniesione zastrzeżenie dotyczące założenia o treści: *Opracowanie koncepcji wykazu sektorów i typów...*

Niezręczność zastosowania tego sformułowania została jednak skutecznie zneutralizowana wobec dobrania w naukowo uzasadniony sposób treści, pozwalających na udoskonalenie dotychczas istniejącego zbioru sektorów i typów podmiotów systemu cyberbezpieczeństwa RP, wraz z wnioskiem końcowym stanowiącym, że powinien on obejmować *wszystkie sektory, systemy i typy podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujące zadania publiczne oraz najszerszy możliwy katalog wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego...* (strona *345.* dysertacji).

Rozdział 6. (strony od *351.* do *398.* dysertacji) posiada tytuł: *Bezpieczeństwo systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP*. Powaga zawartych w tej części ustaleń badawczych Autora została powiązana wraz z uzasadnionym stwierdzeniem, że wyróżnione *podmioty systemu cyberbezpieczeństwa realizują zadania w zakresie zapewnienia bezpieczeństwa usług publicznych i społecznych oraz infrastruktury tych usług poprzez zapewnienie bezpieczeństwa infrastruktury systemów teleinformatycznych oraz reagowanie i zarządzanie incydentami cyberbezpieczeństwa i sytuacjami kryzysowymi wynikającymi z materializacji cyberzagrożeń* (strona *351.* dysertacji).

W poszczególnych podrozdziałach pochylono się zatem nad ustaleniem jakie dotychczas normy i standardy w badanym obszarze cyberbezpieczeństwa są wymagane, i czy porównanie stosowanych w tym względzie rozwiązań pozwoli na wyprowadzenie wniosków o charakterze dodatkowo uzupełniającym?

Założona w ten sposób osnowa ponownie pozwoliła Autorowi na udowodnienie, że posiada teoretyczne i merytoryczne przygotowanie w stopniu pozwalającym na wyprowadzenie konstatacji nie tylko uogólniających badaną materię, ale również wskazujących na umiejętności przygotowania w tym względzie skonkretyzowanej koncepcji *podmiotów bezpieczeństwa systemów teleinformatycznych*. W zasadniczej treści podniesiono zatem, że rozwiązania *zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa...* (strona *394.* dysertacji).

Wprowadzenie na koniec rozprawy pisemnego sprawozdania z badań w postaci dodatkowo wyróżnionego *Podsumowania* (strony od *399.* do *428.* dysertacji) – mimo, że podkreślającego umiejętności warsztatowe Doktoranta – oceniam (jak to już podniosłem powyżej) jako zbędne.

Wysoką z kolei ocenę pod względem merytorycznym – nadaję treściom zawartym w *Zakończeniu* (strony od *429.* do *442.* dysertacji). Zawierają trafnie wyłożoną materię o charakterze ogólnym, ewolucyjnym i wnioskowym. W sposób syntetyczny i adekwatny do zaprezentowanego wcześniej materiału przekazują, że poszukiwania odpowiedzi na odpowiednio wyrażone w rozprawie pytania dla głównego problemu badawczego i problemów szczegółowych – zostały zwieńczone sukcesem, a postawione hipotezy – pozytywnie zweryfikowane. W sposób poruszający wszystkie podniesione w dysertacji kwestie, jednocześnie przypominają o współczesnych determinantach towarzyszących przyśpieszonemu rozwoju cyberprzestrzeni w objawionej erze społeczeństw informacyjnych, ze szczególnymi wyzwaniami dla rozwoju dyscypliny *nauki o bezpieczeństwie* włącznie.

W podsumowaniu tej części recenzji stwierdzam, że przedmiotowa praca, pomimo wyróżnienia pewnych uchybień jest pod względem merytorycznym poprawna, a jednocześnie wnosi określone wartości teoretyczno-poznawcze i postulaty o charakterze merytoryczno-praktycznym na rzecz wyspecyfikowanych badawczo zmian, które mogłyby udoskonalić tytułowo wyróżnioną problematykę organizacji systemu cyberbezpieczeństwa RP.

5. Ocena strony formalnej i edytorskiej

Recenzowana praca obejmuje łącznie 565 stron tekstu, z czego 442. stanowią materiał o charakterze merytorycznym. Zawartą treść dodatkowo wzbogaca: 51. tabel, 38. rysunków i załączniki (arkusz kwestionariusza eksperckiego z zestawieniami odpowiedzi respondentów).

Posiadające taki wymiar dzieło – ma jednocześnie postać poprawną – z formalnego i edytorskiego punktu widzenia. Zostało zatem napisane w sposób świadczący o umiejętności konstrukcji tekstu naukowego, z jednoczesnym upublicznieniem koniecznych treści, w sposób czytelny i komunikatywny dla każdego odbiorcy.

