dr hab. Tomasz Aleksandrowicz
prof. Wyższej Szkoły Policji w Szczytnie

Warszawa, 27.02.2023 r.

RECENZJA

dysertacji doktorskiej Pana mgra inż. Krzysztofa Wosińskiego *Znaczenie wywiadu opartego na otwartych źródłach (OSINT) w zapewnieniu bezpieczeństwa systemów teleinformatycznych i bezpieczeństwa osobowego* wykonanego pod kierownictwem naukowym płk. rez. dr. hab. inż. Piotra Deli, Akademia Kaliska im. Prezydenta Stanisława Wojciechowskiego, Kalisz 2023

Recenzja została wykonana w związku z uchwałą nr 3/NOB/2023 Rady Dyscypliny Naukowej Nauki o Bezpieczeństwie z dnia 26 stycznia 2023 r. w sprawie powołania recenzentów w postepowaniu o nadanie stopnia doktora Panu magistrowi inżynierowi Krzysztofowi Wosińskiemu.

Uwagi ogólne

Pozyskiwanie informacji ze źródeł otwartych stanowiło i stanowi dla wywiadów, organów bezpieczeństwa oraz organów ścigania pewien problem. Z jednej strony, znaczenie źródeł otwartych zawsze było bardzo silnie akcentowane. Już w 1947 roku jeden z założycieli Centralnej Agencji Wywiadowczej i twórca amerykańskiej szkoły analizy wywiadowczej, Sherman Kent, szacował, że w czasie pokoju ok. 80% informacji niezbędnych politykom do podejmowania decyzji należy do kategorii ogólnodostępnych[1]. „Informacje wywiadowcze zdobywa się w różny sposób, nie wszystkie z nich stanowią tajemnice i sekrety. W szczególności dotyczy to białego wywiadu (overt intelligence), w ramach którego wykorzystywane są informacje pochodzące z gazet, książek, publikacji naukowych i technicznych, oficjalnych publikacji rządowych, radia i telewizji. Nawet powieść czy sztuka teatralna może zawierać użyteczne informacje na temat stanu państwa"[2]. Nie ulega wątpliwości, że z biegiem lat, a przede wszystkim ze wzrostem dostępności informacji w rezultacie rewolucji informacyjnej, szacunki ulegały zmianie na korzyść źródeł otwartych; zdaniem gen. Samuela V. Wilsona, b. dyrektora Defence Intelligence

[1] Memorandum Respecting Section 202 (Central Intelligence Agency) of the Bill to Provide for National Defence Establishment, Submitted by Allen W. Dulles, April 25, 1947, reprinted in U.S. Congress, 80th Congress, 1st session, Senate, Committee on Armed Services, National Defence Establishment (Unification of the Armed Services), Hearings, Part 1, s. 525.

[2] Allen Dulles,*The Craft of Intelligence*, Harper&Row, New York 1963, s. 55.

Agency stosunek ten wynosił nawet 90:10.[3] Równocześnie źródła otwarte traktowane były jako źródła „drugiej kategorii" i w związku z tym spychane na margines. Taki stan rzeczy ma bez wątpienia podłoże psychologiczne. Zdobycie informacji ze źródeł operacyjnych jest pracochłonne i niejednokrotnie związane z ryzykiem, człowiek natomiast skłonny jest przywiązywać wagę do tych danych, których zdobycie wiązało się z większym nakładem sił i środków. Jest to zależność wykorzystywana przy planowaniu wszelkich operacji dezinformacyjnych[4]. Jeśli bowiem coś jest powszechnie dostępne, to nie jest zbyt wiele warte.

Problem niedoceniania znaczenia informacji pochodzących z otwartych źródeł stawał się wielokrotnie przedmiotem krytyki amerykańskich służb specjalnych. Podkreślano zwłaszcza, że Wspólnota Wywiadowcza nie bacząc na szybko rosnącą liczbę baz danych, zdaje się ignorować je w swoich analizach, co powoduje przeszacowanie informacji ze źródeł operacyjnych i niedoszacowanie źródeł otwartych. W celu poprawy sytuacji postulowano w szczególności utworzenie w ramach CIA centrum białego wywiadu oraz systematyczne wykorzystywanie opinii zewnętrznych ekspertów[5].

