dr hab. inż. Jerzy Kosiński, prof. AMW
Wydział Dowodzenia i Operacji Morskich
Akademia Marynarki Wojennej w Gdyni

Szczytno, dn. 2 marca 2023 roku

RECENZJA

rozprawy doktorskiej mgra inż. Krzysztofa Wosińskiego pt.:

ZNACZENIE WYWIADU OPARTEGO NA OTWARTYCH ŹRÓDŁACH (OSINT)

W ZAPEWNIENIU BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH

I BEZPIECZEŃSTWA OSOBOWEGO

przygotowanej pod kierunkiem naukowym prof. dr hab. inż. Piotra Deli

Podstawą napisania recenzji jest Uchwała Rady Dyscypliny „Nauki o Bezpieczeństwie"
nr 3/NOB/2023 z dnia 26 stycznia 2023 roku
w sprawie powołania recenzentów w przewodzie doktorskim Pana mgra inż. Krzysztofa Wosińskiego

1. Ocena wstępna

Bezpieczeństwo cyberprzestrzeni, tak ja i sama cyberprzestrzeń, jest „zjawiskiem społecznym" z natury bardzo złożonym. Cyberprzestrzeń jako obszar niematerialny, ponadgranicznym, ale odbijający się w świecie rzeczywistym jest tematem badań wielu dziedzin nauki. Dynamika, intensywność zmian w cyberprzestrzeni implikuje konieczność prowadzenia dogłębnych analiz, które będą stanowiły podstawę działań zapobiegawczych, ale również reakcji na pojawiające się zagrożenia. Media społecznościowe, wortale i portale dostarczające danych na wybrany temat w Internecie stały się dla wielu osób i organizacji podstawowym źródłem informacji. Dotycz to także

tych, którzy chcą naruszyć bezpieczeństwo użytkowanych systemów teleinformatycznych lub osób. OSINT internetowy stał się dla przestępców podstawowym elementem przygotowania późniejszego ataku. Tym samym zachowanie bezpieczeństwa operacyjnego (OPSEC) stanowi jeden z kluczowych aspektów bezpiecznego korzystania z internetu. Z drugie strony spoglądając, pozyskanie informacji z ogólnodostępnych źródeł, można traktować jako narzędzie prewencyjne pozwalające na budowanie ochrony osobistej i organizacyjnej przeciwko działaniom przestępców.

Biorąc powyższe pod uwagę, należy uznać, że wywiad otwartoźródłowy stanowi na ogół duże wyzwanie pod względem praktycznym, a prawie zupełnie nie analizowane pod względem naukowym. Większość narzędzi wywiadu otwartoźródłowego może być wykorzystana zarówno do poprawy bezpieczeństwa, jak i jego naruszenia, a trudno przewidzieć, a jeszcze trudniej zmierzyć jakie będą tego skutki. W warunkach niepełnej i niepewnej informacji jednym z działań wspomagający użytkowników internetu jest gromadzenie, analizowanie i przekazywanie wiedzy na temat OSINT.

W powyższym kontekście, rozprawa Pana mgra inż. Krzysztofa Wosińskiego powinna być postrzegana bardzo pozytywnie. Autor rozprawy za przedmiot swoich badań przyjął: 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.

Tak sformułowany przedmiot badania świadczy dobrze o świadomości Doktoranta problematycznych kwestii dotyczących możliwości stwarzania

przez OSINT zagrożeń w cyberprzestrzeni, a jednocześnie podnoszenia poziomu cyberbezpieczeństwa.

Główny problem badawczy rozprawy zawarty jest w pytaniu:

(a) *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?* (str.17) i uzupełniony 4 pytaniami szczegółowymi:

(b) *Jakie narzędzia i techniki wywiadu otwartoźródłowego są dostępne dla użytkowników Internetu?,*

(c) W jaki sposób należy poddawać analizie zebrane informacje, aby uniknąć ich błędnej interpretacji?,

(d) Jakie zagrożenia płyną z powszechnej możliwości stosowania wywiadu otwartoźródłowego oraz nieprawidłowej analizy danych pozyskanych w ramach przedmiotowych działań w Internecie?,

(e) Jakie są możliwości zabezpieczenia infrastruktury teleinformatycznej oraz zapewnienia bezpieczeństwa osobowego przed działaniami wynikającymi z prowadzonego wywiadu otwartoźródłowego? (str. 17).

Na podstawie dotychczasowej wiedzy i wstępnej obserwacji Autor dysertacji sformułował 5 rozbudowanych hipotez badawczych odpowiadających problemom badawczym (głównemu i 4 szczegółowym):

(1) Zakładam, że 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.

