WSTĘP

Generowane przez procesy globalizacji współzależności między państwami, przyspieszony rozwój technologiczny oraz jakościowe zmiany w systemie międzynarodowym wprowadziły do stosunków międzynarodowych dodatkową supraterytorialną przestrzeń i podległą jej cyberprzestrzeń. Tym samym nastąpiło swego rodzaju „rozdwojenie", hybrydowość, co skutkuje funkcjonowaniem jednocześnie tradycyjnej przestrzeni, interpretowanej w kategoriach terytorialnych oraz dystansów geograficznych, a obok niej tej nowej, pozbawionej miejsca, dystansów geograficznych i granic.

Mając na uwadze powyższe uwarunkowania, potrzebna stała się interdyscyplinarna debata na temat tego nowego wymiaru przestrzeni międzynarodowej – supraterytorialnej cyberprzestrzeni. Tym samym niniejszy tom należy uznać za próbę włączenia się do międzynarodowej debaty o cyberprzestrzeni, co – w zamyśle jego redaktora – przyczyni się do rozwoju badań interdyscyplinarnych tej nowej kategorii przestrzeni społecznej i popularyzacji wiedzy na jej temat. Uwzględniając powyższy cel, w tomie znalazły się publikacje przedstawicieli różnych dyscyplin naukowych, m.in.: nauki o polityce i administracji, nauki o bezpieczeństwie, nauk prawnych, nauki o komunikacji społecznej i mediach, ekonomii i finansów. Badacze ci koncentrują się na różnych elementach konstytuujących cyberprzestrzeń oraz zjawiskach i procesach zachodzących w jej ramach.

W cyberprzestrzeni pojawia się wiele zagrożeń dla bezpieczeństwa państwa o nowych jakościowych cechach. O zwalczaniu cybernetycznych zagrożeń dla bezpieczeństwa państwa z perspektywy rządowych instytucji pisał Jakub Wołyniec. W artykule *The UK Government's Response to Cyber Threats* skoncentrował się na instytucjach odpowiedzialnych za bezpieczeństwo Wielkiej Brytanii w cyberprzestrzeni. Marcin Gołębiowski przeanalizował natomiast porządek prawny Ukrainy w zakresie cyberbezpieczeństwa. W publikacji *Rola i kompetencje prezydenta Ukrainy w zakresie kształtowania reżimu prawnego ochrony cyberprzestrzeni. Analiza teoretycznoprawna regulacji prawnych z zakresu cyberbezpieczeństwa Ukrainy* autor podjął próbę wyjaśnienia, jak konflikt zbrojny we wschodniej części Ukrainy oraz jej aspiracje bycia członkiem Sojuszu Północnoatlantyckiego wpływają na kształt tego porządku. Wskazał także na rolę prezydenta Ukrainy i podległych mu konstytucyjnych organów władzy państwowej w procesie two-

