*Prof. zw. dr hab. Maciej Perkowski*
*Katedra Prawa Międzynarodowego Publicznego*
*Wydziału Prawa*
*Uniwersytetu w Białymstoku*

Białystok, dnia 14 listopada 2018 r.

# Recenzja rozprawy doktorskiej Pana Przemysława Roguskiego

**pt. *Cyberoperacje w świetle prawa międzynarodowego***

W związku z powołaniem przez Radę Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego na recenzenta rozprawy doktorskiej Pana mgr. Przemysława Roguskiego pt. *Cyberoperacje w świetle prawa międzynarodowego* (dalej: rozprawa lub praca doktorska, bądź dysertacja), napisanej pod kierunkiem dr hab. Brygidy Kuźniak (na tymże Wydziale), przedstawiam poniżej jej ocenę.

Cyberprzestrzeń jest dla prawa olbrzymim wyzwaniem. Gdy ludzkość kształtowała prawo jako kluczowy mechanizm regulowania swych relacji i położenia, nie wyobrażano sobie istnienia sfery wirtualnej w znanym nam kształcie. Nawet jeśli klasyczne uogólnienia dawnych myślicieli można do niej ewentualnie dopasować, nie wynika to zapewne z wyobrażania (przezeń) Internetu i jego możliwości, lecz z ich uniwersalnej wymowy. Obecnie liczne filary pojęciowe tworzonego od wieków prawa: terytorium, suwerenność, granice, jurysdykcja (i inne im podobne) w zetknięciu z cyberprzestrzenią okazują się na ogół nieadekwatne. Co prawda bezsporne czynności cybernetyczne realizowane w dobrej wierze, zapewniają prawnikom pozorny spokój (nie weryfikując skuteczności prawa), jednak cyberprzestrzeń coraz intensywniej wymusza zainteresowanie sobą. O ile poruszając się w sferze prywatnoprawnej można przyjąć, że aktywność prawodawcy kształtują potrzeby obrotu prawnego, o tyle w sferze publicznoprawnej sytuacja przedstawia się zgoła odmiennie. Dominująca tu administracja publiczna musi zabezpieczać i porządkować cyberprzestrzeń, co najmniej w wykorzystywanym przez siebie zakresie. Nie jest to bynajmniej zadanie łatwe. To zaś, co sprawia trudności praktyce, (przewrotnie) budzi niekłamane zainteresowanie nauki.

