

RECENZJA

rozprawy doktorskiej mgr. inż. Macieja Jędrzejewskiego pt.

CYBERBEZPIECZEŃSTWO W DOKTRYNIE OBRONNEJ PAŃSTWA IZRAEL

przygotowanej pod kierunkiem prof. dr. hab. Romana Kochnowskiego oraz promotora pomocniczego dr Agnieszki Warchoń

I. Przedstawienie podstawowych danych o rozprawie

Podstawą sporządzenia recenzji jest uchwała Rady Dyscyplin Nauki o Bezpieczeństwie Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie z dnia 8 marca 2023 roku, w sprawie powołania recenzentów rozprawy doktorskiej Pana mgr. inż. **Macieja Jędrzejewskiego** pt. *Cyberbezpieczeństwo w doktrynie obronnej Państwa Izrael*.

W sytuacji globalnych zagrożeń, które współcześnie zyskały niespotykaną wcześniej dynamikę bardzo ważnym aspektem bezpieczeństwa każdego państwa stała się ochrona dostępności, poufności, zapewnienia integralności danych oraz niezakłóconego działania systemów informatycznych. Właśnie cyberbezpieczeństwo poprzez użycie zarówno zaawansowanych technologii, jak też odpowiednich procesów i kontroli ma na celu skuteczną ochronę sieci, programów, systemów, urządzeń i danych przed cyberatakami. Chodzi o zminimalizowanie ryzyka takich zamachów i ochronę przed nieuprawnionym wykorzystaniem systemów, sieci i technologii.

Działalność wywiadowcza ukierunkowana na pozyskiwanie, z reguły niejawnych informacji, coraz częściej polega na stosowaniu wywiadu elektronicznego, który jest prowadzony z pomocą „hakerów” – specjalistów włamujących się do nawet dobrze zabezpieczonych sieci komputerowych. Wzrasta także ofensywna aktywność wywiadowcza w sieci polegająca na kopiowaniu informacji poufnych znajdujących się w cyberprzestrzeni.

Pojawiło się również nowe zjawisko zwane cyberwojną, która będąc rodzajem wojny informacyjnej zakłada konfrontację w Internecie. W ten sposób aktorzy zarówno państwowi jak i niepaństwowi zmierzają do destabilizacji systemów komputerowych wykorzystywanych przez organy rządowe, instytucje bankowe i finansowe celem wprowadzenia chaosu i

BIURO DZIEKANÓW
Wpłynęło dnia 16.05.2023



utrudnień w zarządzaniu państwem. Nie są to jedynie potencjalne zagrożenia, o czym świadczy rosyjski cyberatak przeprowadzony 27 kwietnia 2007 r. na Estonię. Skutkowało on bardzo poważnymi zakłóceniami w funkcjonowaniu państwa, w różnych obszarach jego aktywności.

Stąd istotną kwestią stało się znalezienie rozwiązań, które pozwolą państwom na prawidłowe i szybkie reagowanie na ataki cybernetyczne wzmacniając tym samym ich cyberbezpieczeństwo. Dla władz Izraela kwestie związane z bezpieczeństwem państwa mają charakter absolutnie priorytetowy. Trzeba bowiem pamiętać, że powstanie tego państwa stanowiło fenomen, we współczesnej historii świata. Po blisko dwóch tysiącach lat bezpieczeństwa nastąpił proces reaktywacji struktur państwowych. Stąd dla elit politycznych i militarnych Izraela, ale także całego społeczeństwa przetrwanie i rozwój odrodzonej państwowości jest sprawą organizującą ich działania, które mają ten cel zapewnić.

Przyjęta przez Pana magistra inż. **Macieja Jędrzejewskiego** problematyka wpisuje się w zakres dyskursu naukowego nad tematyką bezpieczeństwa państwa. Biorąc pod uwagę zakres tematyczny podjętych przez Autora rozważań, przedłożona do recenzji rozprawa powinna być postrzegana pozytywnie, zwłaszcza iż dotyczy kluczowego dla polityki bliskowschodniej państwa, mającego status mocarstwa regionalnego.