(2) Przypuszczam, że 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.

(3) Zakładam, że 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.

(4) 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. Zakładam, że brak przygotowania w zakresie 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.

(5) Przypuszczam, że 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.

W celu weryfikacji przedstawionych hipotez Doktorant wykorzystał kilka metod badawczych: badanie dokumentów, studium przypadku, metody jakościowe i przypisane im techniki badawcze oparte na wywiadzie eksperckim Autor przeprowadził także eksperymenty badawcze (opis ss.57-59).

Wszystkie hipotezy robocze zostały pozytywnie zweryfikowane, co Doktorant jawnie potwierdził dla głównej hipotez na s.145 oraz we wnioskach rozdziałów 2-5.

Celem poznawczym badania była 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.

W sensie pragmatycznym do celu badań należało: 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.

Zarówno postawione problemy badawcze, jak i sformułowane hipotezy badawcze są adekwatne do tematu, przyjętego celu pracy i przedmiotu badań.

Przyjęty w pracy schemat postępowania badawczego odpowiednio kierunkował wysiłek Doktoranta na realizację celu pracy i naukową weryfikację postawionych hipotez badawczych.

W kontekście całości pracy należy zwrócić uwagę na, wprawdzie niezbyt obszerne, ale precyzyjne wykorzystanie wiedzy grupy eksperckiej. Niestety Doktorant nie napisał jak licznej grupy ekspertów, ani jakie przyjęto kryterium bycia ekspertem.

Praca została napisana językiem poprawnym z niewielką ilością błędów, chociaż zdarzają się również pojedyncze zapisy nieprecyzyjne. Rozdziały i podrozdziały, ich tematyka i następstwo, tworzą logiczną całość. Pewne zastrzeżenie można mieć do kompletności rozważenia problemu szczegółowego (c), gdyż praktycznie pominięto w nim oceny wiarygodności źródła i informacji (chociaż w pracy Autor kilkukrotnie wspomina, że jest to ważna rzecz).

Recenzowana rozprawa stanowi istotny wkład w rozwój badań w obszarze nauk społecznych, ze szczególnym uwzględnieniem zagadnień bezpieczeństwa narodowego.

2. Zawartość rozprawy

Dysertacja Pana mgra inż. Krzysztofa Wosińskiego liczy ogółem 138 stron tekstu, 6 stron bibliografii (25 poz. powołanej literatury, 10 poz. dokumentów) z netografią (44 poz.), spis rysunków, spis tabel, wykaz skrótów i 21 stron załącznika (wywiad ekspercki). Wykorzystana w pracy literatura przedmiotu, nie jest zbyt obszerna, ani kompletna (np. w zakresie weryfikacji źródeł i informacji).

Podstawowy tekst rozprawy składa się z krótkiego wstępu, pięciu rozdziałów (metodyczny i 4 merytoryczne odpowiadające szczegółowym problemom badawczym) i zakończenia.

We wstępie Doktorant przedstawia ogólny zarys pojęcia wywiadu otwartoźródłowego i precyzuje używane w pracy pojęcia.

W pierwszym rozdziale pt. Założenia badawcze (ss. 13-28) Doktorant opisał genezę problemu i przedmiot badań. Sformułował cel poznawczy oraz utylitarny badań, problem badawczy (1+4), hipotezy robocze (1+4). Bardzo ogólnie przedstawił wykorzystane (oraz nie) metody i techniki badawcze (podrozdział jest właściwie jednym cytatem). Dokonał przeglądu literaturowo-faktograficznego z zakresu wykorzystywanego w poszczególnych rozdziałach. W zakończeniu opisał ograniczenia badawcze (problem weryfikacji informacji i jej źródeł).

W drugim, najobszerniejszym rozdziale pt. Charakterystyka metod pozyskiwania Informacji z otwartych (ss.29-81) źródeł Autor scharakteryzował metody pozyskiwania informacji z otwartych źródeł, nakreślił zakres i podział rozpoznania otwartoźródłowego, a także omówił subiektywnie wybrane techniki działań OSINT-owych.

W trzecim rozdziale pt. Analiza informacji pozyskanych z zasobów Internetowych jako fundament wywiadu (82-101) Doktorant opisuje cykl wywiadowczy, typy rozumowań zachodzących w procesie analizy informacji oraz związane z tym błędy

W trzecim rozdziale pt. Wykorzystanie wywiadu opartego na otwartych źródłach w zakresie bezpieczeństwa systemów teleinformatycznych oraz bezpieczeństwa osobowego i biznesowego (102-123) Doktorant opisał nadmiarowe udostępnianie informacji pozwalające na wyszukanie potencjalnie możliwych zagrożeń, wynikających z prowadzenia wywiadu otwartoźródłowego przeciw osobom lub organizacjom. Sporządził zestawienie zagrożeń i technik ataków wykorzystujących rozpoznanie otwartoźródłowe. W

tym rozdziale przedstawił także możliwości wykorzystania OSINT-u dla zabezpieczenia sfery osobistej, biznesowej i operacyjnej.

