

Katowice, 25 marca 2019 roku

dr hab. Miron Lakomy
Zakład Stosunków Międzynarodowych
Instytut Nauk Politycznych i Dziennikarstwa
Uniwersytet Śląski w Katowicach

RECENZJA ROZPRAWY DOKTORSKIEJ PT.

COMBATING CYBERCRIME: EUROPEAN PRACTICES AND NATIONAL IMPLEMENTATION

autorstwa mgr Ludmiły Dackowej

1. Wstęp

Recenzowana rozprawa stanowi poprawioną i poszerzoną (liczącą 193 strony) wersję pracy, którą miałem okazję ocenić w 2018 roku. Ze względu na fakt, iż zawierała ona wiele błędów formalnych oraz merytorycznych, choć zarazem posiadała pewien potencjał, zasugerowałem skierowanie jej do korekty. Z tego też względu, w niniejszej recenzji pominię obszerną (a obecną w poprzedniej) charakterystykę treści, założeń i struktury pracy autorstwa Ludmiły Dackowej. Skupię się natomiast na zagadnieniach kluczowych, które determinują jej wartość jako oryginalnego opracowania naukowego.

W tym kontekście, chciałbym już na wstępie podkreślić, iż Autorka wykazała się dużą dojrzałością naukową. Nowa wersja jej rozprawy od razu sprawia zgoła inne, lepsze wrażenie. Dowodzi nie tylko znacznej pracy, jaką Doktorantka wykonała nanosząc poprawki, ale i jej wysokich zdolności analitycznych. Nie oznacza to oczywiście, iż praca ta jest pod każdym

względem doskonała, jednak należy docenić starania Autorki, aby zlikwidować najpoważniejsze jej mankamenty.

2. Ocena warstwy formalnej rozprawy

Przede wszystkim, zdecydowanej poprawie uległa strona formalna tej anglojęzycznej rozprawy. Zauważalna jest wyższa jakość użytego języka, który – co widać – został poddany profesjonalnej korekcie. Dzięki temu wywody Autorki stały się w pełni zrozumiałe i klarowne. Co prawda, miejscami zauważalne są jeszcze lapsusy językowe i dość nieporadnie sformułowane zdania (np. na stronie 25), jednak jest to już problem marginalny. Innymi słowy, należy stwierdzić, iż praca została napisana poprawnie pod względem językowym i stylistycznym.

Jeśli chodzi o warstwę techniczną to również trudno mieć większe zastrzeżenia. Autorka ustrzegła się poważniejszych błędów, których zresztą nie było wiele także w poprzedniej wersji rozprawy. Co prawda, zdarzają się w pracy literówki, jednak występują one rzadko (np. w nazwisku profesora P. Sienkiewicza na stronie 7). Również forma bibliografii nie budzi moich zastrzeżeń – została ona przygotowana starannie. Świadczy też korzystnie o wykonanej przez Autorkę kwerendzie. Nieco większym problemem jest natomiast forma odniesień, w których nie zachowano konsekwencji. Chodzi tu m.in. o tytuły pisane bez kursywy, brak kropek na końcu niektórych przypisów (np. s. 86), występowanie na zmianę czcionki normalnej i kursywy w tych samych ich fragmentach (np. numeracja stron czy tytuły – *vide* s. 4, 11, 13). Nie są to jednak niedociągnięcia, które znacząco obniżałyby ocenę pracy pod względem formalnym. Reasumując ten wątek, należy więc podkreślić, iż formalna strona rozprawy jest poprawna.

3. Ocena warstwy metodologicznej i merytorycznej rozprawy

Metodologia pracy, jako taka, nie budzi poważniejszych zastrzeżeń. Hipoteza badawcza nie jest oczywista, a cele badawcze zostały jasno sformułowane. Zastosowany zestaw metod i technik badawczych jest charakterystyczny dla badań nad polityką cyberbezpieczeństwa. Niestety, podobnie jak w poprzedniej wersji, należy się ich bardziej domyślać z treści niż z wyczerpującego opisu ze wstępu. Niestety Doktorantka nie zdecydowała się na szersze omówienie metod i technik badawczych w tej części rozprawy, ograniczając się do pewnych ogólnikowych sformułowań.

Warto odnieść się do najważniejszej dla ostatecznej oceny warstwy merytorycznej. Przede wszystkim, należy zaznaczyć, iż Autorka dołożyła starań, aby uporządkować swoje rozważania, które w poprzedniej wersji rozprawy były miejscami dość chaotyczne. Jej wywody są obecnie klarowne, a poszczególne fragmenty rozprawy są ze sobą logicznie powiązane.

Rozdział pierwszy ma charakter teoretycznego wprowadzenia do tematyki cyberbezpieczeństwa i przestępczości komputerowej. Doktorantka w oparciu o bogatą i prawidłowo dobraną literaturę specjalistyczną dokonała przeglądu najważniejszych podejść do takich zagadnień jak cyberprzestrzeń, bezpieczeństwo teleinformatyczne, cyberatak. Omówiła także najważniejsze formy zagrożeń teleinformatycznych. Do tego interesującego rozdziału mam tylko jedną uwagę. Trudno zgodzić się ze stwierdzeniem ze strony 43, iż hakywizm i cyberterrorizm posiadają podobne cechy. Jest dokładnie odwrotnie! Podczas gdy hakywiści dążą do zwrócenia uwagi opinii publicznej dokonując w sumie nieskomplikowanych ataków komputerowych, działalność organizacji terrorystycznych *online* zmierza do osiągnięcia jak największych zniszczeń i strat w zaatakowanych systemach i sieciach.

