Prof. nadzw. dr hab. Anna Śliz
Instytutu Socjologii
Uniwersytet Opolski
ul. Katowicka 89
45-061 Opole

e-mail: asliz@uni.opole.pl

Recenzja dysertacji doktorskiej mgra Tomasza Pączkowskiego

Cyberprzestępczość w województwie śląskim
Studium z socjologii ryzyka

Uniwersytet Śląski w Katowicach
Wydział Nauk Społecznych
Katowice 2019, stron 371

Promotor: prof. zw. dr hab. Jacek Wódz
Promotor pomocniczy: dr Grzegorz Libor

Recenzowana dysertacja doktorska, o teoretycznym-empirycznym charakterze, poświęcona została aktualnej problematyce związanej z cyberprzestępczością. Analizowany problem został zamknięty przestrzennie w ramach województwa śląskiego. Cyberprzestępczość została zaprezentowana przez Autora w kontekście wyników badań zrealizowanych wśród wyselekcjonowanej grupy śląskich policjantów. Współcześnie, problem cyberprzestępczości jest jednym z ważniejszych w zglobalizowanym świecie. Informatyzacja i cyfryzacja, które oplotły społeczeństwa i ludzkość stają się coraz częściej przedmiotem ataków, co wzbudza lęk zarówno wśród ludzi, jak i wszelakich instytucji.

Recenzowana praca składa się z jedenastu - o zróżnicowanej objętości - rozdziałów. Są one podzielone na liczne podrozdziały. Dysertacja posiada także wstęp, zakończenie, bibliografię oraz aneks. Obszerna bibliografia została zaprezentowana zgodnie z preferowanym w literaturze podziałem, chociaż uwagę zwraca słaba reprezentacja literatury obcojęzycznej a temat sugeruje szersze uwzględnienie takiej bibliografii. W treści wstępu

Autor uzasadnia potrzebę podjęcia tematyki związanej z zagrożeniem cyberprzestępczością oraz prezentuje zasadniczy cel i założenia własnej dysertacji.

Pierwszy rozdział pracy to założenia terminologiczne i teoretyczne związane z socjologią ryzyka. Autor zarówno definiuje pojęcie ryzyka, jak i przedstawia jego rodzaje i klasyfikacje oraz podstawowe ujęcia socjologiczne. Zwraca uwagę na wszelkie ryzyko, które występuje zarówno w rzeczywistości realnej, jak i wirtualnej. Dla tematyki pracy to drugie zagrożenie jest bardziej istotne. Ważne jednak, że Autor odniósł się także do licznych zagrożeń w rzeczywistości społecznej. W czasach wielu aktów i ataków terrorystycznych zwrócenie uwagi na wspomniany aspekt jest istotne. Ważnym było także zwrócenie uwagi, ze ryzyko w realnym świecie dokonuje się przy wykorzystaniu cyberprzestrzeni. Rozdział pierwszy można więc potraktować jako ścisłe i konkretne odniesienie się Autora do problematyki ryzyka. I to poprawne myślenie. Dla mnie jednak ważnym byłoby jeszcze szersze spojrzenie na omawiane zjawisko szczególnie z perspektywy socjologicznej. Omawiana dysertacja jest z zakresu socjologii więc byłoby ważnym uwzględnienie szerszego tła teoretycznego, jak dla przykładu teorii wymiany społecznej, gdzie kluczem jest relacja między zyskiem a stratą związanymi z podejmowanym działaniem. Działania ludzi niosą ze sobą ryzyko stąd jako ważne postrzegam zwrócenie uwagi na potrzebę uwzględnienia kalkulacji zysków i strat, kiedy ludzie decydują się na jakieś działanie szczególnie ryzykowane. Autor powinien także odwołać się teorii zmiany i rozwoju społecznego ze szczególnym uwzględnieniem charakterystyki społeczeństwa informacyjnego. Wydaje się, że sięgnięcie do chociażby tych dwóch odsłon teoretycznych wzbogaciłoby założenia teoretyczne pracy wobec problematyki cyberprzestępczości we współczesnym świecie. Autor jednak wybrał ścieżkę skupienia uwagi na konkretnym zagadnieniu, czyli ryzyku, które zaprezentował w kompetentny sposób. Dobrym wzbogaceniem literaturowym omawianych kwestii byłoby sięgnięcie również do książek Yuvala Noaha Harariego (współczesny izraelski pisarz), który w bardzo przystępny sposób przedstawia i analizuje wszelkie ryzyka i zagrożenia świata XXI wieku. Nie są to prace ściśle naukowe, ale rysują szerokie perspektywy współczesnych zagrożeń i wszelakich ryzyk.

