Dr hab. Michał Polak,
profesor Politechniki Koszalińskiej
Ul. Cisowa 19, 75-644 Koszalin

Koszalin, 10 sierpnia 2026 r.

Recenzja rozprawy doktorskiej mgr. Mateusza Rakowskiego pt. „Hybrydowość i asymetryczność przyszłych wojen w cyberprzestrzeni", napisanej pod kierunkiem naukowym dr. hab. Andrzeja Dubickiego, prof. Uniwersytetu Łodzkiego

Temat, cel pracy oraz założenia badawcze

Problematyka przemian współczesnych konfliktów zbrojnych, wpływu rozwoju technologicznego na funkcjonowanie państw oraz znaczenia cyberprzestrzeni w stosunkach międzynarodowych należy obecnie do istotnych obszarów zainteresowania badaczy reprezentujących nauki społeczne. Rosnąca zależność państw, ich administracji, sił zbrojnych i społeczeństw od infrastruktury cyfrowej powoduje, że cyberprzestrzeń nie może być postrzegana wyłącznie jako techniczne środowisko wymiany informacji. Stała się ona również przestrzenią rywalizacji politycznej, gospodarczej i militarnej, w której uczestniczą zarówno państwa, jak i aktorzy pozapaństwowi.

Przemiany te nabrały szczególnego znaczenia w ostatnich kilkunastu latach. Aneksja Krymu przez Federację Rosyjską w 2014 r., rozwój operacji informacyjnych, cyberataki wymierzone w infrastrukturę państwową i prywatną, a następnie pełnoskalowa agresja Rosji na Ukrainę od lutego 2022 r. spowodowały wzrost zainteresowania kategoriami wojny hybrydowej, konfliktów asymetrycznych, działań prowadzonych poniżej progu wojny czy też szerzej rozumianych operacji w cyberprzestrzeni. Jednocześnie coraz większym problemem badawczym stało się określenie rzeczywistej przydatności tych pojęć oraz ustalenie, czy opisują one jakościowo nowe zjawiska, czy raczej współczesne warianty znanych wcześniej sposobów prowadzenia rywalizacji i konfliktów.

W ten obszar badań wpisuje się rozprawa doktorska mgr. Mateusza Rakowskiego pt. *Hybrydowość i asymetryczność przyszłych wojen w cyberprzestrzeni*. Praca została przygotowana w dyscyplinie nauki o polityce i administracji. Podjęty temat ma niewątpliwie charakter interdyscyplinarny, gdyż łączy elementy politologii, stosunków międzynarodowych, polemologii, studiów strategicznych i badań nad bezpieczeństwem z zagadnieniami technologicznymi. Nie mam jednak wątpliwości, że zasadniczy przedmiot analizy – funkcjonowanie państw, aktorów międzynarodowych, strategie i doktryny, relacje pomiędzy

sektorem publicznym i prywatnym oraz polityczne konsekwencje rozwoju cyberprzestrzeni – pozwala osadzić rozprawę w dyscyplinie nauki o polityce i administracji.

Autor przyjął bardzo szeroki przedmiot badań, obejmujący podstawy teoretyczne i ewolucję zjawiska wojny i konfliktu oraz zastosowanie współczesnych technologii i cyberprzestrzeni w konfliktach asymetrycznych, nieregularnych i hybrydowych. Za cel badań przyjął usystematyzowanie dotychczasowej wiedzy na temat tych zjawisk, określenie kierunków zmian w sposobie prowadzenia wojen oraz zaproponowanie ram teoretycznych pozwalających analizować przyszłe konflikty w warunkach niepewności.

Cel ten oceniam jako ambitny i odpowiadający randze rozprawy doktorskiej. Jednocześnie jego sformułowanie zdradza jedną z cech całej pracy – bardzo szeroki zakres rozważań. Doktorant podejmuje bowiem próbę połączenia analizy historycznej, studiów nad współczesnymi konfliktami, problematyki technologicznej oraz prognozowania przyszłości. Niewątpliwie wzbogaca to rozprawę, ale miejscami powoduje również nadmierne rozproszenie problematyki.

