Katowice, 05.05.2018

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

RECENZJA ROZPRAWY DOKTORSKIEJ PT.

COMBATING CYBER CRIME: EUROPEAN PRACTICES AND NATIONAL IMPLEMENTATION

autorstwa mgr Ludmiły Dackowej

1.1. Wstępna charakterystyka monografii

Rozprawa autorstwa Ludmiły Dackowej koncentruje się na skomplikowanym zagadnieniu, które od wielu lat cieszy się szczególnym zainteresowaniem badaczy zajmujących się szeroko pojętym bezpieczeństwem teleinformatycznym z perspektywy politologii. Problematyka przeciwdziałania przestępczości komputerowej w państwach Unii Europejskiej oraz Sojuszu Północnoatlantyckiego w ostatnich latach była szeroko dyskutowana w wielu interesujących opracowaniach naukowych, które ukazały się zarówno w formie artykułów, książek, jak i raportów. W tym kontekście, podjęty przez Autorkę temat należy uznać za ambitny, ze względu na wymóg oryginalności wniosków, które powinny zostać zawarte w rozprawie doktorskiej.

Struktura recenzowanej pracy ma charakter problemowy, składa się z czterech rozdziałów, a także wstępu, konkluzji oraz bibliografii. Warto podkreślić, iż jest ona stosunkowo krótka, liczy jedynie 145 stron właściwego tekstu (wraz z bibliografią 172). Nie należy traktować tej uwagi jako zarzutu, choć taka objętość powinna wymuszać na Autorce wyjątkowo konkretne i syntetyczne podejście do wielu zagadnień.

Wstęp zawiera wszystkie niezbędne elementy, w tym przede wszystkim ogólne omówienie problemu badawczego oraz cel badawczy ("analysis of the existing approach towards cybersecurity procurement within selected EU Member States as well as current cybersecurity policy within the EU, current problematic moments in the process of cybercrime procurement and propose ways for their solution by applying the experience of the analysed Member States" - s. 4). Na poziomie państw członkowskich Autorka wybrała do analizy: Belgię, Estonię, Francję, Holandię oraz Polskę. Określono również cztery pytania

badawcze dotyczące rozumienia cyberprzestępczości i jej najważniejszych typów, głównych działań podejmowanych przez UE w celu zwalczania tego zjawiska, analizy regulacji w państwach członkowskich UE w zakresie przeciwdziałania przestępczości komputerowej (wraz z ich analizą porównawczą) oraz luk w systemie cyberbezpieczeństwa UE. Autorka zamierzała także odpowiedzieć na pytanie, na ile występujące w nim niedoskonałości mogą zostać poprawione dzięki czerpaniu z doświadczeń państw członkowskich w tej dziedzinie. Hipoteza pracy brzmi następująco: "The EU currently is not using good practices of the Member States in the field of cybercrime procurement. Cybercrime procurement in the EU remains neglected in comparison with other security priorities" (s. 5).

Ponadto, we wstępie można również odnaleźć fragmentaryczne informacje na temat przyjętego przez Autorkę podejścia badawczego (funkcjonalizm), metodologii (metody jakościowe i ilościowe, "analiza, porównanie, synteza" - s. 5), użytych źródeł, cezury badawczej (lata 2000-"do dziś"- czyli zapewne do 2017 r.) oraz struktury rozprawy.

