dr hab. Halina ŚWIEBODA
Akademia Sztuki Wojennej

Warszawa. 14.11.2020r.

RECENZJA

rozprawy doktorskiej autorstwa Pana ppłk mgr inż. Michała SIEKA

na temat:

ANALIZA SYSTEMOWA I PROGNOZOWANIE STANU EZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ W CYBERPRZESTRZENI

napisanej pod kierownictwem naukowym

prof. dr. hab. inż. Piotra Sienkiewicza

1. Uwagi ogólne

Formalną podstawą sporządzenia recenzji była uchwała Rady Dyscypliny Nauki o Bezpieczeństwie Wojskowej Akademii Technicznej przekazanej w piśmie Przewodniczącego Rady pana płk dr. hab. prof. WAT Szymona MITKOW z dnia 05.10.2020r.

Rozprawa doktorska na temat *Analiza systemowa i prognozowanie stanu bezpieczeństwa rzeczypospolitej polskiej w cyberprzestrzeni,* odpowiada na aktualne problemy a przede wszystkim na zapotrzebowanie zwiększania bezpieczeństwa w cyberprzestrzeni. Niezwykle trafny wybór tematu bowiem problemy rozważane w dysertacji dotyczą cyberprzestrzeni skupione jak w soczewce na możliwościach poprawy poziomu jej bezpieczeństwa. Potencjał ekonomiczno-gospodarczy jaki pojawia się wraz z rozwojem ICT i adaptacją rozwiązań w zakresie technologii wspierających różne procesy zarzadzania, kierowania, podejmowania decyzji, są bezsporne. Potwierdzają to badania OECD, Eurostatu, GUSu, a także niektórych ośrodków naukowych. Dzisiaj ochrona zasobów informacyjnych jest głównym czynnikiem warunkującym rozwój kraju. Niestety, w szczególności ostatnie lata, ujawniły intensyfikację a także dynamiczną ewolucję zagrożeń realizujących się w cyberprzestrzeni, które prowadziły do naruszeń bezpieczeństwa państwa, chociaż nie nosiły cech cyberwojny to powodowały straty ekonomiczno-gospodarcze. O przykłady nietrudno. Tylko ostatnie tygodnie obfitują w informacje o atakach na szpitale czy laboratoria pracujące nad szczepionką czy lekami na

COVID-19. Do czynienia mamy z bardzo poważnymi atakami w różnych państwach (np. USA, Ukraina) na sektor energetyczny, w tym energetyki jądrowej, banki i instytucje finansowe. Odpowiedzą na zagrożenia państw jest tworzenie cyberwojsk, których celem jest rozwinięcie zdolności do działań w tym specyficznym środowisku.

Uwagę zawraca oryginalność podejścia w dysertacji do szeroko zakrojonych badań zjawisk związanych z cyberprzestrzenią, z zagrożeniami, problemami wojny informacyjnej, modelami walki. Jak istotne są to problemy świadczą podejmowane inicjatywy i działania w zakresie zwiększania odporności na ataki i poziomu bezpieczeństwa cyberprzestrzeni na poziomie UE, NATO, w kraju ale także w wielu innych państwach. Problemy cyberprzestrzeni są problemami globalnymi. Tym bardziej wydaje się, że kwestia rozpoznania mechanizmów rządzących cyberwojną, sklasyfikowanie ataków oraz próba ich prognozowania pozostaje kwestią zasadniczą. Trafnie doktorant dookreślił obszar niewiedzy lokując swoje badania poznania praw rządzących walką informacyjną (modeli walki informacyjnej), skupiając się na atakach wymierzonych w rzeczywiste cybernetyczne systemy niezbędne do minimalnego funkcjonowania gospodarki. Niewątpliwą wartością dodaną dysertacji jest podjęcie badań prognostycznych realizacji zagrożeń w postaci ataków prowadzonych w cyberprzestrzeni wymierzonych w elementy infrastruktury krytycznej.