Mgr Mateusz Rakowski prawidłowo sformułował zasadnicze pytanie badawcze: w jakim stopniu i w jaki sposób cyberprzestrzeń wpłynęła i będzie wpływać na współczesne konflikty oraz jaką rolę będzie odgrywać w przyszłych wojnach. Uzupełnił je pięcioma pytaniami szczegółowymi odnoszącymi się m.in. do sposobu definiowania cyberprzestrzeni, hybrydowości i asymetrii, przyszłej integracji różnych form prowadzenia walki, odhumanizowania działań oraz możliwości ograniczania zależności państw od środowiska sieciocentrycznego.

Pytania te wyznaczają logiczny kierunek badań, chociaż można odnieść wrażenie, że część z nich ma bardzo szeroki, wręcz prognostyczny charakter. Dotyczy to zwłaszcza pytań o przyszły kierunek ewolucji działań w cyberprzestrzeni. Doktorant sam zresztą dochodzi w dalszej części pracy do wniosku, że podstawowym problemem jest niemożność wiarygodnego przewidywania konkretnych form przyszłych konfliktów.

Podobną uwagę można sformułować wobec hipotezy badawczej. Ma ona charakter rozbudowany i w rzeczywistości mieści w sobie kilka odrębnych założeń: wzrost znaczenia cyberprzestrzeni, wzrost asymetryczności i nieregularności działań, rosnące znaczenie operacji informacyjnych oraz przewidywane dążenie państw do częściowego ograniczania zależności infrastruktury krytycznej od środowiska cyfrowego. Z metodologicznego punktu widzenia bardziej przejrzyste byłoby rozdzielenie tego założenia na hipotezę główną oraz kilka hipotez szczegółowych. Nie traktuję jednak tego jako poważnego uchybienia, ponieważ wszystkie

wskazane elementy zostały następnie poddane analizie, a Autor odniósł się do nich w zakończeniu pracy.

Układ i treść rozprawy

Przekazana mi do recenzji rozprawa liczy 309 stron. Tekst zasadniczy, wraz z zakończeniem, obejmuje 258 stron. Następnie zamieszczono wykazy rysunków, tabel i skrótów oraz obszerną bibliografię. Rozprawa składa się ze wstępu, pięciu rozdziałów oraz zakończenia.

Konstrukcja ma zasadniczo charakter problemowy, uzupełniony elementami układu chronologicznego. Kolejne rozdziały prowadzą czytelnika od historycznych i konceptualnych podstaw hybrydowości i asymetrii, poprzez krytyczną analizę współczesnych koncepcji, aż do konfliktów ery cyfrowej i próby wskazania kierunków ich dalszego rozwoju. W mojej ocenie jest to rozwiązanie prawidłowe.

Rozdział pierwszy poświęcony został pojęciu hybrydowości w teorii nowych wojen. Autor nie ogranicza się do współczesnego rozumienia wojny hybrydowej, lecz podejmuje próbę ukazania historycznych antecedencji łączenia działań regularnych i nieregularnych. Rozważania rozpoczyna od starożytności, następnie przechodzi przez średniowiecze i epokę nowożytną do konfliktów XX i XXI wieku. Cennym elementem tej części jest konsekwentne podważanie przekonania, jakoby hybrydowość była zjawiskiem całkowicie nowym. Autor słusznie zwraca uwagę, że łączenie różnych instrumentów oddziaływania oraz wykorzystywanie sił nieregularnych towarzyszy wojnom od stuleci.

Przyjęcie tak szerokiej perspektywy historycznej ma jednak również słabszą stronę. Stosowanie współczesnych kategorii analitycznych do wydarzeń starożytnych czy średniowiecznych zawsze wiąże się z ryzykiem pewnego anachronizmu. Doktorant jest tego problemu świadomy, niemniej momentami odnosi się wrażenie, że historyczne przykłady są podporządkowywane współczesnej definicji hybrydowości. Zdecydowanie ważniejsze są dla głównego problemu rozprawy późniejsze partie rozdziału, odnoszące się bezpośrednio do cyberprzestrzeni i współczesnych aktorów politycznych.

Rozdział drugi dotyczy asymetryczności w konfliktach dawnych, współczesnych i przyszłych. Podobnie jak w pierwszej części rozprawy Autor szeroko wykorzystuje analizę historyczną, aby wykazać trwałość zjawiska asymetrii. Zaletą tego podejścia jest odejście od częstego w literaturze traktowania konfliktu asymetrycznego jako produktu ostatnich dekad. Asymetria potencjałów i poszukiwanie sposobów wykorzystania słabości silniejszego przeciwnika należą przecież do najbardziej trwałych elementów historii wojen.

