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

Gdynia, 21.10.2019 r.

RECENZJA

rozprawy doktorskiej Pana **mgr. Jana ŻUKOWSKIEGO**

nt. ***Wykorzystanie Internetu jako środka zagrożenia bezpieczeństwa w konflikcie asymetrycznym***

1. UWAGI OGÓLNE

Przedstawiona do recenzji rozprawa doktorska Pana mgr. Jana Żukowskiego pt. *„Wykorzystanie Internetu jako środka zagrożenia bezpieczeństwa w konflikcie asymetrycznym"* została opracowana pod naukowym kierownictwem Pana dr. hab. Tomasza Aleksandrowicza na Wydziale Bezpieczeństwa Wyższej Szkoły Policji w Szczytnie.

Rozważania naukowe podjęte przez Autora dotyczą zdefiniowania możliwości wykorzystania Internetu, jako współczesnego środka zagrożenia bezpieczeństwa państwa w konflikcie asymetrycznym. Doktorant skupił swój wysiłek badawczy na ocenie możliwości prowadzenia działań w sieciach komputerowych wobec najbardziej czułych i istotnych dla bezpieczeństwa państwa sfer: ekonomicznej, militarnej, politycznej oraz społecznej. Należy podkreślić, że problematyka ta jest bardzo aktualna i istotna w dobie rozwoju społeczeństwa informacyjnego oraz lawinowego wzrostu zagrożeń mających swoje źródło w cyberprzestrzeni. Przestrzeni, która z jednej strony jest doskonałym środowiskiem funkcjonowania administracji publicznej, podmiotów gospodarczych oraz zaawansowanych technologicznie społeczeństw, a z drugiej strony stanowi przedmiot zainteresowania zorganizowanych grup przestępczych, organizacji terrorystycznych czy też sił zbrojnych.

Cyberprzestrzeń wprowadza nieosiągalne do tej pory możliwości w prowadzeniu konfliktów zbrojnych. Jest też elementem rewolucji w filozofii i metodach prowadzenia konfliktów pomiędzy państwami i organizacjami. Najbardziej zaawansowane technologicznie państwa rozwijają już od dłuższego czasu swój potencjał do prowadzenia działań w cyberprzestrzeni. Należą do nich przede wszystkim Stany Zjednoczone, Izrael, Chińska Republika Ludowa oraz Rosja. Duży potencjał w tym obszarze posiada również Korea Północna.

Doktorant trafnie zauważa, że działania w cyberprzestrzeni posiadają cechy działań asymetrycznych. Pod niektórymi względami przypominają one bardziej operacje prowadzone przez terrorystów niż przez żołnierzy. Wojna zmienia się w konflikt o charakterze wieloelementowym, w którym tradycyjne siły zbrojne tracą na znaczeniu wobec działań niekonwencjonalnych zwanych też asymetrycznymi czy hybrydowymi. Jesteśmy świadkami kształtowania się nowej formy walki, która przypuszczalnie będzie wykorzystywana w przyszłości na szeroką skalę. Zjawisko to wymaga prowadzenia badań naukowych i niewątpliwie naprzeciw tym potrzebom wychodzą badania oraz proponowane rozwiązania w recenzowanej rozprawie doktorskiej. Wyniki badań opracowane przez Autora wzbogacają aspekt metodyczny i poznawczy dotyczący wykorzystania Internetu w konflikcie asymetrycznym. W pracy widoczne jest również bardzo dobre przygotowanie merytoryczne Doktoranta do prowadzenia dociekań naukowych w tej materii.

2. OCENA KONCEPCJI METODOLOGICZNEJ PRACY

Koncepcja metodologiczna rozprawy została umieszczona w rozdziale pierwszym (ss. 11-19), w którym przedstawiono wszystkie podstawowe elementy naukowej metodologii badawczej, obejmującej: przedmiot badań, cel badań, problemy badawczy, hipotezy badawcze, procedurę badawczą, metody, techniki i narzędzia badawcze, ograniczenia badawcze oraz analizę krytyczną literatury przedmiotu badań. Przyjętą koncepcję metodologiczną należy uznać za formalnie poprawną i adekwatną do potrzeb rozprawy. Doktorant określił poprawnie cel główny badań oraz cztery cele szczegółowe. Następnie sformułował główny problem badawczy, którego rozwiązanie wymagało znalezienia odpowiedzi na cztery szczegółowe problemy badawcze. Na wstępie prowadzenia badań przyjął również główną hipotezę badawczą oraz szczegółowe hipotezy badawcze, które weryfikował prowadząc proces badawczy.