Z drugiej strony – i nauce nie przychodzi łatwo zajmowanie się problematyką cyberprzestrzeni. W warunkach balansowania pomiędzy tym, co jeszcze nie poddaje się metodologii naukowej, a tym, co już przestarzałe i przez praktykę marginalizowane trudno jest uchwycić istotę rzeczy. Nie sprawdza się też w prawniczym badaniu cyberprzestrzeni (często praktykowane) podążanie „krok w krok" z praktyką, jako jej obserwator i sprawozdawca, gdyż na ogół praktyka wyprzedza, a nieraz i „gubi" obserwatora. Nie oznacza to oczywiście sprowadzenia nauki do metaforycznej roli barona Munchausena (któremu – wbrew fizyce – przyszło wydobyć się z bagna chwytem „za swą czuprynę"). Wydaje się, że zadaniem nauki jest kreacja lub identyfikacja nowych rozwiązań dla cyberprzestrzeni i konstruktywne proponowanie ich praktyce, a ważniejsza od (nieodzownej skądinąd) wiedzy, jest tu (odpowiedzialna) wyobraźnia. Skalę wyzwania, jakim jest prawnicze ujęcie cyberprzestrzeni doprawdy trudno przecenić. Z drugiej strony zagadnieniem tym zajmować się trzeba. Geometryczny przyrost problemów i zagrożeń w połączeniu z nieodwracalnością ludzkiej ekspansji w cyberprzestrzeń powodują, że wypracowanie prawniczych rozwiązań optymalizacyjnych jawi się potrzebą chwili, zaś znalezienie adekwatnego paradygmatu cyberprzestrzeni stanowi jedno z poważniejszych wyzwań cywilizacyjnych. Z uznaniem przyjąłem więc wybór tematyki rozprawy doktorskiej Pana magistra Przemysława Roguskiego, która warta jest rozprawy doktorskiej, obrony i... konstruktywnej krytyki. Nauka – jeśli od początku nie zgłębi kompleksowo tak złożonych nowych problemów – utrwala niekompletne ujęcia, które później korzystają z „ochrony przed podważaniem" (jak niektóre prawne aspekty ochrony klimatu, czy... własności intelektualnej). Dlatego też, niezależnie od doceniania (na które Doktorant zasługuje) warto poszukać w rozprawie tego, co można rozważyć pod kątem doskonalenia. Odnośnie tematyki rozprawy – słowa uznania chciałbym skierować także wobec Pani Promotor – Prof. Brygidy Kuźniak, która z pewnością przyczyniła się do przedmiotowego ulokowania rozprawy oraz klarownego ujęcia tematu („Cyberoperacje w świetle prawa międzynarodowego"). Po przeanalizowaniu pracy pozwolę sobie wszakże zgłosić uwagę odnośnie relacji tytułu i treści recenzowanej pracy. Otóż Autor skupiając się podmiotowo na państwach (z czym polemizuję w dalszej części recenzji) powinien odzwierciedlić to wprost, tytułując rozprawę: „Cyberoperacje państw w świetle prawa międzynarodowego". W obecnym ujęciu można oczekiwać podmiotowego uwzględnienia wprost (a nie tylko pośrednio) „non-state actors" (co ostatecznie byłoby dla rozprawy korzystne naukowo).

Autor recenzowanej pracy stawia sobie za cel zidentyfikowanie standardów postępowania państw w cyberprzestrzeni. Innymi słowy, zamiarem Autora jest zbadanie, w jaki sposób należy interpretować podstawowe prawa i obowiązki państw, wynikające m.in. z Karty Narodów Zjednoczonych oraz reguł dotyczących odpowiedzialności międzynarodowej państw, w specyficznych warunkach cyberprzestrzeni. Autor postanowił ustalić (główny problem badawczy), 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. Hipoteza badawcza Przemysława Roguskiego jest trzystopniowa: po pierwsze, praca zakłada – jako warunek *sine qua non* – że prawo międzynarodowe ma zastosowanie w cyberprzestrzeni; po drugie, obowiązujące prawo międzynarodowe jest wystarczające do wyznaczenia ram prawnych działań państw w cyberprzestrzeni, jednakże konieczna jest jego wykładnia pod kątem specyfiki wykorzystywanej technologii informacyjnej i telekomunikacyjnej; po trzecie, jako postulat *de lege ferenda*, ze względu na specyfikę cyberprzestrzeni niektóre zagadnienia wymagają stworzenia bardziej konkretnych norm postępowania, uwzględniających aspekty techniczne sieci komputerowych oraz globalny, transgraniczny i anonimowy charakter cyberprzestrzeni, by uniknąć sytuacji *non liquet*. Założenia wydają się klarowne i pomysłowe. Już na tym etapie rodzi się wrażenie o intuicji badawczej Doktoranta. Z drugiej wszak strony pojawia się obawa, czy takie właśnie podejście nie wpisuje się w przyczyny nieskuteczności prawa międzynarodowego w cyberprzestrzeni? Wszak cyberprzestrzeń (Internet) – sama w sobie – nie poddaje się łatwo pojęciom i procedurom dotychczasowego prawa, a podejście życzeniowe okazuje się czasem naiwne (jak przy ochronie klimatu). To, że nie narodziła się – póki co – koncepcja specjalnego uregulowania cyberprzestrzeni – nie powinno automatycznie prowadzić do wniosku o braku potrzeby takowej. Poszukiwać symbolicznego „Graala" (w tym zakresie oczywiście) warto, a w tym czasie można (a nawet trzeba) stosować odpowiednio obecne prawo międzynarodowe, w czym zgadam się z Przemysławem Roguskim. Z tym większym zaciekawieniem można skłonić się ku analizie treści poszczególnych rozdziałów recenzowanej rozprawy.