Wszechstronne przedstawienie przez Doktoranta problematyki cyberbezpieczeństwa w doktrynie obronnej Izraela, usystematyzowanie wiedzy w tym obszarze świadczy o przygotowaniu Autora do prowadzenia dyskursu naukowego w przedmiotowej tematyce i służy pogłębieniu stanu dotychczasowych badań.

Tym samym przedstawiona do recenzji rozprawa Pana mgr. inż. Macieja Jędrzejewskiego pt.: *Cyberbezpieczeństwo w doktrynie obronnej Państwa Izrael* posadowiona jest w obszarze wiedzy i dziedzinie nauk społecznych oraz w dyscyplinie nauk o bezpieczeństwie, a więc w obszarze nauki i dyscypliny, w których kandydat ubiega się o nadanie stopnia doktora.

II. Merytoryczna ocena rozprawy

Autor w rozprawie zdefiniował cel badawczy, wskazał przedmiot badania oraz sformułował szczegółowe problemy i cząstkowe hipotezy badawcze. Omawiając problematykę pracy zaznaczył ograniczenia determinujące zakres podjętego procesu



badawczego. Zmierając do realizacji przyjętych celów Doktorant wykorzystał wybrane metody, technik i narzędzia badawcze.

Cel podjętego badania określony został jako:

przedstawienie, w ujęciu kompleksowym problematyki cyberbezpieczeństwa w doktrynie obronnej Izraela, a więc systematyzacja informacji w tym zakresie. Praca ma się przyczynić do pogłębienia stanu badań w tym obszarze.

To sformułowanie nie jest pod względem logicznym poprawne. Rozprawa doktorska w swojej istocie jest opracowaniem naukowym stanowiącym sprawozdanie z przeprowadzonych badań, a jej celem jest uzyskanie promocji doktorskiej. Natomiast celem badań naukowych jest ściśle określony wynik takich badań, a więc w założeniach badawczych powinien być wskazany cel badań, a nie cel rozprawy.

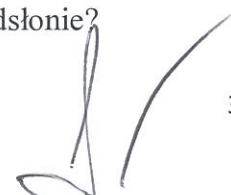
Zakładając jednak, iż autorowi chodziło właśnie o cel przeprowadzonych badań, to można uznać, że jest on zgodny z zakresem merytorycznym pracy, którym jest cyberbezpieczeństwo w doktrynie obronnej Państwa Izrael. Nie mniej właściwym było opracowanie celu głównego, który zakładałby realizację celów szczegółowych. Swą treścią winny one korespondować z postawionymi problemami badawczymi oraz założonymi hipotezami. Udzielenie odpowiedzi na problemy badawcze pozwala w konsekwencji na realizację celów badań. Stąd brak adekwatnych do problemów badawczych celów, można uznać za pewien mankament.

W pracy brak jest sformułowanego głównego problemu badawczego. To także należy uznać za uchybienie, które jednak nie dyskwalifikuje przeprowadzonego procesu badawczego.

Autor wprowadzając czytelnika w zakres problemów badawczych napisał: *W pracy zostanie podjęta próba odpowiedzi na następujące pytania badawcze:* Takie sformułowanie nie jest prawidłowe gdyż proces badawczy dał już odpowiedź na postawione pytania. Rozprawa została już zredagowana, stąd należy odwoływać się do jej treści w czasie przeszłym, a nie przyszłym. Niezrozumiałe jest też użycie zachowawczego określenia, wyrażonego w zwrocie „podjęta próba”. Badania naukowe mają mieć określony wynik, a na pewno nie jest nią „próba” jego osiągnięcia.