Umiejętność planowania i prowadzenia badań przez Doktoranta została zaprezentowana w opisie *Procedury badawczej*. Proces badawczy został podzielony na trzy główne etapy. Składał się on z etapu badań wstępnych, etapu badań właściwych oraz z etapu interpretacji uzyskanych wniosków.

Główny problem badawczy został sformułowany w postaci pytania *„Jakie są możliwości użycia Internetu, jako środka zagrożenia bezpieczeństwa, w konflikcie między państwami?"* Rozwiązaniu, tak sformułowanego problemu, towarzyszą cztery

szczegółowe problemy badawcze, wspomagające Autora w procesie naukowego poznania. Należy zauważyć, że tematyka prowadzonych badań jest bardzo złożona o czym świadczy rozległość przedmiotu badań. Obejmował on historyczne kierunki tworzenia, rozwoju i wykorzystania Internetu do celów wojskowych i cywilnych, zagrożenia dla bezpieczeństwa państwa generowane przez wykorzystanie Internetu, możliwości zastosowania Internetu w konflikcie asymetrycznym oraz wykorzystanie Internetu w sytuacji konfliktu międzypaństwowego przez wybrane państwa.

Głównym celem badań było *„zdefiniowanie możliwości wykorzystania Internetu jako współczesnego środka zagrożenia bezpieczeństwa państwa w konflikcie asymetrycznym"*. Cel ten został osiągnięty poprzez realizację celów szczegółowych, które objęły: określenie, na gruncie historycznym rozwoju, kierunków tworzenia i wykorzystania Internetu do celów wojskowych i cywilnych, identyfikację Internetu w obszarze źródeł zagrożenia bezpieczeństwa państwa, określenie możliwości wykorzystania Internetu w konflikcie asymetrycznym oraz wskazanie, na przykładzie wybranych państw, możliwości wykorzystania Internetu w sytuacjach konfliktów międzypaństwowych. Wyniki badań w tym zakresie niewątpliwie wskazują znaczący wkład Autora w dyscyplinie nauk o bezpieczeństwie.

Na wstępie prowadzonych badań Doktorant przyjął hipotezę roboczą o charakterze poznawczym. Stwierdził On, że *„iż użycie Internetu przyczynia się do wywoływania znaczących, negatywnych skutków w sferze ekonomicznej, politycznej, społecznej i militarnej w państwie zaatakowanym w cyberprzestrzeni. Jednocześnie kraj atakujący ponosi niewielkie ryzyko przy korzystnym stosunku koszt-efekt. Główna hipoteza badawcza mówi, iż jest to metoda walki ewoluująca o dużym polu rozwoju, która będzie rozwijana w kierunku jednego z głównych narzędzi walki"*. Weryfikacji tak postawionej hipotezy roboczej towarzyszą szczegółowe hipotezy robocze odnoszące się do wstępnego rozwiązania szczegółowych problemów badawczych. Doktorant twierdzi, *„iż poznanie dotychczasowego procesu tworzenia się Internetu pozwoli na lepsze jego zrozumienie oraz wskaże jego cechy stałe takie jak: dynamiczny rozwój, niewielka lub żadna możliwość jego stałej kontroli pod względem kierunków jego ewolucji, brak możliwości skutecznych metod ograniczania jego zasobów i dostępów oraz wykorzystywanie przestrzeni cywilnej do działań militarnych"* oraz, że *„największe zagrożenie generowane obecnie przez Internet skierowane jest na kwestie danych mających wpływ na bezpieczeństwo państwa (np. nowe technologie, dane wywiadowcze itp.), system finansowy oraz wykorzystanie Internetu*

do działań ze sfery ogólnie rozumianej wojny informacyjnej. Wzrastać będzie poziom zagrożenia generowanego wobec infrastruktury krytycznej, w tym dążenie do wywoływania zniszczeń fizycznych". Ze wstępnych badań przeprowadzonych przez Doktoranta wynika, *„że walka w cyberprzestrzeni posiada cechy metody walki asymetrycznej. Składają się na to głównie takie elementy jak trudność wykrycia sprawców oraz niekonwencjonalne metody prowadzenia walki obejmujące m.in. działania psychologiczne"* oraz, że *„możliwości działania w cyberprzestrzeni są zwiększane przez takie kraje jak Federacja Rosyjska i Stany Zjednoczone. Powyższe wynika z potrzeby uczestnictwa w wyścigu o globalne zasoby, w którym cyberprzestrzeń pozwala na osłabianiu przeciwnika jednocześnie nie prowokując odwetu militarnego"*.