Sześć kolejnych rozdziałów pracy to omówienie konkretnych przypadków zagrożeń cybernetycznych. Autor rozpoczyna od ryzyka w pracy policjantów, co jest zgodne z tematem opiniowanej dysertacji. To przede wszystkim policja jest formacją, której zadaniem jest walka z wszelkimi przejawami cyberprzestępczności. To walka bardzo trudna, gdyż sieciowi

przestępcy z reguły są o krok przed policją czy innymi służbami, która pomimo coraz lepszych wyników własnych działań wciąż ma jeszcze wiele do zrobienie w tej kwestii. Wybiegając nieco, świadczą o tym także wyniki przeprowadzonych przez Doktoranta badań empirycznych., które wyraźni pokazują braki w tym zakresie badanych polskich mundurowych.

Kolejno Autor robi krótkie wprowadzenie do zagadnienia terroryzmu w cyberprzestrzeni ze szczególnym uwzględnieniem roli Internetu jako narzędzia łączącego terrorystów, którzy nie tylko atakują w cyberprzestrzeni, ale także w realnym świecie. Mamy wiele przykładów siatek terrorystycznych, które przy użyciu Internetu planują a następnie przeprowadzają ataki. Szkoda, że Doktorant nie zwrócił tutaj uwagi na pewien paradoks. Terroryści, najczęściej islamscy, atakują rozwinięty cywilizacyjnie świat oskarżając go o własne zacofanie, wykorzystując przy tym najnowsze osiągnięcia technologii państw zachodnich. Walczą więc przy użyciu narzędzi, przeciwko którym występują.

W kolejnych rozdziałach Autor analizuje cyberzagrożenia związane z bezpieczeństwem państwa. Zwraca uwagę, że nie chodzi tylko o terroryzm w ramach konkretnego państwa, ale także o jego wymiar globalny. Ważnym problemem jest cyberzagrożenie dla prawidłowego funkcjonowania społeczeństwa. Tutaj Doktorant odwołuje się do konkretnych przypadków zagrożeń związanych dla przykładu ze zdrowiem i życiem ludzi poprzez zatrucie żywności czy wody. Ale najbardziej niebezpieczne wydają się ataki na elektrownie czy inne strategiczne instytucje i punkty, które są absolutnym fundamentem istnienia współczesnych społeczeństwa. Pamiętamy zdarzenie z Nowego Jorku, kiedy przez kilka godzin energii został pozbawiony Manhattan. Jak wielki zapanował tam chaos. Ludzie nie umieli żyć. Nie pracowali, zostali uwięzieni w metrze, windach. Nie mogli opuścić mieszkań czy biur. Najbogatsza dzielnica Nowego Jorku w kilka minut zamieniła się w teren katastrofy. Podobne zagrożenia dotyczą komunikacji czy transportu, opieki zdrowia. Niezwykle ważne są także wszelkie zagrożenia systemów informatycznych, które są przypisane rozmaitym instytucjom administracji państwowej. Gromadzą one wszelkie dane o obywatelach i atak na nie to utrata danych, które zagrażają każdemu obywatelowi – dane bankowe, o stanie zdrowie, przebytych chorobach, dane skarbowe. Takie zdarzenia są równocześnie wielkim niebezpieczeństwem dla zwykłych obywateli, którzy nie tylko tracą prywatność, ale często także dorobek materialny życia. Dużym zagrożeniem są wszelkiego rodzaju „wirusy" czy „robaki", które ludzie otrzymują w mailach a które niszczą całą zasobność komputera. Musimy także pamiętać o codziennych niebezpieczeństwach, które są

związane z nękaniem za pomocą telefonów czy sms-ów. Jest to poważne zagrożenie dla kondycji psychicznej, ale i fizycznej człowieka. I na te elementy terroryzmu Doktorant zwraca uwagę. W tej prezentacji przytacza wiele empirycznych punktów odniesienia, co jest istotne, gdyż to one w sposób najbardziej wyraźny przemawiają do świadomości każdego z nas. Na koniec tej części dysertacji Autor dokonuje krótkiego porównania skali i rodzajów cyberprzestępczości w Polsce, wybranych krajach Unii Europejskiej oraz Stanach Zjednoczonych. Jest faktem, że kraje o wyższym poziomie rozwoju cywilizacyjnego stają się częstszym obiektem wszelkich ataków terrorystycznych zarówno tych realnych, jak i wirtualnych. Przykład państw Europy Zachodniej dobrze to ilustruje – ataki we Francji, Belgii czy Niemczech. Polska w tych statystykach nie odgrywa kluczowej roli, ale z każdym rokiem to się zmienia. Zależy to zarówno od pozycji czy roli państwa w systemie światowym, jak i nasycenia życia społecznego informatyką i cybernetyką. Im bardziej nasze życie staje się „usieciowione" tym w większym stopniu jesteśmy narażeni na niebezpieczeństwo cyberataku. To bardzo ważne kwestie charakteryzujące współczesny świat. Autor zwrócił na nie uwagę, co świadczy o dobrej znajomości przez Niego przedmiotu i problematyki dysertacji, którą napisał.

