dr hab. inż. Jerzy Kosiński, prof. AMW
Wydział Dowodzenia i Operacji Morskich
Akademia Marynarki Wojennej w Gdyni

Szczytno, dn. 17 listopada 2020 roku

RECENZJA

rozprawy doktorskiej mgr. Michała Sieka pt.:

ANALIZA SYSTEMOWA I PROGNOZOWANIE STANU BEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ W CYBERPRZESTRZENI

przygotowanej pod kierunkiem naukowym prof. dr hab. inż. Piotr Sienkiewicza

Podstawą napisania recenzji jest Uchwała Rady Dyscypliny „Nauki o Bezpieczeństwie"
nr 63/RDN NoB/2020 z dnia 30 września 2020 roku
w sprawie powołania recenzentów w przewodzie doktorskim Pana mgr. Michała Sieka

1. Ocena wstępna

Bezpieczeństwo cyberprzestrzeni jest zjawiskiem społecznym z natury bardzo złożonym. Cyberprzestrzeń jako obszar niematerialny, ponadgranicznym, ale odbijającym się w świecie rzeczywistym jest tematem badań wielu dziedzin nauki. Dynamika, intensywność zmian w cyberprzestrzeni implikuje konieczność prowadzenia dogłębnych analiz, które będą stanowiły podstawę działań zapobiegawczych, ale również reakcji na pojawiające się zagrożenia. Kluczowe w tym względzie wydaje się poznanie determinantów wzrostu lub spadku bezpieczeństwa w cyberprzestrzeni. Weryfikacja tych czynników stanowi na ogół duże wyzwanie pod względem naukowym. Większość narzędzi statystycznych lub ekonometrycznych wykorzystuje do prognozowania szeregi czasowe, ale otrzymywane w ich wyniku nie są dokładne – w zjawiskach społecznych pojawiają się trudne do przewidzenia związki/opóźnienia między zmiennymi. Co gorsza istnieją zmienne, które nie są uwzględniane w analizach, a część zmiennych jest niemożliwa do zmierzenia (chociaż istotnie wpływa na zjawisko). Występowanie nieciągłych zmian środowisku cyberprzestrzeni/cyberbezpieczeństwa powoduje, że w analizie cyberprzestrzeni należy uwzględniać wielowymiarowe i wielowariantowe możliwości przyszłych jej stanów. Każdy bowiem z czynników wpływających obecnie na cyberprzestrzeń może w przyszłości zmienić się w nieprzewidywalny

sposób, i wywrzeć na nią korzystny lub niekorzystny wpływ. W warunkach niepełnej i niepewnej informacji jedną z metod wspomagających planowanie strategiczne jest prognozowanie scenariuszowe. Przyszłości nie da się przewidzieć z całą pewnością, ale można ją zaprojektować. Co więcej opracowując strategię działania w cyberprzestrzeni należy uwzględniać wielowariantowość działań, zależnych od zmian zachodzących w tym specyficznym środowisku, a do tego prognozowanie scenariuszowe nadaje się bardzo dobrze.

W powyższym kontekście, rozprawa Pana mgr. Michała Sieka powinna być postrzegana bardzo pozytywnie. Autor rozprawy za przedmiot swoich badań przyjął: cyberwojnę (zjawisko), ochrony i obrony Rzeczypospolitej Polskiej i jej obywateli w cyberprzestrzeni (zawężony do infrastruktury krytycznej) (system) oraz procesy zarządzania bezpieczeństwem i prognozowania zagrożeń (proces). Cyberwojnę rozumie jako podzbiór wojny informacyjnej, podkreślając jednak, że cyberwojna może razić także cele fizyczne i zagrażać społeczeństwu czy oddziaływać na organizmy żywe. Doktorant świadomie ogranicza cyberprzestrzeń skupiając się na Polskim systemie ochrony i obrony cyberprzestrzeni, ale analizując go uwzględnia bliższe i dalsze otoczenie RP. Autor trafnie zauważa, że horyzont prognozowania w środowisku tak zmiennym jak cyberprzestrzeń, nie może być odległy. Sens mają prognozy krótkookresowe. Za racjonalny dla prognozowania możliwych i prawdopodobnych scenariuszy zagrożeń Doktorant ustalił horyzont prognozowania do roku 2022.

Tak sformułowany przedmiot badania świadczy to dobrze o świadomości Autora problematycznych kwestii dotyczących możliwości prognozowania zagrożeń w cyberprzestrzeni w celu ich wykorzystania do propozycji modyfikacji obowiązującej strategii cyberbezpieczeństwa.