Efekty owych przemyśleń znalazły swoje odbicie w Intelligence Reform and Terrorism Protection Act z 2004 roku, który stanowi m.in., że biały wywiad musi stać się integralną częścią cyklu wywiadowczego tak, aby decydenci dysponowali kompleksową, pełną informacją.[6]

Ten przydługi wstęp ma na celu podkreślenie znaczenia recenzowanej dysertacji. Temat podjęty przez Doktoranta jest bardzo istotny zarówno w sferze teoretycznej, jak i praktycznej, trudno jest także odmówić mu aktualności. Wiąże się to z dynamicznym rozwojem społeczeństwa informacyjnego i rewolucji informacyjnej, przede wszystkim w aspekcie digitalizacji informacji, rosnących możliwości dostępu do niej i trudności w zachowaniu informacji w poufności. Z drugiej strony, Doktorant słusznie podkreśla „ograniczony zasób aktualnej literatury naukowej w języku polskim w temacie samej istoty wywiadu otwartoźródłowego, jego podstaw, technik, wykorzystywanych

---

[3] Open Source Intelligence (OSINT): Issues for Congress. Congressional Research Service Report for Congeress, December 5, 2007, s. 4. http://www.fas.org/sgp/crs/intel/RL34270.pdf

[4] Zob. T. Aleksandrowicz, *Analiza informacji w administracji i w biznesie*, op. cit., s. 99 i nast. oraz A. Codevilla, *Informing Statecraft: Intelligence for the New Century*, The Free Press, A Division of Macmillan Inc., New York 1992, s. 431.

[5] Takie wnioski postawiły m.in. Komisja Aspina – Browna, Komisja WMD i Komisja 9/11. *Zob. Preparing for the 21st Century: An Appraisal for the U.S. Intelligence. Commission on the Roles and Capabilities of the United States Intelligence Community, March 1, 1996, http://www.access.gpo.gov/intelligence/int/; The Commission on the Capabilities of The United States Regarding Weapons of Mass Destruction, March 31, 2005, The National Commission on Terrorist Attacs Upon the United States (The 9/11 Report). http://www.fas.org/irp/offdocs/911comm.html*

[6] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem* (w:) *Rola mediów w przeciwdziałaniu terroryzmowi*, K.Liedel, P. Piasecka (red. nauk.), Warszawa 2009, s. 82 - 83

narzędzi oraz, przede wszystkim, metod obrony przed OSINT-em, realizowanym przez osoby lub organizacje, które mogą zagrozić bezpieczeństwu osobistemu i biznesowemu." (s. 7).
Dysertacja bez wątpienia plasuje się w ramach dyscypliny nauki o bezpieczeństwie.

Ocena metodologiczna
Metodyka zastosowana w badaniach, których efektem jest recenzowana dysertacja nie budzi zastrzeżeń. Jako przedmiot badań Doktorant wskazał zabezpieczenia systemów teleinformatycznych, podłączonych do Internetu oraz procedury bezpieczeństwa osobowego w zakresie ochrony informacji o aktualnym położeniu i statusie osób, a także w odniesieniu do informacji technologicznych z nimi związanych (s. 16).

Główny cele poznawczym określono jako „identyfikacja i ustalenie możliwości uzyskania szczegółowych informacji, wynikających z przeprowadzanego wywiadu otwartoźródłowego, w odniesieniu do systemów teleinformatycznych oraz indywidualnych osób, a także zidentyfikowanie zagrożeń wynikających z tego typu działań oraz metod skutecznej obrony przed przedmiotowym rozpoznaniem (s. 17); „w sensie pragmatycznym" (chyba utylitarnym? – pm. TA) jako cel badań Doktorant wskazał „opracowanie koncepcji identyfikacji i weryfikacji dostępnego zbioru informacji zawierających szczegóły techniczne, osobowe oraz geolokalizacyjne, dotyczące systemów teleinformatycznych oraz osób, a także określenie możliwości wprowadzenia zabezpieczeń przed działaniem zidentyfikowanych technik" (s. 17).