Przedmiotem analizy prawnej (w świetle prawa międzynarodowego publicznego) przeprowadzonej przez Pana Przemysława Roguskiego są „cyberoperacje" (przez które rozumie on działania państw w cyberprzestrzeni, skierowane przeciwko infrastrukturze cybernetycznej innych państw). Autor nie odnosił się tu do prawnokarnych aspektów działań indywidualnych hakerów, których nie da się przypisać państwu, natomiast zbadał działania

podmiotów niepaństwowych, wykorzystujące infrastrukturę cyberprzestrzenną państwa do szkodliwych czynności skierowanych przeciwko bezpieczeństwu innego państwa i mogące naruszać międzynarodowy pokój i bezpieczeństwo, którym państwo powinno przeciwdziałać (w ramach należytej staranności). Jak już podnosiłem – takie podejście (jedynie pośrednie ujęcie non-state actors) wydaje się nie w pełni adekwatne wobec realiów cyberprzestrzeni, a w konsekwencji może prowadzić do nieadekwatnych wniosków i nieuchronnych sprzeczności (Doktorant sam przyznaje, że dotychczas pomimo mnogości cyberoperacji – jak dotąd żadne państwo nie stwierdziło istnienia konfliktu w cyberprzestrzeni, co ogranicza możliwości badania praktyki państw, a oparcie się na domniemaniach jest dalece niewystarczające). Z drugiej strony, gdyby (z jakichś względów) państwa podchwyciły idealistyczne założenie (czego wykluczyć nie można), równocześnie wypracowując skuteczne metody operacyjne zabezpieczania cyberprzestrzeni – wówczas zamiast ukształtowania się międzynarodowego ładu cybernetycznego doszłoby do rozciągnięcia się ładu międzynarodowego na cyberprzestrzeń. Poza zakresem swojej analizy Autor pozostawił też zagadnienia związane ze stosowaniem międzynarodowego prawa humanitarnego w sytuacji konfliktów zbrojnych w cyberprzestrzeni (zwłaszcza, że – jak już podkreślałem – dotychczas żadne państwo nie stwierdziło istnienia konfliktu zbrojnego w cyberprzestrzeni). Zabrakło tu wyraźniejszej refleksji nad mocno problematyczną kwestią właściwości. Nie przekonuje zaś stwierdzenie, że odniesienie się do dyskusji *de lege ferenda* o potrzebie stworzenia instrumentów prawnych zakazujących niektórych metod walki w cyberprzestrzeni przekracza ramy rozprawy. Zakreśliwszy w taki sposób zakres przedmiotowy rozprawy Doktorant postanowił rozstrzygnąć: czy prawo międzynarodowe obowiązuje w cyberprzestrzeni?, czy działanie państwa w cyberprzestrzeni może być sklasyfikowane jako użycie siły (w rozumieniu art. 2 ust. 4 KNZ)?, czy cyberoperacja może naruszyć zakaz interwencji oraz suwerenność i zwierzchnictwo terytorialne państwa?, w jakich sytuacjach państwo ponosi odpowiedzialność międzynarodową za cyberoperacje?, a ponadto – czy państwo ma obowiązek zapobiegania wykorzystaniu jego cyberinfrastruktury do przeprowadzenia operacji przeciwko innemu państwu? Służy temu odpowiednio ukształtowana struktura recenzowanej rozprawy.