Należy stwierdzić, że przyjęta przez Doktoranta koncepcja metodologiczna rozprawy i zaproponowane metody badawcze są poprawne i adekwatne do potrzeb rozpatrywanej tematyki badawczej. Precyzyjnie zdefiniowane elementy procesu badawczego pozwoliły Doktorantowi zrealizować cel pracy oraz zweryfikować przyjęte hipotezy badawcze.

Praca została napisana językiem poprawnym. Autor wykazał się bardzo dobrą znajomością warsztatu pisarskiego. Rozdziały i podrozdziały tworzą logiczną całość. Zdarzające się niedociągnięcia edytorskie nie pomniejszają pozytywnej oceny końcowej pracy.

3. OCENA MERYTORYCZNA PRACY

Wyniki badań Doktorant przedstawił w formie dojrzałego dzieła naukowego, które pod względem merytorycznym nie budzi żadnych wątpliwości. Recenzowana rozprawa doktorska systematyzuje i poszerza wiedzę z zakresu możliwości wykorzystania Internetu jako współczesnego środka zagrożenia bezpieczeństwa państwa w konflikcie asymetrycznym.

Opracowanie zawiera wszystkie wymagane elementy redakcyjne prac naukowych, w tym wstęp, założenia badawcze, cztery rozdziały merytoryczne, zakończenie oraz bibliografię.

W rozdziale pierwszym pt. *„Założenia badawcze"* (ss. 11-19) przedstawiono podstawy metodologiczne badań, potwierdzające znajomość procedury badawczej stosowanej w naukach o bezpieczeństwie.

W rozdziale drugim pt. *„Historia rozwoju Internetu"* (ss. 20-66) omówiono koncepcja wojskowej sieci komputerowej, rozwój Internetu cywilnego, proces tworzenia szkodliwego oprogramowania, powstanie zjawiska hakerstwa oraz scharakteryzowano ukrytą sieć– Deep Web. Treści merytoryczne zaprezentowane w tym rozdziale, pozwoliły zbudować Doktorantowi wiedzą dotyczącą potencjału Internetu, jako środowiska do prowadzania różnego rodzaju działań. Przeprowadzone badania pozwoliły wysnuć wartościowe wnioski i spostrzeżenia mówiące o tym, *że globalna sieć komputerowa stale rozwija się w kierunku postępującej niezależności od instytucji państwowych, organizacji międzynarodowych, działających na całym świecie firm i korporacji, przez co państwa zaczynają tracić wiele płaszczyzn, do tej pory tradycyjnie dla nich zarezerwowanych.*

Rozdział trzeci pt. *„Zagrożenia dla państwa"* (ss. 67-96) zawiera rozważania dotyczące kategoryzacji zagrożeń dla państwa, zagrożeń dla państwa wynikających z ewolucji porządku międzynarodowego, erozji westfalskiego modelu suwerenności, kształtowania się społeczeństwa informacyjnego, kryzysu demokracji liberalnej oraz konfliktu asymetryczny w odniesieniu do cyberprzestrzeni. Przeprowadzone w tym rozdziale badani pozwoliły opracować Doktorantowi listę czynników wpływających na poziom bezpieczeństwa państwa. Analizie poddano zarówno czynniki stałe takie jak wojny czy katastrofy naturalne jak i czynniki wynikające z ewolucji i dynamiki społeczno-ekonomiczno-politycznej, które obecnie wpływają na struktury państw. Wskazane zostały czynniki szczególnie w obszarze ładu międzynarodowego oraz ewolucji społecznej mające bezpośredni negatywny wpływ na poziom bezpieczeństwa tradycyjnych struktur państwowych. Powyższe czynniki pokazują, że konflikt w cyberprzestrzeni w sposób naturalny staje się konfliktem asymetrycznym, gdyż obecne zmiany ewolucyjne w ładzie światowym sprzyjają działaniom niekonwencjonalnym, które nie prowadzą do bezpośredniego starcia ani dużych zniszczeń, mogących zagrozić wytworzonej międzynarodowej sieci powiązań społecznych, ekonomicznych i politycznych.