2. Ocena metodologiczna rozprawy

Metodyka badawcza (założenia, cele, metody)

Z metodologicznego punktu widzenia rozprawa doktorska autorstwa Pana ppłk mgr inż. Michała Sieka nie budzi większych zastrzeżeń. Doktorant spełnił podstawowe wymagania, co do organizacji i przebiegu procesu badawczego. Dysertacja stanowi oryginalną, zamkniętą i spójną tematycznie całość a jej konstrukcja jest prawidłowa. Treści zaprezentowano na 346 stronach z czego 313 stron to strony merytoryczne, pozostałe są uzupełnieniem rozprawy w postaci spisu literaturowego, spisu rysunków (109) i tabel (42) oraz załączników (2). Tu uwaga techniczna bibliografia powinna pojawić się przed spisami rysunków i tabel. Strukturę pracy tworzy 5 rozdziałów, których kolejność odpowiada zaplanowanym badaniom, przy czym zachowano proporcje pomiędzy poszczególnymi rozdziałami. Treść podjętych i przeprowadzonych przez Autora rozważań i badań odpowiada tytułowi, mocno rozbudowanemu i tematowi pracy. Tytuł pracy zapowiada rozległy obszar badawczy i rzeczywiście taki jest, zapowiada badania (analizę systemową) stanu bezpieczeństwa RP w cyberprzestrzeni i prognozowanie jako proces, który może być wykorzystany w

bezpieczeństwie cyberprzestrzeni RP i adekwatnie do tytułu rozprawy prowadzone są założenia metodologiczne.

Sytuację problemową i uzasadnienie potrzeby podjęcia badań o charakterze prognostycznym w celu dokonania predykcji wydarzeń oraz diagnozowania możliwych scenariuszy prowadzenia działań wojennych w cyberprzestrzeni doktorant zaprezentował w szerokim kontekście koncepcji walki w cyberprzestrzeni wraz z komponentami CYBEROPS i INFOOPS. Konceptualizacji badań dokonano w metodologii analizy systemowej przyjmując odpowiednio za: (1) zjawisko cyberwojnę, (2) system, to system ochrony i obrony RP w cyberprzestrzeni (zawężony do infrastruktury krytycznej) (3) procesy – wyrażone procesami zarządzania bezpieczeństwem, prognozowania zagrożeń oraz analizy i oceny ewaluacji ich ryzyka (s.20). Zaznaczając jednocześnie, że istotne będą też badania otoczenia bliższego i dalszego RP, a horyzont prognozy wyznaczono do roku 2022.

Zarysowany we „Wstępie" cel dysertacji (s.8-9) doktorant precyzuje i dookreśla w rozdziale metodologicznym (s.22), prezentując cel poznawczy jakim jest kreacja możliwych scenariuszy realizacji zagrożeń w cyberprzestrzeni, i cel praktyczny wyrażony oczekiwaniami co do możliwości sformułowania na podstawie badań wniosków i konkluzji zaleceń do formułowania strategii obrony RP.

W części formułowania problemów badawczych i hipotez doktorant nie ustrzegł się nieścisłości. Problemu głównego doktorant nie sformułował, natomiast sformułował 6 pytań, z czego 2 są trywialne, w szczególności te, na które są odpowiedzi co prawda nie udowodnione ale są podejrzenia, które oficjalnie pojawią się w przestrzeni informacyjnej. Dotyczy to pytania 1 i 2, dodać należy, ze autor informuje co trzeba zrobić aby móc przewidywać ataki i wiemy o co chodzi ale nie zostało to wyrażone explicite. Podobny problem występuje z pozostałymi pytaniami, bowiem wymaga czasu aby je dopasować do poszczególnych rozdziałów. W końcu pojawia się problem relacji koszt efekt", który później nie jest rozwijany i nie znalazł uzasadnienia w hipotezie, która jest rozbudowana i jest odpowiedzią na postawione wadliwie pytania w szczególności 1-2. Natomiast 3 hipoteza jest poprawna jest odpowiedzią znowu na nie do końca wyartykułowane pytanie o możliwości zastosowania analizy systemowej i prognozowania, jako podstawy do opracowywania racjonalnej polityki bezpieczeństwa i strategii cyberobrony RP.