Doktorant zaplanował strukturę rozprawy dwojako. Z jednej strony wydaje się ona prosta, gdyż zasadza się na zaledwie czterech rozdziałach. Z drugiej strony każdy z rozdziałów został bogato rozplanowany wewnątrz (do czterocyfrowej klasyfikacji numerycznej), co każe ostatecznie uznać strukturę rozprawy za złożoną. Pewne wątpliwości budzi sekwencja rozdziałów I i II. Obecny rozdział II omawia zagadnienie wyjściowe

przedmiotowo dla całej rozprawy, a jego roszada z obecnym rozdziałem pierwszym udoskonaliłaby strukturę rozprawy także względem kolejnych rozdziałów. W takim wariancie po objaśnieniu czytelnikowi ogólnych założeń stosowania prawa międzynarodowego w cyberprzestrzeni (proponowany rozdział I, obecnie II), przedstawione zostałyby aspekty pojęciowe tytułowych cyberoperacji (rozdział II, obecnie I), by kontynuując – rozważyć ich kwalifikacje prawną (rozdział III) i odpowiedzialność zań (rozdział IV). Niezależnie od uwag odnośnie sekwencji rozdziałów – w obecnym ujęciu rozprawy (skupionym podmiotowo na państwach) sugerowałbym doprecyzowanie tytułu obecnego rozdziału I (który proponowałem jako II), jako „Definicje i przykłady cyberoperacji państw", a także tytułu rozdziału III (jako „Kwalifikacja prawna cyberoperacji państw"). Ponadto należałoby włączyć do spisu treści „zagubiony" tytuł rozdziału IV („Odpowiedzialność międzynarodowa państw za cyberoperacje"). W obecnym rozdziale II sugerowałbym zmodyfikować tytuł podrozdziału 2.1, aby nie powtarzał on (w zasadzie) tytułu rozdziału, zachowując logiczny związek ze swą treścią (np. „Teoretyczne koncepcje stosowania prawa międzynarodowego w cyberprzestrzeni" itp.). Względem chętnie stosowanych w rozprawie częściowych podsumowań, które oceniam jako atut pracy, zabrakło nadrzędnych reguł ich ujmowania [„Podsumowanie" (jak w przypadku 1.3), czy „Podsumowanie rozdziału i wnioski" (jak w przypadku 2.4), czy również „Podsumowanie i wnioski" na poziomie podrozdziału (jak w przypadku 3.1.5, 3.2.4), „Wnioski" na poziomie punktu odnośnie „Podsumowania i wniosków" (jak w przypadku 3.3.4.3)]. Tendencja zaczerpnięta, jak się wydaje, z metodologii niemieckiej (a na pewno dlań charakterystyczna) jest korzystna dla naukowej ewaluacji i prezentacji rozważań, jednak wymaga „żelaznej" konsekwencji metodologicznej. Ponadto – wobec tak wielu tytułowo ujętych „podsumowań" sugerowałbym zwieńczyć rozprawę „Zakończeniem", co będzie mieć też korzystny wpływ na adekwatność (wszak Doktorant nie tylko podsumował tam wyniki badań, ale zawarł też stosowne wnioski i postulaty). W kwestii struktury – gorliwości optymalizacyjnej nigdy nie jest za wiele. Odwrotnie rzecz się ma z elementami funkcjonalnymi rozprawy, gdzie nadgorliwość przyjmowanych rozwiązań przywodzi na myśl pytanie o zasadność (np. ujmowanie w wykazie skrótów, obok istotnie nieoczywistych także tych, które wątpliwości w żadnej mierze nie budzą, np. ONZ, ZSRR, USD itp.).

Odnosząc się do treści recenzowanej rozprawy, a poczynając od jej klarownego „Wstępu" – także udało mi się sformułować kilka uwag. Odnoszę wrażenie, że Doktorant wskutek nabycia ogromnej wiedzy w przedmiocie tytułowej problematyki, bywa czasem

