

Recenzja

rozprawy doktorskiej pt.

„Hybrydowość i asymetryczność przyszłych wojen w cyberprzestrzeni”,

opracowanej przez mgr. Mateusza Rakowskiego

pod kierunkiem naukowym dr. hab. Andrzeja Dubickiego, prof. UŁ

Znaczenie podjętego tematu rozprawy doktorskiej

Współczesne środowisko bezpieczeństwa charakteryzuje się rosnącą złożonością, przenikaniem sfery militarnej i pozamilitarnej oraz postępującym zacieraniem granic między pokojem, kryzysem i wojną. W tych warunkach szczególnego znaczenia nabierają hybrydowość i asymetryczność konfliktów, rozumiane nie tyle jako całkowicie nowe typy wojny, ale jako istotne wymiary współczesnej rywalizacji strategicznej. Jak podkreśla prof. Marek Wrzosek „wojna hybrydowa łączy działania konwencjonalne, nieregularne, cybernetyczne, a w zależności od sytuacji, również inne sposoby destrukcji. Ponadto eksponuje się fakt, że jest prowadzona bez oficjalnego jej wypowiedzenia, przez co pozwala agresorowi na całkowite lub w znacznej części uniknięcie odpowiedzialności politycznej”¹.

Aktywność na granicy progu wojny oraz elementy wojny hybrydowej w różnych częściach świata (zwłaszcza rosyjskie działania w Ukrainie po aneksji Krymu w 2014 r.) sprawiły, że hybrydowość i asymetryczność działań zaczęły odgrywać istotną rolę w strategii bezpieczeństwa. Nie ulega więc wątpliwości, że temat rozprawy doktorskiej

¹: M. Wrzosek, *Scenariusz wojny hybrydowej – wnioski i doświadczenia*, [w:] *Międzynarodowy wymiar bezpieczeństwa w XXI wieku*, red. Robert Białoskurski, Puzikow Rustan, Jacek Zieliński, Siedlce 2019, s. 11.

„Hybrydowość i asymetryczność przyszłych wojen w cyberprzestrzeni”, jest ważnym zagadnieniem wymagającym naukowego wyjaśnienia. Autor dysertacji słusznie stwierdził, że „asymetryczność i hybrydowość konfliktów są historycznie trwałymi cechami, lecz ich współczesna dynamika została radykalnie przekształcona przez cyfryzację, która zwiększyła skalę, tempo i wielowarstwowość działań. Rewolucja informacyjna przyspieszyła obieg danych, obniżyła próg wejścia dla aktorów niepaństwowych i umożliwiła prowadzenie operacji poniżej progu wojny. Zatarło to granicę między pokojem oraz konfliktem, czyniąc cyberprzestrzeń środowiskiem stałej presji strategicznej”.

Praca ma charakter interdyscyplinarny na styku kilku dyscyplin naukowych – nauk o polityce i administracji, nauk o bezpieczeństwie oraz stosunków międzynarodowych. Z jednej strony jest to jej atut, gdyż autor umiejętnie wykorzystał teorie oraz metody badawcze z różnych dyscyplin w dziedzinie nauk społecznych. Jednak z drugiej strony wymogi formalne wymagają zakwalifikowanie dysertacji do konkretnej dyscypliny naukowej. Dlatego mimo początkowych wątpliwości, po dokładnej analizie stwierdzam, że praca „Hybrydowość i asymetryczność przyszłych wojen w cyberprzestrzeni” mieści się w dyscyplinie nauki o polityce i administracji i tak powinna być traktowana.