Cyberprzestrzeń nie stworzyła asymetrii, lecz – jak przekonująco argumentuje Doktorant – istotnie zwiększyła jej skalę i znaczenie.

Za szczególnie wartościową uważam część rozdziału odnoszącą się do odmiennych sposobów postrzegania cyberprzestrzeni przez państwa zachodnie, Federację Rosyjską i Chińską Republikę Ludową. Pozwala ona uniknąć ograniczenia całej analizy do zachodnich kategorii pojęciowych oraz pokazuje związki pomiędzy kulturą strategiczną, systemem politycznym i sposobem postrzegania przestrzeni informacyjnej.

Rozdział trzeci ma charakter bardziej teoretyczny i krytyczny. Autor porównuje zachodnie, rosyjskie i chińskie spojrzenie na hybrydowość oraz asymetrię, a następnie podejmuje próbę oceny przydatności obu kategorii. Jest to – w mojej ocenie – jedna z ważniejszych części rozprawy z punktu widzenia nauk o polityce i administracji. Doktorant pokazuje bowiem, że określenie „wojna hybrydowa" z kategorii analitycznej stopniowo przekształcało się również w kategorię dyskursu politycznego i publicystycznego. Cenne jest krytyczne podejście Autora do przypisywania Federacji Rosyjskiej tzw. „doktryny Gierasimowa". Doktorant dostrzega problem mechanicznego przenoszenia zachodnich kategorii na rosyjską myśl strategiczną i zwraca uwagę na odmienność rosyjskiego języka opisu konfliktu. W konsekwencji dochodzi do wniosku, że pojęcie wojny hybrydowej jest zbyt szerokie, aby stanowiło precyzyjne narzędzie analityczne.

Rozdział czwarty dotyczy konfliktów okresu rewolucji cyfrowej. Autor przechodzi tu od historyczno-teoretycznych podstaw do analizy przemian realnego środowiska konfliktów. Szczególnie interesująco przedstawia proces utraty przez państwo monopolu na zarządzanie przekazem informacyjnym. Rozwój Internetu, mediów społecznościowych, działalność podmiotów pozapaństwowych, organizacji terrorystycznych i środowisk hakerskich doprowadziły do zasadniczej zmiany sposobu tworzenia, dystrybucji i kontroli informacji.

Ważnym elementem rozdziału jest analiza wojny rosyjsko-ukraińskiej. Autor trafnie zauważa, że konflikt ten nie potwierdził najbardziej radykalnych prognoz dotyczących dominującego znaczenia cyberwojny. Znacznie większe znaczenie dla przebiegu działań miały m.in. systemy bezzałogowe, klasyczna artyleria, rozpoznanie, logistyka oraz wykorzystanie informacji w dowodzeniu. Cyberoperacje okazały się jednym z elementów konfliktu, a nie jego substytutem. Oceniam tę obserwację jako ważną, ponieważ chroni rozprawę przed technologicznym determinizmem.

Ostatni, piąty rozdział zawiera próbę określenia perspektyw rozwoju konfliktów cyfrowych i zaproponowania nowych ram ich analizy. Autor poddaje krytyce mechaniczne przenoszenie terminologii właściwej tradycyjnemu polu walki do cyberprzestrzeni, a następnie

formułuje koncepcję stałej niepewności jako jednego z podstawowych uwarunkowań funkcjonowania państw w środowisku cyfrowym. Najbardziej oryginalnym elementem rozdziału jest przedstawienie probabilistycznego modelu oceny ryzyka. Model ma integrować informacje techniczne, operacyjne i strategiczne oraz umożliwiać aktualizowanie ocen w miarę pojawiania się nowych danych. Jego założeniem jest również możliwość prowadzenia analizy na szczeblu taktycznym, operacyjnym i strategicznym.