Główny problem badawczy Doktorant sformułował w postaci pytania, w jakim zakresie dostępne narzędzia, służące do gromadzenia informacji w ramach wywiadu otwartoźródłowego oraz techniki ich analizy wpływają na bezpieczeństwo systemów teleinformatycznych oraz bezpieczeństwo osobowe, a także jakie są możliwości obrony przed zidentyfikowanymi technikami; określił także problemy szczegółowe (również w formie pytań), a więc: jakie narzędzia i techniki wywiadu otwartoźródłowego są dostępne dla użytkowników Internetu; w jaki sposób należy poddawać analizie zebrane informacje, aby uniknąć ich błędnej interpretacji; jakie zagrożenia płyną z powszechnej możliwości stosowania wywiadu otwartoźródłowego oraz nieprawidłowej analizy danych pozyskanych w ramach przedmiotowych działań w Internecie; jakie są możliwości zabezpieczenia infrastruktury teleinformatycznej oraz zapewnienia bezpieczeństwa osobowego przed działaniami wynikającymi z prowadzonego wywiadu otwartoźródłowego (s. 17).

Z problemami badawczymi korespondują postawione przez Doktoranta hipotezy badawcze. Doktorant zakłada, iż w związku z coraz szerszym wachlarzem

narzędzi i usług, dostarczających szeroki zakres danych w Internecie oraz poprzez coraz powszechniejszy dostęp do Internetu i znajomości sposobów na wyszukiwanie w nim treści, a także ze względu na fakt, że praktycznie wszystkie aspekty życia osobistego i zawodowego mają swoje odzwierciedlenie w systemach operujących w chmurze, istnieje zwiększające się zagrożenie zarówno dla bezpieczeństwa systemów teleinformatycznych, które te dane przetwarzają, jak i bezpieczeństwa osobowego, które jest bezpośrednio związane z kwestią poufności i integralności przetwarzanych danych. Możliwości i umiejętności użytkowników Internetu dają im sposobność na sprawdzenie jakie dane mogą zdobyć bez narażania się na bezpośrednie niebezpieczeństwo związane z infiltracją źródeł danych. Szczegółowe hipotezy badawcze Doktorant sformułował następująco: ewolucja wyszukiwarek internetowych, zarówno umożliwiających przeglądanie zindeksowanej części Internetu, jak i wyszukiwarek kontekstowych i branżowych, operujących w wąskim zakresie niezindeksowanych danych, umożliwia dotarcie do zakresu danych praktycznie w każdym obszarze informacyjnym. Narzędzia, umożliwiające dostęp do danych graficznych, jak mapy drogowe i satelitarne, obrazy z kamer i zdjęcia opatrzone informacją o ich geolokalizacji, dają możliwość weryfikacji zdarzeń praktycznie w każdym miejscu na Ziemi. Należy także sądzić, że liczba agregatorów danych i materiałów szkoleniowych, dotyczących wywiadu otwartoźródłowego umożliwia bardzo prosty dostęp do całego portfolio narzędzi i wiedzy, które jeszcze do niedawna znane były jedynie osobom, zajmującym się profesjonalnie przedmiotowymi tematami. Poprzez niedoskonałość psychiki ludzkiej oraz wielu aspektów wpływających na możliwość zupełnie bezstronnej i nieograniczonej oceny zbieranych w procesie wywiadu otwartoźródłowego danych, wiele procesów jest zaburzonych przez ograniczenia związane z próbą uzyskania pożądanych efektów, a także z uproszczeniami i uogólnieniami tworzonymi podświadomie przez umysł osoby zajmującej się analizą zebranych danych. Należy sądzić, że uświadomienie analityków w zakresie sposobów nieprawidłowej i spolaryzowanej analizy danych jest w stanie uchronić te osoby przed popełnieniem błędów w zakresie błędnego procesu wnioskowania i uzyskiwania mylnych wyników. Wykorzystanie ogólnodostępnych narzędzi i technik wywiadu otwartoźródłowego daje każdej osobie możliwość dotarcia do szerokiego zakresu informacji, bez wstępnej weryfikacji czy profil danej osoby jest odpowiedni do uzyskania dostępu do określonego zbioru danych i ich późniejszego wykorzystania. Doktorant zakłada również, że brak przygotowania wzakresie poprawnej analizy danych skutkuje wyciąganiem błędnych i często spolaryzowanych wstępnie wniosków, co przekłada się na późniejszą możliwość wysuwania nieprawidłowych oskarżeń i tworzenia fałszywego obrazu sytuacji (umyślnie bądź nieumyślnie). Efekt wytworzenia sensacyjnego wyniku analizy danych może spowodować spolaryzowanie większej ilości użytkowników Internetu, co z kolei może prowadzić do efektu kuli śnieżnej, polegającego na