Część drugą, która charakteryzuje politykę cyberbezpieczeństwa Unii Europejskiej, należy uznać za najbardziej wartościowy fragment tej rozprawy. Autorka bardzo ciekawie omówiła ewolucję tej polityki, scharakteryzowała najważniejsze dokumenty w tej dziedzinie, a także przedstawiła działalność organów UE, które posiadają kompetencje w zakresie bezpieczeństwa teleinformatycznego. Całość rozważań została oparta na bogatych źródłach oraz literaturze specjalistycznej.

W części trzeciej, omawiającej rozwiązania w zakresie cyberbezpieczeństwa przyjęte w wybranych do analizy państwach członkowskich UE, również widoczna jest znaczna poprawa. Przede wszystkim, Autorka usystematyzowała swoje rozważania w poszczególnych podrozdziałach, biorąc pod uwagę te same elementy (m.in. sposób penalizacji aktów cyberprzestępczości). Dzięki temu możliwe stało się porównanie tych polityk ze sobą. O wiele ciekawiej przedstawiono także uwarunkowania polityki bezpieczeństwa teleinformatycznego Holandii, Estonii, Francji, Polski oraz Belgii. Do tego fragmentu można mieć jednak jedną uwagę ogólną. Miejscami zbyt mało miejsca poświęcono przedstawieniu założeń najważniejszych dokumentów i koncepcji regulujących politykę cyberbezpieczeństwa w poszczególnych państwach. Było to szczególnie ewidentne w przypadku Francji. Dość wyrywkowo Autorka podeszła także do charakterystyki najważniejszych zagrożeń pojawiających się *online* – można było je nieco szerzej omówić w oparciu o statystyki

publikowane przez zespoły CERT. Te naturalnie były przywoływane, ale tylko fragmentarycznie.

Ostatni rozdział koncentruje się na wyzwaniach dla polityki cyberbezpieczeństwa zarówno na poziomie państw, jak i na poziomie Unii Europejskiej. Jakkolwiek pierwszy podrozdział zdaje się nieco zbyt krótki i ogólnikowy, to drugi (4.2) został napisany bardzo dobrze. Autorka wykazując się dużym zrozumieniem tej trudnej tematyki wskazała na najważniejsze problemy, które napotyka Unia Europejska w swojej aktywności na rzecz poprawienia stanu bezpieczeństwa teleinformatycznego w państwach członkowskich. Ostatni podrozdział stanowi pewne dopełnienie, omawiając perspektywy rozwoju tego wymiaru aktywności UE w przyszłości.

Zakończenie zawiera wszelkie niezbędne elementy. Wnioski sformułowane przez Autorkę mają pokrycie w treści rozprawy, są rzeczowe i logiczne.

4. Podsumowanie

Reasumując, poprawioną rozprawę doktorską Pani Ludmiły Dackowej oceniam pozytywnie. Jakkolwiek nie jest ona wolna od mankamentów, wśród których należy wymienić przede wszystkim miejscami zbyt ogólnikową charakterystykę często bardzo skomplikowanych zagadnień (treści dokumentów, działalności instytucji zajmujących się sferą cyberbezpieczeństwa), to zawiera ona w sobie wiele wartościowych elementów. Należy podkreślić, iż Doktorantka wykonała olbrzymią pracę zbierając i analizując wielojęzyczną literaturę specjalistyczną, a także źródła, których forma nie zawsze jest łatwa w odbiorze dla przedstawicieli nauk społecznych. Wykazała się ona również nie tylko dobrym zrozumieniem skomplikowanych zagadnień natury teleinformatycznej, ale przede wszystkim uwarunkowań zjawisk pojawiających się w cyberprzestrzeni oraz ich implikacji dla polityki i bezpieczeństwa państw. Wreszcie, jak wspomniano na początku, wykazała się dojrzałością naukową, dokonując głębokich (i nie zawsze łatwych) poprawek w rozprawie doktorskiej.

Pozostaje mi stwierdzić, iż w rodzimej literaturze przedmiotu nie ukazała się dotychczas praca, która porównałaby ze sobą polityki cyberbezpieczeństwa wybranych państw europejskich, na tle działań podejmowanych przez samą UE. Wśród wielu publikacji na temat cyberbezpieczeństwa, które ukazały się w ostatnich latach w Polsce, jest to więc dzieło interesujące, które pozwala lepiej zrozumieć naturę zagrożeń teleinformatycznych w Europie oraz najważniejsze sposoby przeciwdziałania im na terenie UE. Powyższa konstatacja pozwala mi stwierdzić, iż rozprawa doktorska pani Ludmiły Dackowej stanowi

oryginalne rozwiązanie problemu naukowego, tym samym spełniając podstawowy warunek stawiany przez ustawę o stopniach naukowych i tytule naukowym oraz o stopniach i tytułach w zakresie sztuki. Co za tym idzie, wnoszę do Rady Wydziału Studiów Międzynarodowych i Politycznych Uniwersytetu Jagiellońskiego o przyjęcie rozprawy i dopuszczenie mgr Ludmiły Dackowej do dalszych etapów przewodu doktorskiego.


dr hab. Miron Lakomy