Stanisław Koziej*

Miron Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, ss. 488

DOI: 10.26399/meip.1(64).2019.13/s.koziej

Doktor hab. Miron Lakomy jest adiunktem w Instytucie Nauk Politycznych i Dziennikarstwa na Wydziale Nauk Społecznych Uniwersytetu Śląskiego. Ma bogaty dorobek w dziedzinie nauk o polityce, w tym w zakresie stosunków międzynarodowych. Należy do grona polskich specjalistów zajmujących się naukowo coraz bardziej dynamicznie rozwijającą się problematyką polityki, w tym polityki bezpieczeństwa, w cyberprzestrzeni. Odzwierciedleniem tego jest recenzowana praca poświęcona stosunkom międzynarodowym w cyberprzestrzeni, na podstawie której w 2016 roku uzyskał stopień doktora habilitowanego.

Praca została opublikowana w 2015 roku przez Wydawnictwo Uniwersytetu Śląskiego w Katowicach, w serii: Prace Naukowe Uniwersytetu Śląskiego w Katowicach, Nr 3293 (ISBN 978-83-8012-357-1). Recenzentem wydawniczym jest prof. dr hab. Michał Chorośnicki z Uniwersytetu Jagiellońskiego w Krakowie. Monografia liczy 488 stron. Składa się ze: wstępu, pięciu rozdziałów merytorycznych, zakończenia, bibliografii, indeksu osobowego oraz podsumowania w językach angielskim i francuskim.

Niewątpliwie cyberprzestrzeń to najnowsza sfera ludzkiej aktywności. Często wymienia się ją jako piątą przestrzeń po: lądowej, morskiej, powietrznej i kosmicznej. Nie jest to w pełni uprawnione. Jest to w istocie zupełnie nowa jakość, odmienna od tradycyjnych kategorii geoprzestrzennych lub kosmicznej. Jeśli już porównywać z nimi cyberprzestrzeń, to stanowi ona raczej odpowiednik ich wszystkich razem wziętych, a nie dodatek „równoprawny" z każdą z nich z osobna.

* Stanisław Koziej – prof. dr hab., Uczelnia Łazarskiego w Warszawie, Wydział Ekonomii i Zarządzania, stanislaw.koziej@lazarski.pl

Dziś już nie ulega wątpliwości, że człowiek coraz bardziej przenosi się ze swoim życiem do cyberprzestrzeni. Stopniowo realizuje w niej już nie tylko zwykłe funkcje informacyjne (komunikacyjne, dydaktyczne, naukowe itp.), ale także służy ona do świadczenia i korzystania z wszelkich usług (finanse, handel, ochrona itd.), a ostatnio także wprost produkcji (w technologii 3D). Co oczywiste: w cyberprzestrzeni pojawiły się natychmiast wszelkie problemy związane z bezpieczeństwem, z zagrożeniami dla ludzi, społeczności, państw i ze sposobami radzenia sobie z tymi zagrożeniami.

Innymi słowy – nie ma już dziedziny ludzkiej aktywności, która nie byłaby lub nie mogłaby być realizowana w cyberprzestrzeni. Jeśli już w cyberprzestrzeni ludzie mogą także kochać się, to znaczy, że nie ma granic i że wszystko, co dotychczas działo się w geoprzestrzeni, może i musi dziać się także w cyberprzestrzeni. Choć już wiele rzeczy się w tym zakresie wydarzyło, to wciąż jesteśmy, jako ludzkość, na początku drogi uczenia się życia w cyberprzestrzeni.

W tej sytuacji nikogo nie dziwi, że także polityka, w tym międzynarodowa, wchodzi do cyberprzestrzeni, a sprawy cyberbezpieczeństwa stają się priorytetowe. Dlatego wszelkie poszukiwania badawcze, mogące podpowiadać, jak radzić sobie w cyberprzestrzeni, są ze wszech miar pożyteczne. W tym też kontekście postrzegam znaczenie problemu podjętego w recenzowanej pracy. Problematyka cyber- w różnych aspektach ma już oczywiście bogatą literaturę. Ale stosunkowo niewiele jest jej analiz w kontekście stosunków międzynarodowych, a w tym polityki zagranicznej państw. Studia w tym zakresie nie przekraczały w zasadzie kwestii cyberzagrożeń, w tym cyberwojny. Z pewnością na gruncie polskim jest to w ogóle pierwsza praca podejmująca w tak kompleksowy sposób rolę cyberprzestrzeni w stosunkach międzynarodowych.