W rozdziale czwartym pt. *„Współczesne kierunki rozwoju konfliktu w sieci"* (ss. 97-117) Doktorant omówił problematykę wojny informacyjnej, współczesne aspekty działań w cyberprzestrzeni, zjawisko konfliktu w cyberprzestrzeni jako elementu wojny przyszłości oraz relacje zachodzące pomiędzy prowadzeniem działań w cyberprzestrzeni i wykorzystaniem nowych technologii informatycznych, takich jak sztuczna inteligencja, komputery kwantowe czy kryptowaluty. Treści merytoryczne zamieszczone w tym

rozdziale doprowadziły Doktoranta do wniosku, że naturalnym miejscem prowadzenia konfliktów pomiędzy państwami staje się cyberprzestrzeń. Pozwala ona na zadanie przeciwnikowi poważnych strat w szeroko rozumianym potencjale obronnym i jednocześnie pozostawia dość duże możliwości wycofania się lub ukrycia swoich działań bez narażania się na otwarty konflikt. Taki stan rzeczy powoduje, że w przyszłości narzędzia do prowadzenia konfliktów w cyberprzestrzeni będą stale się rozwijać.

Rozdział piąty pt. *„Kierunki rozwoju zdolności oddziaływania na bezpieczeństwo za pomocą działań w sieci na przykładzie wybranych państw"* (ss. 118-169) zawiera wyniki analizy dotyczące wybranych państw, które intensywnie rozwijają swoje zdolności do działania w aspekcie konfliktu w cyberprzestrzeni. Doktorant zwrócił w nim szczególną uwagę na wyraźny podział w filozofii wykorzystania cyberprzestrzeni, kierunków rozwoju zdolności, zmian w ustawodawstwie oraz sposobie działania wyspecjalizowanych w tym aspekcie służb. Badania wykazały, że podobne kierunki rozwoju przejawiają Federacja Rosyjska i Chińska Republika Ludowa w aspekcie zabezpieczenia własnej cyberprzestrzeni od wpływów z zewnątrz oraz, że w obu państwach zauważalne są tendencje do prowadzenia działań zaczepnych i ofensywnych. Odwrotną filozofię, zdaniem Doktoranta, wykazują Stany Zjednoczone oraz Wielka Brytania. Starają się one głównie zabezpieczyć przed atakami oraz nie ograniczać swobody dostępu do cyberprzestrzeni.

Rozprawę wieńczy *„Zakończenie"*, w którym Doktorant w sposób umiejętny dokonał podsumowania badań, odniósł się do celów i problemów badawczych oraz uzyskanych rezultatów i proponowanych kierunków dalszych badań. Zwrócił również uwagę, że poważnym ograniczeniem badań był brak możliwości poznania najnowocześniejszych metod ataków przygotowywanych do działań w cyberprzestrzeni przez państwa. Poruszanie się w obszarze niejawnym wybranych państw uniemożliwiało Doktorantowi poznanie ich dokładnych struktur, metod działania, posiadanych sił i środków.

Część merytoryczną pracy zamyka związana z tematyką rozprawy bibliografia, zamieszczona na ss. 173-193 i zawierająca źródła w postaci dokumentów, encyklopedii, słowników, leksykonów, monografii i opracowań, prac w opracowaniach, artykułów w czasopismach oraz publikacji internetowych.

Podsumowując należy stwierdzić, że pod względem merytorycznym rozprawa jest poprawna. Układ rozdziałów i podrozdziałów tworzy logiczną całość. Treści kolejnych

rozdziałów i podrozdziałów wynikają z poprzedzających je rozważań. Brzmienie poszczególnych tytułów i podtytułów odpowiada zawartej w nich treści i dokładnie określa zakres merytoryczny danej partii materiału.

4. WNIOSEK KOŃCOWY

Recenzowana rozprawa doktorska Pana mgr. Jana ŻUKOWSKIEGO nt. *„Wykorzystanie Internetu jako środka zagrożenia bezpieczeństwa w konflikcie asymetrycznym"* jest dziełem autorskim i oryginalnym, spełnia podstawowe kryteria stawiane rozprawom doktorskim.

W ocenie recenzenta praca wnosi istotny wkład w rozwój nauk o bezpieczeństwie. Systematyzuje i poszerza znaną dotychczas problematykę prowadzenia działań w cyberprzestrzeni. Znaczącym walorem rozprawy jest aktualność podjętej tematyki badawczej oraz poprawnie sformułowana koncepcja metodologiczna, która była podstawą konsekwentnie prowadzonych badań naukowych – w wymiarze teoretycznym i empirycznym.

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