Hipotezę Doktorant ujął w rozbudowanej formie właśnie w odniesieniu do sześciu problemów cząstkowych. Tak skonstruowana hipoteza badawcza może świadczyć o dużym zasobie wiedzy, zwłaszcza praktycznej, wynikającym z wieloletnich obserwacji i dogłębnym

przygotowaniu merytorycznym, chociaż problemy i pytania na, które hipoteza ma odpowiadać nie są precyzyjnie postawione.

Nie zgłaszam zastrzeżeń do doboru metod, technik i narzędzi badawczych zastosowanych w procesie badawczym. Podczas badań teoretycznych wykorzystywano analizę, syntezę, abstrahowanie, uogólnianie, wnioskowanie, analogię i porównywanie. W badaniach empirycznych Doktorant wykorzystał wiele metod z zakresu predykcji i prognostyki (scenariusz) posługując się autorska metodą, wykorzystał badanie ankietowe do wywiadów eksperckich – badanie przeprowadzono w metodologii Delphi: Zastosowanie takich metod, narzędzi i technik znajduje uzasadnienie, bowiem w procesie badawczym badano opinie i poglądy określonych osób a stwierdzone empirycznie prawidłowości mają wysoki stopień prawdopodobieństwa.

Z wielką precyzją ujęto organizację badań wyjaśniając różnicę pomiędzy podejściem redukcjonistycznym a systemowym doprecyzowując to czego nie ujęto w pytaniach badawczych niejako równoważąc nieścisłości. Dokonano wyczerpującej oceny piśmiennictwa obejmującego zakres publikacji wojny informacyjnej, cyberwojny, cyberprzestępstw bezpieczeństwa cyberprzestrzeni, predykcji i prognostyki jednocześnie wskazując na źródła teorii.

Stwierdzam, że zastosowana w dysertacji procedura badawcza odpowiada wymogom logicznym i metodologicznym. Z punktu widzenia założeń procesu badawczego, zachowano logiczną wynikowość układu rozprawy. Każdy ze sformułowanych w rozdziale pierwszym problemów szczegółowych znajduje swoje rozwiązanie w części merytorycznej. Stąd ogólna ocena metodologiczna recenzowanej dysertacji jest bardzo pozytywna. Po lekturze rozprawy, jestem przekonana, że zakładany cele badań zostały osiągnięte przez Doktoranta.

3. Ocena merytoryczna rozprawy

Wykorzystana literatura

Doktorat wykorzystał 268 pozycji bibliograficznych z czego połowę stanowią publikacje w języku angielskim, ilość przywołanych publikacji świadczy o umiejętności wykorzystania przez autora rozprawy literatury przedmiotu. Literatura dobrana prawidłowo, jest zróżnicowana i bogata. Zatem pracę wyróżnia solidna baza źródłowa, która niewątpliwie została dobrana do tematu rozprawy. Wyszczególnione pozycje zwarte, dokumenty normatywne, artykuły, materiały źródłowe raporty, i strony internetowe w moim przekonaniu są reprezentatywne i dające możliwość rzetelnego opisania badanych zagadnień.

4. Szczegółowa ocena merytoryczna poszczególnych części rozprawy

Pod względem merytorycznym rozprawa zasługuje na pozytywną ocenę. Warto jednak poczynić pewne uwagi, które mogą mieć charakter dyskusyjny ale na pewno pozwalają dopracowywać warsztat naukowy. Przyjęta metodyka rozwiązania problemów badawczych dla osiągnięcia celu pracy wpłynęła na strukturę dysertacji. Pierwsza i druga część o charakterze wyjaśniającym i koncepcyjnym, oparta o literaturę krajową i zagraniczną stanowiła punkt odniesienia do czwartej i piątej, badawczej części rozprawy. Dysertacja w części zasadniczej składa się ze wstępu, rozdziału metodologicznego, czterech rozdziałów merytorycznych, zakończenia, w którym zawarto kierunki dalszych badań. Wszystkie rysunki i tabele w sposób czytelny obrazują wyniki badań. Generalnie należy podkreślić, że wyniki procesu badawczego w zakresie możliwości predykcji i prognostyki, zostały zilustrowane dobrze i w sposób rzetelny. Należy również podkreślić badania dotyczące sieci TOR, które przeprowadził doktorant.