bazowaniu kolejnych osób na pierwotnie nieprawidłowo przetworzonych informacjach. Wprowadzenie zasad, wynikających z wcześniejszej dogłębnej analizy możliwych do uzyskania danych w ramach prowadzonego wywiadu otwartoźródłowego, jest w stanie zmniejszyć ekspozycję systemów teleinformatycznych na zagrożenia płynące ze zbyt otwartej polityki w zakresie udostępniania danych oraz niedoskonałości oprogramowania, podatnego na techniki pozyskiwania danych pozornie ukrytych i niedostępnych dla przeciętnego użytkownika, a możliwych do uzyskania za pomocą wiedzy specjalistycznej. Doktorant zakłada także, że procedury bezpieczeństwa, wynikające z dokumentów normatywnych, takich jak rodzina norm ISO 27000, a także zasady wynikające zprzeszkolenia w zakresie bezpieczeństwa prowadzenia działań (ang. Operations Security – OPSEC) oraz bezpieczeństwa osobowego (ang. Personal Security – PERSEC), dają możliwości przeciwdziałania technikom wywiadu otwartoźródłowego i pozyskiwania danych, mogących mieć wpływ na bezpieczeństwo osób. Istotnym jest zatem określenie efektywnych metod ochrony przed zidentyfikowanymi technikami, które będą możliwe do wdrożenia w systemach teleinformatycznych oraz procedurach bezpieczeństwa osobowego (s. 18 -20).

Przedstawiając metody, techniki i narzędzia badawcze (s. 22 – 23) Doktorant *de facto* ograniczył się do stwierdzenia, iż „W niniejszej dysertacji zdecydowano się na wybór metody jakościowej prowadzenia badań" oraz że „W celu zweryfikowania hipotez, założonych w niniejszej dysertacji, przeprowadzono wywiad ekspercki". Pozostawia to u czytelnika niedosyt, zwłaszcza, że Doktorant słusznie zauważa na s. 22: „Obszar badań, ujęty w niniejszej pracy, wykracza niejako poza obszar nauk społecznych, w ramach którego funkcjonują nauki o bezpieczeństwie, wskazując na transdyscyplinarny charakter". Trudno się z tym stwierdzeniem nie zgodzić, jednak zasadne staje się pytanie, jakimi konkretnie – poza metodami ogólnologicznymi i wspomnianym powyżej wywiadem eksperckim – metody, narzędzia i techniki badawcze zostały przez Doktoranta wykorzystane.