Główny problem badawczy rozprawy zawarty jest w pytaniu:

(a) *Jakie mogą być możliwe i prawdopodobne cele ataków cyfrowych w cyberprzestrzeni w RP?* (str.23) i uzupełniony pytaniami szczegółowymi:

(b) *Czy realne są ataki cyfrowe realizowane w cyberprzestrzeni przez podmioty państwowe?,*

(c) Czy istnieje ryzyko cyberwojny z RP w cyberprzestrzeni?,

(d) Jakie systemy są kluczowe dla RP w cyberprzestrzeni?,

(e) Jakie mają podatności i jak są chronione?,

(f) Jak są powiązane (skorelowane) ze sobą?,

(g) W jakim (stopniu) zakresie (wskazane, oszacowane) zagrożenia cyberwojny wpływają na poziom bezpieczeństwa RP? (str. 23).

Istotne w badaniu były również wskazane w opisie problemów dwa zagadnienia i wynikające z nich pytania:

(h) Jaka jest relacja koszt-efekt poszczególnych ataków?,

(i) Jakich użyć modeli prognozowania – adekwatnych do warunków wewnętrznych i zewnętrznych oraz jak określić horyzont czasowy? (str. 23).

Na podstawie dotychczasowej wiedzy i wstępnej obserwacji Autor dysertacji sformułował 3 następujące hipotezy badawcze odpowiadające problemom badawczym:

(1) Stały rozwój technologii informatycznych i postępująca cyfryzacja państwa powoduje wzrost zagrożeń bezpieczeństwa informacyjnego państwa, w tym wysoce ustrukturyzowanymi atakami realizowanymi w cyberprzestrzeni, jak cyberwojna.

(2) Cyberwojna stanowi realne i prawdopodobne zagrożenie bezpieczeństwa państwa, w szczególności dla jej systemów infrastruktury krytycznej (a)(b)(c)(d).

(3) Zastosowanie analizy systemowej i metod prognozowania, stwarza możliwość opracowania racjonalnej polityki bezpieczeństwa, a także zapewnienia pożądanego poziomu bezpieczeństwa informacyjnego i ewaluacji wariantów strategii obrony państwa w cyberprzestrzeni (i) [(e)(f)(g)(h)].

W celu weryfikacji przedstawionych hipotez Doktorant wykorzystał kilka metod badawczych: analizę systemową, analizę krytyczną, obserwacji, studium przypadku, badanie dokumentów, a także metodę analizy i konstrukcji logicznej. Do prognozowania przyszłości bezpieczeństwa RP w cyberprzestrzeni Autor wykorzystał popularną od lat 60-tych XX w. w naukach o zarządzaniu metodę heurystyczną – scenariuszową.

Wszystkie hipotezy robocze zostały pozytywnie zweryfikowane, co Doktorant jawnie potwierdził na s.311-312.

Celem poznawczym badania było zaprojektowanie możliwych scenariuszy realizacji zagrożeń w cyberprzestrzeni. Określenie przesłanek do budowy nowej strategii cyberbezpieczeństwa RP było celem utylitarnym (s.21,36). Udało się przewidzieć, jakie mogą być prawdopodobne i możliwe do rażenia cele ataków cyfrowych w cyberprzestrzeni RP. Końcowym elementem badań była ocena ewaluacji ryzyka zdiagnozowanych i prognozowanych zagrożeń bezpieczeństwa RP w cyberprzestrzeni w ramach przewidzianych scenariuszy. W działaniach przestępczych uczestniczą pojedyncze osoby, zorganizowane grupy przestępcze oraz grupy sponsorowane przez instytucje

rządowe i siły zbrojne państw prowadzących ofensywne działania w cyberprzestrzeni. Tym samym bardzo realne, w kontekście zrealizowanych badań, wydają się także ataki, za którymi stoją podmioty państwowe, a co za tym idzie ryzyko realizacji wysoce ustrukturyzowanych ataków w cyberprzestrzeni, jakich egzemplifikacją jest cyberwojna, również musi być brane pod uwagę, w konstruowaniu strategii bezpieczeństwa państwa i jego obywateli w cyberprzestrzeni.

Zarówno postawione problemy badawcze, jak i sformułowane hipotezy badawcze są adekwatne do przyjętego celu pracy i przedmiotu badań.

Przyjęty w pracy schemat postępowania badawczego odpowiednio kierunkował wysiłek Doktoranta na realizację celu pracy i naukową weryfikację postawionych hipotez badawczych.

W kontekście całości pracy należy zwrócić uwagę na obszerne i jednocześnie precyzyjne wykorzystanie wiedzy grupy eksperckiej (9 z potencjalnych 20) do sporządzenia prognoz, co w kontekście szacowanych braków ilościowych w tej grupie wydaje się całkowicie wystarczające.

Praca została napisana językiem poprawnym z niewielką ilością błędów (np. pisownia słowa phishing), chociaż zdarzają się również pojedyncze zapisy nieprecyzyjne. Rozdziały i podrozdziały, ich tematyka i następstwo, tworzą logiczną całość.