W pierwszym rozdziale dysertacji przedstawiono metodologiczne podstawy badań procesów walki informacyjnej, wyjaśniono genezę oraz sformułowano główny problem badawczy w odniesieniu do zdefiniowanego hierarchicznego przedmiotu badań, który przedstawiono w trójpoziomowym aspekcie zjawiska-systemu-procesu. Szczegółowo omówiłam problemy metodologiczne w części poświęconej metodologii badań.

W drugim rozdziale zatytułowanym „Modele walki informacyjnej" przedstawiono sposoby definiowania terminu informacja w odniesieniu do różnych nauk. Wskazano na kluczowe znaczenie informacji we współczesnym świecie, co czyni ją zasobem strategicznym. Omówiono następnie pojęcie wojny informacyjnej i jego ewolucję, wskazując problemy, z jakimi spotykają się współczesne organizacje w przetwarzaniu informacji. Jeden z podrozdziałów tego fragmentu rozprawy doktorskiej poświęcono modelom walki. Scharakteryzowano w nim typowe modele walki zarówno deterministyczne jak i stochastyczne. Wskazano wykorzystanie ogólnych modeli walki do analizy zagadnień wojny informacyjnej. Szczególne miejsce poświęcono modelowi Helmbold'a i dającym mu podstawę równaniom Lanchester'a. Następnie w dysertacji zaprezentowano modele odnoszące się wprost do walki informacyjnej. Rozdział szerzej traktuje o modelu procesu informacyjnego Waltz'a oraz ujęciu wojny informacyjnej modelem kanału Shannon'a. Przy wykorzystaniu tego ostatniego przedstawiono pięć strategii realizacji działań wojny informacyjnej, które następnie ujęto w ramy modelu hipergry. W tym fragmencie dysertacji uchwycono relacje zachodzące pomiędzy

przedstawionymi modelami walki informacyjnej. Ostatnim szeroko omówionym w rozdziale modelem jest sieciocentryczny model walki. Rozważania zawarte w rozdziale skłaniają do wniosków, że ciężar wojny informacyjnej w znacznej mierze przesuwa się do cyberprzestrzeni. Omówieniu tych zagadnień posłużył kolejny rozdział: „Analiza systemowa cyberwojny" to tytuł wyodrębnionej części dysertacji, którą rozpoczęto od próby zdefiniowania pojęcia cyberprzestrzeni. W rozdziale tym zamiast koncentrowania wysiłku na próbie zadowalającego ujęcia pojęcia cyberprzestrzeń, zaprezentowano wieloaspektowość tego antropogenicznego, specyficznego środowiska walki. Wskazano występujące konwergencje socjosfery, infosfery oraz technosfery, które kształtują cyberprzestrzeń. Skomentowano przy użyciu diagramu Tibbs'a relacje zachodzące pomiędzy podmiotami prowadzącymi działania w tym specyficznym środowisku walki. Odniesiono się zarówno do współpracy, kooptacji, jak i bezpardonowej walki. Rozważania przeprowadzono dla fizycznego desygnatu cyberprzestrzeni oraz wirtualnego, a także poznawczego. Przedstawiono proste techniki ataków i omówiono, na czym polegają ataki wysoce skorelowane, wysoce ustrukturyzowane, których egzemplifikacją może być cyberwojna. Zaprezentowano różnice w podejściu do definiowania w Polsce i w Unii Europejskiej infrastruktury krytycznej, która najprawdopodobniej będzie głównym celem ataków realizowanych w ramach cyberwojny. Wykorzystując zmodyfikowany model walki Warden'a przedstawiono jak może być osiągnięta przewaga informacyjna w cyberprzestrzeni i do czego może doprowadzić oraz jakie są związki cyberprzestrzeni z pozostałymi tradycyjnie ujmowanymi wymiarami. Poczyniono próby definiowania cyberwojny, jednocześnie prezentując, na czym ona może polegać i jakie mogą być jej cele. Rozdział zawiera również analizę raportów stanu bezpieczeństwa cyberprzestrzeni oraz opis w formie case study znanych i zrealizowanych w cyberprzestrzeni konfliktów (jak atak na Estonię, Ukrainę, Irak czy Stany Zjednoczone). Wysunięto główne tezy dotyczące trendów w atakach realizowanych w cyberprzestrzeni oraz omówiono wykorzystywaną w tych atakach cyberbroń - zdefiniowaną głównie w oparciu o analizę raportów ENISA. Ważnym zagadnieniem rozdziału jest zdefiniowanie łańcucha ataku, który służy dalszym analizą cyberbroni, określając m.in. jej użyteczność. Rozdział zamyka opis zrealizowanej przez autora samodzielnej eksploracji ciemnej strony sieci (sieci TOR) przeprowadzony głównie pod kątem oceny dostępności oprogramowania złośliwego. Rozdział utwierdza w przekonaniu, że główną areną działań wojny informacyjnej stała się cyberprzestrzeń oraz wskazuje do dalszej analizy zagrożenia, w postaci cyfrowych ataków realizowanych w systemach infrastruktury krytycznej, jakie będą podlegały prognozowaniu. Jest też gruntem w tworzeniu przesłanek prognostycznych dla

