dr hab. Grzegorz Krasnodębski
Akademia Marynarki Wojennej
Wydział Dowodzenia i Operacji Morskich

Gdynia, 06.01.2025 r.

RECENZJA
rozprawy doktorskiej Pana mgr. **Dawida DUDY**
nt. **Kompetencje cyfrowe użytkowników cyberprzestrzeni newralgicznym komponentem systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej**

1. UWAGI OGÓLNE

Przedstawiona do recenzji rozprawa doktorska Pana mgr. Dawida DUDY nt. *Kompetencje cyfrowe użytkowników cyberprzestrzeni newralgicznym komponentem systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej* została opracowana pod naukowym kierownictwem Pani dr hab. Moniki SZYŁKOWSKIEJ, prof. WAT, na Wydziale Bezpieczeństwa, Logistyki i Zarządzania Wojskowej Akademii Technicznej w Warszawie. Promotorem pomocniczym była Pani dr Sylwia SZYBOWSKA.

Zgodnie z wymaganiami stawianymi rozprawom doktorskim Doktorant przedstawił dzieło, które prezentuje wiedzę teoretyczną w dyscyplinie nauki o bezpieczeństwie w zakresie cyberbezpieczeństwa oraz stanowi oryginalne rozwiązanie problemu naukowego odnoszącego się do społecznej części systemu cyberbezpieczeństwa państwa.

Problematyka badań i analiz, jaką Doktorant podjął w swoim dziele, jest z pewnością istotna z perspektywy funkcjonowania systemu bezpieczeństwa narodowego ze szczególnym uwzględnieniem cyberbezpieczeństwa oraz obejmuje bardzo aktualne wyzwania jakie stoją przed naszym społeczeństwem w zakresie budowania odporności na zagrożenia z cyberprzestrzeni. Należy zgodzić się z Doktorantem, że skuteczne zwiększanie poziomu świadomości i kompetencji cyfrowych może mieć kluczowe znaczenie dla kształtowania systemu cyberbezpieczeństwa państwa.

Biorąc pod uwagę powyższe fakty należy stwierdzić, że badania podjęte przez Pana mgr Dawida Dudę są z całą pewnością zasadne i lokują się w naukach o bezpieczeństwie. Rekomendacje przedstawione we wnioskach niewątpliwe mogą

przyczynić się do podniesienia efektywności funkcjonowania systemu cyberbezpieczeństwa w Polsce, w szczególności poprzez realizację działań profilaktycznych mających na celu zwiększenie wiedzy społeczeństwa z zakresu reagowania na cyberzagrożenia.

W mojej opinii Doktorant osiągnął przyjęty główny cel pracy, którym było zbadanie istniejących rozwiązań w zakresie działań państwa polskiego realizowanych w ramach systemu cyberbezpieczeństwa RP na rzecz budowania i podnoszenia kompetencji cyfrowych użytkowników określonych w dokumentach strategicznych i regulacjach prawnych w zakresie cyberbezpieczeństwa RP.

Podsumowując uwagi ogólne dotyczące dysertacji stwierdzam, że przedłożone do recenzji dzieło jest dojrzałe, posiada wysokie walory merytoryczne oraz praktyczne i stanowi materiał nadający się do naukowego uwzględnienia jako podstawa do dalszego postępowania w przewodzie doktorskim.

2. OCENA KONCEPCJI METODOLOGICZNEJ PRACY

Koncepcja metodologiczna rozprawy została umieszczona w rozdziale pierwszym pt. *Metodologiczne podstawy dysertacji* (ss. 9-23), w którym przedstawiono podstawowe elementy naukowej metodologii badawczej, obejmującej: przyczyny podjęcia badań, przedmiot badań, cel badań, problemy naukowe, hipotezę roboczą, metody badawcze, ograniczenia badawcze oraz analizę stanu wiedzy.

Przyjętą koncepcję metodologiczną należy uznać za formalnie poprawną i w pełni wystarczającą do potrzeb rozprawy. Opis procesu badawczego, pokazuje, że Doktorant potrafił zaplanować i przeprowadzić badania oraz, że doskonale porusza się w problematyce będącej przedmiotem badań, który został określony w zakresie przedmiotowym i podmiotowym.