Pierwszy rozdział zatytułowano "Theoretical approach to the category of cybercrime: definitions, classifications, differences from the other categories in the domain". Słusznie skoncentrowano się w nim na omówieniu podstawowych pojęć z zakresu szeroko pojętego cyberbezpieczeństwa, które zostały użyte w dalszych częściach pracy. Autorka rozpoczęła go od przedstawienia głównych wniosków z dyskusji środowiska akademickiego na temat wpływu rewolucji informatycznej na funkcjonowanie społeczeństw i państw. W pierwszym podrozdziale podjęła próbę zdefiniowania cyberprzestrzeni oraz jej najważniejszych cech, zarówno od strony społecznej, jak i technicznej. W drugim przeszła do omówienia nowej kategorii bezpieczeństwa w ujęciu przedmiotowym, tzn. cyberbezpieczeństwa jako pożądanego stanu przestrzeni teleinformatycznej, wskazując na szereg wyzwań pojawiających się w tym środowisku, m.in. ze względu na anonimowość sprawców przestępstw (s. 14). W podrozdziale trzecim Autorka podjęła próbę omówienia roli komputera jako narzędzia przestępstwa, *ergo* scharakteryzowała takie kategorie jak przestępczość komputerowa, cyberataki oraz cyberterroryzm. Wskazała np. na czynniki, które doprowadziły do tak szybkiego rozwoju cyberprzestępczości w środowisku internetowym. Dokonała również przeglądu różnych typów aktów kryminalnych w tej domenie, zarówno z perspektywy nauk prawnych, informatyki, jak i politologii. Co ciekawe, w rozdziale omówiono także zjawisko cyberwojny, choć nie jest to zagrożenie o charakterze przestępczym.

Rozdział drugi ("The EU legal procurement of cybercrime") Autorka słusznie rozpoczęła od omówienia struktury Unii Europejskiej pod kątem głównych zasad oraz podstaw prawnych jej funkcjonowania. Stanowiło to odpowiedni wstęp do podrozdziału

drugiego, w którym podjęto się przedstawienia polityki cyberbezpieczeństwa UE. Autorka omówiła szereg dokumentów (dyrektyw, strategii) dotyczących tej problematyki, które zostały opracowane przez instytucje Unii od początku XXI wieku, choć wspomniała także o Konwencji Rady Europy o Cyberprzestępczości. W kolejnym podrozdziale scharakteryzowała z kolei zadania i uprawnienia instytucji odpowiedzialnych za cyberbezpieczeństwo UE, w tym np. EC3 oraz ENISA.

W rozdziale trzecim ("Combating cybercrime: practices of the chosen EU Member States") skoncentrowano się na omówieniu działalności wybranych instytucji odpowiedzialnych za zwalczanie zagrożeń teleinformatycznych w kilku państwach członkowskich Unii Europejskiej: Holandii, Estonii, Francji, Polski oraz Belgii. Scharakteryzowano także przyjęte w nich regulacje prawne oraz dokumenty koncepcyjne. Próbę badawczą dobrano na podstawie ich sytuacji geopolitycznej, występujących źródeł zagrożeń teleinformatycznych, oraz dominujących typów przestępczości komputerowej (s. 69). Autorka częściowo omówiła także niektóre typy cyberprzestępczości, które występują w każdym z tych państw, głównie w oparciu o raporty przygotowywane przez korporacje transnarodowe, a także krajowe i międzynarodowe instytucje zajmujące się tą problematyką. Zabrakło jednak szerszego odniesienia do uwarunkowań polityki cyberbezpieczeństwa poszczególnych członków UE, w tym np. stopnia komputeryzacji i informatyzacji społeczeństw oraz infrastruktury krytycznej, jak również omówienia najpoważniejszych incydentów teleinformatycznych, które determinowały ich strategię w tej dziedzinie. Przykładowo, niemal zupełnie pominięto masowe ataki przeciwko Estonii w 2007 roku (nie licząc wzmianki na s. 78).

Rozdział ostatni ("Propositions and recommendations for possible improvement to the cybercrime policy within the EU") rozpoczął się od bardzo ogólnej charakterystyki europejskich statystyk dotyczących cyberprzestępczości. W podrozdziale 4.1. Autorka skupiła się na omówieniu głównych wyzwań dla polityki bezpieczeństwa teleinformatycznego państw członkowskich, dotyczących m.in. rozwoju partnerstwa publiczno-prywatnego czy wymiany doświadczeń i informacji. Następnie przeszła do omówienia wyzwań dla skutecznej polityki cyberbezpieczeństwa samej Unii Europejskiej, odnosząc się np. do rozdrobnienia instytucjonalnego w tej dziedzinie. W podrozdziale trzecim poddała natomiast analizie główne kierunki rozwoju polityki cyberbezpieczeństwa UE w przyszłości.