kolejnego rozdziału, zawiera opis dominujących trendów oraz podatności, jakie mogą wykorzystać wybrane zagrożenia.

W Rozdziale IV „Podstawy prognozowania bezpieczeństwa państwa w cyberprzestrzeni" omówiono, na czym polega prognozowanie racjonalne i naukowe oraz zaprezentowano metody i technik prognozowania. Wskazuje różnicę między prognozowaniem a przewidywaniem. Przegląd teorii i towarzyszących im narzędzi badawczych rozpoczęto od najprostszych metod prognozowania do bardziej skomplikowanych. Jako pierwsze poddano ocenie metody wykorzystujące szeregi czasowe. Tą część analizy wsparto własnymi badaniami. Następnie omówiono metody pozwalające nadążyć za dużą dynamika zmienności cyberprzestrzeni. W tym fragmencie dysertacji Autor omówił szeroko metody scenariuszowe. Następnie przyjęto konkretne metody tworzenia scenariuszy, które wykorzystane zostały w badaniach. Punktem wyjścia do opracowania konstruktu własnych badań systemowych nad przyszłością, w których centralnym punktem są metody scenariuszowe.

Ostatni rozdział „Prognozowanie stanu bezpieczeństwa RP w cyberprzestrzeni" jest opisem przeprowadzonych przez autora badań oraz zawiera opracowane na ich podstawie scenariusze. Zaprezentowano w nim charakterystykę grupy eksperckiej, która została wybrana z zachowaniem należytej triangulacji m. in. pod względem charakteru wykonywanej pracy, miejsca pracy oraz obszaru zainteresowań. Zaprezentowane wyniki badań analizy otoczenia cyberprzestrzeni pozwoliły na sformułowanie czterech scenariuszy stanów otoczenia cyberprzestrzeni: należą do nich scenariusz najbardziej prawdopodobny oraz niespodziankowy, a także para scenariuszy: najkorzystniejszego i pesymistycznego. Z kolei przedstawione wyniki analizy zagrożeń, w postaci ataków cyfrowych na elementy infrastruktury krytycznej przyczyniły się do stworzenia scenariusza zdarzeń (zagrożeń). Ujęto w nim wyniki ewolucji poszczególnych ataków. Zespolenie obu scenariuszy pozwoliło ukonstytuować „scenariusz bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni na lata 2021-2022. Stał się on podstawą do analizy obowiązującej strategii cyberbezpieczeństwa RP i sformułowania wniosków dotyczących określenia nowej strategii (podkreślono w nich mocne strony strategii oraz wskazano jej braki).