Główny cel badań został przedstawiony we *Wprowadzeniu* (*s. 7*) natomiast dodatkowe cele w liczbie ośmiu znajdują się w podrozdziale 1.3 (*ss. 10-11*) i obejmują:

- *analizę istniejących rozwiązań w zakresie działań państwa polskiego realizowanych na rzecz budowania oraz podnoszenia kompetencji cyfrowych użytkowników określonych w dokumentach strategicznych i regulacjach prawnych w zakresie cyberbezpieczeństwa RP, m.in.*

w ustawie o krajowym systemie cyberbezpieczeństwa, Doktrynie Cyberbezpieczeństwa RP oraz Strategii Cyberbezpieczeństwa RP;

- *określenie miejsca Krajowego Systemu Cyberbezpieczeństwa w całym systemie cyberbezpieczeństwa RP, w ramach którego wyodrębnia się trzy podsystemy: kierowania, ogniwa operacyjne, publiczne i prywatne ogniwa wsparcia;*
- *ocenę działania Krajowego Systemu Cyberbezpieczeństwa i określenie kierunków jego rozwoju;*
- *wskazanie podmiotów i instytucji kluczowych w obszarze budowania świadomości i kompetencji cyfrowych użytkowników;*
- *oszacowanie poziomu wiedzy i umiejętności użytkowników sieci;*
- *określenie cyberzagrożeń szczególnie istotnych z punktu widzenia funkcjonowania państwa;*
- *wzbogacenie wiedzy w zakresie poziomu świadomości cyberzagrożeń i kompetencji cyfrowych wskazanej grupy badawczej w przypadku badania sondażowego przeprowadzonego za pomocą anonimowej ankiety;*
- *w obszarze wywiadów eksperckich: ocenę kierunków kluczowych zagrożeń w dziedzinie cyberbezpieczeństwa, uzyskanie opinii na temat realizowania zadań w obszarze budowania świadomości i cyfrowych kompetencji, ocenę sposobów edukacji i metod użytkowników sieci.*

Główny problem badawczy został sformułowany w postaci pytania: *Jakie czynniki i działania mają wpływ na budowanie świadomości oraz kompetencji cyfrowych w zakresie cyberbezpieczeństwa? (s. 13)* Rozwiązaniu, tak sformułowanego problemu, towarzyszy 9 szczegółowych problemów badawczych, wspomagające Autora w procesie naukowego poznania, określonych w formie następujących pytań (s. 13):

1. *Które przepisy prawne regulują kwestie cyberbezpieczeństwa w RP?*
2. *Które ze wskazanych w przepisach podmiotów i instytucji mają określone zadania w obszarze budowania świadomości i kompetencji cyfrowych użytkowników?*
3. *Jaki jest istniejący zakres wiedzy użytkowników oraz sposób jej pozyskiwania w zakresie cyberbezpieczeństwa?*
4. *Jakie standardy obowiązują w zakresie kompetencji cyfrowych?*

5. *Jaki jest poziom kompetencji obywateli w zakresie cyberbezpieczeństwa?*
6. *Jaki jest poziom świadomości w obszarze cyfrowych zagrożeń wśród użytkowników sieci?*
7. *Jakie istnieją metody i obszary edukacji użytkowników?*
8. *Które z zagrożeń w dziedzinie cyberbezpieczeństwa mogą oznaczać największe wyzwanie dla funkcjonowania państwa?*
9. *Czy kompetencje cyfrowe mogą mieć wpływ na poziom cyberbezpieczeństwa?*

Na wstępie prowadzonych badań Doktorant przyjął hipotezę roboczą w formie przypuszczenia. Uważa On, że: *skuteczne zwiększanie poziomu świadomości i kompetencji cyfrowych może mieć kluczowe znaczenie dla kształtowania systemu cyberbezpieczeństwa państwa. (s. 14).*

Weryfikacji, tak postawionej hipotezy roboczej, towarzyszą hipotezy szczegółowe (ss. 14-15) mówiące, że:

- *użytkownicy bez odpowiednich kompetencji w zakresie cyberbezpieczeństwa mogą stanowić jedno ze słabszych ognisk systemu cyberbezpieczeństwa;*
- *edukacja może przekładać się bezpośrednio na poziom świadomości użytkowników w cyberprzestrzeni i ich kompetencje cyfrowe;*
- *poziom świadomości obywateli korzystających z sieci - w zakresie cyberbezpieczeństwa jest niewystarczający;*
- *stałe rozwijanie kompetencji cyfrowych może pozwolić na minimalizację ryzyka wystąpienia określonych zagrożeń w cyberprzestrzeni.*

W trakcie prowadzonych badań Doktorant wykorzystał metodę statystyczną i sondażu diagnostycznego, analizę i krytykę piśmiennictwa oraz metodę analizy i konstrukcji logicznej. Techniki badawcze objęły wywiad, ankietowanie i badanie dokumentów. Jako narzędzia badawcze zostały wykorzystane kwestionariusze ankiety i wywiadu. Dodatkowo Doktorant określił zmienne niezależne i zależne oraz ograniczenia badawcze.

Dużym walorem rozdziału metodologicznego jest analiza stanu wiedzy przeprowadzona w oparciu o przegląd literatury przedmiotu.