nieostrożny, zważywszy na specyfikę cyberprzestrzeni. Czy na pewno można bez zastrzeżeń stwierdzić „najnowsze statystyki", dodając „(z marca 2017 r.)", gdy mowa o dostępie do Internetu? Sugerowałbym tu zwrot wyjaśniający podejście, a zabezpieczający Autora przed zarzutem nieaktualności. Dalej Doktorant formułuje zdanie „Można zaryzykować stwierdzenie, iż idea pionierów cyberprzestrzeni, by powstała nowa, przekraczająca wszelkie granice „przestrzeń" międzyludzka, stała się rzeczywistością", lecz nie wyjaśnia, jakich pionierów ma na myśli, ani nie odsyła do wyjaśniających tą wątpliwość opracowań. Ciekawie jawi się za to pogrupowanie problemów/wyzwań politycznych i prawnomiędzynarodowych (od s. 2). Tu miałbym uwagę, że problemem wartym uwagi z perspektywy badacza prawa międzynarodowego jest z pewnością „suwerenność w cyberprzestrzeni" (która ujawnia się nieuchronnie dalej, choćby w rozważaniach odnośnie jurysdykcji w cyberprzestrzeni), jako warunek wstępny dla ujęcia tytułowej problematyki, które zaproponował Doktorant (skupienie się na państwach). Zagadnienie – samo w sobie niełatwe – można było teoretycznie odnieść do znakomitej rekonstrukcji idei w prawie międzynarodowym, którą stworzył przed laty Roman Kwiecień, pokusiwszy się przy tym o rozważania prekursorskie, adekwatne względem tytułowej problematyki. Można było też odnieść się w tym względzie do poglądów innych badaczy prawa w cyberprzestrzeni, których prace *nota bene* zawierają się w bibliografii recenzowanej rozprawy. Pierwszy rozdział rozprawy Pan Przemysław Roguski poświęcił sprecyzowaniu warstwy pojęciowej, a zwłaszcza zagadnień: cyberprzestrzeni, cyberoperacji oraz cyberataku. Stopniowo zaznajamiając czytelnika z tytułową problematyką, także w ujęciu praktycznym, omówił aktualne przykłady cyberoperacji. Na uwagę zasługuje tu zwłaszcza przegląd definicji (ss. 12-13 i 20-21), a także rozważania na ss. 16-17. W rozdziale drugim (bardzo dobrym!) Doktorant rozważył problem stosowania prawa międzynarodowego w cyberprzestrzeni. Słusznie przewidywał, że gdyby badanie wykazało, 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. Przy czym istnienie takiej normy o charakterze zwyczajowym musiałoby być udowodnione na podstawie analizy praktyki państw oraz *opinio iuris*. Dalsze badanie przedmiotowego problemu polegałoby więc przede wszystkim na ustaleniu zakresu dotychczasowej praktyki oraz *opinio iuris*. W odwrotnym przypadku, a więc jeśli badania wykazałyby, że obecne prawo międzynarodowe ma zastosowanie w cyberprzestrzeni, dalszy przebieg analizy koncentrowałby się na wykładni (opartej o praktykę państw i doktrynę) traktatowych i zwyczajowych norm prawa międzynarodowego w odniesieniu do