Dlatego należy bardzo wysoko ocenić znaczenie podjętego problemu. Wychodzi ono dużo dalej niż podjęte już i realizowane – wciąż bardzo wolno i słabo – w Polsce sprawy samego cyberbezpieczeństwa jako coraz ważniejszego transsektorowego obszaru (dziedziny) bezpieczeństwa narodowego. Problematyka ta została podjęta i szeroko przeanalizowana w ramach przeprowadzonego w latach 2011–2012 pierwszego w Polsce Strategicznego Przeglądu Bezpieczeństwa Narodowego, którego rezultaty zostały zawarte w przyjętym przez Radę Bezpieczeństwa Narodowego raporcie, a jego jawna wersja ujęta w Białej Księdze Bezpieczeństwa Narodowego z 2013 roku (*Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013, ss. 263).

Można oczekiwać, że recenzowana praca stanie się w Polsce kolejnym impulsem do jeszcze szerszego niż tylko sprawy cyberbezpieczeństwa i pogłę-

bionego zajmowania się zarówno teoretycznego, badawczego, jak i praktycznego funkcjonowaniem państwa w cyberprzestrzeni. Wydaje się wręcz, że może ona zainspirować podjęcie jeszcze szerszej problematyki: roli cyberprzestrzeni nie tylko w kontekście polityki zagranicznej, ale także wewnętrznej, czyli w ogóle „cyberpolityki" państwa.

Temat pracy został dobrze ustawiony w kontekście badawczym. Autor zidentyfikował trafnie pewne luki w teorii stosunków międzynarodowych, dotyczące kompleksowej roli cyberprzestrzeni w praktyce tych stosunków na poziomie głównych ich podmiotów, tj. państw i organizacji międzynarodowych. Identyfikacja owych luk posłużyła do postawienia problemu i celu badawczego oraz rozbicia go na szczegółowe pytania badawcze, a także wysunięcia stosownych hipotez odpowiadających wstępnie na pytania badawcze. Można mieć tylko wątpliwości co do sposobu przedstawienia tych kwestii we wstępie pracy, gdzie najpierw omówione zostały hipotezy, a potem dopiero problem i pytania badawcze. Jeśli przyjmiemy, że hipotezy są wstępną, próbną („przedbadawczą") odpowiedzią na postawione problemy badawcze, która to odpowiedź będzie metodycznie weryfikowana w badaniach, to powinny być także umieszczone w pracy w takiej właśnie kolejności: najpierw problem, potem hipoteza.

Zastrzeżenia może również budzić sposób potraktowania we wstępie pracy relacji między celem i problemem badawczym, a mianowicie stawianie celu badań przed problemem badawczym. Wszakże celem badań jest pewien stan „pobadawczy" będący rozwiązaniem problemu. Najpierw więc należy zdefiniować problem, by wiedzieć, co chcemy rozwiązać, jak uzupełnić lukę, jak usunąć przeszkodę itp., i dopiero wtedy możemy opisać, scharakteryzować cel. Szczegółowe metody i techniki badawcze stosowane w pracy są właściwe dla nauk o polityce: analiza krytyczna i porównawcza literatury, dokumentów, praktyki instytucjonalnej, metody statystyczne, synteza, opis itp. Na podkreślenie zasługuje doskonałe wykorzystanie bardzo bogatej krajowej i zagranicznej literatury przedmiotu. W sumie warstwa metodologiczna recenzowanej pracy, mimo drobnych uwag, świadczy o dobrze przeprowadzonych badaniach i uwiarygadnia prezentowane w niej wnioski.