Podsumowując, należy stwierdzić, że przyjęta przez Doktoranta koncepcja metodologiczna rozprawy i zaproponowane metody, techniki i narzędzia badawcze są poprawne i adekwatne do potrzeb rozpatrywanej tematyki badawczej.

3. OCENA MERYTORYCZNA PRACY

Wyniki badań Doktorant przedstawił w formie dojrzałego dzieła naukowego, które pod względem merytorycznym nie budzi wątpliwości. Recenzowana rozprawa doktorska systematyzuje wiedzę z zakresu świadomości i kompetencji cyfrowych społeczeństwa w kontekście budowania odporności na cyberzagrożenia.

Opracowanie przygotowane na 330 stronach, zawiera wszystkie wymagane elementy redakcyjne prac naukowych, w tym wprowadzenie, sześć rozdziałów merytorycznych, zakończenie, załączniki, wykaz literatury, spis rysunków, tabel i wykresów oraz streszczenie w języku polskim i angielskim.

W rozdziale pierwszym pt. „*Metodologiczne podstawy dysertacji”* (ss. 9-23) przedstawione zostały podstawy metodologiczne badań, do których odniesiono się w poprzedniej części niniejszej recenzji.

Rozdział drugi pt. „*Istota cyberbezpieczeństwa”* (ss. 24-47) zawiera treści dotyczące aparatu pojęciowego z zakresu cyberprzestrzeni, cyberbezpieczeństwa, społeczeństwa informacyjnego. Rozdział ten ma charakter odtwórczy i systematyzujący wiedzę niezbędną do prowadzenia dalszych badań. Rozważania rozpoczęto od omówienia definicji, aspektów technicznych, technologicznych i społecznych cyberprzestrzeni. Następnie poddano analizie pojęcie cyberbezpieczeństwa i „globalnej wioski”. Treści rozdziału kończą wnioski, w których przedstawiono syntezę przeprowadzonych analiz i zwrócono uwagę na różnorodność definicji podstawowych pojęć występujących w badanym wycinku rzeczywistości.

W rozdziale trzecim pt. „*Dokumenty strategiczne i regulacje prawne w obszarze cyberbezpieczeństwa”* (ss. 48-93) dokonano przeglądu krajowych i międzynarodowych dokumentów strategicznych z zakresu cyberbezpieczeństwa, omówiono regulacje prawne Unii Europejskiej i krajowe, poddano analizie działalność jednostek organizacyjnych odpowiedzialnych za kształtowanie kompetencji cyfrowych i cyberbezpieczeństwa oraz scharakteryzowano system cyberbezpieczeństwa RP. Materiały źródłowe wykorzystane do przeprowadzenia badań zostały przez Doktoranta dobrane właściwie i pozwoliły Mu trafnie ocenić istniejące rozwiązania. Należy zgodzić się z Autorem, że wszelkie działania mające na calu zapewnienie bezpieczeństwa cyberprzestrzeni *powinny być ukierunkowane na bezpieczeństwo obywateli jak i całego państw, tak aby każdy użytkownik mógł*

swobodnie i bez obaw w pełni korzystać z wynalazków jakie niesie za sobą cyfryzacja i rozwój technologii teleinformatycznych.

Rozdziały czwarty pt. „*Zagrożenia i wyzwania cyberbezpieczeństwa"* (ss. 94-134) zawiera identyfikację, klasyfikację i charakterystykę zagrożeń występujących w cyberprzestrzeni. Przedstawione dane statystyczne są aktualne i pochodzą z rzetelnych źródeł. W rozdziale zwrócono uwagę na zagrożenia, które mają wpływ na bezpieczeństwo infrastruktury krytycznej państwa i stanowią wyzwania w budowaniu systemu cyberbezpieczeństwa.

Rozdziały piąty pt. „*Kompetencje cyfrowe użytkowników"* (ss. 135-159) zawiera treści merytoryczne dotyczące społecznej świadomości cyberzagrożeń i poziomu kompetencji cyfrowych użytkowników nowoczesnych technologii. W rozdziale tym przeprowadzono również analizę porównawczą kompetencji cyfrowych naszego społeczeństwa na tle wybranych państw bazując na ogólnie dostępnych materiałach źródłowych. Ważnym osiągnięciem Autora w tym miejscu jest zaproponowanie własnej definicji kompetencji cyfrowych, która mówi, że jest to *zbiór umiejętności i wiedzy pozwalających na sprawne i bezpieczne korzystanie z technik i technologii cyfrowych w tym komunikowanie się, a także dążenie do ciągłego rozwoju w tej dziedzinie*.