Spoglądając na przedmiotową materię w ujęciu nieco krytycznym stwierdzić trzeba, że można się tam doszukać pewnych sytuacyjnych bądź incydentalnie występujących uchybień.

Doktorant stosował zatem *odwołania* w sposób miejscami nazbyt ogólnikowy, bądź zgoła niezrozumiały – czego dowodem może być chociażby jedno z pierwszych przywołań (nr *2*) o treści: *Sformułowania: system zarządzania kryzysowego, krajowy system cyberbezpieczeństwa i system informatyzacji publicznych zostały użyty przez autora w: Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych (2020), Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne (2020), Organizacja systemu cyberbezpieczeństwa RP (2020).*

Stosunkowo często pojawiały się w tekście powtórzenia tych samych pojęć, słów, określeń – czego dowodzi przykład ze strony *9.* dysertacji: *Rozdział drugi stanowi przeprowadzone w podrozdziałach rozważania nad istotą i pojęciami bezpieczeństwa narodowego oraz współczesnym pojęciem cyberbezpieczeństwa, jego istotą i rolą* bądź inny ze strony *44.* dysertacji: *Bezpieczeństwo, jak też bezpieczeństwo narodowe mają wiele definicji i ujęć, z których warto przytoczyć kilka, jako szeroki kontekst do ujęcia pojęcia cyberbezpieczeństwa, ulokowanego w ramach bezpieczeństwa i bezpieczeństwa narodowego. Bezpieczeństwo, czy też bezpieczeństwo narodowe lub bezpieczeństwo państwa nie są pojęciami tożsamymi i mają swoje odrębne definicje.*

Można było również dostrzec zapisy z ograniczeniami w zakresie czytelności bądź z tak zwanymi *literówkami*, czego przykładem ze strony *10.* dysertacji może być tekst: *Jakie są aktualne kontekst, warunki i środowisko prawne (...).*

Miejscowo wystąpiły także sformułowania niepoprawne gramatycznie. Na przykład, na stronie *11.* dysertacji: *Podsumowanie streszcza założenia metodologiczne rozprawy (...).*

W pojedynczych przypadkach nie potrafiono również utrzymać zasadniczej dla każdego twórcy reguły, by *przestrzegać jednej i tej samej zasady postępowania.* Zastrzeżenie to dotyczy przykładowo stosowania lub niestosowania *kursywy* (przykładowo na stronie *18.* dysertacji: przy przywołaniu odnoszącym się do nr *16* i tytułu dzieła S. Nowaka). Dyskusyjne jest także nadanie – począwszy od strony *56.* dysertacji – niektórym *tabelom* i *wykresom* nazwy: *rysunek.*

W podsumowaniu tej części recenzji chciałbym jednakże podkreślić, że w moim przekonaniu wystąpienie wyłonionych niedociągnięć nie ma specjalnego wpływu na wartość merytoryczną i metodologiczną recenzowanej rozprawy doktorskiej.

6. Wniosek końcowy

Reasumując stwierdzam, że recenzowana rozprawa doktorska autorstwa Pana mgr. Grzegorza MĄKOSY pod tytułem *Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej* stanowi oryginalne opracowanie o istotnych walorach dla dyscypliny: *nauki o bezpieczeństwie.*

Będąc pisarskim sprawozdaniem z przeprowadzonych badań jednocześnie potwierdza metodologiczne, merytoryczne i redakcyjne przygotowanie Doktoranta do warsztatowego określenia przedmiotu, celu badań, podjęcia i rozwiązania przyjętego problemu naukowego wraz ze stanowieniem o wyartykułowanych wcześniej hipotezach badawczych.

Wykonując w ten sposób odpowiednio zaplanowane czynności badawcze Pan mgr Grzegorz MĄKOSA dowiódł tym samym, że posiada niezbędną wiedzę, szereg cennych umiejętności i kompetencji, a w tym związanych między innymi z: projektowaniem postępowania naukowego, samodzielnym przeprowadzeniem badań, jak również końcowym upublicznieniem wyników swojej pracy w postaci dysertacji.

Przeprowadzona ocena badanej rozprawy, a w tym pod względem metodologicznym i merytorycznym pozwala – jako recenzentowi – na sformułowanie wniosku końcowego: dysertacja spełnia warunki określone w ustawie z dnia 14 marca 2003 roku *o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki* (Dz. U. Nr 56, poz. 595 z późniejszymi zmianami).

W związku z powyższym wnoszę o dopuszczenie Pana mgr. Grzegorza MĄKOSY do publicznej obrony recenzowanego dzieła.

/dr hab. Ireneusz.T. Dziubek/