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

*Kinga Smoleń**

W nauce o stosunkach międzynarodowych do początku lat 90. XX wieku dominowało tradycyjne, geopolityczne ujmowanie przestrzeni międzynarodowej w kategoriach politycznej, państwowej kontroli nad nią, która przejawiała się w formie podboju, dominacji, rywalizacji o strefy wpływów, kolonializmu i imperializmu z zastosowaniem siły. Takie podejście związane było z dokonywaniem analizy kategorii przestrzeni w warunkach westfalskiego systemu międzynarodowego. Procesy globalizacji, obok czynnika technologicznego, stały się głównym stymulatorem procesualnych zmian w systemie międzynarodowym, które przyczyniły się do wyodrębnienia przestrzeni transnarodowej wraz z jej wymiarami m.in. w postaci cyberprzestrzeni. Tym samym ma miejsce swego rodzaju „rozdwój”, hybrydowość, co skutkuje jed-

noczesnym funkcjonowaniem tradycyjnej przestrzeni, interpretowanej w kategoriach terytorialnych oraz dystansów geograficznych, a obok niej, cyberprzestrzeni pozbawionej miejsca, dystansów geograficznych i granic.

Powyższe jakościowe zmiany przyczyniły się do poszerzenia zakresu badań w naukach społecznych – chociaż nie tylko w nich – właśnie o supraterytorialną cyberprzestrzeń, która staje się areną coraz większej aktywności państw i podmiotów pozapaństwowych. Cyberprzestrzeń znalazła się więc w kręgu zainteresowań badaczy z Polski i zagranicy. Wydaje się naturalne, że po początkowym okresie badań, w którym dominowało podejście nie *stricte* naukowe, lecz raczej fantastyczno-naukowe, dokonując analizy istoty i specyfiki cyberprzestrzeni, należałoby wskazywać na wyraźną korelację, jaka zachodzi pomiędzy postępem naukowo-technicznym a procesami politycznymi, gospodarczymi i kulturowymi. Tym-

* Uniwersytet Marii Curie-Skłodowskiej w Lublinie, Wydział Politologii.

czasem bardzo wielu autorów opracowań naukowych koncentruje się przede wszystkim na bezpieczeństwie teleinformatycznym, czyli na tych działaniach, które stanowią zagrożenie dla niezakłóconego i prawidłowego funkcjonowania cyberprzestrzeni, zwłaszcza cyberterroryzmie oraz wojnach informacyjnych. W tym kontekście na uwagę zasługują takie pozycje jak m.in. P. Hessa (ed.), *Cyberterrorism and information war*, New Dheli 2001; J. Carra, *Inside Cyber Warfare*, Sebastopol 2010; J.V. Blane'a (ed.), *Cyberwarfare: Terror at a click*, Huntington 2001; R.A. Clarke'a, R. Kna-ke'a, *Cyberwar: The Next Threat to National Security and what to Do About it*, Ecco 2010; T. Rida, *Cyber War Will Not Take Place*, London 2013; J.A. Lewisa, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington 2002; D.C. Molandera, A.S. Riddle'a oraz P.A. Wilsona, *Strategic Inormation Warfare: A New Face of War*, Santa Monica 1996.

Podobną optykę prezentuje wielu przedstawicieli ośrodków naukowych w Polsce. Do najważniejszych opracowań ich autorstwa należą monografie: E. Lichockiego, *Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego*, Warszawa 2008; K. Liedela (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011; M. Madeja, M. Terlikowskiego (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009; T. Jemioły, J. Kisielnickiego, K. Rajche-

la (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009; A. Bógdał-Brzezińskiej, M.F. Gawryckiego, *Cyberterroryzm i problemy bezpieczeństwa teleinformatycznego we współczesnym świecie*, Warszawa 2003; R. Białoskórskiego, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa 2011. Część publikacji polskojęzycznych ukazuje jeszcze inne podejście do problemu i koncentruje się na funkcjonowaniu społeczeństwa informacyjnego oraz jego wpływie na jednostkę. Przykładem są opracowania L.H. Habera (red.), *Spółczeństwo informacyjne – wojna czy rzeczywistość*, Kraków 2003 oraz pod redakcją M. Borkowskiego, M. Stańczyk-Minkiewicz, I. Ziemi-kiewicz-Gawlik pt.: *Wyzwania i zagrożenia w XXI wieku: cyberprzestrzeń a bezpieczeństwo jednostki*, Toruń 2012. Jeszcze inne dotyczą m.in. działania sił zbrojnych w cyberprzestrzeni oraz marketingu politycznego w środowisku wirtualnym.