Problemy badawcze zostały zawarte w pytaniach:

1. Jaką rolę pełni cyberprzestrzeń w doktrynie obronnej państwa Izrael?
2. Co współcześnie stanowi i będzie stanowić w przyszłości o sile i znaczeniu Izraela na arenie międzynarodowej, zarówno w jej wojskowej jak i cywilnej odsłonie?



3. Co w przyszłości będzie przesądzać o powodzeniu na polu walki?
4. Jakie znaczenie w konflikcie zbrojnym pełnią nowoczesne technologie?

Problemy te znajdują się w tematyce podjętego badania.

W dysertacji przedstawiono hipotezy odnoszące się do wskazanych problemów badawczych, bez formułowania głównej hipotezy roboczej. Jest to konsekwencją braku postawienia głównego problemu badawczego, któremu taka hipoteza winna odpowiadać.

Autor napisał, że: *W odpowiedzi na pytania badawcze przyjęte zostały hipotezy badawcze.* To sformułowanie nie jest prawidłowe. Hipotezy nie są bowiem odpowiedziami. Te pojawiają się dopiero gdy przeprowadzony zostaje proces badawczy i otrzymane zostaną jego wyniki. Hipotezy są tylko założeniami, które w toku badań zostają poddane weryfikacji. Mogą się potwierdzić bądź nie.

W pracy zostały sformułowane następujące hipotezy odpowiadające problemom badawczym:

1. Cyberprzestrzeń pełni kluczową rolę w doktrynie obronnej państwa Izrael.
2. Rozwój technologiczny jak również intelektualny w sferze cyberprzestrzeni, mierzony siłą elit politycznych państwa Izrael stanowi i będzie stanowić w przyszłości o sile i znaczeniu tego państwa na arenie międzynarodowej – zarówno w jej wojskowej jak i cywilnej odsłonie.
3. W przyszłości jednym z kluczowych elementów powodzenia na polu walki będzie przewaga w cyberwojnie.
4. Rozwój nowoczesnych technik walki decyduje o zwycięstwie lub porażce w konflikcie zbrojnym.

Zaproponowane przez Doktoranta hipotezy znajdują się w obszarze tematycznym podjętej dysertacji.

Autor wskazał jako przedmiot podjętego badania: cyberprzestrzeń.

Doktorant przygotowując dysertację przyjął właściwą procedurę badawczą przeprowadzając szeroką kwerendę zasobów bibliograficznych, aktów prawnych, opracowań, artykułów naukowych w drukach zwartych oraz czasopismach, artykułów prasowych oraz netografii. Warte podkreślenia jest szerokie wykorzystanie literatury obcojęzycznej, a także dokumentów, raportów, tekstów źródłowych stanowiących bogate źródło wiedzy o cyberprzestrzeni i cyberzagrożeniach. Zgromadzony materiał został poprawnie pogrupowany i poddany dalszemu procesowi badawczemu.



W tym zakresie Autor wykorzystał kilka metod badawczych stosowanych nie tylko w naukach o bezpieczeństwie. Zastosował: studium przypadku, metodę porównawczą, metodę scenariuszową oraz krytyczną analizę piśmiennictwa.

Analizie poddał ważne i znaczące monografie odnoszące się do przedmiotu badań – cyberprzestrzeni, takich autorów jak: Hanna Batorowska pt. *Kultura bezpieczeństwa informacyjnego w środowisku walki o przewagę informacyjną*, Richard Clarke i Robert Knake pt. *Cyber War. The next threat to National Security and what to do about it*, Claudia Eckhert pt. *IT – Sicherheit. Konzepte – Verfahren- Protokolle*.