W konkluzjach Autorka potwierdziła pierwszą część postawionej we wstępie hipotezy, stwierdzając, iż rozwiązania w zakresie cyberbezpieczeństwa przyjmowane w badanych

państwach członkowskich nie są brane pod uwagę przez instytucje Unii Europejskiej (s. 143-144). Wskazała ona także na istotną poprawę w tej dziedzinie w UE od 2014 roku.

1.2. Ocena metodologiczna i formalna pracy

Rozprawa mgr L. Dackowej pod względem *stricte* edycyjnym nie budzi poważniejszych zastrzeżeń. Forma spisu treści, przypisów oraz bibliografii jest generalnie prawidłowa. W tekście występują, co prawda, tzw. literówki (np. s. 62), jednak na tyle rzadko, iż nie obniża to istotnie oceny pracy pod tym względem.

Niestety inaczej należy ocenić warstwę językową. Trudno mi ocenić powody napisania pracy w języku angielskim, jednak już lektura tytułów poszczególnych rozdziałów oraz wstępu dowodzi, iż Autorka nie dokonała należytej korekty tekstu przed jego skierowaniem do recenzji. Jest on bowiem przepełniony błędami stylistycznymi i składniowymi. W wielu fragmentach pojawiają się niewłaściwe zwroty lub słowa, które utrudniają zrozumienie nawet ogólnego sensu wywodu Autorki. Dzieje się tak mimo tego, iż budowane przez nią zdania mają z reguły bardzo uproszczoną strukturę. Kilka przykładów:

- "(...) topic related in relation" (s. 11),
- "(...) another consideration is the fact that in cyberspace, there is no clear definition of the kind of scale of any necessary defence versus any kind of attack" (s. 18),
- "(...) written that are used as tools for the cyberattacks are written..." (s. 19),
- "(...) not all the public awareness programmes provided to Dutch citizens provide" (s. 75),
- "(...) are also lack complexity" (s. 92),
- uporczywe użycie "programmeming" zamiast "programming".

Co więcej, w wielu miejscach Autorka pozostała niekonsekwentna jeśli chodzi o stosowaną w pracy specjalistyczną nomenklaturę. Przykładowo, słowo Internet pisała raz z wielkiej, a raz z małej litery (w tym samym znaczeniu). Cyberprzestrzeń była określana zarówno jako "cyber-space", jak i "cyberspace". Podobnie z cyberbezpieczeństwem, które raz było zapisywane jako "cyber security", a raz jako "cybersecurity".

Niestety nie lepiej należy ocenić stronę metodologiczną pracy. Jakkolwiek sam dobór tematu nie budzi większych zastrzeżeń, to hipoteza badawcza oraz zastosowane metody badawcze już tak. Stwierdzenie, iż w pracy użyto zarówno jakościowych, jak i ilościowych metod analizy nic nie wyjaśnia. Dalsze uszczegółowienie, iż metody jakościowe obejmują

analizę (jaką?), porównanie (czego i w jaki sposób?) i syntezę również. Nic więcej na temat metodologii Autorka nie napisała. Zarówno cel badawczy, jak i pierwsza część hipotezy sugerują, iż obok analizy treści dokumentów oraz analizy decyzyjnej, podstawową metodą stosowaną w tej pracy powinna być metoda porównawcza. Tymczasem nie wiemy, które elementy polityki cyberbezpieczeństwa Doktorantka wzięła pod uwagę. Dla celów analizy porównawczej każdy podrozdział dotyczący państw oraz rozdział dotyczący Unii Europejskiej powinien być skonstruowany tak samo i podejmować identyczną grupę problemów, obejmującą m.in. występujące rodzaje zagrożeń, strukturę systemu cyberbezpieczeństwa, kompetencje poszczególnych instytucji, penalizację przestępstw komputerowych, priorytety strategii bezpieczeństwa teleinformatycznego itp. Tak niestety nie jest. W związku z tym, konkluzje przyjęły bardziej formę luźnych spostrzeżeń, które co prawda są generalnie zgodne z rzeczywistością, ale nie wynikają z rzetelnie przeprowadzonej analizy porównawczej. Nie mogły zatem posłużyć do pełnej weryfikacji pierwszego zdania hipotezy.