W rozdziale piątym pt. Możliwe do wprowadzenia zalecenia bezpieczeństwa w zakresie przeciwdziałania wywiadowi otwartoźródłowemu (ss. 124-142) Doktorant zaproponował możliwe do wprowadzenia zalecenia przeciwdziałania technikom wywiadu otwartoźródłowego, w oparciu o istniejące normy, standardy oraz inne wytyczne, w tym zasady OPSEC i PERSEC, a także przedstawił zasady cyberzabezpieczeń odnoszące się do kluczowych osób w organizacjach.

Zakończenie (ss. 143-148) stanowi właściwą syntezę badań. Doktorant podkreślił, że techniki, dostępne dla każdego użytkownika internetu, umożliwiają szeroki wachlarz możliwości rozpoznania i uzyskania odpowiedzi na pytania wywiadowcze, sformułowane w stosunku do analizowanego podmiotu. Jednocześnie zagrożenia wynikające z przeniesienia znacznej części działań osobistych oraz biznesowych do internetu znacznie zwiększają ekspozycję podmiotów na OSINT, a także stwarzają bardziej bezpośrednie niebezpieczeństwo wykonania ataku z jednoczesnym znikomym ryzykiem, związanym z wykryciem i konsekwencjami działań atakujących.

Na uwagę zasługuje to, że Doktorant na zakończenie każdego rozdziału dokonuje krótkiego podsumowania treści rozdziału. Całość pracy jest przedstawiona w sposób bardzo zwięzły, ale interesujący i zrozumiałym językiem, co w konsekwencji pozwala wystawić Autorowi wysoką ocenę.

Przeprowadzone badanie i wnioski końcowe świadczą o dojrzałości naukowej kandydata do stopnia doktora.

3. Ocena merytoryczna dysertacji

Doktorant poddał wnikliwej analizie problem badawczy, odpowiadając na postawione pytania i weryfikując założone hipotezy. Określenie problemu badawczego, opis celów i uwarunkowań danego problemu zawarte w rozdziałach 2-5, zostały przedstawione na tyle szczegółowo, aby można było odpowiednio zaplanować badanie (opisane w Załaczniku). Należy stwierdzić, że układ rozdziałów i podrozdziałów jest logicznie uzasadniony i hierarchicznie uporządkowany, tytuły i podtytuły dokładnie określają zakres merytoryczny i odpowiadają zawartej w nich treści. Treści kolejnych rozdziałów i podrozdziałów wynikają z postawionych problemów badawczych i poprzedzających je rozważań.

Zarówno w konstrukcji, jak i treści pracy widać bardzo duży, pozytywny wpływ promotora.

Należy zauważyć, że autor pewnie porusza się w niełatwej dziedzinie wiążącej zagadnienia prawne, organizacyjne i techniczne (informatyczne) z przewagą tych ostatnich.

W nawiązaniu do rozważań szczegółowych warto podkreślić, że recenzowana praca stanowi cenną inspirację do dalszej naukowej dyskusji (przynajmniej w obszarze wskazanym w zakończeniu), a tym samym do dalszego rozwoju nauk o bezpieczeństwie.

W pracy występują incydentalne błędy redakcyjne (w wersji cyfrowej, z której korzystał recenzent), które nie obniżają wysokiej wartości recenzowanej pracy.

Reasumując: uznaję, że dysertacja pt.: „Znaczenie wywiadu opartego na otwartych źródłach (OSINT) w zapewnieniu bezpieczeństwa systemów

teleinformatycznych i bezpieczeństwa osobowego" s**pełnia wszystkie wymogi formalne i merytoryczne** określone w art. 13 ust. 1 Ustawa z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (z późniejszymi zmianami) oraz ustawie z dnia 20 lipca 2018 r., Prawo o szkolnictwie wyższym i nauce, art. 179.1. dotyczący: „przewody doktorskie, postępowania habilitacyjne i postępowania o nadanie tytułu profesora wszczęte i niezakończone przed dniem wejścia w życie ustawy, o której mowa w art. 1, są przeprowadzane na zasadach dotychczasowych i **wnioskuję o dopuszczenie Pana mgra inż. Krzysztofa Wosińskiego do publicznej obrony doktoratu**.