Rozdziały szósty pt. „*Wyniki badań własnych"* (ss. 160-286) zawiera zasadniczy element twórczy, kategoryzujący recenzowaną pracę do rangi rozprawy doktorskiej. W rozdziale tym Autor przedstawił analizę wywiadów eksperckich, wyniki badań sondażowych oraz zaprezentował autorską koncepcję zmian w zakresie włączenia zadań w obszarze budowania i podnoszenia świadomości społecznej cyberbezpieczeństwa jako elementu struktury krajowego systemu cyberbezpieczeństwa RP.

Każdy z powyższych rozdziałów merytorycznych zamykają syntetyczne autorskie uwagi i wnioski badawcze w formie podsumowania, co bardzo dobrze świadczy o precyzji i konsekwencji procesu myślowego Autora.

W zakończeniu Autor dokonał podsumowania przeprowadzonego procesu badawczego odnosząc się do głównego celu pracy, problemów badawczych oraz hipotez.

Część merytoryczną pracy zamykają 2 załączniki oraz związany z tematyką rozprawy wykaz literatury, zawierający łącznie 218 pozycji, w tym pozycje książkowe - 48, artykuły w czasopismach – 20, artykuły na konferencjach – 1, normy – 1,

ustawy – 14, akty prawa międzynarodowego – 6, rozporządzenia – 6, doktryny i strategie – 7, opracowania i raporty z badań – 6, strony i komunikaty Internetowe – 109. Pracę kończą wykazy rysunków (7 pozycji), tabel (13 pozycji) i wykresów (80 pozycji).

Podsumowując należy stwierdzić, że pod względem merytorycznym rozprawa nie budzi wątpliwości. Praca została napisana językiem poprawnym. Autor wykazał się bardzo dobrą znajomością warsztatu pisarskiego. Rozdziały i podrozdziały tworzą logiczną całość. Zauważalne niedociągnięcia edytorskie nie pomniejszają pozytywnej oceny końcowej pracy.

4. NOWATORSKIE I WARTOŚCIOWE OSIĄGNIĘCIA DOKTORANTA

Do zasadniczych osiągnięć Doktoranta predestynujących do ubiegania się o stopień doktora nauk społecznych w dyscyplinie nauki o bezpieczeństwie, należy zaliczyć:

- usystematyzowanie aparatu pojęciowego z zakresu cyberbezpieczeństwa;
- usystematyzowanie wiedzy z zakresu zagrożeń identyfikowanych w cyberprzestrzeni;
- przeprowadzenie analizy kompetencji cyfrowych naszego społeczeństwa oraz opracowanie autorskiej definicji kompetencji cyfrowych;
- opracowanie rekomendacji w obszarze budowania i podnoszenia świadomości społecznej cyberbezpieczeństwa.

5. ZAGADNIENIA DO WYJAŚNIENIA PODCZAS PUBLICZNEJ OBRONY ROZPRAWY DOKTORSKIEJ

1. Proszę o wyjaśnienie pojęcia „ognisko systemu cyberbezpieczeństwa”, które Doktorant zamieścił w jednej z hipotez roboczych?
2. Proszę o wyjaśnienie pojęcia cyberbezpieczeństwo i bezpieczeństwo cybernetyczne?
3. W jaki sposób można zwiększyć efektywność procesu przekazywania wiedzy z zakresu cyberbezpieczeństwa wśród młodego pokolenia naszego społeczeństwa?

6. WNIOSEK KOŃCOWY

Recenzowana rozprawa doktorska Pana mgr. Dawida DUDY nt. *Kompetencje cyfrowe użytkowników cyberprzestrzeni newralgicznym komponentem systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej* jest dziełem autorskim i oryginalnym, spełnia podstawowe kryteria stawiane rozprawom doktorskim. Doktorant przedstawił dzieło, które prezentuje wiedzę teoretyczną w dyscyplinie nauki o bezpieczeństwie w zakresie cyberbezpieczeństwa oraz stanowi oryginalne rozwiązanie problemu naukowego odnoszącego się do społecznej części systemu cyberbezpieczeństwa państwa.

W mojej ocenie praca wnosi istotny wkład w rozwój nauk o bezpieczeństwie i wypełnia lukę dotyczącą problematyki kompetencji cyfrowych i świadomości naszego społeczeństwa w kontekście współczesnych cyberzagrożeń. Rozważania, analizy, hipotezy, propozycje zawarte w pracy mogą być istotnym impulsem do kolejnych badań i tym samym rozwoju nauk o bezpieczeństwie.

Wobec faktu, że recenzowana praca spełnia wszystkie warunki, stawiane rozprawom doktorskim, określone w przepisach prawa powszechnie obowiązującego, wnoszę o dopuszczenie Pana mgr. Dawida DUDY do publicznej obrony rozprawy doktorskiej.