

*Research Handbook on International Law and Cyberspace*, red. Nicholas Tsagourias, Russell Buchan, wyd. 2, Cheltenham: Edward Elgar Publishing 2021, ss. 672.

DOI: <http://doi.org/10.18290/imp23334.7>

Pierwsze wydanie omawianego podręcznika zostało opublikowane w 2015 r. Od tego czasu cyberprzestrzeń przeniknęła do wszystkich dziedzin ludzkiej działalności, co otworzyło nowe możliwości, ale także przyniosło nowe wyzwania. Liczne państwa i instytucje podjęły niemałe wysiłki, aby zrozumieć, w jaki sposób prawo międzynarodowe ma zastosowanie do cyberprzestrzeni i działań w niej zachodzących, lecz mimo to nadal uchwytna jest wyraźna różnica zdań odnośnie do zastosowania w praktyce międzynarodowych zapisów prawa. Drugie wydanie książki, zaktualizowane i rozszerzone, oferuje teksty autorstwa ekspertów, którzy w sposób kompetentny i autorytatywny przeanalizowali szereg kwestii prawnych związanych z samą cyberprzestrzenią i działaniami w niej.

Otwierająca książkę lista autorów (s. VIII-XIII) wyczerpująco przedstawia zainteresowania badawcze każdej z wymienionych osób, dalej (s. XIV) zamieszczono pochodzący od redaktorów *Wstęp*. Na szczególną uwagę zasługują *Wykaz spraw (Table of cases; s. XV-XX)* oraz *Wykaz przepisów (Table of legislation, s. XXI-XXVII)*, stanowiące nieodzowną pomoc przy poruszaniu się w gąszczu spraw omówionych w publikacji. W zamieszczonym dalej *Wprowadzeniu (Introduction, s. 1-7)* Michael N. Schmitt niezwykle skrupulatnie omówił po kolei wszystkie zawarte w pracy teksty. Owa prezentacja stanowi niezwykle cenną pomoc dla czytelnika, bowiem zwalnia go ze żmudnego obowiązku „kartkowania” publikacji w poszukiwaniu interesujących go treści. Zamykający pracę rozbudowany Index (615-634) z powodzeniem koresponduje z ww. partią pracy.

Część I podręcznika oferuje analizy statusu prawnego cyberprzestrzeni oraz przedstawia sposób, w jaki odnoszą się do niej określone zasady prawa międzynarodowego. Obejmują one zasady suwerenności, nieinterwencji, jurysdykcji, odpowiedzialności państwa, praw człowieka, indywidualnej odpowiedzialności karnej oraz międzynarodowego prawa inwestycyjnego i arbitrażu. Zawiera ona również rozdziały, w których zbadano rozwój norm w cyberprzestrzeni oraz sposób, w jaki podmioty państwowe i niepaństwowe sprawują władzę za pośrednictwem tej domeny. Część II przedstawia i analizuje zasady prawne mające zastosowanie do cyberterroryzmu, cyberszpiegostwa

i cyberprzestępczości. W części III pomieszczono analizy zasad dotyczących niestosowania siły i samoobrony ze szczególnym uwzględnieniem cyberataków operacji cybernetycznych, odstraszania cybernetycznego i tego, w jaki sposób prawo międzynarodowe stosuje się do utrzymania pokoju w cyberprzestrzeni. Część IV dostarcza rozważań poświęconych zastosowaniu międzynarodowego prawa humanitarnego do cyberwojny. Baczną uwagę położono w niej na omówienia kwestii etycznych dotyczących broni cybernetycznej, klasyfikacji konfliktów cybernetycznych, pojęcia ataku, zasady proporcjonalności i ostrożności oraz prawo neutralności. Część V wreszcie analizuje międzynarodowe i regionalne podejścia do regulacji cyberprzestrzeni oraz zastosowanie prawa międzynarodowego do cyberprzestrzeni, a także polityki bezpieczeństwa cybernetycznego Rosji, Chin, UE, NATO, krajów Azji i Pacyfiku oraz Organizacji Narodów Zjednoczonych.

Recenzowany podręcznik z powodzeniem może zatem służyć jako przewodnik dla naukowców, praktyków, badaczy i studentów po zasadach i przepisach prawa międzynarodowego, które mają zastosowanie do cyberprzestrzeni i działań cybernetycznych. Bez krzty przesady można powiedzieć, że stanowi on bogate źródło wiedzy, przydatne jako podstawa do dalszych rozważań w tej dziedzinie.

*Witold Mazurek*

*Szkola Główna Mikołaja Kopernika*

*witold.mazurek@sgmk.edu.pl*

*ORCID: <https://orcid.org/0000-0002-4651-8601>*