Należy zwrócić uwagę, że zaprezentowane powyżej pozycje badaczy polskojęzycznych nie koncentrują się *stricte* na ukazaniu istoty i specyfiki cyberprzestrzeni w stosunkach międzynarodowych. Pewną próbę zastosowania takiego podejścia stanowią monografie autorów angielskojęzycznych, m.in. S.S. Costigana, J. Perry'e-go (eds.), *Cyberspaces and Global Affairs*, Ashgate 2012 oraz pod redakcją J.F. Kremera i B. Mullera pt. *Cyberspace and International Relations*, Springer 2014.

W polskiej literaturze przedmiotu przez wiele lat brakowało zaś takiego ujęcia.

W tym kontekście za ważną i potrzebną należy uznać wydaną w 2015 roku monografię autorstwa Mirona Lakomego pt.: *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Cel poznawczy monografii stanowi analiza rywalizacji i współpracy państw w cyberprzestrzeni przy jednoczesnym określeniu ich konsekwencji dla praktyki polityki zagranicznej państw oraz całokształtu stosunków międzynarodowych. Za główną hipotezę badawczą autor przyjął zaś założenie, że cyberprzestrzeń stała się nowym wymiarem, w którym państwa w XXI wieku realizują swoją politykę zagraniczną.

Cyberprzestrzeń stanowi swego rodzaju nową kategorię przestrzeni społecznej. Jest tworzona przez człowieka i dla jego potrzeb. Tym samym można ją pojmować przez pryzmat wirtualnego odzwierciedlenia fizycznej rzeczywistości. W przypadku założenia Lakomego – areny, na której dochodzi do urzeczywistniania przez państwo jego celów polityki zewnętrznej. Podobnie jak w tradycyjnej, określonej przez czynnik geograficzny przestrzeni – także w cyberprzestrzeni dochodzi do stałego poszerzenia zakresu przedmiotowego działań o te o charakterze politycznym, gospodarczym, społecznym, kulturowym, technologicznym, a także wojskowym. Autor monografii słusznie stwierdza więc, że w świecie wirtualnym państwo stosuje rozmaite instrumenty polityki zagranicznej, m.in. cyberterroryzm, cyberszpiegostwo, operacje zbrojne, czynnik ludzki w postaci korzystania z umiejętności i wiedzy wysoko wykwa-

lifikowanych ekspertów w dziedzinie IT, inwestycje w rozwój nowoczesnych technologii itp. Środki te – z jednej strony – pozwalają mu w niestandardowy sposób osiągać takie cele jak zapewnienie bezpieczeństwa, wzrost potęgi oraz pozycji i prestiżu w systemie międzynarodowym. Z drugiej jednak – stanowią nowy rodzaj zagrożeń dla bezpieczeństwa narodowego i międzynarodowego.

Należy podkreślić, że Miron Lakomy prezentuje odmienne niż dominujące w literaturze przedmiotu podejście – zgodnie z którym w odpowiedzi na wzrastającą skalę oraz rodzaj nowych zagrożeń o charakterze asymetrycznym w cyberprzestrzeni państwa zmuszone są sięgać po niewojskowe instrumenty bezpieczeństwa przy jednoczesnym ograniczeniu instrumentów wojskowych. Badacz potwierdza w tym kontekście istotną rolę działań o charakterze niemilitarnym, zwłaszcza *soft power*. Jednocześnie stwierdza jednak, że państwo ma szansę na optymalną realizację założeń koncepcji polityki zagranicznej przy równoległym stosowaniu instrumentów wojskowych i pozawojskowych. Co potwierdzać ma przypadek konfliktu zbrojnego Gruzji i Rosji, do którego doszło w sierpniu 2008 roku.

Odnosząc się do wspomnianych powyżej zagrożeń asymetrycznych, podkreślić należy, że w ramach przestrzeni wirtualnej dochodzi do równoważenia sił podmiotów państwowych i pozapaństwowych. Powyższe zjawisko generowane jest przez istotę cyberprzestrzeni w postaci aterytorialności.

Podjmowanie w cyberprzestrzeni na coraz większą skalę skutecznej aktywności przez podmioty tej drugiej kategorii, czyli niepaństwowe, pozwala stwierdzić, że w przestrzeni wirtualnej doszło do odejścia – od charakterystycznego w warunkach westfalskiego systemu międzynarodowego – państwowocentrycznego podejścia, zgodnie z którym państwo narodowe jest głównym i najważniejszym uczestnikiem stosunków międzynarodowych. Uwzględniając, że w cyberprzestrzeni podmioty pozapaństwowe stale zyskują na znaczeniu, dochodzi w niej do charakterystycznej dla sfery transnarodowej bifurkacji podmiotowej struktury systemu oraz dynamicznej demopolizacji siły państwa.