Stwierdzam, że generalnie cele postawione przez Doktoranta zostały w toku rozważań osiągnięte. Jednocześnie konstrukcja rozprawy została zdeterminowana przez przyjęte cele badań. Przedstawione w pracy treści obejmują aspekty teoretyczne, metodologiczne i praktyczne odnoszące się do problemów stanu bezpieczeństwa cyberprzestrzeni RP wyrażanej poziomem zagrożeń oraz predykcji i prognostyki jako podstawy tworzenia strategii

cyberobrony. Problematyka podjęta w dysertacji jest ciekawa i istotna dla bezpieczeństwa cyberprzestrzeni RP

W wymiarze praktycznym praca jest adresowana do osób zajmujących się przedmiotową złożoną i aktualną problematyką cyberwojen, cyberzagrożeń cyberbezpieczeństwa i cyberstrategii. Mogą po nią sięgnąć i traktować jako swoisty poradnik osób odpowiedzialnych za realizację tego obszaru. Praca może być przydatna pracownikom nauki, zajmującym się zarówno przedmiotowym obszarem tematycznym, jak również szeroko pojmowanym zarządzaniem bezpieczeństwem, a także studentom, jako pomoc w dydaktyce i badaniach.

W podsumowaniu recenzji, proszę Doktoranta o odniesienie się do kilku zagadnień, które nasunęły mi się podczas studiowania dysertacji:

1. Czy mógłby Pan przybliżyć sposób prowadzenia analizy krzyżowej, w rozprawie znajdują się wyniki interesuje mnie jak pan je otrzymał?
2. Jakie mechanizmy obecnego systemu ochrony infrastruktury krytycznej są najbardziej skuteczne?
3. Jak Pan ocenia miarodajność próby ekspertów poddanej badaniom.

4. Wnioski końcowe

Mimo wspomnianych przez mnie wątpliwości i pewnej ilości niedociągnięć, jak sądzę niezmierzonych uchybień, dysertacja stanowi oryginalną próbę przedstawienia autorskiego wkładu w rozwój nauk o bezpieczeństwie, jest przykładem udanej adaptacji metod stosowanych głównie w ekonomii na grunt nauk o bezpieczeństwie. Wypełnia luki w wiedzy o cyberprzestrzeni jednocześnie daje podstawy dla praktycznego działania w obszarze cyberobrony.

W podsumowaniu recenzji stwierdzam, że – uwzględniając złożoność przedmiotu badań, różnorodność wykonanych badań - Doktorant podjął się ambitnego zadania. Przedstawione w rozprawie treści wskazują na umiejętności Autora dysertacji zarówno w zakresie identyfikowania sytuacji problemowej, gromadzenia i analizowania materiału badawczego oraz prezentowania uzyskanych wyników. Rozprawa została przygotowana w oparciu o szerokie studia literaturowe i równie szeroko zakrojone badania empiryczne. Doktorant dobrze orientuje się nie tylko w zakresie ogólnych, ale również specjalistycznych

zagadnień, związanych z bezpieczeństwem cyberprzestrzeni. Duża ilość informacji oraz liczne przypisy źródłowe stanowią solidną podstawę do dalszego zgłębiania prezentowanych treści.

Recenzowana dysertacja stanowi indywidualny dorobek Pana mgr inż. Michała Sieka, która spełnia wymagania ustawowe, by zostać doktorem nauk społecznych w specjalności nauki o bezpieczeństwie. Jest samodzielnym rozwiązaniem problemu badawczego. Świadczy o znacznym zasobie wiedzy merytorycznej i wystarczającym przygotowaniu metodologicznym Autora do prowadzenia badań w dziedzinie nauk społecznych.

Dysertacja spełnia warunki określone w art.179 Ustawy z dnia 3 lipca 2018 roku *Przepisy wprowadzające ustawę Prawo o szkolnictwie wyższym i nauce* z 30.08.2018) w oparciu o Ustawę z dnia 14 marca 2003 roku *o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki* (Dz. U. z 2003 r. nr 65, poz. 595 z późn. zm.) i zasługuje na wyróżnienie. Kwalifikuje jej Autora do kontynuowania procedury zmierzającej do nadania stopnia naukowego doktora w dziedzinie nauk społecznych, w dyscyplinie nauki o bezpieczeństwie. Dlatego wnoszę o dopuszczenie Pana mgr. inż. Michała Sieka do jej publicznej obrony.

dr hab. Halina ŚWIEBODA