Wykorzystał również metodę historyczną. Autor dokonał krytycznej analizy monografii odnoszących się do historii Izraela, szczególnie tej najnowszej, sporo uwagi poświęcając organizacji jego sił zbrojnych. Skorzystał tu między innymi z monografii: Elli Barbera i Krzysztofa Urbańskiego pt. *Gadany przewodnik po teraźniejszości i historii Izraela*, Martina Gilberta pt. *Israel a history*, Krzysztofa Kubiaka i Łukasza Mamerta Nadolskiego pt. *Konflikt bliskowschodni 1945-1982. Broń-Ludzie-Tarnowskie epizody*, Ronalda Payna pt. *Mossad. Israels most secret service* i Johna Petera Rousseau pt. *The history and impact of Unit 8200 on Israeli Hi-Tech Entrepreneurship*.

Wysoko należy także ocenić przeprowadzone badanie komparatystyczne, które pozwoliły na porównanie rozwiązań stosowanych w zwalczaniu cyberzagrożeń przez Izrael z tymi, które zostały przyjęte w innych państwach, takich jak: Chiny, Rosja, USA czy Korea Północna. Dokonując analizy porównawczej autor skorzystał z monografii takich badaczy jak: Marek Budzisz pt. *Wszystko jest wojną, Rosyjska kultura strategiczna*, Daniel Damian Kasprzycki pt. *Rosyjska wizja wojny przyszłości. Formuła wykorzystania instrumentarium koncepcji wojny nowej generacji w oparciu o doświadczenia z działań wobec Ukrainy*, Jacek Bartosiak pt. *Pacyfik i Euroazja. O wojnie*, Bogdan Góralczyk pt. *Nowy długi marsz. Chiny ery Xi Jinpinga, Chiński Feniks. Paradoksy wschodzącego mocarstwa*.

Określony w dysertacji plan postępowania badawczego umożliwił Panu magistrowi inż. Maciejowi Jędrzejewskiemu realizację celu pracy i naukową weryfikację przyjętych hipotez.

III. Formalna ocena rozprawy

Praca została napisana poprawnym językiem przy zastosowaniu właściwego warsztatu pisarskiego. Rozdziały i podrozdziały tworzą logiczną całość. Dysertacja Pana mgr. inż. Macieja Jędrzejewskiego liczy ogółem 235 stron, w tym 24 strony bibliografii (227 poz.



przywołanej literatury i aktów prawnych, 12 poz. czasopism, 117 poz. źródeł internetowych). Zabrakło w niej spisu tabel (5 poz.) oraz spisu rysunków (2 poz.).

Autor nie uniknął jednak pewnych zwrotów, które nie powinny się pojawiać w dyskursie naukowym mających charakter publicystyczny, czy potoczny, jak przykładowo: s.11 „Co ciekawe...”, s.15 „Jak się wydaje...”, s.19 „nawiasem mówiąc...”, s.206 „o czym zresztą już wspomniałem...”, s.207 „poza tym, co raz jeszcze podkreślić wypada...”. Za pewien skrótowy lapsus trzeba uznać stwierdzenie, które pojawia się na s.56 „Niniejsza rozprawa analizuje również...”. To nie rozprawa analizuje, lecz autor-badacz dokonuje analizy.

Rozprawa składa się ze wstępu, czterech rozdziałów oraz zakończenia.

We Wstępie (ss. 5-10) autor dokonał wprowadzenia do przeprowadzonych badań i zaprezentował założenia metodologiczne procesu badawczego. Przetawił przedmiot badań, określił jego cel, sformułował problemy badawcze oraz postawił odpowiadające im hipotezy. Zaprezentował także strukturę rozprawy. Wskazał użyte przez siebie metody badawcze i najważniejsze źródła, które wykorzystał w procesie badawczym.

W pierwszym rozdziale *Cyberbezpieczeństwo. Podstawowe pojęcia i problemy* (ss. 11-82) doktorant przedstawił rozumienie i istotę cyberprzestrzeni, opisał znaczenie kryptografii oraz ochrony informacji niejawnych. Zdefiniował zagrożenia wynikające z działalności wywiadowczej, cyberszpiegostwa oraz wskazał na nowy rodzaj wojny - prowadzonej w cyberprzestrzeni. Zwrócił także uwagę na zagrożenia jakie generuje Darknet oraz ataki dokonywane na łańcuchy dostaw przedstawiając również aktualne dane z raportów Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Dokonał także prezentacji modeli i schematów determinujących cyberbezpieczeństwo państwa.