W odrębnym punkcie Doktorant zawarł mówienie zatytułowane „Analiza krytyczna literatury z zakresu przedmiotu badań" (s. 23 – 27). Nie jest to jednak opis metody badawczej, lecz jedynie wskazanie wymienienie źródeł, z jakich przygotowując dysertację korzystał Doktorant. Jest to zestawienie bardzo obszerne, należy jednak wytknąć Doktorantowi brak uwzględnienia literatury polskiej, choćby pozycji K. Liedela i T. Serafina „Otwarte źródła informacji w działalności wywiadowczej" (Warszawa 2011), czy też K. Liedela, P. Piaseckiej i T. Aleksandrowicza „Analiza informacji. Teoria i praktyka" (Warszawa 2012). Ma to swoje konsekwencje, o których będzie mowa w części niniejszej recenzji zawierającej uwagi krytyczne. Warto też odnotować uchybienie edytorskie: nie

każde źródło internetowe zostało opisane poprzez podanie pełnego adresu strony i daty dostępu.

Generalnie część metodyczną pracy należy ocenić pozytywnie, spełnia ona ustawowe kryteria dysertacji doktorskiej.

Ocena merytoryczna

Dysertacja składa się ze Wstępu, pięciu merytorycznych rozdziałów, Zakończenia, Bibliografii, spisów rysunków i tabel, wykazu skrótów oraz omówienia wyników wywiadu eksperckiego.

Rozdział pierwszy – „Założenia badawcze" – został omówiony powyżej.

W rozdziale drugim – „Charakterystyka metod pozyskiwania informacji z otwartych źródeł" – Doktorant przedstawia szczegółowo metody wykorzystywane w zdobywaniu informacji ze źródeł otwartych, nie pomijając przy tym kwestii wykorzystania mediów społecznościowych.

Rozdział trzeci – „Analiza informacji pozyskanych z zasobów internetowych jako fundament wywiadu" – poświęcony został, zgodnie z tytułem, metodom analizy informacji. Godzi się w tym miejscu zasygnalizować, że metodyka analizy informacji dokonywana jest za pomocą metod, które znajdują zastosowanie nie tylko w obszarze OSINT, lecz stosowane są wobec informacji pochodzących ze wszystkich źródeł (tzw. *all – source analysis*).

W rozdziale czwartym – „Wykorzystanie wywiadu opartego na otwartych źródłach w zakresie bezpieczeństwa systemów teleinformatycznych oraz bezpieczeństwa osobowego i biznesowego" – Doktorant dokonuje identyfikacji możliwych zagrożeń, wynikających z prowadzenia wywiadu otwartoźródłowego przeciw osobom lub organizacjom; prezentuje także także możliwości wykorzystania OSINT-u dla zabezpieczenia sfery osobistej, biznesowej i operacyjnej.

Rozdział piąty – „Możliwe do wprowadzenia zalecenia bezpieczeństwa wzakresie przeciwdziałania wywiadowi otwartoźródłowemu" – zawiera możliwe, zdaniem Doktoranta, zalecenia bezpieczeństwa w zakresie przeciwdziałania mogącym stanowić zagrożenie technikom wywiadu otwartoźródłowego, w oparciu o istniejące normy, standardy oraz inne wytyczne, w tym zasady OPSEC i PERSEC, a także przedstawiono zasady zabezpieczeń odnoszące się do kluczowych osób w organizacjach.

Układ dysertacji jest logiczny i przemyślany. Analiza jej treści pozwala na stwierdzenie, że cele, jakie postawił przed sobą Doktorant, zostały osiągnięte,

problemy badawcze rozwiązane, a hipotezy zweryfikowane. Całość została napisana językiem adekwatnym dla pracy naukowej, a równocześnie czytelnym i zrozumiałym. Zrozumienie skomplikowanych niekiedy zagadnień z zakresu informatyki w znacznej mierze ułatwiają zamieszczone w dysertacji ryciny.

Merytoryczna ocena dysertacji jest zatem pozytywna.