Drugie zdanie hipotezy zostało natomiast tak skonstruowane, iż jest nie do zweryfikowania przy tak określonym temacie i strukturze pracy. Odpowiedź na pytanie czy zwalczanie cyberprzestępczości w UE jest zaniedbywane w porównaniu z pozostałymi priorytetami bezpieczeństwa tej organizacji wymagałoby bowiem napisania innej rozprawy, w której wszystkie obszary polityki bezpieczeństwa Unii zostałyby poddane analizie. Zresztą, do tej drugiej części hipotezy Autorka na koniec w zasadzie się nie odnosi. Szkoda też, że nie poszerzyła ona hipotezy głównej o hipotezy robocze, dotyczące poszczególnych rozdziałów. W obecnym kształcie hipotezy, wiele rozważań w pracy nie służy jej weryfikacji.

Cel badawczy pracy został określony bardzo szeroko i miejscami jest niejasny ("current problematic moments in the process of cybercrime procurement" - s. 4). Dla klarowności, jego część powinna przyjąć formę celów szczegółowych (np. kwestia sformułowania rekomendacji). Ponadto, pytania badawcze powinny znaleźć się zaraz za celem badawczym, a nie za hipotezą. Wreszcie, trzecie pytanie badawcze zostało źle sformułowane. "Analiza" regulacji nie może być celem badawczym. Analiza może być środkiem do realizacji celu badawczego.

Poważnym zarzutem jest również relacja między określoną we wstępie cezurą czasową pracy a jej treścią. W rozprawie jedynie fragmentarycznie wspomina się bowiem o wydarzeniach sprzed 2010 roku, skupiając się raczej na drugiej dekadzie XXI wieku. Tymczasem, zgodnie ze słowami zawartymi we wstępie (s. 5), analiza powinna objąć ewolucję polityki cyberbezpieczeństwa UE od roku 2000.

Istotną zaletą recenzowanej rozprawy jest wielojęzyczna bibliografia, użyta szczególnie w rozdziale III. Autorka sięgnęła do opracowań wydanych nie tylko w j. polskim czy angielskim, ale także we francuskim. Należy się jej za to uznanie. Mimo to, podstawie źródłowej można postawić dwa zarzuty. Po pierwsze, wiele kluczowych dla tego tematu prac, które ukazały się w ostatnich latach zarówno w języku polskim, jak i angielskim, nie zostało przez Autorkę wykorzystanych, co obniża wartość merytoryczną ocenianego tekstu. Po drugie, wbrew dobremu obyczajowi akademickiemu, w bibliografii zawartej na końcu rozprawy znalazły się liczne opracowania, których nie można odnaleźć w przypisach. Dotyczy to m.in. pozycji autorstwa piszącego te słowa, jak i Promotora rozprawy.

1.3. Ocena merytoryczna

Przechodząc do oceny merytorycznej rozprawy, warto na wstępie zaznaczyć, iż jest ona generalnie poprawnie napisana. Autorka w wielu miejscach, a w szczególności w rozdziale II, przeprowadziła rzetelny przegląd rozwiązań przyjętych w UE w zakresie zwalczania cyberprzestępczości. Jej sposób dowodzenia, którego odbiór ze względów językowych bywa trudny, jest generalnie logiczny, a wnioski z reguły mają pokrycie w zaprezentowanych faktach.

