

Uniwersytet Warszawski
Wydział Prawa i Administracji
Instytut Prawa Międzynarodowego
Mgr Tomasz Welanyk

Autoreferat rozprawy doktorskiej

"Istnienie i granice suwerenności w cyberprzestrzeni. Analiza prawna"

Promotor: dr hab. Paweł Czubik, prof. UEK

Promotor pomocniczy: dr Paweł Filipek

Recenzenci:

dr hab. Elżbieta Karska, prof. UKSW

prof. dr hab. Maciej Perkowski

Warszawa, 2020

1. Przedmiot rozprawy

Rozprawa niniejsza ma na celu próbę odpowiedzi na pytanie, jaki jest wpływ cyberprzestrzeni i wynikłych z niej środków technicznych na podstawową cechę państwa jaką jest suwerenność zarówno pojmowana czynnie - jako wykonywanie jurysdykcji, jak i biernie tj. jako zespół interesów państwa. Istnienie cyberprzestrzeni ma istotny wpływ na obydwie te zakresy. Skuteczne wykonywanie jurysdykcji, niezbędnej do chronienia tego zespołu interesów wymaga (wobec cech wszechobecności i niemożliwości fizycznego zlokalizowania cyberprzestrzeni) najczęściej działania albo w niej samej, albo też w świecie fizycznym jednakże w tym przypadku często poza granicami własnego terytorium. Implikuje to odwrócenie porządków jurysdykcyjnych, w których kluczowa staje się jurysdykcja nadzwyczajna - poza cyberprzestrzenią mająca charakter subsydiarny. Wykonywanie jurysdykcji w samej cyberprzestrzeni jest niezmiernie skomplikowane ze względu na istotne problemy faktyczne, związane choćby z kwestią nieterytorialności informatycznej części cyberprzestrzeni. Ta ostatnia bowiem, ze względu na jej znaczącą odrębność od zakresów przedmiotowych tradycyjnych gałęzi prawa międzynarodowego - daje początek nowej gałęzi prawa międzynarodowego publicznego, tzw. *lex informatica*, podobnego do historycznego *lex mercatoria* - historycznego prawa handlowego tworzonego opartego o zwyczaj, konsens uczestników obrotu i zasadę *ex aequo et bono*. System ów stanowi unikalne połączenie technologii i prawa - i działa w oparciu o tzw. normowanie faktyczne, a więc zbiór norm mających jednocześnie charakter prawny jak i skutek faktyczny. Normy takie bowiem są konstruowane w drodze wywierania za pomocą środków prawnych wpływu na architekturę cyberprzestrzeni. Normy te mają więc skutek bezpośrednio normujący - określają bowiem nie tyle zachowania dozwolone lub zakazane, co możliwe lub niemożliwe. Ponieważ jednak na normowanie faktyczne wpływ ma także sama architektura - w drodze tzw. *metanorm*, a więc takich norm faktycznych, które stanowią funkcję regulacji ściśle prawnych jak i faktycznych afordancji. Ich istnienie prowadzi więc do decentralizacji ośrodków *sui generis* prawodawstwa, ponieważ skutek prawny w ramach *lex informatica* mogą mieć także działania podjęte przez podmioty tradycyjnie nieuznawane za podmioty prawa międzynarodowego publicznego lub wręcz aktorów

nie mających *sensu stricto* osobowości prawnej, nawet w świetle prawa wewnętrznego państw.