Dotychczas omawiane rozdziały pracy można uznać jako pierwszą jej część o charakterze teoretycznym, chociaż z licznymi odniesieniami do danych statystycznych i odniesień empirycznych. Druga zaś część dysertacji, bardziej obszerna, to część metodologiczno-badawcza, w której Autor najpierw prezentuje założenia metodologiczne planowanych badań empirycznych, aby kolejno przedstawić i omówić ich wyniki.

Rozdział ósmy rozprawy doktorskiej został zatytułowany „Metodologia badań własnych". Wprawdzie w jego treści znalazły się wszelkie niezbędne elementy założeń metodologicznych, ale zostały one zaprezentowany w mało precyzyjny i uporządkowany sposób. Adekwatna wiedza znalazła się poza podrozdziałem, który sugerowałby, że właśnie w tym miejscu ona się znajdzie. Na początku rozdziału Autor nie zdefiniował celu i przedmiotu badań, co w pracach empirycznych jest ważnym elementem. Jako główny problem badawczy Autor wskazał walkę ze zjawiskiem cyberprzestepczości w świadomości policjantów. Kolejno przedstawił długą listę pytań badawczych, które rozbił na pytania szczegółowe. Zaprezentował również dyspozycje do wywiadów, które zrealizował z policyjnymi specjalistami od cyberprzestępczności. Autor nie sformułował hipotez, ale to w socjologii empirycznej zabieg akceptowalny. Jeśli chodzi o tę część założeń to jest ona skonstruowana

w sposób poprawny. Pewne uwagi i sugestie mam wobec założeń związanych z prezentacją metod, technik i narzędzi badawczych. Nie zostały one jasno i wyraźnie przedstawione. Wprawdzie pojawiają się w treści rozdziału, ale nie w podrozdziale, który został zatytułowany jako „Metody, techniki i narzędzia badawcze". Gdyby tak się stało logika układu treści całego rozdziału byłaby dużo lepsza. Podobnie zaprezentował Autor informacje o doborze próby, która w rzeczywistości zyskała wymiar pięciu korpusów wynikających z hierarchicznej struktury polskiej policji. Jak dla mnie dużym zaskoczeniem jest podrozdział „Charakterystyka badanej grupy badawczej", gdyż w treści nie ma tutaj praktycznie nic o badanych a są informacje o skali dostępności do Internetu gospodarstw domowych czy liczby osób korzystających z Internetu. To ważne informacje dla problematyki pracy, ale zapewne powinny się znaleźć w innej części dysertacji. Tymczasem charakterystyka badanych grup policjantów i specjalistów od cyberprzestępcznosci została umieszczona w „Przebiegu badań", aby następnie znowu pojawił się opis badanej populacji. I to tutaj pojawiły się informacje o cechach społeczno-demograficznych respondentów. Można więc przyjąć, że w rozdziale metodologicznym zostały przedstawione wszystkie niezbędne informacje, ale nie została zachowana w pełni kolejność i miejsce prezentacji, która jest przyjęta w tego rodzaju rozprawach naukowych z zakresu socjologii. Rozdział metodologicznie jest poprawny, ale nieco chaotycznie zaprezentowany.