Niestety, w pracy występuje wiele błędów merytorycznych i logicznych, a także niepotrzebnych uproszczeń i zaniedbań, które zasadniczo obniżają jej wartość jako oryginalnego opracowania problemu badawczego. Dla większej przejrzystości zostaną one omówione w punktach poniżej:

1. We wstępie wiele informacji przywoływanych przez Autorkę (s. 3-4) nie zawiera przypisów.
2. Wbrew temu co napisała Autorka na stronie 5, pierwsze akty cyberprzestępcze miały miejsce zdecydowanie wcześniej niż w roku 2000 (*vide* np. Markus Hess, Legion of Doom, 414s). Zdanie tłumaczące dobór cezury badawczej jest więc nieprawdziwe.
3. W rozdziale I Autorka nie przywołała jakiejkolwiek pełnej, politologicznej typologii zagrożeń teleinformatycznych, przez co jej rozważania na ten temat są mocno chaotyczne i miejscami nielogiczne. Pomieszała ona w strukturze tej części charakterystykę form zagrożeń komputerowych w ujęciu technicznym (*phishing*, *malware*) z niektórymi typami wyróżnionymi na gruncie nauk prawnych i politologii. W efekcie, z treści tego rozdziału nie dowiemy się czym w zasadzie różni się przestępczość komputerowa od innych szkodliwych zjawisk w cyberprzestrzeni.

4. W rozdziale I Autorka stosowała wiele fachowych pojęć, których w żaden sposób nie wyjaśniła (np. "new media").
5. Wiele stwierdzeń zawartych w rozdziale I to truizmy, które przy tak syntetycznej formie pracy nie powinny się tutaj znaleźć, bowiem zostały już wielokrotnie udowodnione w innych publikacjach. Oczywiście, należało w nim omówić podstawowe kategorie, które w dalszych częściach pracy zostały wykorzystywane, ale czy jest sens pisać o tym, iż "cybersecurity is a complex issue" (s. 13)? Nie wiadomo też co Autorka miała na myśli twierdząc, iż "Each and every subject acting in cyber-space provides additional knowledge while exploiting and exploring vulnerabilities in the infrastructure of their target's infrastructure" (s. 17). Podobnych, oczywistych bądź trudnych do zrozumienia stwierdzeń jest w tym rozdziale zdecydowanie więcej, w tym na stronach 10, 13, 17, 19.
6. W rozdziale tym pojawiały się także stwierdzenia, które są nieprawdziwe bądź zbytnio upraszczają bardzo skomplikowaną naturę zjawisk pojawiających się na styku cyberprzestrzeni i bezpieczeństwa państw. Przykładowo, na stronach 26 i 27 Autorka podała definicję cyberataku w prawie międzynarodowym...mimo, że taka nie istnieje. Powołała się ona na pracę S. Beidlemana z U.S. Army War College, w akapicie, który brzmi następująco: "Such a definition is also supported by international law where it has been concretised that a cyberattack is any kind of use of 'unarmed, non-military physical force' that can produce the same severe effects as an armed attack". Tymczasem w oryginale pracy Beidlemana (notabene nie na stronach 7-8, jak twierdzi Autorka w przypisach, ale na stronie 13) czytamy: "(...) This is supported by international law where it is recognized that the use of 'unarmed, non-military physical force' can produce the same severe effects as an armed attack (...) Cyber attacks may not exactly fit the unarmed, non-military physical force paradigm, but they can cause commensurate effects (S. Beidleman, *Defining and Deterring Cyber War*, US Army War College 2009, s. 13). Tym samym, nie dość, że Doktorantka pomyliła stronę źródła, to jeszcze zupełnie przeinaczyła jego sens. Beidleman nie podał bowiem nigdzie definicji cyberataku w prawie międzynarodowym. Autorka myli się też twierdząc, iż fundamentalnym elementem konstytuującym cyberataki jest użycie siły ("force"). Większość badaczy akcentuje właśnie zasadnicze różnice między klasycznym użyciem siły a działaniem w przestrzeni teleinformatycznej. Inny przykład dotyczy stwierdzenia ze strony 28, iż *malware* nie są wykorzystywane do poważnych ataków komputerowych, co jest sprzeczne z rzeczywistością.