Struktura wykładu – od wstępu z omówieniem procedury badań, poprzez poszczególne problemy merytoryczne przedstawione metodą „od istoty danego zjawiska do jego praktyki" – daje możliwość dobrego zapoznania się z problematyką i prezentowanymi rozwiązaniami oraz wnioskami. Praca składa się z pięciu rozdziałów merytorycznych: 1) Rewolucja informatyczna, 2) Cyberprzestrzeń jako źródło nowych wyzwań i zagrożeń dla bezpieczeństwa państw, 3) Formy zagrożeń teleinformatycznych dla bezpieczeństwa państw,

4) Cyberprzestrzeń jako nowy wymiar rywalizacji państw, 5) Cyberprzestrzeń jako nowy wymiar współpracy państw. Rozdziały podsumowuje syntetyczne zakończenie.

Dwa pierwsze rozdziały mają charakter wprowadzający w zasadniczą problematykę badawczą. Zawierają w istocie charakterystykę procesu rewolucji informatycznej oraz samej cyberprzestrzeni jako nowej domeny aktywności człowieka. Rewolucja informatyczna została przedstawiona m.in. w kontekście koncepcji tzw. trzeciej fali cywilizacyjnej Alvina Tofflera oraz koncepcji społeczeństwa informacyjnego. Słusznie podkreśla się rosnące znaczenie cyberprzestrzeni, z uwzględnieniem zarówno pozytywnych, jak i negatywnych konsekwencji tego procesu. Na dziś niewątpliwie, co trafnie odnotowuje się w recenzowanej pracy, istotniejsze są negatywne aspekty rewolucji informatycznej, przejawiające się w ujawnianiu się coraz to nowych rodzajów i form zagrożeń, w tym dla bezpieczeństwa narodowego i międzynarodowego.

Charakterystykę cyberprzestrzeni rozpoczyna się od analitycznego przeglądu jej definicji, jako podstawowej dla całej pracy kategorii. W rezultacie analiz przyjęto własne rozumienie tego pojęcia, traktujące cyberprzestrzeń jako:

> „domenę przetwarzania, przechowywania i przesyłania informacji w formie cyfrowej, funkcjonującą w oparciu o transmisję sygnałów cyfrowych oraz promieniowanie elektromagnetyczne" (s. 83).

Z punktu widzenia głównego celu badawczego zidentyfikowano podstawowe właściwości cyberprzestrzeni, jak aterytorialność, anonimowość, niskie koszty operowania w niej, trudności współpracy międzynarodowej, faworyzowanie działań ofensywnych nad defensywnymi, trudności odstraszania w niej potencjalnego przeciwnika.

Taka charakterystyka procesu rewolucji informatycznej, jak i samej cyberprzestrzeni stanowi punkt wyjścia do trzech kolejnych rozdziałów poświęconych już działaniom państw i organizacji międzynarodowych w cyberprzestrzeni.

Trzeci rozdział pracy zawiera analizę zagrożeń dla bezpieczeństwa państw w cyberprzestrzeni. Co do podmiotów mogących stwarzać takie zagrożenia wyróżnia się: a) państwa i ich organizacje, b) wysoce zorganizowane nielegalne podmioty pozapaństwowe (organizacje terrorystyczne, przestępcze, grupy rebelianckie), c) wysoce zorganizowane legalne podmioty pozapaństwowe (korporacje transnarodowe), a także tzw. podmioty nieustrukturalizowane (przestępcy, hakerzy, aktywiści, „cyberwojownicy", amatorzy). Zaproponowana została tutaj także typologia cyberzagrożeń obejmująca: haking, haktywizm, haktywizm patriotyczny, cyberprzestępczość, cyberterroryzm, cyberszpiegostwo oraz operacje zbrojne w cyberprzestrzeni, w tym

cyberwojnę. Każda z tych form przemocy w cyberprzestrzeni została poddana szczegółowej analizie, w tym zwłaszcza jako potencjalny instrument polityki zagranicznej w konfrontacji z innymi państwami.