2. Uzasadnienie wyboru przedmiotu rozprawy

Rozwoju technologii informatycznych przy jednoczesnym ich wpływie na nieomal każdą dziedzinę życia (a w konsekwencji także na funkcjonowanie państw), czyni z nich kluczową dziedzinę dla regulacji prawnych. Międzynarodowy charakter cyberprzestrzeni, w oczywisty sposób umiejscawia ją w domenie prawa międzynarodowego publicznego. Jednak szybkość wspomnianego rozwoju technologicznego jest znacząco większa niż szybkość tworzenia się stabilnego prawa. Wskutek tej dysproporcji prawo internetu - w szczególności na szczeblu międzynarodowym, pozbawionym jednolitego ośrodka normowania - nie jest wolne od istotnych luk. Co istotne, ze względu na normowanie cyberprzestrzeni przez *lex informatica*, a więc system prawny oparty głównie o praktykę międzynarodową i zwyczaj (także ciągle ostatecznie nieukonstytuowany) ograniczone są także prace doktryny w zakresie prawa cyberprzestrzeni. Dotychczasowy stan badań, koncentrował się raczej na możliwości suwerenności samej cyberprzestrzeni czy też funkcjonowaniu jurysdykcji wykonywanej w świecie fizycznym w odniesieniu cyberprzestrzeni, poprzez wpływ na jej fizyczne elementy (jak prace teoretyków prawa z Uniwersytetu Harvarda, jak L. Lessig, T. Wu, czy J. Goldsmith), lub też koncentrowały się bezpośrednio na analizie prawa konfliktów cyberprzestrzennych (jak *Tallinn Manual*). O ile kwestia suwerenności w cyberprzestrzeni stanowiła przedmiot rozważań Grupy Ekspertów Centrum Obrony Cyberprzestrzennej NATO (przede wszystkim w ramach corocznych konferencji Cyber Conflict , czy też teoretyków związanych z armią amerykańską (jak Patrick Franzese), brak jednak kompleksowych opracowań tego zakresu. Nie sposób więc uznać, że problem stanowiący przedmiot rozprawy niniejszej został już kompleksowo opracowany w literaturze przedmiotu. Nadto, należy zauważyć że wszystkie wspomniane prace to prace zagraniczne, brak bowiem piśmiennictwa polskojęzycznego we wspomnianym zakresie. Przedmiotowa rozprawa ma stanowić próbę przynajmniej częściowego wypełnienia wspomnianej luki.

3. Struktura rozprawy.

Pierwsza część pracy zawiera definicje pojęć dla pracy podstawowych. Podejmuje więc kwestie konstrukcji cyberprzestrzeni, jej podział na fizyczną i informatyczną część a także skutki faktyczne i prawne tego podziału. Zawiera ona także próbę opisaną w jaki sposób powstanie i rozwój cyberprzestrzeni zmieniało desygnaty wskazanych powyżej pojęć podstawowych dla prawa międzynarodowego publicznego.

Rozdział drugi poświęcony jest kwestii prawa cyberprzestrzeni. Przede wszystkim podano tu argumenty popierające uznanie cyberprzestrzeni za *global commons*, i co stanowi konsekwencję tego poglądu; argumenty za istnieniem odrębnego prawa cyberprzestrzeni. W dalszej części wywodu, poddano analizie powstanie *lex informatica*, jego genezę, rozwój i współczesny kształt ze szczególnym uwzględnieniem pojęcia *normowania faktycznego*, a więc sposobu tworzenia norm *lex informatica* wynikających z wzajemnego oddziaływania na siebie prawa i technologii. Przeanalizowano także współdziałanie norm wynikających wyłącznie z *lex informatica* i tych, mających swoje źródło w prawie międzynarodowym publicznym, w tym wybranych zasad prawa międzynarodowego, wywodzących się z orzecznictwa Międzynarodowego Trybunału Sprawiedliwości, Stałego Trybunału Sprawiedliwości Międzynarodowej i Międzynarodowego Trybunału Karnego ds. Byłej Jugosławii.

Część trzecia opisuje cyberprzestrzenne zagrożenia dla suwerenności, zarówno te wynikające z użycia siły i siły zbrojnej, jak i naruszenia ograniczające się wyłącznie do złamania zasad nieinterwencji i nieinterferencji. Jest także próbą analizy powstającego dopiero prawa cyberkonfliktu, przesłanek uznania ataku cybernetycznego za atak mający ekwiwalencję kinetyczną, samoobrony i uderzeń prewencyjnych.