Zdecydowana większość dobrze przygotowanych włamań bazuje właśnie na zaawansowanym, złośliwym oprogramowaniu. Wreszcie, na stronie 30 Doktorantka stwierdziła, iż "phishing is a form of malware", co również jest nie jest zgodne z prawdą. Jakkolwiek znaczna część tego rozdziału jest napisana dość dobrze, to niestety takich stwierdzeń w tej części można znaleźć więcej.

7. W rozdziale 1.3.4. Autorka zbyt pobieżnie omówiła zjawisko cyberszpiegostwa, twierdząc, iż "today there is still not much information regarding the possible sophistication of the cyberespionage capabilities of the national states" (s. 34). Wbrew temu stwierdzeniu, w ostatniej dekadzie powstało wiele opracowań i raportów technicznych (np. korporacji Mandiant), które podają bardzo ciekawe informacje na ten temat. Na tej samej stronie rozprawy napisano też, iż "Ghostnet" był wirusem komputerowym, choć w rzeczywistości jest to nazwa operacji cyberszpiegowskiej. Wykorzystany w niej złośliwy program był trojanem, a nie wirusem, który nosił nazwę "Gh0st Rat".
8. Trudno zrozumieć, dlaczego w podrozdziale dotyczącym cyberterroryzmu Autorka scharakteryzowała haktywizm, który jest odrębnym, posiadającym odmienne cechy zjawiskiem.
9. W rozdziale drugim, który w mojej ocenie ma największą wartość merytoryczną, brakuje na wstępie szerszego omówienia uwarunkowań polityki cyberbezpieczeństwa UE, tzn. stopnia komputeryzacji, informatyzacji na tym obszarze, postępów rewolucji informatycznej czy występujących zagrożeń dla systemów komputerowych (dokładne statystyki). Na koniec tej części Autorka mogła się też pokusić o szersze nakreślenie ewolucji działań Unii Europejskiej w tej dziedzinie. Nie odwołała się ona też w większym stopniu do komentarzy naukowców dotyczących konsekwencji wdrażania kolejnych dokumentów przez UE, co obniża wartość merytoryczną wywodu.
10. Na stronie 64 Autorka opisała European Defence Agency. Powstaje jednak pytanie, na ile ta instytucja odgrywa jakąkolwiek rolę w działaniach UE w zakresie zwalczania przestępczości komputerowej?
11. Na stronie 69 Autorka mało przekonująco wyjaśniła taki, a nie inny dobór próby badawczej (państw). Stwierdzenie, iż oparto ją na istniejących typach cyberzagrożeń w tych krajach nic nie wnosi. W tym kontekście, dziwi pominięcie Wielkiej Brytanii, która posiada bardzo zaawansowane rozwiązania w dziedzinie zwalczania przestępczości komputerowej.