W tym kontekście należy podkreślić, że nauki o bezpieczeństwie jako stosunkowo młoda dyscyplina naukowa utworzona w 2011 r. wywodzi się nie tylko z dorobku nauk wojskowych, ale również nauk o polityce. To właśnie w naukach o polityce wielokrotnie podejmowano badania nad zagadnieniami bezpieczeństwa (zwłaszcza w aspekcie stosunków międzynarodowych)². Również dyscyplina stosunki międzynarodowe (utworzona w Polsce w 2022 r.) ma swoje korzenie w dziedzinie nauk o polityce. Nie może więc dziwić, że naukowcy z nauk o polityce w swoich pracach badawczych nadal podejmują ważne zagadnienia dotyczące bezpieczeństwa i tak jest właśnie w przypadku rozprawy doktorskiej Mateusza Rakowskiego.

² R. Szpyra, *Bezpieczeństwo militarne państwa*, Warszawa 2012, s. 20-21.

Ogólna charakterystyka pracy

Recenzowana rozprawa doktorska liczy 309 stron, w tym: spis treści, wstęp, pięć rozdziałów, zakończenie, wykazy rysunków i tabel oraz bibliografię. Jest to klasyczna struktura akademicka. Układ rozprawy uważam za przemyślany i poprawny.

We wstępie autor przedstawia kontekst rewolucji cyfrowej, sformułował przedmiot i cel badań, pytania badawcze, hipotezę, a także metody badawcze. Rozdział pierwszy został poświęcony pojęciu hybrydowości w teorii nowych wojen; rozdział drugi – asymetrii w konfliktach historycznych, współczesnych i przyszłych; rozdział trzeci – krytyce dotychczasowych systemów pojęciowych oraz sporowi o sens kategorii „wojna hybrydowa”; rozdział czwarty – analizie empirycznej wybranych konfliktów i operacji w cyberprzestrzeni; rozdział piąty – prognozie perspektyw rozwoju wojen cyfrowych oraz propozycji ram analitycznych w postaci probabilistycznego modelu ryzyka. W zakończeniu rozprawy autor odniósł się do problemów badawczych oraz do weryfikacji hipotezy postawionych we wstępie metodologicznym.

Praca ma wyraźnie teoretyczny charakter, choć zawiera też liczne studium przypadku (m.in. wojna w Zatoce Perskiej, operacje rosyjskie przeciw Gruzji i Ukrainie, ataki na infrastrukturę krytyczną, operacje informacyjne). Brak typowych badań empirycznych tak często stosowanych w rozprawach doktorskich nie obniża oceny pracy. Teoretyczny charakter dysertacji jest świadomym wyborem autora i udźwignął to trudne zadanie. Doceniam to, bo teoretyczne rozprawy doktorskie w dziedzinie nauk społecznych zdarzają się w ostatnich latach coraz rzadziej.

Ocena rozdziału metodologicznego

Zagadnienia metodologiczne autor przedstawił we wstępie dysertacji wyodrębniając odrębne podrozdziały: „Podstawy teoretyczne podejmowanej problematyki”, „Przedmiot i cel badań”, „Pytania badawcze”, „Hipoteza badawcza” oraz „Podejście i metody badawcze”. Jest to poprawne podejście. Jednak ze względu na wiele rozbudowanych elementów bardziej pragmatycznym rozwiązaniem byłoby przygotowanie krótkiego wstępu i odrębnego rozdziału metodologicznego.

Przedmiot badań – „podstawy teoretyczne i ewolucja zjawiska wojny, konfliktu, środowiska i zmiennych odnoszących się do tej problematyki jak również wykorzystanie nowoczesnych technologii oraz użycie cyberprzestrzeni we współczesnych i przyszłych konfliktach o naturze asymetrycznej, nieregularnej oraz hybrydowej” został wskazany prawidłowo. Mam natomiast zastrzeżenia co do sformułowania celu badań (a właściwie jego pierwszej części). Autor podkreślił bowiem, że „celem badań stało się dokonanie analizy i usystematyzowania dotychczasowej wiedzy odnoszącej się do różnych form i zjawisk związanych ze współczesnymi konfliktami (...)”. W rozprawie doktorskiej cel nie powinien ograniczać się do wskazania czynności badawczej. Analiza jest metodą lub etapem procesu badawczego, a nie pełnym rezultatem naukowym, do którego badanie ma doprowadzić.

