mgr Przemysław Roguski

Streszczenie rozprawy doktorskiej pt. „Cyberoperacje w świetle prawa międzynarodowego"

napisanej pod kierunkiem naukowym
dr hab. Brygidy Kuźniak

Przygotowana rozprawa doktorska na temat „Cyberoperacje w świetle prawa międzynarodowego" ma za cel zidentyfikowanie standardów postępowania państw w cyberprzestrzeni. Przedmiotem rozważań jest interpretacja podstawowych praw i obowiązków państw, wynikających m.in. z Karty Narodów Zjednoczonych oraz reguł dotyczących odpowiedzialności międzynarodowej państw, w specyficznych warunkach cyberprzestrzeni, rozumianej jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Głównym problemem badawczym jest ustalenie, czy obecne normy prawa międzynarodowego są wystarczające do wytyczenia ram prawnych działań państw w cyberprzestrzeni, czy też istnieje potrzeba stworzenia nowego katalogu praw i obowiązków, specyficznych dla cyberprzestrzeni.

Realizacja wskazanego celu nastąpiła przez analizę praktyki państw, przede wszystkim w oparciu o dokumenty strategiczne oraz deklaracje przedstawicieli państw podjęte na forum międzynarodowym, dokumenty i oświadczenia organizacji międzynarodowych oraz międzyrządowych, a także akty prawa wewnętrznego. Ponadto zbadano poglądy teoretyków prawa oraz judykatury, ze szczególnym uwzględnieniem orzecznictwa Międzynarodowego Trybunału Sprawiedliwości.

Praca podzielona jest na cztery główne części. Pierwsza część pracy poświęcona jest zdefiniowaniu kluczowych dla problemu badawczego pojęć: cyberprzestrzeni, cyberoperacji oraz cyberataku. W celu lepszego zobrazowania przedstawianych aspektów technicznych, omawiane są w niej aktualne przykłady cyberoperacji, stanowiące stan faktyczny, leżący u podstaw analizy prawnej, dokonanej w kolejnych rozdziałach.

Rozdział drugi podejmuje problem stosowania prawa międzynarodowego w cyberprzestrzeni. Zagadnienie to ma znaczenie fundamentalne dla dalszego toku rozprawy, gdyż wyznacza jej ramy normatywne: jeżeli badanie wykazałoby bowiem, iż cyberprzestrzeń postrzegana jest przez społeczność międzynarodową jako nowa, dotychczas nieregulowana przestrzeń międzynarodowa, wówczas operacje państw w cyberprzestrzeni objęte byłyby pełną swobodą działania, do granicy wyznaczonej przez ewentualne normy zakazujące. Analiza praktyki państw oraz *opinio iuris* wykazała jednak, że państwa zgodne są co do tego, iż prawo międzynarodowe ma zastosowanie w cyberprzestrzeni bez konieczności stworzenia odrębnego instrumentu prawnego. Kluczowe dla osiągnięcia porozumienia w tej sprawie były odbywające się w latach 2012-2013 oraz 2014-2015pod egidą ONZ prace Grup Ekspertów Rządowych. Wypracowane w ramach obrad porozumienie, które spotkało się z szeroką akceptacją wśród państw, obejmuje stosowanie w cyberprzestrzeni zasad Karty Narodów Zjednocznonych, w tym w szczególności zakazu użycia siły, zakazu interwencji w sprawy wewnętrzne, nakazu poszanowania suwerenności państwa, a także zasad odpowiedzialności międzynarodowej.

W trzeciej części autor omawia kwalifikację prawną cyberoperacji. Analiza ta dotyczy trzech głównych norm ujętych w Karcie Narodów Zjednoczonych oraz zwyczaju międzynarodowym: zakazu użycia siły, zakazu interwencji w sprawy wewnętrzne oraz nakazu poszanowania suwerenności i zwierzchnictwa terytorialnego państwa. Każdej z ww. norm poświęcony jest odrębny podrozdział. W pierwszym podrozdziale podjęta zostaje próba ustalenia czy cyberoperacje mogą stanowić użycie siły w rozumieniu art. 2 ust. 4 KNZ. Omawiane są ponadto kryteria, które należy przyjąć, aby zakwalifikować działanie państwa za pośrednictwem cyberprzestrzeni jako równoznaczne z użyciem siły. Drugi i trzeci podrozdział dotyczą odpowiednio zakazu interwencji w sprawy wewnętrzne oraz nakazu poszanowania suwerenności i zwierzchnictwa terytorialnego. Szczególną uwagę poświęcono przy tym kwestii, czy suwerenność państwa jest jedynie zasadą prawa międzynarodowego, z której wynikają konkretne normy zakazowe, czy też tworzy (również) osobną normę pierwotną, zakazującą naruszenia chronionego zakresu suwerenności poprzez akty władcze. Ponadto analizowana jest kwestia kwalifikacji działań *de minimis* oraz aktów cyberszpiegostwa w świetle ww. norm.

Rozdział czwarty podejmuje tematykę odpowiedzialności międzynarodowej państw za przypisane im działania w cyberprzestrzeni, jak również za operacje aktorów niepaństwowych, działających z ich terytorium. Szczególna uwaga poświęcona jest problematyce przypisania cyberoperacji państwu w świetle anonimowości cyberprzestrzeni i związanych z tym trudności technicznych przy identyfikacji autora cyberoperacji. Dyskutowane jest zarówno wykształcenie się *lex specialis* w zakresie cyberodpowiedzialności, jak i, na zasadzie *de lege ferenda*, możliwość modyfikacji obowiązujących zasad atrybucji oraz reguł dowodowych.

Opracowanie zamyka podsumowanie oraz ocena końcowa problemu badawczego. Autor prezentuje wnioski wypracowane w poprzednich rozdziałach oraz przedstawia własną ocenę konieczności podjęcia kolejnych kroków w celu uściślenia wykładni norm Karty Narodów Zjednoczonych oraz zasad odpowiedzialności międzynarodowej w kontekście cyberprzestrzeni.

11.06.2018

Przemysław Roguski