cyberprzestrzeni. Próba odpowiedzi na pytanie o stosowanie prawa międzynarodowego w cyberprzestrzeni podjęta została na podstawie analizy opinii państw i organizacji międzynarodowych potwierdzających formowanie się praktyki oraz *opinio iuris* w tym zakresie. Powtórzę tu, że obecny rozdział drugi powinien rozpoczynać rozprawę, choć oczywiście Autorowi należny jest przywilej kształtowania rozprawy (z czym wiąże się też stosowna odpowiedzialność). W rozdziale trzecim Autor rozważył kwalifikację prawną cyberoperacji. W szczególności, podjął próbę ustalenia, czy cyberoperacje mogą stanowić użycie siły w rozumieniu art. 2 ust. 4 KNZ, a także kryteriów kwalifikowania działań państw w cyberprzestrzeni jako użycia siły. Ponadto rozważa kwalifikację prawną tzw. operacji „*below the threshold*" (poniżej progu użycia siły) w świetle zakazu interwencji w sprawy wewnętrzne oraz zakazu naruszenia suwerenności i integralności terytorialnej państw. W rozdziale czwartym (który obok obecnego rozdziału II oceniam najwyżej) Doktorant podjął tematykę odpowiedzialności międzynarodowej państw za przypisane im działania w cyberprzestrzeni, jak również za operacje aktorów niepaństwowych, działających z ich terytorium. Szczególna uwaga poświęcona została problematyce przypisania cyberoperacji państwu w świetle anonimowości cyberprzestrzeni i związanych z tym trudności technicznych przy identyfikacji realizatora cyberoperacji. To właśnie tymi rozważaniami Doktorant jest w stanie odeprzeć (albo zrównoważyć) krytykę podejścia ograniczającego stronę podmiotową rozprawy do państw (którą i ja zgłosiłem). 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. Na zakończenie Doktorant niepotrzebnie powtórzył *in extenso* całe frazy ze wstępu. Na s. 259 zasygnalizował sytuację patową w pracach nad uregulowaniem cyberprzestrzeni w sposób, ku któremu się skłania, wskazując przy tym, że zgłaszane są inne koncepcje (np. dobrowolnego samoograniczania), ale nie były one przedmiotem Jego rozważań (a szkoda!). Ustalenia odnośnie możliwości kwalifikowania cyberataków wedle formuły użycia siły z Karty Narodów Zjednoczonych jawią się elokwentnie, ale problemu nie rozwiązują (wszak masowe naruszenia praw człowieka mogą być uznane za zagrożenie bezpieczeństwa i pokoju światowego, ale nie zawsze... i w tym problem). Interpretacja jest z natury względna, a cybernetyczni atakujący bezwzględni w wykorzystywaniu tego, dlatego rozwiązań trzeba szukać nadal. Wydaje się, że normą prawa zwyczajowego, którą Doktorant mógł odpowiednio wykorzystać (przy rozważaniach zwierzchnictwa terytorialnego nad infrastrukturą ICT i odpowiedzialnością za jej użycie przeciwko celom w innym państwie) jest zasada dobrego sąsiedztwa (teoretyczne rozważana, opisana i ugruntowana). Interesująco

jawi się kwestia, jak Doktorant wyobraża sobie egzekwowanie (także instytucjonalnie) dynamicznej wykładni Karty Narodów Zjednoczonych w praktyce? Mam też wątpliwość, czy słusznie ostatnią odpowiedź (na pytanie 5: „państwo ma obowiązek przeciwdziałania wykorzystaniu swego terytorium oraz znajdującej się na nim infrastruktury ICT do przeprowadzenia szkodliwych cyberoperacji przez aktorów niepaństwowych...") opatrzył On zastrzeżeniem („... o ile posiada wiedzę o planowanej lub trwającej cyberoperacji"). Mimowolnie nasuwa się tu zaprzeczanie przez Władimira Putina obecności rosyjskich żołnierzy na terytorium Ukrainy w trakcie kryzysu krymskiego i secesji wschodnich obszarów Ukrainy... Niezależnie od zgłoszonych uwag chciałbym podkreślić, że rozprawa zawiera ogrom danych, wyjaśnień i powiązań przedmiotowych, które stanowią wkład Pana Przemysława Roguskiego do dorobku nauki prawa międzynarodowego. Po ewentualnym udoskonaleniu rozprawy (o ile zgłoszone przez recenzentów i dyskutantów uwagi Doktorant zechce w tym celu wykorzystać) warto ją z pewnością opublikować, najlepiej w języku angielskim, do czego zdecydowanie zachęcam.