Główny problem badawczy (pytanie badawcze) oceniam pozytywnie - „W jakim stopniu oraz w jaki sposób cyberprzestrzeń wpłynęła i będzie miała wpływ na współczesne konflikty oraz jaką rolę odgrywać będzie ona w przyszłych wojnach?”. Problem badawczy jest też spójny z dość rozbudowaną hipotezą, która również została sformułowana prawidłowo i jest możliwa do weryfikacji w procesie badawczym. Zaskakuje natomiast dlaczego autor nie przedstawił dodatkowych hipotez szczegółowych. Tym bardziej, że wcześniej zaprezentował 5 pytań szczegółowych. Niewątpliwie wpłynęłoby to lepszą jakością procesu badawczego.

Podsumowując wstęp zawierający zagadnienia metodologiczne należy uznać za prawidłowy. Autor nie ustrzegł się pewnych błędów, ale generalnie podszedł do metodologii badań w sposób właściwy i zgodny z regułami sztuki.

Ocena merytoryczna rozprawy

Po wstępie kolejne pięć rozdziałów zawiera merytoryczne rozważania. Układają się one razem w logiczną całość, a autor konsekwentnie krok po kroku realizuje swoje założenia badawcze.

W rozdziale pierwszym „Pojęcie hybrydowości w teorii nowych wojen” autor definiuje i porządkuje pojęcie wojny hybrydowej, pokazując jej historyczne korzenie w działaniach nieregularnych oraz ewolucję od starożytności po współczesne konflikty. Ważnym elementem rozważań jest spór definicyjny wokół „hybrydowości”. Autor słusznie

krytykuje używanie tego pojęcia jako „słowa-wytrychu”. Ponadto autor dysertacji zwrócił szczególną uwagę na rolę cyberprzestrzeni w hybrydowości – pokazując, jak środowisko sieciocentryczne jest wykorzystywane i kształtowane przez działania hybrydowe, w tym ataki na infrastrukturę krytyczną, operacje informacyjne i powiązania między państwem a sektorem prywatnym.

Rozdział jest bogaty w odniesienia do literatury przedmiotu i dobrze pokazuje spór definicyjny oraz krytykę pojęcia wojny hybrydowej (a także jego praktyczne konsekwencje). Miałem jednak wrażenie, że czasami autor zastosował nadmierne nagromadzenie cytatów, co zacierało jego własne opinie i przemyślenia.

Rozdział drugi „Asymetryczność w konfliktach dawnych, współczesnych i przyszłych” dotyczy asymetrii jako cechy konfliktów zbrojnych, od dawnych wojen po czasy współczesne, z naciskiem na porównanie skali asymetrii historycznej i nowoczesnej oraz jej znaczenia dla aktualnych i przyszłych wojen.

Autor skoncentrował się na wskazaniu jak różnice potencjału, organizacji i technologii przekładają się na strategie słabszych podmiotów (państwa, aktorzy niepaństwowi) oraz jak cyberprzestrzeń – ze względu na swoją strukturę i zależności – immanentnie sprzyja asymetrii. Szczególną uwagę zwrócił też na zachodnie, rosyjskie i chińskie koncepcje wykorzystania cyberprzestrzeni, strukturę asymetrycznych zagrożeń oraz udział aktorów pozapaństwowych w konfliktach cyfrowych.

Autor słusznie wskazał, że asymetria nie jest nowym zjawiskiem, lecz zawsze stanowiła istotny element prowadzenia konfliktów. Cennym elementem jest również refleksja nad „sprywatyzowaną” przemocą i rosnącą rolą aktorów niepaństwowych, co koresponduje z debatą o erozji monopolu państwa na użycie siły. Autor słusznie zauważył, że współczesne konflikty charakteryzują się często wysoką asymetrią między stronami, ale jednocześnie pozwalają słabszym podmiotom wykorzystać przewagi taktyczne i operacyjne.