12. Uwaga strukturalna. Wydaje się, iż dla klarowności i logiki wywodu zdecydowanie lepszym rozwiązaniem byłaby zamiana kolejności rozdziałów II i III. Najpierw Autorka powinna opisać doświadczenia państw członkowskich, a dopiero później UE, tym bardziej, iż jej zamiarem było wskazanie, na ile Unia korzysta z ich doświadczeń.
13. W przypadku każdego państwa omawianego w rozdziale III zabrakło analizy uwarunkowań polityki cyberbezpieczeństwa, w tym postępów rewolucji informatycznej, uzależnienia infrastruktury krytycznej od ICT czy konkretnych statystyk dotyczących przestępczości komputerowej (Autorka wspomina o występujących cyberzagrożeniach ale w sposób bardzo ogólny). Ciekawym rozwiązaniem byłby też przegląd kodeksów karnych pod kątem penalizacji aktów przestępczości komputerowej (niektóre regulacje zostały przywołane, np. na stronie 88, ale jest to zdecydowanie zbyt mało). Te braki sprawiają, iż studia przypadków (państw) nie wyczerpują tematu, bowiem analiza ich systemów cyberbezpieczeństwa jest niejako "zawieszona w próżni".
14. Na jakiej podstawie Autorka stwierdziła, iż Holandia stała się drugim po Estonii wiodącym krajem w UE w zakresie cyberbezpieczeństwa (s. 69)? W podrozdziale poświęconym temu państwu zabrakło także szerszego omówienia instytucji odpowiedzialnych za zwalczanie przestępczości komputerowej.
15. W przypisie 442 (s. 72) Autorka jako źródło podała lokalizację znajdującą się na twardym dysku jej (?) komputera.
16. Jak wspomniano wyżej, bardzo poważnym niedopatrzeniem w podrozdziale dotyczącym Estonii jest brak szerszego omówienia ataków komputerowych, które miały miejsce w kwietniu i maju 2007 roku (jedynie o nich krótko wspomniano). Jest to zasadniczy błąd, ponieważ charakter tzw. pierwszej cyberwojny przeciwko Estonii w zasadniczym stopniu determinuje przyjęte przez Tallin regulacje w tej dziedzinie.
17. Na stronie 77 podano niewłaściwą nazwę natowskiego centrum w Tallinie (powinno być CCD COE). Doktorantka nie wyjaśniła także, dlaczego akurat MSZ Estonii odgrywa kluczową rolę w polityce cyberbezpieczeństwa tego kraju.
18. Podrozdział 3.3. został dość chaotycznie napisany, co utrudnia jego odbiór. Autorka na zmianę bowiem omawiała dokumenty z instytucjami (ANSSI). Ponadto, o zagrożeniach teleinformatycznych powinna wspomnieć na początku, a nie na końcu tej części.

19. Na jakiej podstawie stwierdzono, iż 40 000 przestępców komputerowych działających we Francji to mało (s. 88)? Czy istnieją jakieś dane dotyczące liczby cyberprzestępców w państwach UE?
20. Istotnym mankamentem podrozdziału dotyczącego Polski jest pominięcie niemal zupełnym milczeniem zawartości kluczowych dokumentów regulujących kwestie cyberbezpieczeństwa RP ("Polityka Ochrony Cyberprzestrzeni...", "Krajowe Ramy Polityki Cyberbezpieczeństwa...", wcześniejsze dokumenty i ich projekty), ewolucji polityki w tej dziedzinie od 2008 roku, a także tylko szczątkowa charakterystyka instytucji wchodzących w skład krajowego systemu cyberbezpieczeństwa. Zapomniano np. o roli działającego w strukturach NASK zespołu CERT Polska. Autorka nie odniosła się także do stosunkowo bogatej, rodzimej literatury poświęconej bezpieczeństwu teleinformatycznemu RP. W efekcie, przeprowadzona przez nią analiza jest bardzo pobieżna i zupełnie nie oddaje charakteru polityki cyberbezpieczeństwa Polski.
21. Na stronach 98-99 Autorka podsumowuje swoje wcześniejsze rozważania przywołując różne typy przestępczości komputerowej występujących w poszczególnych krajach. Nie podaje jednak żadnych statystyk na poparcie swoich wniosków.
22. Rozdział czwarty jako całość jest dość ciekawy, choć niestety mało oryginalny. Zdecydowana większość "rekomendacji" Autorki pokrywa się bowiem z przywoływanymi przez nią dokumentami. Jej własnych spostrzeżeń i uwag, opartych na wcześniejszej analizie, jest natomiast bardzo mało. Świadczy o tym liczba odwołań do rozmaitych opracowań naukowych i raportów, w tym szczególności do "Stacktaking, Analysis and Recommendations...". Uwagę zwraca także fakt, iż w tym rozdziale, w przypisach nie podawała ona z reguły dokładnych stron źródeł, z których korzystała. W efekcie, trudno więc określić ten fragment rozprawy jako rozdział analityczny (tak opisano go we wstępie). Ma on bowiem bardziej formę deskryptywną, stanowi syntezę rozmaitych podejść do kwestii polityki cyberbezpieczeństwa zarówno w UE, jak i w państw członkowskich.
23. Doktorantka na stronie 110 napisała, iż nie wszystkie środki cyberbezpieczeństwa wykorzystywane w jednym kraju będą skuteczne w innym. Tym samym stawia pod znakiem zapytania sens prowadzenia rozważań w tym rozdziale.
24. Miejscami rozdział IV jest napisany chaotycznie. Przykładowo, na stronie 111, w podrozdziale dotyczącym państw członkowskich, Autorka pisała o Komisji