rzenia i przestrzegania prawa w cyberprzestrzeni. W artykule *The Problem of Cyber Attacks on the Critical Infrastructure of the State in the Energy Sector. The Case of Turkey* Kinga Smoleń przeanalizowała istotny problem cyberataków na infrastrukturę krytyczną państwa w sektorze energetycznym. W ramach *case study* zaprezentowała Turcję, która ze względu na odgrywanie roli „korytarza tranzytowego" dla węglowodorów posiada silną pozycję na międzynarodowym rynku surowców energetycznych. Autorka artykułu stwierdziła między innymi, że w warunkach procesów globalizacji doszło do poszerzenia zakresu podmiotowego i przedmiotowego bezpieczeństwa. Podkreśliła, że bezpieczeństwo energetyczne stało się jednym z autonomicznych wymiarów w strukturze szeroko pojmowanego bezpieczeństwa. Problem potencjalnej kolizji pomiędzy prawami i wolnościami osobistymi a uprawnieniami państwa, związanymi z zapewnieniem bezpieczeństwa ogólnego podjął Marcin Rojszczak w artykule *Prawne dylematy regulacji cyberprzestrzeni: konflikt pomiędzy bezpieczeństwem narodowym a prawem do prywatności z perspektywy prawodawstwa UE i USA*. Autor podkreślił konieczność refleksji w kontekście sposobu formułowania uniwersalnych praw jednostki, a także nadmiernie elastycznego definiowania tak kluczowych pojęć, jak bezpieczeństwo narodowe. Przemysław Sikorski w artykule *Prawnokarne i prawnomiędzynarodowe regulacje związane z ochroną przed pedofilią w cyberprzestrzeni* zawęził problem działania państwa na rzecz bezpieczeństwa ogólnego do analizy tworzonych przez nie prawnokarnych rozwiązań w ramach walki z pedofilią w cyberprzestrzeni. Część rozważań w artykule dotyczy zabezpieczeń międzynarodowych przed pedofilią. Marta Stanisławska z kolei skoncentrowała się na działaniach państwa w celu przeciwdziałania przestępczości gospodarczej w cyberprzestrzeni. Wskazała na konieczność dalszego udoskonalania zabezpieczeń pliku .jpk w kontekście przekazywania za jego pośrednictwem danych wrażliwych organom podatkowym. Analizy cyberprzestrzeni z perspektywy nowego, tzw. piątego pola walki i rywalizacji pomiędzy państwami o strefy wpływów podjęła się Aleksandra Kuczyńska-Zonik w artykule *Infotainment i dezinformacja w mediach rosyjskojęzycznych w państwach bałtyckich*. Autorka zwróciła uwagę na rolę mediów rosyjskojęzycznych w kształtowaniu opinii publicznej na Litwie, Łotwie i w Estonii. Jej zdaniem propagandowy przekaz tych mediów służy realizacji celów władz Rosji, głównie destabilizacji sytuacji wewnętrznej w państwach bałtyckich przez dyskredytowanie ich elit, wspieranie postaw antyrządowych, wzniecanie konfliktów społecznych i promowanie pozytywnego obrazu Rosji. Na obecność w cyberprzestrzeni podmiotów pozapaństwowych wskazały Liliana Węgrzyn-Odzioba, Justyna Kięczkowska oraz Maria Ochab. Liliana Węgrzyn-Odzioba zwróciła uwagę na stałe poszerzanie katalogu społecznych zagrożeń funkcjonowania w cyberprzestrzeni. Justyna Kięczkowska z kolei skoncentrowała się na zagrożeniach dla bezpieczeństwa zdrowotnego w tej nowej przestrzeni. Przytoczyła argumenty za tym, że są one generowane przez dynamiczny rozwój czynnika technologicznego, powszechny dostęp do internetu, a także zmianę modelu pracy, komunikacji społecznej i funkcjonowa-

nia w społeczeństwie, która przejawia się stałą obecnością online. Maria Ochab natomiast w artykule *Cyberprzestrzeń jako środowisko społeczeństwa obywatelskiego w Brazylii* przeanalizowała wpływ nowoczesnych technologii dostępnych w cyberprzestrzeni na rozwój organizacji pozarządowych. Na przykładzie Brazylii pozytywnie zweryfikowała hipotezę, zgodnie z którą cyberprzestrzeń jest przyjaznym środowiskiem dla prowadzenia aktywności pozarządowej nawet w społeczeństwach, które charakteryzują się bardzo dużymi dysproporcjami rozwojowymi i wysokim poziomem wykluczenia społecznego. Problem zagrożeń dla bezpieczeństwa międzynarodowego w cyberprzestrzeni został poruszany w artykułach Jolanty Cichosz *Kierunki działań instytucji europejskich na rzecz podnoszenia poziomu bezpieczeństwa podmiotów państwowych i niepaństwowych w cyberprzestrzeni – wybrane przykłady* oraz Krzysztofa Gawkowskiego *Bezpieczeństwo cyberprzestrzeni w regulacjach UE*. Jolanta Cichosz, odnosząc się do cyberbezpieczeństwa Unii Europejskiej, podkreśliła, że kluczowym wyzwaniem dla organizacji jest sprecyzowanie zakresu obowiązków dotyczących zaangażowanych instytucji i podmiotów gospodarczych. Scentralizowany nadzór ze strony Unii Europejskiej uznała za rozwiązanie mało efektywne. Wskazała na konieczność współpracy sektora państwowego z prywatnym oraz indywidualnymi użytkownikami w sieci w ramach ustalonych strategii politycznych i ram prawnych na szczeblu krajowym oraz Unii Europejskiej. Potrzebę intensyfikacji współpracy międzynarodowej, międzyresortowej oraz wypracowanie metod współdziałania sektora rządowego z prywatnym podkreślił także Krzysztof Gawkowski. Pierwszą część tomu *Cyberprzestrzeń jako środowisko zagrożeń bezpieczeństwa* zamyka artykuł Dominiki Dziwisz *The Future of the Internet – the Traps of Forecasting. The Internet of Things and Augmented Reality in a Military Context*, w którym autorka wskazała możliwe kierunki rozwoju dwóch technologii internetowych: Internetu Rzeczy i Rzeczywistości Rozszerzonej, a także przeanalizowała błędy popełniane przy prognozowaniu ich przyszłości.