W kolejnym rozdziale „Porównanie i krytyka koncepcji hybrydowości i asymetryczności” autor zajął się krytyczną analizą i porównaniem koncepcji hybrydowości oraz asymetryczności, wskazując braki w aktualnej wiedzy i niespójności systemów pojęciowych w różnych tradycjach strategicznych. Ciekawym aspektem jest

zestawieniu perspektywy zachodniej, rosyjskiej i chińskiej i wskazanie na odmienne rozumienie hybrydowości, asymetrii oraz ich miejsca w doktrynach.

Mocną stroną rozdziału jest krytyczna refleksja nad metaforami i kalkami pojęciowymi, które utrudniają adekwatne zrozumienie zjawisk cyfrowych. Autor słusznie wskazał, że cyberprzestrzeń wymyka się logice linii i granic, a ataki mogą pochodzić z nieprzewidzianych kierunków, w tym z wnętrza własnych struktur. Zwrócił też uwagę na znaczenie problemu atrybucji, roli małych grup hakerskich oraz powiązań między przestępczością, polityką i wojskowością. Rozdział ma dużą wartość diagnostyczną - pokazuje ograniczenia dotychczasowych paradygmatów i potrzebę nowych ram analitycznych, które nie będą prostym „transponowaniem” tradycyjnych kategorii.

W następnym rozdziale „Analiza konfliktów czasów rewolucji cyfrowej” autor przedstawiał oblicze nowych wojen poprzez analizę konfliktów toczących się w epoce rewolucji cyfrowej, od pierwszych zmian pola walki po współczesne operacje w cyberprzestrzeni. Skoncentrował się na trzech fazach: dominacji wojska w zarządzaniu informacją, rozpadzie monopolu narracji oraz wzroście znaczenia asymetrycznych aktorów cyfrowych, analizując konsekwencje tych przeobrażeń dla bezpieczeństwa międzynarodowego. Szczególną uwagę zwrócił na wyzwania dla prawa międzynarodowego i NATO, znaczenie sektora prywatnego, rosnącą rolę sztucznej inteligencji i automatyzacji w atakach oraz infrastruktury krytycznej jako kluczowego celu operacji cyfrowych.

Ten rozdział stanowi część bardziej empiryczną, gdzie autor analizuje konkretne konflikty i operacje od początków rewolucji cyfrowej do współczesności, konfrontując teoretyczne koncepcje z realnymi działaniami. Rozdział jest bogaty w przykłady i pokazuje praktyczne zastosowanie koncepcji hybrydowości i asymetrii w różnych kontekstach geopolitycznych. Muszę jednak zauważyć, że wartość pracy wzrosłaby, gdyby autor zastosował bardziej wyraźnie zarysowaną strukturę studiów przypadków (*case studies*), co wzmocniłoby rygor analityczny.

Wreszcie rozdział piąty „Prognoza perspektyw i nowe ramy analizy wojen cyfrowych” dotyczy prognozy rozwoju wojen cyfrowych i przedstawia nowe ramy analizy konfliktów w cyberprzestrzeni, wychodząc od krytyki tradycyjnych metafor wojny w

odniesieniu do sieci. Autor przedstawił własną propozycję probabilistycznego, rekurencyjnego modelu oceny ryzyka, jego architekturę, metryki i możliwości integracji z procesami decyzyjnymi na poziomie strategicznym, operacyjnym i taktycznym jako kluczowy kierunek myślenia o przyszłych wojnach cyfrowych.

Rozdział piąty jest kluczowy z punktu widzenia oryginalnego wkładu pracy. Autor krytycznie omówił dotychczasowe próby prognozy rozwoju wojen cyfrowych i wskazał na napięcie między potrzebą przewidywania a świadomością ograniczeń poznawczych. Pokazał, że wiele prognoz nadmiernie eksponowało czynniki technologiczne, nie doceniając dynamiki politycznej i społecznej. Na uwagę zasługuje zwłaszcza zaproponowane przez autora alternatywne podejście oparte na probabilistycznym modelu oceny ryzyka, który uwzględnia prawdopodobieństwo, skutki i podatności systemów.