Recenzowana rozprawa stanowi istotny wkład w rozwój badań w obszarze nauk społecznych, ze szczególnym uwzględnieniem zagadnień bezpieczeństwa narodowego.

2. Zawartość rozprawy

Dysertacja Pana mgr. Michała Sieka liczy ogółem 307 stron tekstu, 11 strony bibliografii (162 poz. powołanej literatury, 38 poz. raportów, 20 poz. aktów normatywnych) z netogtafią (48 poz.) i 18 stron załączników (szablony ankiety). Należy z uznaniem odnieść się do wykorzystanej w pracy literatury przedmiotu, nie tylko ze względu na obszerność, ale na jej kompletność.

Podstawowy tekst rozprawy składa się ze wstępu, pięciu rozdziałów i zakończenia.

We wstępie Doktorant przedstawia ogólny zarys problematyki objętej tematem pracy oraz opisuje strukturę pracy.

W pierwszym rozdziale pt. Metodologiczne podstawy badań procesów walki informacyjnej (ss. 15-37) Doktorant opisał genezę problemu i przedmiot badań. Sformułował cel poznawczy oraz utylitarny badań, problem badawczy, hipotezy robocze (3). Przedstawił wykorzystane metody i techniki badawcze. W zakończeniu rozdziału dokonał przeglądu literaturowo-faktograficznego

dotyczącego przejścia z ery przemysłowej do ery informacyjnej (społeczeństwa informacyjnego) i powiązanych z tym zagrożeń, a także poświęconych badaniom systemowym i prognozowaniu (wykorzystanej w pracy organizacji badań). Odniósł się także do używanych w pracy pojęć cyberprzestrzeni, cyberbezpieczeństwa wskazując na wagę ich precyzyjnego określenia.

W drugim rozdziale pt. Modele walki informacyjnej (ss. 38-85) Doktorant wychodząc z założenia, że definicje i modele walki wymagają opisu tych pojęć, przedstawia deterministyczne i stochastyczne modele w różnych ujęciach walki i wojny informacyjnej. Główną konstatacją tego rozdziału jest stwierdzenie, że ciężar wojny informacyjnej w znacznej mierze przesuwa się do cyberprzestrzeni.

W trzecim rozdziale pt. Analiza systemowa cyberwojny (ss. 86-17) Autor przedstawia szczegółową analizę tego antropogenicznego, specyficznego środowiska walki. Wskazuje w nim na konwergencję socjosfery, infosfery oraz technosfery. Przedstawia także proste techniki ataków i ataki wysoce skorelowane, wysoce ustrukturyzowane, których egzemplifikacją może być cyberwojna. Rozdział zawiera również analizę raportów stanu bezpieczeństwa cyberprzestrzeni oraz opis w formie case study zrealizowanych w cyberprzestrzeni konfliktów. Treść rozdziału, zawierająca opis dominujących trendów oraz podatności, jakie mogą wykorzystać wybrane zagrożenia, tworzy przesłanki prognostyczne dla kolejnego rozdziału.

Kolejny, czwarty rozdział pt. Podstawy prognozowania bezpieczeństwa państwa w cyberprzestrzeni (ss. 168-208) to rozdział, w którym Autor opisuje i analizuje metody i techniki prognozowania. Szerzej przedstawia metody scenariuszowe, w szczególności te, które zostały wykorzystane w badaniach. Omówione jest w nim również podejście systemowe do prognozowania w ujęciu H. Świebody, które stało się punktem wyjścia do opracowania konstruktu własnych badań systemowych nad przyszłością, w których centralnym punktem są metody scenariuszowe.

W rozdziale piątym, objętościowo dominującym, pt. Prognoza stanu bezpieczeństwa RP w cyberprzestrzeni (ss. 209-305) Doktorant dokonał opisu przeprowadzonych badań, charakterystykę grupy eksperckiej. Zawarł w nim opracowane na ich podstawie cztery scenariusze stanów otoczenia cyberprzestrzeni (najbardziej prawdopodobny, najkorzystniejszy, pesymistyczny i niespodziankowy). Przedstawione w rozdziale wyniki analizy zagrożeń infrastruktury krytycznej, w postaci scenariusza bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni na lata 2021-2022, Autor wykorzystał do analizy obowiązującej strategii cyberbezpieczeństwa RP i sformułowania wniosków dotyczących określenia nowej strategii.