Dwa kolejne rozdziały pracy to prezentacja i analiza wyników badań empirycznych. Autor zastosował w badaniach trzy techniki: badania ankietowe, wywiady z ekspertami oraz analizę adekwatnych do problematyki dokumentów. W sposób najbardziej szeroki prezentuje wyniki badań ankietowych, które odnosi do pięciu wyselekcjonowanych grup respondentów. Należy podkreślić, że Doktorant prezentuje wyniki badań, stosując urozmaiconą grafikę, co uatrakcyjnia pracę. Oprócz takich prezentacji dokonuje analizy zebranego materiału odnosząc go do zasadniczej problematyki pracy. Analizując za Autorem wyniki badań niektóre z nich wyraźnie mnie zaskakiwały. Wydawać by się powinno, że policjanci są bardzo wyczuleni na możliwość występowania wszelkich niebezpieczeństw w Internecie a tutaj okazuje się, że wielu z badanych otwiera, np. maile wysłane z nieznanego adresu. To raczej podstawowa zasada korzystania z poczty mailowej, ze wyrzuca się automatycznie do kosza listy od nieznanego lub w jakiś sposób podejrzanego nadawcy. Może mniej zaskakujące, ale zapewne dające do myślenia jest stwierdzenie, ze wyżej stojący w hierarchii policjanci są dużo gorzej przygotowani do walki z cyberprzestępcznością niż młodsi funkcjonariusze. Jest faktem, co pokazują badania socjologiczne, ze im starsi Polacy tym znajomość Internetu mniejsza, ale od

pracowników służb powołanych do pilnowania bezpieczeństwa państwa i społeczeństwa należy wymagać więcej. Trzeba także podkreślić, że prezentacja wyników badań jest przejrzysta. Autor odnosi wyniki do kolejnych pytań badawczych analizując je w kontekście konkretnej grupy respondentów. Wyniki własnych badań przeplata danymi, które mówią o skali cyberprzestępczości w Polsce. Na tym tle województwo śląskie wykazuje dużą skuteczność, chociaż z roku do roku spada liczba wszczętych postępowań oraz liczba podejrzanych. Trudno jednak wnioskować czy można mówić o rzeczywistym spadku cyberprzestępczości czy staje się ona coraz mniej wykrywalna dla policji. Jest także faktem, o czym pisze Doktorant, ze statystyki odnoszące się do skali cyberprzestepczości są niepełne, co zapewne wynika z tego, że jest to wciąż zjawisko stosunkowo nowe. A jeśli tak to wymaga kolejnych badań. Dobrze się więc stało, ze Pan Tomasz Pączkowski podjął się próby analizy tego groźnego społecznie zjawiska.

Ostatni zasadniczy rozdział dysertacji to relacja z wywiadów przeprowadzonych wśród policjantów profesjonalnie zajmujących się walką z cyberprzestępcznością. Jak twierdzą są świadomi wszelkich zagrożeń, ale walka z nimi jest bardzo trudna, gdyż praktycznie każdego dnia przestępcy wymyślają nowe narzędzia ataku w cyberprzestrzeni. Dobrze jednak, że policjanci zdają sobie sprawę ze specyfiki przestępstw, do zwalczania których zostali powołani.

Pracę kończą rekomendacje, co do przyszłości walki z cyberprzestępczością wynikające zarówno z wyników badań własnych, analizy literatury przedmiotu i dostępnych danych zastanych. Ważnym jest również, że Autor dysertacji dostrzega powagę omawianego problemu i potrzebę dalszych badań w kierunku socjologicznej, chociaż nie wyłącznie, analizy tego zjawiska.

Ostatnie akordy rozprawy doktorskiej to bibliografia oraz aneks, w którym zostały zamieszczone m.in. narzędzia badawcze wykorzystane przez Autora w realizacji własnych badań empirycznych.

Na koniec kilka uwag technicznych, które nie wpływają na ogólną pozytywną ocenę dysertacji, ale mam nadzieję, że pomogą Autorowi uniknąć w przyszłości podobnych niedociągnięć. Zauważalny jest brak pełnych imion przywoływanych autorów oraz błędy językowe i literowe. Nie zrozumiała jest także numeracja wykresów umieszczonych na

stronie 168 (wykres 159) i stronie 175 i 176 (wykresy 160 i 161) podczas, gdy na stronie 165 jest wykres 16 a na stronie 181 wykres 17. To zapewne przeoczenie, ale zwraca uwagę czytelnika.

***

Ważąc zalety rozprawy doktorskiej mgra Tomasza Pączkowskiego oraz jej nieliczne niedostatki i braki stwierdzam, że dysertacja spełnia wymogi ustawy z dn. 14 marca 2003 roku o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (Dz. U. Nr 65, poz. 595, z późn. zm.) i wnoszę o nadanie biegu dalszym etapom postępowania doktorskiego. Zakładam jednocześnie, że publiczna obrona rozprawy doktorskiej pozwoli na rozstrzygnięcie recenzenckich wątpliwości i zrodzi interesującą dyskusję merytoryczną.

Katowice - Opole, kwiecień 2019