W drugim rozdziale *Geopolityczne oraz militarne uwarunkowania doktryny obronnej państwa Izrael* (ss. 83-11) autor opisał położenie geograficzne Izraela dostrzegając, jak determinuje ono jego możliwości i ograniczenia w sferze obronnej. Zaprezentował historię sił zbrojnych Izraela wskazując na ich decydujące znaczenie, w zapewnianiu przetrwania i rozwoju tego państwa. Charakteryzując doktrynę obronną Izraela zwrócił uwagę na znaczenie nowoczesnych technologii oraz zmodernizowanego przemysłu obronnego. Jako reprezentacyjny przykład podał stworzenie przez Izrael własnego, ultranowoczesnego systemu raketowego określanego jako „żelazna kopuła”. Opisując współczesne determinanty zagrożeń z jakimi zмага się to państwo odniósł się również do doświadczeń wynikających z wojen izraelsko-arabskich, w latach 1948-1952.



W rozdziale trzecim *Jednostka 8200. Cybernetyczne ramię AMANU* (ss. 112-146) autor przedstawił zagadnienia dotyczące wywiadu, działalności niejawnej w aspekcie przedsięwzięć prowadzonych w sieci przez służby specjalne i wyspecjalizowane jednostki sił zbrojnych. Szczególną uwagę poświęcił znaczeniu Amanu wskazując obszar i metody jego działania. Skoncentrował się na celach stawianych przed tą formacją dostrzegając, że jej skuteczność w obszarze cyberbezpieczeństwa determinuje faktyczne możliwości obronne Izraela.

W rozdziale czwartym *Doktryna Cyberbezpieczeństwa Sił Zbrojnych Izraela na tle wybranych państw* (ss. 147-204) autor dokonał porównania potencjałów mocarstw światowych, pod kątem ich działań ofensywnych prowadzonych w cyberprzestrzeni. Odnosił się do takich państw, o istotnym znaczeniu dla globalnego bezpieczeństwa jak: USA, Rosja, ChRL, Federacja Rosyjska i Korea Północna. Zaprezentował możliwości tych państw, zarówno w obszarze wykorzystania przez nie narzędzi walki w cyberprzestrzeni, jak i obrony własnych systemów informatycznych.

W Zakończeniu (ss. 205-210) autor przedstawił treści, które pozwalają przyjąć, że cel procesu badawczego został osiągnięty i zweryfikowano postawione hipotezy badawcze. Zabrakło jednak odniesienia się bezpośrednio do poszczególnych hipotez, czy problemów badawczych, co dla klarowności rozprawy byłoby pożądane. Stąd należało podać odpowiedzi uzyskane w toku badań na postawione problemy badawcze ze wskazaniem, jaki był wynik weryfikacji założonych hipotez.

Autor zaprezentował pożądany, profesjonalny warsztat pisarski posługując się przy tym zrozumiałym językiem, co w konsekwencji pozwala na wystawienie mu pozytywnej oceny. Przedstawiona do recenzji dysertacja Pana magistra inż. Macieja Jędrzejewskiego pt. *Cyberbezpieczeństwo w doktrynie obronnej Państwa Izrael jest oryginalnym opracowaniem badawczym oraz spełnia wszystkie wymogi formalne i merytoryczne* określone w art. 187 ust.1 i 2 Ustawy dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce*, Dz. U. 2018 poz. 1668.

W związku z powyższym **wniosuję o dopuszczenie Pana magistra inż. Macieja Jędrzejewskiego do publicznej obrony doktoratu.**

dr hab. Andrzej Czop prof. Uniwersytetu WSB Merito