Zakończenie (ss. 306-313) stanowi właściwą syntezę badań. Doktorant podkreślił, że ryzyko realizacji wysoce ustrukturyzowanych ataków w cyberprzestrzeni, jakich egzemplifikacją jest cyberwojna, również musi być brane pod uwagę w konstruowaniu strategii bezpieczeństwa państwa i jego obywateli w cyberprzestrzeni. Zauważył, że analiza systemowa pozwala na zrozumienie mechanizmów współczesnej wojny informacyjnej prowadzonej w cyberprzestrzeni, jako złożonego systemu (a także daje możliwość poznania samej cyberprzestrzeni i jej wewnętrznych oraz zewnętrznych relacji). Zwrócił uwagę, że pomimo zastrzeżeń (istniejących kontrowersji) metodologicznych oraz trudności wynikających z dysponowania niepełnymi, a także niepewnymi danymi wejściowymi modelu, prognozy powinny być sporządzane, gdyż to one powinny stanowić podstawę podejmowania decyzji.

Przeprowadzone badanie i wnioski końcowe świadczą o dojrzałości naukowej kandydata do stopnia doktora.

Na uwagę zasługuje to, że Doktorant na zakończenie każdego rozdziału dokonuje krótkiego podsumowania treści rozdziału i czasami wprowadzenia do tematyki następnego rozdziału. Całość pracy jest przedstawiona w sposób bardzo interesujący i zrozumiałym językiem, co w konsekwencji pozwala wystawić Autorowi wysoką ocenę.

3. Ocena merytoryczna dysertacji

Doktorant poddał wnikliwej analizie problem badawczy, odpowiadając na postawione pytania i weryfikując założone hipotezy. Określenie problemu badawczego, opis celów i uwarunkowań danego problemu zawarte w rozdziałach 1-4, zostały przedstawione na tyle szczegółowo, aby można było odpowiednio zaplanować badanie (opisane w rozdziale 5). Należy zaakcentować, że Autor opracowując dysertację korzystał z bardzo dobrze dobranej i różnorodnej literatury źródłowej przedmiotu oraz dużej ilości aktów prawnych. Bardzo dobrze opracował metodologię prowadzenia badań aktowych, co jest istotne w procesie badawczym. Należy stwierdzić, że układ rozdziałów i podrozdziałów jest logicznie uzasadniony i hierarchicznie uporządkowany, tytuły i podtytuły dokładnie określają zakres merytoryczny i odpowiadają zawartej w nich treści (można jedynie zasugerować, skrócenie tytułu I rozdziału do „Metodologiczne podstawy badań”, gdyż walka informacyjna wprowadzana jest w kolejnym rozdziale). Treści kolejnych rozdziałów i podrozdziałów wynikają z poprzedzających je rozważań.

Zarówno w konstrukcji, jak i treści pracy widać bardzo duży, pozytywny wpływ promotora.

Należy zauważyć, że autor pewnie porusza się w niełatwej dziedzinie wiążącej zagadnienia prawne, organizacyjne i techniczne (informatyczne). Warto podkreślić, że zaprezentowane w pracy rozważania obejmują liczne problemy i zagadnienia szczegółowe, których analiza nie ogranicza się jedynie do odtworzenia dotychczas istniejących poglądów, ale następuje po niej propozycja zmierzająca do rozwiązania problemu (np. własna definicja scenariusza).

W nawiązaniu do rozważań szczegółowych warto podkreślić, że recenzowana praca stanowi cenną inspirację do dalszej naukowej dyskusji (przynajmniej w obszarze wskazanym w zakończeniu), a tym samym do dalszego rozwoju nauk o bezpieczeństwie.

W pracy występują incydentalne błędy redakcyjne, które nie obniżają wysokiej wartości recenzowanej pracy.

Reasumując: uznaję, że dysertacja pt.: „Analiza systemowa i prognozowanie stanu bezpieczeństwa Rzeczypospolitej polskiej w cyberprzestrzeni" s**pełnia wszystkie wymogi formalne i merytoryczne** określone w art. 13 ust. 1 Ustawa z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (z późniejszymi zmianami) oraz ustawie z dnia 20 lipca 2018 r., Prawo o szkolnictwie wyższym i nauce, art. 179.1. dotyczący: „przewody doktorskie, postępowania habilitacyjne i postępowania o nadanie tytułu profesora wszczęte i niezakończone przed dniem wejścia w życie ustawy, o której mowa w art. 1, są przeprowadzane na zasadach dotychczasowych i **wnioskuję o dopuszczenie Pana mgr. Michała Sieka do publicznej obrony doktoratu**.

Wojna i walka informacyjna zdefiniowana na str. 40 a używana wcześniej

wojna informacyjna rozegra się przy użyciu, i wobec wszystkich narodowych źródeł informacji oraz systemów (procesów) informacyjnych (str.55) a w pracy jest mowa o bezpieczeństwie cyberprzestrzeni (atakach hakerskich i złośliwym oprogramowaniu)

Scenariusze są uznawane za metodę prognozowania długookresowego – Pan przyjął horyzont 2-3 letni, czyli raczej krótki – jak to wytłumaczyć?

Ankietę rozesłano do grupy około 20 ekspertów – jakie przyjęto kryterium bycia ekspertem?