Ostatnia część poświęcona jest zjawisku *cyberlawfare*; a więc zjawisku *lawfare* w cyberprzestrzeni. *Lawfare* definiowane jest w doktrynie jako stosowanie prawa jako broni w konflikcie, poprzez ograniczanie zakresu lub wymuszanie określonej

odpowiedzi drugiej strony. Dalsza część wywodu obejmuje wzajemne oddziaływanie *lawfare* i *lex informatica* skutkujące powstaniem *cyberlawfare*, a także środki tego sposobu prowadzenia cyberoperacji, jak utrudnianie atrybucji działań, stosowanie kryptowalut czy fałszowanie tożsamości.

4. Metodologia użyta w rozprawie.

Punktem wyjścia i podstawowym środkiem prowadzenia naszkicowanych powyżej rozważań musi być obserwacja praktyki państw dotyczącej cyberprzestrzeni. Ze względu na specyfikę opartego o *lex informatica* systemu prawa cyberprzestrzeni, ma ona podstawowe znaczenia dla określenia sposobu jej normowania. *Opinio iuris* będzie bowiem istotne wyłącznie w zakresie norm prawa międzynarodowego wpływających na cyberprzestrzeń oraz metanorm, wpływających zarówno na *lex informatica* jak i na prawo międzynarodowe. W aktualnym stanie prawnym brak jest bowiem znaczących traktatów czy kodyfikacji dotyczących *stricto* prawa cyberprzestrzeni. Natomiast normy prawa międzynarodowego stosowane odpowiednio lub w drodze analogii do prawa cyberprzestrzeni mają ograniczony zakres przedmiotowy. Brak także wypracowanych mechanizmów interpretacyjnych tych norm, które uwzględniałyby specyfikę cyberprzestrzeni. Prawo regulujące cyberprzestrzeń jest sumą prawa międzynarodowego publicznego, krajowych porządków prawnych, natywnego dla cyberprzestrzeni *lex informatica* tworzonego poprzez tzw. afordancje¹ normowania faktycznego i metanormy - należące do *lex informatica* i prawa międzynarodowego publicznego jednocześnie i tworzące mechanizm wzajemnego normowania się tych systemów.

Poza przeprowadzeniem opisanych powyżej analiz prawa, metodologia niniejszej rozprawy musi objąć także rozważania i analizę literatury przedmiotu dotyczące stanu

¹ Polskie tłumaczenie terminu *affordances*, oznaczającego możliwe dla jednostki środki interakcji z otoczeniem, w tym wypadku cyberprzestrzeń. zob. Preece J., Rogers Y., Sharp H., Benyon D., Holland S., Carey T. *Human-Computer Interaction*, Addison-Wesley Longman Press, (1994), ss. 6 i n.- Afordancje jako środek służący do świadomego projektowania możliwości cyberprzestrzeni opisuje także Donald Norman [w: *The Design of Everyday Things*, Basic Books, 2002]

faktycznego cyberprzestrzeni. Cyberprzestrzeń jest bowiem zjawiskiem bez precedensu - stanowiąc niefizyczne *quasi-terytorium* działające w oparciu o infrastrukturę zlokalizowaną w świecie fizycznym. Suma wszystkich wspomnianych elementów pozwala na określenie w jaki sposób normowana jest cyberprzestrzeń i określenie skutków prawnych cech natywnych dla konstrukcji cyberprzestrzeni. Rozprawa zawiera także próbę zbadania czy do tworzącego się *lex informatica* stosują się (bezpośrednio lub odpowiednio) fundamentalne zasady prawa międzynarodowego publicznego, w szczególności dotyczące suwerenności i jurysdykcji wypracowane w orzecznictwie sądów i trybunałów międzynarodowych jak też w praktyce międzynarodowej. Podobnej analizie poddano także prawo konfliktów zbrojnych, w celu odpowiedzi na dwa kluczowe dla kwestii suwerenności pytania: (1) na ile normy tego prawa stosowalne są do konfliktów cyberprzestrzennych, (2) jakim regulacjom poddane są konflikty prowadzone jednocześnie w cyberprzestrzeni i w świecie fizycznym.