W recenzowanej rozprawie Doktorant zastosował metodologię charakterystyczną dla nauk prawnych. W szczególności – metodę formalno-dogmatyczną, zastosował przy badaniu treści aktów prawnych, zaś metodę porównawczą, przy omawianiu cyberstrategii państw. Przeprowadził analizę licznych dokumentów źródłowych (deklaracji, komunikatów, ekspertyz, cyberstrategii oraz innych oficjalnych dokumentów) stałych członków Rady Bezpieczeństwa ONZ, Polski, Niemiec oraz szeregu innych państw i organizacji międzynarodowych (starając się analizować teksty źródłowe w językach urzędowych, zaś w przypadku Rosji i Chin – udostępnione przezeń wersje anglojęzyczne dokumentów oficjalnych). Ponadto przeanalizował obszerną literaturę z zakresu tytułowej problematyki, głównie w języku polskim, niemieckim, a przede wszystkim angielskim, akcentując prymat zaawansowania doktryny anglojęzycznej w obszarze cyberoperacji. Wiele z tych publikacji ma charakter interdyscyplinarny, łącząc analizę prawną z analizą techniczną, wojskową i polityczną. Pomimo względnego bogactwa literatury przedmiotu niewiele opracowań kompleksowo analizuje obowiązywanie norm prawa międzynarodowego w cyberprzestrzeni w odniesieniu do działań państw (abstrahując od słuszności, bądź nie samego założenia). Tym niemniej (jak zauważa sam Autor) opracowania tytułowej problematyki istnieją, także w piśmiennictwie polskim. Byłoby elegancko i merytorycznie zasadnie, aby śmielej wykorzystywać (także krytycznie) to, co w zakresie tytułowej problematyki zaproponowali

inni autorzy. Niezależnie od tego – recenzowana rozprawa – z powodzeniem – podejmuje próbę wypełnienia doktrynalnej luki.

Strona formalna recenzowanej rozprawy zasługuję na pozytywny odbiór, jednakże i tu można zgłosić pewne uwagi. Przypisy warto wyrównać i usunąć nieplanowane odstępy między nimi. Choć w opracowaniach naukowych o dużej objętości usuwanie uchybień językowych wydaje się procesem „bez końca", to jednak tak ambitna rozprawa warta jest usunięcia usterek, które na poszczególnych jej etapach udaje się zidentyfikować (np. na stronie 5 zwrot „co rodzi to pytanie"; na s. 10 jest „dotyczący", zamiast „dotyczącym"; na s. 11 jest „M Kowalski", zamiast „M. Kowalski"; w przypisie 32 została „zdublowana" J. Kulesza; na s. 16 jest „Wszystkie..." zamiast „wszystkie..."; dyskusyjne tytułowanie małymi literami dalszych członów nazw czasopism w przypisach: 146, 153, 233, a wielką literą dalszych członów tytułu książki w przypisie 290; problematyczne rozciągnięcie przypisów na 2 pełnych stronach – 95 i 96). Wskazane uchybienia mają charakter techniczny i w żadnej mierze nie uchybiają walorom merytorycznym recenzowanej rozprawy, tym niemniej właśnie owym walorom warto „oszczędzić nieodpowiedniego towarzystwa" (usterek).

*

Po zapoznaniu się z rozprawą doktorską Pana mgr. Przemysława Roguskiego pt. *Cyberoperacje w świetle prawa międzynarodowego*, napisanej pod kierunkiem naukowym dr hab. Brygidy Kuźniak, stwierdzam, że stanowi ona oryginalne rozwiązanie problemu naukowego oraz wykazuje ogólną wiedzę teoretyczną kandydata w dziedzinie nauk prawnych w dyscyplinie prawo oraz umiejętność samodzielnego prowadzenia pracy naukowej. Oznacza to, że rozprawa ta spełnia wszystkie wymogi, określone w art. 13 ust. 1 ustawy z dnia 14 marca 2003 roku o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (t.j. Dz. U. z 2017 r. poz. 1789). Tym samym może ona stanowić podstawę do przeprowadzenia dalszych czynności w przewodzie doktorskim, w tym do nadania stopnia naukowego doktora nauk prawnych w zakresie prawa. Na tej podstawie wnioskuję o przyjęcie rozprawy doktorskiej Pana mgr. Przemysława Roguskiego pt. *Cyberoperacje w świetle prawa międzynarodowego* oraz rekomenduję dopuszczenie jej do publicznej obrony.