Europejskiej. W innym miejscu porównuje rozwiązania przyjęte w UE z tymi z USA, o których wcześniej nic nie pisała (s. 123).

25. Wiele opinii sformułowanych w tym rozdziale ma bardzo ogólny charakter i nie wnosi wiele do debaty nad poprawą skuteczności polityki cyberbezpieczeństwa w UE. Przykładowo, na stronie 114 wspomniano, iż Europol powinien mieć możliwość szybkiego i bezpośredniego dostępu do informacji pochodzących z sektora prywatnego. Jednocześnie Doktorantka wspomina o potrzebie zapewnienia prawa do prywatności i praw człowieka obywatelom Unii. Nie wyjaśnia jednak w jaki sposób pogodzić te sprzeczne ze sobą potrzeby.
26. Rozdział IV powinien być lepiej zorganizowany oraz uporządkowany pod względem struktury treści. Osobno Autorka powinna scharakteryzować wyzwania dla UE i państw członkowskich, a osobno tytułowe rekomendacje. Mieszanie obu tych zagadnień nie było dobrym pomysłem.
27. W pracy brakuje też szerszej refleksji nad tym, na ile Unia Europejska powinna w ogóle kopiować rozwiązania narodowe w dziedzinie cyberbezpieczeństwa. A jest to zagadnienie kluczowe z punktu widzenia wybranego problemu badawczego. W pewnym sensie ma to też szerszy związek z obecnym, wieloletnim przestojem w UE, jeśli chodzi o rozwój WPZiB/WPBiO.

1.4. Podsumowanie

Rozprawę doktorską mgr L. Dackowej w obecnej formie trudno uznać za dobre dzieło naukowe. Autorka popełniła zbyt wiele rażących błędów, aby móc ją ocenić w ten sposób. Największe wątpliwości budzą kwestie metodologiczne, które siłą rzeczy rzutują na jakość sformułowanych wniosków. Mimo tych uwag, należy zarazem podkreślić, iż wiele fragmentów pracy zostało poprawnie napisanych. Jest to szczególnie widoczne, jeśli chodzi o podrozdział 1.3.2, większość rozdziału II oraz fragmenty rozdziału III. Większość rozdziału IV, jakkolwiek mało odkrywcza, też nie budzi zastrzeżeń merytorycznych. W efekcie, praca ma zadatki na oryginalne dzieło naukowe, gdyby Autorka dokonała niezbędnych poprawek oraz dokończyła, w oparciu o jasno sformułowane zasady, rzetelną analizę porównawczą rozwiązań w zakresie cyberbezpieczeństwa występujących na poziomie państw członkowskich UE oraz w samej Unii Europejskiej. Warto podkreślić, iż taka praca dotychczas nie pojawiła się w polskiej literaturze specjalistycznej.

Biorąc pod uwagę powyższe, rekomenduję skierowanie rozprawy doktorskiej mgr L. Dackowej do poprawy.

M. Lakomy

dr hab. Miron Lakomy