Powyższą prawidłowość charakteryzującą późnowestfalski system międzynarodowy i przekładającą się na specyfikę cyberprzestrzeni potwierdza autor monografii. Lakomy klasyfikuje podmioty pozapaństwowe funkcjonujące w sieci ze względu na stopień organizacji, cele oraz motywacje przeprowadzanych cyberataków (s. 117 i nast.). Wskazuje także na stale rosnącą rolę hakywistów oraz hakywistów patriotycznych, szczególnie istotną w przypadku polityki zagranicznej Federacji Rosyjskiej zwłaszcza wobec Litwy i Estonii.

W monografii wyraźnie dominuje jednak państwowocentryczna optyka. Dla autora książki to właśnie charakterystyczne dla westfalskiego systemu międzynarodowego, określone granicami państwa narodowe są jednymi z głównych podmiotów, które kształtują parametry przestrzeni wir-

tualnej i realizują w jej ramach swoje interesy związane głównie z potęgą, prestiżem międzynarodowym oraz bezpieczeństwem. Prezentowane podejście do funkcjonowania państwa w cyberprzestrzeni, związane jest z ujmowaniem jej przez Lakomego – obok lądu, morza, przestrzeni powietrznej i kosmicznej jako środowiska prowadzenia walki, które stanowi tzw. piąty wymiar pola walki. Tym samym można ją uznać za nową, współczesną postać geopolityki. Przykładami potwierdzającym powyższe założenie są – przeanalizowane przez autora monografii – *casusy* Estonii, Syrii oraz Gruzji.

W książce Miron Lakomy przytacza regulacje m.in. Organizacji Narodów Zjednoczonych, Międzynarodowego Związku Telekomunikacyjnego oraz kilku organizacji regionalnych, które mają zwiększać bezpieczeństwo państwa w przestrzeni wirtualnej. Jednocześnie słusznie akcentuje stosunkowo niską efektywność norm prawnych, a także pluralizm podejść w procesie ich wypracowywania. Co warunkowane jest przez specyfikę cyberprzestrzeni, w której wyraźnie zauważalny jest brak zjawiska scentralizowanej władzy. Możliwość wertykalnego zorganizowania sieci została w cyberprzestrzeni zastąpiona układem o charakterze horyzontalnym. Zjawisko to potwierdza istnienie anarchii także w przestrzeni wirtualnej. W rezultacie w sieci nie ma jednego podmiotu, który byłby zdolny kontrolować i gwarantować bezpieczeństwo. W zamian istnieje pluralizm norm zapewniania względnego porządku, a także

jednoczesne współpraca oraz rozbieżności podmiotów państwowych i pozapaństwowych w procesie wypracowywania mechanizmów wzajemnego zapewnienia bezpieczeństwa.

Struktura monografii ma charakter problemowy. Składa się ona z pięciu rozdziałów. W pierwszym z nich przedstawiono etapy, istotę i konsekwencje rewolucji informatycznej. Scharakteryzowano główne osiągnięcia i odkrycia poczynione w XX i XXI wieku w obszarze telekomunikacji i informatyki. W kontekście rozwoju cyberprzestrzeni właściwe jest zaakcentowanie znaczenia czynnika technologicznego. Z drugiej jednak strony wyraźnie brakuje wyeksponowania przez autora znaczenia procesów globalizacji, które determinując jakościowe, procesualne zmiany w systemie międzynarodowym, umożliwiły uformowanie się przestrzeni transnarodowej i jednego z jej wymiarów w postaci właśnie cyberprzestrzeni.

Zaprezentowane powyżej, przyjęte przez autora monografii założenia wskazują na cechy charakterystyczne cyberprzestrzeni, takie jak: odterytorialniony charakter, horyzontalna struktura sieci i brak scentralizowanej władzy, bifurkacja podmiotowej struktury przy jednoczesnym wzroście znaczenia podmiotów pozapaństwowych, transsektorowość, nowe wirtualne pole walki i rywalizacji oraz dzieło człowieka. Powyższe elementy są akcentowane szczególnie przez badaczy stosunków międzynarodowych. Niezależnie od nich w rozdziale drugim monografii Miron Lakomy prze-