Rozdział czwarty to studia konkretnych przypadków konfliktów i incydentów międzypaństwowych w cyberprzestrzeni, mających istotne znaczenie z punktu widzenia praktyki stosunków międzynarodowych w XXI wieku. Są to zdarzenia cyberprzestrzenne w stosunkach estońsko-rosyjskich, litewsko-rosyjskich, gruzińsko-rosyjskich, kirgisko-rosyjskich, izraelsko-syryjskich, izraelsko-amerykańsko-irańskich, międzykoreańskich (Korea Płn. – Korea Płd.) oraz amerykańsko-chińskich. Przedstawiona tu została dość szczegółowa analiza każdego przypadku cyberataków na tle i w kontekście relacji politycznych między danymi państwami oraz charakteru konkretnego konfliktu lub kryzysu międzynarodowego. Pozwoliło to na zbadanie możliwości użycia i scharakteryzowanie cyberataków jako instrumentów polityki zagranicznej państw w sytuacjach konfliktowych i kryzysowych we współczesnych stosunkach międzynarodowych.

W rozdziale piątym, podobnie jak w rozdziale czwartym, poddane zostały analizie praktyczne przypadki uwzględniania i wykorzystywania działań w cyberprzestrzeni we współpracy państw w ramach różnych organizacji międzynarodowych. Dotyczy to dziewięciu organizacji, jak Organizacja Narodów Zjednoczonych, Międzynarodowy Związek Telekomunikacyjny, NATO, Unia Europejska, Rada Europy, Szanghajska Organizacja Współpracy, Organizacja Współpracy Gospodarczej Azji i Pacyfiku, Organizacja Współpracy Gospodarczej i Rozwoju, Unia Afrykańska.

Są to najważniejsze rozdziały pracy ukazujące praktyczne i rosnące bezustannie znaczenie we współczesnych stosunkach międzynarodowych aktywności w cyberprzestrzeni. Badania te uzmysławiają, na jak znaczną już skalę upowszechnia się praktyka stosowania instrumentów cyberprzestrzennych w polityce międzynarodowej, zwłaszcza w sytuacjach konfliktowych i kryzysowych. Pokazują też, jak w istocie zapóźniona wobec tej praktyki jest teoria w zakresie stosunków międzynarodowych.

Praca stanowi istotny krok w badaniu szerokiego obszaru aktywności państw i organizacji międzynarodowych, który można byłoby określić „polityka w cyberprzestrzeni (cyberpolityka)". Koncentruje się zwłaszcza na polityce zagranicznej państw i polityce bezpieczeństwa. Wykazuje dobitnie, że cyberprzestrzeń jest nowym, coraz ważniejszym wymiarem tej polityki w praktyce i że jest ona, jak dotąd, wykorzystywana przede wszystkim w celach rywalizacyjnych, w ramach konfrontacji, jako nowy, dodatkowy instrument stosowania przemocy i generowania zagrożeń, zwłaszcza w formie cybersz-

piegostwa, cyberdywersji, a przez podmioty niepaństwowe – cyberterroryzmu. Autor zasadnie wykazuje przyczynę takiego stanu rzeczy: przewagę działań ofensywnych i skrytych nad defensywnymi oraz brak międzynarodowego ustanowienia regulacji prawnych w tym zakresie. To ostatnie jest podstawowym wyzwaniem, jakie stoi przed społecznością międzynarodową.

Recenzowana praca wnosi niewątpliwie istotny wkład w rozwój nauki o stosunkach międzynarodowych. Dodaje do niej coś, co mógłbym określić jako „elementy wprowadzenia do teorii cyberpolityki międzynarodowej, w tym cyberpolityki zagranicznej państw". Rozważania, analizy, hipotezy, propozycje w niej zawarte mogą być istotnym impulsem do kolejnych badań, a tym samym do rozwoju nauki o stosunkach międzynarodowych.

Cytuj jako:

Koziej S., recenzja książki: Miron Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, ss. 488, „Myśl Ekonomiczna i Polityczna" 2019 nr 1(64), 329–334. DOI: 10.26399/meip.1(64).2019.13/s.koziej

Cite as:

Koziej, S. (2019) book review (in Myśl Ekonomiczna i Polityczna 1(64), 329–334: Miron Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw ['*Cyberspace as a new dimension of competition and cooperation between states*'], Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, 488 pp. DOI:10.26399/meip.1(64).2019.13/s.koziej