Rozdział końcowy jest najbardziej twórczy. Pokazuje własną propozycję ram analitycznych dla badania wojen w cyberprzestrzeni, krytycznie przegląda istniejące paradygmaty i wskazuje na potrzebę myślenia w kategoriach systemowego zarządzania ryzykiem i niepewnością

Ocena zakończenia rozprawy

Zakończenie rozprawy stanowi syntetyczne przedstawienie wniosków z pracy. Autor podzielił je na kilka części: „Usystematyzowanie kontekstu badań i podstaw teoretycznych podejmowanej problematyki”, „Odpowiedź na pytania badawcze”, „Weryfikacja hipotezy badawczej” oraz „Wnioski”. Takie podejście należy ocenić bardzo pozytywnie.

Autor dysertacji dość ostrożnie uznał w zakończeniu, że „sformułowana we wstępie hipoteza zasadniczo znajduje potwierdzenie w przeprowadzonych analizach”. Należy się z tym zgodzić. Merytoryczne wnioski z pięciu rozdziałów potwierdzają, że „cyberprzestrzeń nie funkcjonuje już jako odrębna domena, lecz przenika strukturalnie inne obszary działań, prowadząc do bezprecedensowego sprzężenia informacji, infrastruktury i operacji. Ścisłe powiązanie środowiska sieciocentrycznego z innymi domenami wzmacnia asymetrię oraz nieregularność konfliktów”.

W kontekście odpowiedzi na postawione pytania badawcze tym bardziej należy żałować, że autor nie zdecydował się na przedstawienie hipotez szczegółowych (spójnych z pytaniami badawczymi). Jak już wspomniałem podniosłoby to wartość pracy.

Zakończenie w sposób spójny domyka narrację o hybrydowości, asymetrii oraz roli cyberprzestrzeni w przyszłych konfliktach. Choć część postulatów ma charakter ogólny i mogłaby zostać doprecyzowana w formie bardziej konkretnych rekomendacji dla polityki bezpieczeństwa, co wzmocniłoby praktyczny wymiar dysertacji.

Wniosek końcowy

Problematyka recenzowanej rozprawy mieści się w zakresie dyscypliny nauk o polityce i administracji i porusza ważne problemy bezpieczeństwa. Analizowana rozprawa prezentuje szerokie, interdyscyplinarne ujęcie hybrydowości i asymetryczności przyszłych wojen w cyberprzestrzeni, osadzając je zarówno w klasycznych teoriach wojny, jak i we współczesnej debacie o cyberbezpieczeństwie i nowych formach konfliktu. Należy podkreślić, że mocną stroną pracy jest również bogata baza źródłowa (monografie, artykuły, dokumenty doktrynalne, raporty techniczne), krytyczna refleksja nad istniejącymi pojęciami oraz propozycja własnych ram analitycznych (szczególnie w rozdziale piątym).

Autor wykazał się dużą wiedzą na temat badanego zagadnienia i prawidłowo przeprowadził proces badawczy. Oczywiście nie ustrzegł się też pewnych uchybień i niedoskonałości, co jest normalne na tym etapie rozwoju naukowego. Praca zasługuje na uznanie i posiada wiele mocnych stron, co starałem się mocno uwypuklić w recenzji.

Stwierdzam, że rozprawa doktorska pt. „Hybrydowość i asymetryczność przyszłych wojen w cyberprzestrzeni”, opracowanej przez mgr. Mateusza Rakowskiego pod kierunkiem naukowym dr. hab. Andrzeja Dubickiego, prof. UŁ stanowi oryginalne rozwiązanie problemu naukowego, a także odpowiada warunkom określonym w przepisach ustawy z dnia 20 lipca 2018 roku – Prawo o szkolnictwie wyższym i nauce.