Poza rozważaniami prawnymi, rozprawa obejmuje także szkic stanu badań dotyczącego cyberprzestrzeni ujmowanej przez nauki informatyczne. Szkic ów ma za zadanie przybliżyć i ułatwić zrozumienie stanów faktycznych, których subsumpcja stanowi podstawę wywodów prawnych w niej przeprowadzonych.

5. Tezy badawcze

Podstawowym problemem badawczym, które porusza rozprawa niniejsza jest kwestia czy suwerenność w cyberprzestrzeni istnieje. Istotne jest tu przede wszystkim rozstrzygnięcie kwestii czy cyberprzestrzeń stanowi przedłużenie suwerenności istniejącej w świecie fizycznym, czy też stanowi nowe pojęcie prawa międzynarodowego publicznego. W celu rozważenia wspomnianego problemu, praca podejmuje kwestię tego, jak w ujęciu prawnym należy traktować cyberprzestrzeń, rozpatrując koncepcję jej eksterytorialności, suwerenności czy też koncepcji traktowania jej jako *res communis omnium*. Rozpatrywane jest także zagadnienie granic w cyberprzestrzeni, ich technicznych i prawnych aspektów jak też sposobów ich delimitacji i demarkacji. Na kanwie wspomnianych rozważań możliwe jest przeprowadzenia analizy naruszeń suwerenności i powstającego prawa konfliktów cybernetycznych jak i konfliktów fizyczno-cybernetycznych a także możliwych do zastosowania remediów - prawnych i faktycznych. Opisanie wspomnianych remediów pozwala na wskazanie środków, za pomocą których państwa mogą chronić własną suwerenność zarówno cyberprzestrzenną jak i fizyczną przed naruszeniem mającymi swoje źródło w cyberprzestrzeni.

Ostatnim analizowanym zjawiskiem, jest tzw. *cyberlawfare*, a więc pojęcie denotujące stosowanie *Lawfare* - tj. zjawiska militaryzacji prawa, a więc takiego jego stosowania w konflikcie asymetrycznym które ma na celu spowodowanie określonej reakcji po stronie drugiej strony konfliktu- w cyberprzestrzeni . Wobec faktu, że prawo cyberprzestrzeni ciągle jest w fazie wczesnego rozwoju, a normy tradycyjnego prawa międzynarodowego (w tym prawa konfliktów zbrojnych) stosowane do cyberprzestrzeni w drodze analogii ciągle nie są poparte ugruntowaną praktyką międzynarodową - stosowanie *lawfare* w cyberprzestrzeni prowadzi do znaczącego utrudnienia skutecznej obrony własnej suwerenności, zarówno cyberprzestrzennej (wobec naruszeń wyłącznie informatycznych) jak i fizycznej (wobec możliwości prowadzenia operacji cyberprzestrzennych mających skutki kinetyczne).

6. Główne ustalenia.

Podstawowym wnioskiem płynącym z rozważań przeprowadzonych w rozprawie niniejszej jest potwierdzenie tezy o istnieniu specyficznej cyberprzestrzennej suwerenności. Suwerenność ta jest jednak oparta o granice funkcjonalne - stanowiące

funkcję suwerenności opartej o zasadę terytorialności (a więc tradycyjnej wykonywanej w świecie fizycznym) jak i kluczowych interesów państwa realizowanych w informatycznej części cyberprzestrzeni (a więc mających odniesienie do jego fizycznego terytorium) - stanowiących *sui generis* terytorium cyfrowe. Ta konstatacja prowadzi do wniosku o konieczności zmiany "kolejności" wykonywania jurysdykcji; wobec wszechobecności cyberprzestrzeni - podstawowym środkiem ochrony suwerenności w rozumieniu opisanym powyżej staje się jurysdykcja nadzwyczajna. Jurysdykcja zwyczajna staje się *de facto* (choć jak się wydaje - nie *de iure*) subsydiarna.