Oceniam ten fragment przede wszystkim z punktu widzenia jego osadzenia w przyjętym problemie badawczym i użyteczności dla analiz politologicznych i strategicznych. Nie ulega wątpliwości, że sam rachunek prawdopodobieństwa, twierdzenie Bayesa czy modelowanie ryzyka nie stanowią nowych rozwiązań matematycznych. Wartość propozycji Doktoranta widzę raczej w próbie ich połączenia z analizą strategiczną oraz zastosowania do wielopoziomowej oceny zagrożeń w cyberprzestrzeni.

Autor zachowuje przy tym potrzebną ostrożność. Wyraźnie przyznaje, że zaproponowana konstrukcja nie jest gotowym, empirycznie zweryfikowanym narzędziem predykcyjnym i wymaga dalszej kalibracji na danych rzeczywistych. Jest to ważne zastrzeżenie. Z tego względu zaproponowany model traktowałbym przede wszystkim jako autorską ramę analityczną i propozycję dalszych badań, a nie jako zweryfikowany system umożliwiający przewidywanie przyszłych cyberkonfliktów.

Rozprawę wieńczy obszerne zakończenie. Oceniam je pozytywnie. Autor powraca w nim do postawionych pytań badawczych, przeprowadza weryfikację hipotezy i eksponuje najważniejsze ustalenia. Jest to rozwiązanie szczególnie pożądane w pracy o tak szerokim zakresie rzeczowym.

Warsztat badawczy – metodologia, źródła i literatura

Strona badawcza rozprawy stanowi niewątpliwie jeden z jej mocnych elementów. Doktorant wykorzystał analizę systemową, porównawczą i historyczną. Odwołuje się również do paradygmatu interpretatywnego, syntezy, generalizacji, indukcji i dedukcji oraz abstrahowania izolującego. Taki dobór odpowiada interdyscyplinarnemu charakterowi problematyki. Szczególnie uzasadnione wydają się analiza porównawcza oraz historyczna. Pierwsza pozwala Autorowi zestawiać podejście zachodnie, rosyjskie i chińskie, druga natomiast służy weryfikowaniu założenia, czy hybrydowość i asymetryczność są rzeczywiście jakościowo nowymi elementami konfliktu.

Pewien niedosyt budzi natomiast stopień operacjonalizacji tych metod. Wstęp zawiera ich obszerne omówienie, jednak mniej miejsca przeznaczono na jednoznaczne przedstawienie

sposobu doboru konkretnych przypadków analizowanych w dalszych rozdziałach. Autor wielokrotnie odwołuje się do przykładów historycznych oraz współczesnych cyberincydentów, jednak kryteria ich reprezentatywności mogłyby zostać przedstawione bardziej precyzyjnie. Ułatwiłoby to czytelnikowi rozróżnienie pomiędzy przykładem ilustrującym argument a przypadkiem stanowiącym materiał służący jego weryfikacji.

W rozprawie dostrzegam również pewne napięcie metodologiczne pomiędzy interpretatywnym, historyczno-porównawczym sposobem badania zjawisk politycznych w pierwszych czterech rozdziałach a ilościową logiką modelu zaprezentowanego pod koniec pracy. Nie jest to połączenie nieprawidłowe, ale przejście pomiędzy obiema perspektywami mogłoby zostać przez Autora dokładniej wyjaśnione. Czytelnik powinien otrzymać jednoznaczną odpowiedź, w jaki sposób jakościowe ustalenia dotyczące strategii państw i zachowań aktorów mają być przekształcane w wartości wejściowe wykorzystywane przez model oceny ryzyka.

Baza wykorzystanej literatury i materiałów źródłowych jest bardzo obszerna. Autor wykorzystuje dokumenty strategiczne i doktrynalne USA, NATO, Unii Europejskiej, Federacji Rosyjskiej i Chin, publikacje agencji rządowych, służb oraz zespołów zajmujących się cyberbezpieczeństwem. Sięga również do raportów specjalistycznych przedsiębiorstw sektora cyberbezpieczeństwa. W przypadku analizowania konkretnych operacji cybernetycznych jest to często materiał konieczny, ponieważ właśnie podmioty techniczne dysponują najbardziej szczegółowymi informacjami dotyczącymi przebiegu ataków.