Uwagi krytyczne

Doktorant dość pobieżnie potraktował kwestię analizy informacji, głównie koncentrując swoją uwagę na błędach analitycznych. Poza uwagą doktoranta pozostał podział technik analitycznych na techniki diagnostyczne (*diagnostic techniques*), techniki sporu (*conrarian techniques*) i techniki z użyciem wyobraźni (*imaginative thinking techniques*)oraz techniki bazowe (*basic techniques*), eksploracyjne (*exploration techniques*), diagnostyczne (*diagnostic techniques*), przekształceń (*reframing techniques*) oraz techniki wsparcia procesów decyzyjnego (*decision suport techniques*) i prognostyczne (*foresight techniques*); brak też wzmianki o technikach służące formułowaniu analiz ostrzegawczych i szacowania ryzyka (*warning and estimative intelligence*). Doktorant nie wspomina też o kategorii *ustrukturowanych technik analitycznych* (*structured analytic techniques* – SAT).[7]

Doktorant przytacza znane stwierdzenie Donalda Rumsfelda o kategorii *niewiadome niewiadome* (s. 87). Oczywiście nie sekretarz obrony był twórcą tej zasady; była ona stosowana w analizach National Security Agency, jak też przywoływana w pracach naukowych dotyczących zarządzania w warunkach niepewności[8]. Koncepcja *nieznane nieznane* znalazła swoje rozwinięcie w pracach socjologów. Christopher Daase i Oliver Kessler, zgadzając się z podstawową tezą Rumsfelda stwierdzają, iż rama kognitywna dla praktyki politycznej może być zdeterminowana związkiem pomiędzy tym, *co wiemy*, tym *czego nie wiemy* i tym *czego wiedzieć nie możemy*; do tej triady badacze dodają jeszcze jedną kategorię, a mianowicie to *czego nie chcemy wiedzieć*.[9] W tym kontekście nie od rzeczy będzie przytoczyć odpowiedź jednego z b. szefów brytyjskiej Secret Intelligence Service (MI6) na pytanie historyka Christophera Andrew co tak naprawdę jest podstawowym obowiązkiem szefa wywiadu;

---

[7] Zob. np.: *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. Prepared by the US Government, Washington, DC, March 2009; R. H. Pherson, R. J. Heuer, *Structured Analytic Techniques for Intelligence Analysis*, Thousand Oaks, California 2021

[8] Zob. np.: H.Courtney, J.Kirkland, P.Viguerie, *Managing Uncertainty. Strategy Under Uncertainty, Harvard Business Review*, November – December 1997, https://hbr.org/1997/11/strategy-under-uncertainty dostęp 3.02.2023 r.

[9] Ch.Daase, O.Kessler, *Knowns and Unknowns in the "War on Terror": Uncertainty and the Political Construction of Danger*, Security Dialogue, December 2007; vol. 38, nr 4, s. 411–434.

indagowany odparł lakonicznie: mówić premierowi to, czego ten nie chce wiedzieć.[10]

Doktorantowi należy także wytknąć pominięcie jednego z kluczowych elementów analizy informacji jakim jest określenie wiarygodności źródła informacji i – odrębnie – wiarygodności samej informacji, co wobec coraz większej roli dezinformacji staje się coraz istotniejszym elementem pracy analityka.

Wskazane uchybienie nie zmieniają jednak ogólnej pozytywnej oceny recenzowanej dysertacji.

Konkluzje

Reasumując stwierdzam, że Doktorant w recenzowanej dysertacji zaprezentował swoją ogólną wiedzę teoretyczną w dyscyplinie nauki o bezpieczeństwie oraz umiejętność samodzielnego prowadzenia pracy naukowej. Równocześnie stwierdzam, że przedmiotem recenzowanej dysertacji doktorskiej jest oryginalne rozwiązanie problemu naukowego oraz oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej, a tym samym recenzowana dysertacja spełnia kryteria określone w art. 187 ust. 1 i 2 Ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, Dz. U. 2022 poz. 574.

W związku z powyższym wnoszę o dopuszczenie Doktoranta, Pan mgra inż. Krzysztofa Wosińskiego, do obrony pracy doktorskiej i nadanie mu stopnia naukowego doktora nauk w dyscyplinie nauki o bezpieczeństwie.

[10] Zob.: T. Aleksandrowicz, *Kluczowe megatrendy w bezpieczeństwie państwa w XXI wieku,* Warszawa 2020, s. 137 - 138