Wspomniane powyżej niejasności, nie ograniczają się wyłącznie do suwerenności i jurysdykcji. Podobne okoliczności wpływają też na konstrukcję norm prawa międzynarodowego publicznego regulujących cyberprzestrzeń, które muszą mieć na uwadze istnienie i specyficzną konstrukcję *lex informatica*. W połączeniu z coraz większą faktyczną rolą cyberprzestrzeni w obrocie publicznoprawnym - dochodzi więc do inkorporacji nowego *sui generis* systemu prawnego do prawa międzynarodowego publicznego. Powoduje to także, że normowanie faktyczne i afordancje stają się *de facto* źródłami prawa międzynarodowego publicznego, w konsekwencji rozszerzając katalog jego podmiotów daleko poza jego tradycyjne pojmowanie. Wzrasta bowiem rola aktorów niepaństwowych, czy wręcz podmiotów prawa prywatnego, które w drodze normowania faktycznego zyskują wpływ na cyberprzestrzeń i jej prawo.

Faktyczne zmiany wywołane przez cyberprzestrzeń zachodzące w systemie prawa międzynarodowego w szczególności redefinicja suwerenności i jurysdykcji, jak i swoista "demokratyzacja" obrotu międzynarodowego, ma znaczący wpływ na prawo konfliktów zbrojnych. Traci ono bowiem swoją ostrość, ze względu na powstające luki prawne - wynikłe z istnienia i stosowania *lex informatica*, afordancji i normowania faktycznego. Ponieważ suwerenność w cyberprzestrzeni nie może być ze swej natury jasno rozgraniczona, dochodzi do znaczącego rozmycia możliwości obrony suwerenności przez państwa (zarówno w jej fizycznym jak i cyberprzestrzennym aspekcie)

7. Podsumowanie.

Rozprawa niniejsza jest próbą wskazania, że istnienie cyberprzestrzeni ma wpływ na niewątpliwe i daleko idące zmiany w samej istocie państwowości, dotychczas opierającej się na wykonywaniu jurysdykcji wobec określonego terytorium przez suwerennych aktorów prawa międzynarodowego. Pomimo tych zmian, państwa ciągle wykonują przyimoty suwerenności, zachowując jej istotę - którą jest ochrona kluczowych interesów państwa. Przywołane w rozprawie elementy praktyki międzynarodowej, jak i orzecznictwa międzynarodowego, a także odpowiedniego stosowania do cyberprzestrzeni ogólnych i utrwalonych już zasad prawa międzynarodowego publicznego wydają się potwierdzać postawioną w rozprawie tezę badawczą. Badania w niej przeprowadzone wydają się potwierdzać tezę o istnieniu suwerenności w cyberprzestrzeni. O ile bowiem ta ostatnia prowadzi do istotnych zmian w funkcjonowaniu współczesnego świata, przedwczesne wydaje się wieszczenie zmięczenia państw narodowych i załamania się możliwości wywierania przez nie wpływu na kształt tego świata. Utrzymanie jednak tej roli, za pomocą zupełnie nowych narzędzi i w zupełnie nieznanym wcześniej środowisku prawnym, skutkuje także istotnym przededefiniowaniem prawa międzynarodowego publicznego. To ostatnie bowiem doznaje zmian z dwóch powodów. Po pierwsze, dochodzi do zmiany sposobu wykonywania już istniejących norm prawa międzynarodowego, przede wszystkim zwyczajów, ze względu na zmianę stosunków faktycznych. Po drugie, cyberprzestrzeń skutkuje powstaniem równoległego do tradycyjnego *ius gentium* systemu prawa ponadnarodowego jakim jest *lex informatica*. Należy także zauważyć, że wspomniane zmiany mają istotny wpływ na prawo międzynarodowe publiczne *per se*, także w zakresach przedmiotowych wykraczających poza kwestie leżące w polu zainteresowania rozprawy niniejszej.