Literatura naukowa jest szeroka, międzynarodowa i w znacznej części aktualna. Autor wykorzystuje zarówno klasyczne prace dotyczące teorii wojny, jak i współczesny dorobek związany z nowymi wojnami, hybrydowością, asymetrią, cyberkonfliktem i odstraszaniem. Widoczna jest również dbałość o wykorzystanie literatury reprezentującej różne perspektywy kulturowe i polityczne. Na uznanie zasługuje fakt, że literatura obejmuje wiele publikacji z ostatnich lat, w tym z lat 2024–2025. Przy tak szeroko zakreślonym temacie nie sposób oczywiście oczekiwać uwzględnienia wszystkich ważnych pozycji. Można jednak wskazać kilka kierunków, które warto byłoby uwzględnić szerzej w dalszych badaniach. Dotyczy to zwłaszcza współczesnych empirycznych analiz ograniczonej skuteczności cyberoperacji oraz koncepcji trwałej rywalizacji w cyberprzestrzeni, określanej jako *cyber persistence*. W przyszłości przydatne mogłoby być szersze odniesienie do tej tematyki, np. na przykładzie prac Brandona Valeriano i Ryana Manessa, Michaela Fischerkellera, Emily Goldman i Richarda Harknetta czy Lennarta Maschmeyera. Nieobecności tych publikacji nie traktuję jednak jako istotnej wady rozprawy, lecz jako wskazanie możliwego kierunku pogłębienia analizy.

Interesującym i zarazem wymagającym odnotowania elementem metodologicznym jest ujawnienie przez Autora korzystania podczas przygotowywania rozprawy z narzędzi uczenia maszynowego i modeli językowych. Doktorant wskazuje, że były one stosowane m.in. przy tłumaczeniu źródeł oraz wspieraniu redakcji i korekty tekstu. Pozytywnie oceniam samo transparentne poinformowanie o wykorzystaniu tych narzędzi. Przygotowując ewentualną wersję książkową rozprawy, warto jednak dokładniej wyjaśnić zakres takiego wykorzystania oraz procedury weryfikacji tłumaczeń wykonanych w językach nieznanych Autorowi.

Wartość naukowa i oryginalność rozprawy

Wkład rozprawy w stan badań oceniam pozytywnie. Nie polega on, moim zdaniem, na udowodnieniu, że istnieją wojny hybrydowe lub asymetryczne, lecz w znacznej mierze na zakwestionowaniu użyteczności tak prostego sposobu ich kategoryzowania.

Za ważne ustalenie uważam wykazanie historycznej trwałości hybrydowości i asymetrii. Cyberprzestrzeń nie stworzyła tych zjawisk. Zmieniła natomiast tempo działań, liczbę podmiotów zdolnych do wywierania wpływu, koszty wejścia do konfliktu oraz możliwość osiągania skutków strategicznych przez relatywnie słabych aktorów.

Istotną wartość poznawczą ma również porównanie zachodnich, rosyjskich i chińskich sposobów myślenia o konfliktach. Autor pokazuje, jak niebezpieczne może być analizowanie obcych kultur strategicznych wyłącznie przy pomocy kategorii utworzonych w zachodnim dyskursie naukowym.

Interesujące jest także zakwestionowanie przekonania o przyszłej dominacji cyberwojny. Doświadczenia wojny rosyjsko-ukraińskiej wskazują, że cyberprzestrzeń niezwykle silnie wpływa na prowadzenie wojny, ale nie zastępuje walki kinetycznej. W tym sensie przyszłość należy raczej do konfliktów wielodomenowych, w których komponent cyfrowy będzie przenikał działania prowadzone na lądzie, morzu, w powietrzu czy przestrzeni kosmicznej.

Za autorską propozycję należy uznać sformułowanie paradygmatu stałej niepewności i próbę jego przełożenia na wielopoziomową ocenę ryzyka. Jak zaznaczyłem wcześniej, sama matematyczna konstrukcja wykorzystywanych narzędzi nie jest nowa. Nowość rozwiązania wynika raczej ze sposobu ich integracji z politologiczną i strategiczną analizą cyberprzestrzeni. Trzeba jednocześnie wyraźnie zastrzec, że model nie został jeszcze wystarczająco zweryfikowany empirycznie. Sam Autor przyznaje, że wymaga on kalibracji, dalszych testów i zasilenia reprezentatywnymi danymi. Oceniam tę świadomość ograniczeń pozytywnie.