prowadza analizę cyberprzestrzeni jako źródła nowych wyzwań i zagrożeń dla bezpieczeństwa państwa. W tym celu dokonuje przeglądu definicji cyberprzestrzeni, bada jej właściwości techniczne, a także podkreśla te cechy, które decydują o bezpieczeństwie państwa i zagrożeniach w tego nowego rodzaju przestrzeni. W tym kontekście autor monografii określa specyfikę cyberprzestrzeni, wskazując na – pojawiające się rzadziej w literaturze nauk politycznych – elementy, m.in.: anonimowość; niskie koszty działania w jej ramach; brak wczesnego ostrzegania, oceny prawdopodobieństwa ataków oraz wywiadu strategicznego; prymat działań ofensywnych nad defensywnymi; zwiększoną możliwość prowadzenia działań propagandowych. Wskazuje, że współczesne, niepożądane działania w sieci, generowane są przez różnorodne czynniki, m.in. religijne, ideologiczne, kryminalne itp. Tym samym podkreśla, że zagrożenia teleinformatyczne mają dynamiczny, wielowymiarowy i wielopłaszczyznowy charakter oraz przyjmują zróżnicowane formy. Są to akty przestępcze, wirtualnego terroru, operacje zbrojne. W tym ujęciu cyberprzestrzeń przedstawiana jest jako nowy wymiar bezpieczeństwa narodowego i międzynarodowego.

W rozdziale trzecim książki autor podjął się próby sformułowania podstawowej siatki pojęciowej dotyczącej zagrożeń dla bezpieczeństwa teleinformatycznego. Identyfikuje podmioty, które są inspiratorami i wykonawcami szkodliwych działań w cyberprzestrzeni z uwzględnieniem stopnia ich

organizacji oraz motywacji. Definiuje, czym są cyberataki oraz jakie są ich główne metody w ujęciu technicznym. Na tej podstawie Lakomy skonstruował uproszczoną typologię zagrożeń teleinformatycznych, do których zalicza: hakytywizm, hakytywizm patriotyczny, cyberprzestępczość, cyberterroryzm, cyberszpiegostwo oraz wirtualne operacje zbrojne. Na szczególną uwagę zasługuje – podjęta przez Lakomego – próba określenia istoty cyberwojny z perspektywy przedmiotu debaty naukowej. Badacz jednoznacznie, słusznie określa, że wpisuje się ona w kategorię wojen hybrydowych. Przyjmując założenie, że cyberprzestrzeń stanowi nową arenę, do której dochodzi do rywalizacji państw, w rozdziale czwartym monografii autor poddaje analizie empiryczne przykłady sporów i konfliktów podmiotów państwowych w sieci oraz ich konsekwencje, m.in.: *casus* Estonii, operację *Orchard*, wirtualną rywalizację Korei Północnej i Południowej oraz Stanów Zjednoczonych i Chińskiej Republiki Ludowej, unikatową operację *Stuxnet*. Podejmuje się próby określenia, czy cyberataki rzeczywiście zostały wykorzystane w charakterze nowego, unikatowego środka polityki zagranicznej.

Rozdział piąty stanowi szczegółowe zestawienie regulacji, mających zwiększyć bezpieczeństwo państwa w cyberprzestrzeni, wprowadzonych przez podmioty o charakterze powszechnym: Organizację Na-

rodów Zjednoczonych, Międzynarodowy Związek Telekomunikacyjny oraz te o charakterze regionalnym, m.in.: Sojusz Północnoatlantycki, Radę Europy, Unię Europejską, Szanghajską Organizację Współpracy, Współpracę Gospodarczą Azji i Pacyfiku, Unię Afrykańską. Jak zostało wspomniane powyżej, Lakomy konkluduje, że współpraca podmiotów państwowych w procesie tworzenia norm zwiększających ich bezpieczeństwo teleinformacyjne jest mało efektywna ze względu na ich rozbieżne interesy oraz podejścia do problemu. Pluralizm stanowisk warunkowany ma być także przez wertykalną strukturę cyberprzestrzeni i brak centralnego ośrodka władzy.

Reasumując, należy wyraźnie podkreślić, że recenzowana monografia jest ważnym, wartościowym i potrzebnym głosem w debacie na temat zyskującego na znaczeniu obszaru badawczego w postaci cyberprzestrzeni. Analiza czynników, które warunkują powstanie cyberprzestrzeni, określenie jej istoty i specyfiki, wskazanie podmiotów oraz metod i form działania z perspektywy zagrożeń i działań na rzecz zapewnienia bezpieczeństwa państwa są wartościowym wkładem w dalszy rozwój tego obszaru badawczego, jednocześnie istotnego dla praktyki politycznej. Wartość monografii wzmacnia siatka pojęciowa oraz metody i techniki badawcze, które znajdują zastosowanie w naukach społecznych.