Uwagi ogólne i postulaty

Pomimo wysokiej oceny rozprawy, jej lektura prowadzi również do kilku uwag krytycznych. Pierwsza dotyczy zakresu pracy. Autor podjął temat niezwykle rozległy, prowadząc narrację od starożytności do prognozowania przyszłości konfliktów cyfrowych. W niektórych fragmentach szerokość spojrzenia odbywa się kosztem głębokości analizy. Rozbudowane partie historyczne w dwóch pierwszych rozdziałach są interesujące i pozwalają wykazać trwałość analizowanych zjawisk, ale część przykładów można byłoby ograniczyć bez szkody dla zasadniczych wniosków pracy. Pozwoliłoby to więcej miejsca poświęcić empirycznej analizie współczesnych operacji cybernetycznych.

Druga uwaga dotyczy relacji pomiędzy tytułem rozprawy a jej ostatecznymi ustaleniami. Tytuł eksponuje „przyszłe wojny", podczas gdy jednym z ważniejszych wniosków Autora jest niemożność wiarygodnego przewidywania ich konkretnego charakteru. Nie uważam tego za sprzeczność dyskwalifikującą pracę. Przeciwnie, dojście do takiego wniosku może być wynikiem prawidłowo przeprowadzonych badań. Wydaje się jednak, że bardziej precyzyjne byłoby mówienie o określaniu warunków, trendów i ryzyk przyszłych konfliktów niż o ich prognozowaniu w ścisłym rozumieniu tego słowa.

Podobny problem dotyczy hybrydowości. Jest ona jednym z dwóch głównych pojęć umieszczonych w tytule rozprawy, a ostatecznie Autor dochodzi do daleko idącej krytyki jej przydatności analitycznej, stwierdzając wręcz postępującą utratę naukowego znaczenia tej kategorii. Jest to interesujący rezultat badań, ale podczas obrony warto byłoby, aby Doktorant jednoznacznie wyjaśnił, dlaczego mimo tak krytycznej oceny pozostawił hybrydowość jako centralny element tytułu rozprawy.

Kolejna uwaga dotyczy terminologii. W pracy pojawiają się pojęcia cyberprzestrzeni, środowiska sieciocentrycznego, przestrzeni cyfrowej, przestrzeni informatycznej oraz przestrzeni informacyjnej. Autor na ogół prawidłowo rozróżnia ich znaczenie, jednak przy tak szerokiej problematyce szczególnie ważna jest maksymalna konsekwencja terminologiczna. Dotyczy to również rozróżnienia cyberoperacji, cyberwojny, działań informacyjnych i działań prowadzonych poniżej progu konfliktu zbrojnego.

W odniesieniu do proponowanego modelu ryzyka najważniejsza uwaga nie dotyczy jego konstrukcji matematycznej, ale stanu weryfikacji. Model pozostaje w dużej mierze propozycją teoretyczną. Aby można było jednoznacznie ocenić jego wartość predykcyjną i praktyczną, należałoby przetestować go na większym zbiorze rzeczywistych przypadków. W obecnym kształcie jego znaczenie widzę przede wszystkim jako uporządkowanie zmiennych

i mechanizmów, które mogą zostać wykorzystane w dalszych badaniach. Takie ograniczenie Autor zresztą sam dostrzega, co przemawia na jego korzyść.

Mam również uwagę dotyczącą wykorzystania w rozprawie materiałów pochodzących od instytucji państwowych, służb, zespołów CERT/CSIRT oraz prywatnych firm zajmujących się cyberbezpieczeństwem. W przypadku badań nad cyberoperacjami źródła tego rodzaju są często niezbędne, ponieważ zawierają dane techniczne i operacyjne niedostępne w klasycznej literaturze naukowej. Ich wykorzystanie wymaga jednak szczególnie konsekwentnej krytyki źródła, uwzględniającej zarówno interes i pozycję instytucji publikującej dany raport, jak również stosowaną przez nią metodologię oraz ograniczoną możliwość niezależnej weryfikacji części informacji. Dotyczy to w szczególności problemu atrybucji cyberataków. Doktorant wykazuje świadomość tej trudności i generalnie konfrontuje informacje pochodzące z różnych źródeł, jednak warto byłoby jeszcze wyraźniej zaznaczyć, według jakich kryteriów oceniał wiarygodność przypisania określonych operacji konkretnym państwom, służbom lub grupom APT oraz w jakim zakresie konfrontował takie ustalenia z materiałami pochodzącymi z innych, niezależnych źródeł. Informacja taka mogłaby z powodzeniem znaleźć się w części metodologicznej pracy.

Uwagi szczegółowe i redakcyjne

Strona redakcyjna rozprawy jest generalnie poprawna, jednak w tak obszernej pracy nie udało się uniknąć drobnych usterek językowych i edytorskich. Przykładowo na s. 16 znalazło się niezręczne sformułowanie pytania badawczego: „w jakim kierunku będzie ewoluowały działania", wymagające korekty gramatycznej. Na s. 19 występują m.in. literówki w określeniach metod badawczych. W części prezentującej model zauważalne są drobne usterki redakcyjne, w tym powtórzenia oraz niespójności w numeracji kolejnych elementów wyliczeń. Ujednolicenia wymaga również sposób zapisu niektórych wzorów i oznaczeń probabilistycznych, zwłaszcza prawdopodobieństwa warunkowego. Są to kwestie przede wszystkim techniczne i redakcyjne, które należałoby zweryfikować przed ewentualnym przygotowaniem rozprawy do publikacji.

Bibliografia jest bardzo obszerna, ale wymaga jeszcze końcowej korekty technicznej. Zauważyć można pojedyncze literówki w tytułach, nazwach czasopism i datach publikacji.

Powyższe uchybienia są łatwe do usunięcia na etapie przygotowania rozprawy do druku i nie wpływają na jej ocenę merytoryczną.

Konkluzja

Rozprawa doktorska mgr. Mateusza Rakowskiego pt. *Hybrydowość i asymetryczność przyszłych wojen w cyberprzestrzeni* jest dojrzałym i ambitnym opracowaniem naukowym podejmującym aktualny i istotny problem badawczy. Autor wykazał się bardzo dobrym rozpoznaniem krajowej i międzynarodowej literatury przedmiotu, umiejętnością wykorzystania szerokiego i zróżnicowanego materiału, jak również zdolnością krytycznego odnoszenia się do utrwalonych w literaturze pojęć i interpretacji. Szczególnie pozytywnie oceniam odejście od bezkrytycznego traktowania wojny hybrydowej jako jakościowo nowego zjawiska, porównanie perspektyw zachodniej, rosyjskiej i chińskiej oraz wnioski dotyczące roli cyberprzestrzeni jako środowiska przenikającego wszystkie współczesne domeny konfliktu.

Zaletą rozprawy jest również umiejętność korygowania początkowych założeń w konfrontacji z materiałem badawczym. Autor nie podtrzymuje prostych futurystycznych wizji cyberwojny zastępującej działania kinetyczne. Przeciwnie, wskazuje na trwałość klasycznych mechanizmów wojny oraz na wspierającą, przenikającą i wzmacniającą rolę cyberprzestrzeni.

Zaproponowany probabilistyczny model oceny ryzyka traktuję jako interesującą autorską propozycję uporządkowania wyników badań oraz możliwy punkt wyjścia do dalszych analiz. Jego pełna ocena praktyczna będzie możliwa dopiero po przeprowadzeniu szerszej walidacji empirycznej, co sam Doktorant dostrzega i wyraźnie zaznacza.

Sformułowane w niniejszej recenzji uwagi krytyczne mają przede wszystkim charakter metodologiczny, porządkujący i redakcyjny. Nie podważają zasadniczych wyników badań ani mojej pozytywnej oceny rozprawy.

W mojej ocenie rozprawa mgr. Mateusza Rakowskiego spełnia wymagania art. 187 ust. 1 i 2 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce. Doktorant wykazał się znajomością problematyki właściwej dla nauk o polityce i administracji, umiejętnością samodzielnego prowadzenia badań, krytycznej analizy zróżnicowanych źródeł i literatury oraz formułowania własnych wniosków i propozycji badawczych.

W związku z powyższym wnoszę o dopuszczenie mgr. Mateusza Rakowskiego do publicznej obrony rozprawy doktorskiej i dalszych etapów postępowania w sprawie nadania stopnia doktora w dyscyplinie nauki o polityce i administracji.