STUDIA POLITOLOGICZNE VOL. 54
DOI: 10.33896/SPolit.2019.54.11

MICHAEL BAZZELL

Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information

Createspace Independent Publishing Platform, 6th ed., Charleston 2018, 461 s.

(Bartosz Biderman
ORCID: 0000-0002-8503-5207)

SŁOWA KLUCZOWE:
biały wywiad, wyszukiwanie informacji, infobrokering, wywiad jawnoźródłowy

Michael Bazzell jest postacią powszechnie rozpoznawaną, zarówno w środowisku osób zajmujących się białym, jak i szarym wywiadem internetowym. Sam siebie określa jako międzynarodowego konsultanta do spraw prywatności[1]. W branży białego wywiadu ma bardzo duże doświadczenie. Przez ponad 18 lat w imieniu rządu USA badał przestępstwa komputerowe. Większość tego czasu pracował dla Federalnego Biura Śledczego, gdzie był przydzielony do grupy zadaniowej Cyber Crimes Task Force[2]. Skupiał się tam na przeprowadzaniu badań online i gromadzeniu danych typu otwarte źródła informacji (ang. *open source intelligence*, OSINT). Jako

[1] Ang. *International Privacy Consultant*; zob. oficjalny profil autora publikacji: https://twitter.com/inteltechniques (dostęp: 16.12.2018).

[2] Wydział Cybernetyczny FBI, jednostka powstała w 2002 r. Zajmuje się cyberterroryzmem w czterech głównych dziedzinach: włamania komputerowe, kradzieże tożsamości, wykorzystywanie seksualne dzieci i poważne cyberoszustwa, w tym szpiegostwo. Ten pododdział FBI wykorzystuje informacje zebrane podczas śledztwa w celu informowania społeczeństwa o aktualnych tendencjach w cyberprzestępczości. *The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat*, U.S. Department of Justice Office of the Inspector General Audit Division, April 2011, s. 2–4, https://itlaw.wikia.org/wiki/The_Federal_Bureau_of_Investigation%27s_Ability_to_Address_the_National_Security_Cyber_Intrusion_Threat (dostęp: 21.06.2019).

aktywny detektyw był zaangażowany w wiele poważnych śledztw kryminalnych, w tym prowadzonych w sprawie nagabywania dzieci przez Internet do czynności seksualnych, uprowadzeń dzieci, porwań, morderstw na zlecenie, gróźb terrorystycznych i włamań komputerowych.

Obecnie M. Bazzell od kilku lat zajmuje się przeprowadzaniem szkoleń z technik pozyskiwania i przetwarzania OSINT. W tym czasie wyszkolił tysiące osób (zarówno pracowników administracji państwowej, jak i w sektorze prywatnym), również w korzystaniu ze swoich autorskich rozwiązań i technik śledczych. Jako doradca techniczny wystąpił w pierwszym sezonie programu telewizyjnego *Mr. Robot*. Jego książki *Open Source Intelligence Techniques* (2012, szóste wydanie – 2018) oraz *Hiding from the Internet* (2012, czwarte wydanie – 2018) są najlepiej sprzedającymi się w Stanach Zjednoczonych i Europie pozycjami w zakresie OSINT[3].

Książka *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information* (nr ISBN-13: 978-1984201577, nr ISBN-10: 1984201573) jest praktycznym wprowadzeniem do nauki pozyskiwania i przetwarzania informacji. W wyszukiwarce Google Scholar pod hasłem „OSINT" oprócz omawianej monografii odnaleźć można ponad pięć tysięcy innych druków zwartych i rozproszonych. Interesującym faktem jest, iż publikacja pierwszej edycji książki M. Bazzella pokrywa się z nagłym wzrostem popularności hasła „OSINT" w wyszukiwarce internetowej Google.com[4]. Od 2012 roku zarówno hasło „OSINT", jak i zwroty blisko z nim powiązane (między innymi nazwy oprogramowań: Maltego, FOCA) nieustannie zyskują na popularności. Wraz z kolejnymi edycjami książki zauważalne są skokowe wzrosty wyszukiwań (drugie wydanie – 2013, następne kolejno: 2014, 2015 i 2016). Na tej podstawie wnioskować można, iż autor wnosi znaczny wkład w popularyzację białego wywiadu oraz jego rozwój.

W omawianej monografii, oprócz przedstawienia powszechnie znanych w środowisku OSINT metod pozyskiwania informacji, M. Bazzell z dumą prezentuje również swoje autorskie rozwiązania mające znaczny wkład w rozwój cyberbezpieczeństwa. Jednym z nich jest stworzony w 2017 roku (we współpracy z Davidem Westcottem) Buscador Linux[5], któremu poświęcony został cały drugi rozdział oraz fragmenty w dalszych częściach publikacji. System ten ma za zadanie umożliwienie przeprowa-

[3] Oficjalna strona autora publikacji, gdzie streszczony jest jego życiorys: https://inteltechniques.com/live-keynotes.html (dostęp: 16.12.2018).

[4] Nagły, ponad pięciokrotny skok wyszukiwań można było zaobserwować w przeciągu dwóch miesięcy styczeń–luty 2012, https://trends.google.com (dostęp: 16.12.2018).

[5] System jest darmowy (niektóre narzędzia są dodatkowo płatne) i można go pobrać ze strony głównej autora. Najnowsza wersja 2.0 (ze stycznia 2019) dostępna pod adresem: https://inteltechniques.com/buscador/ (dostęp: 16.12.2018).

dzania badań online również osobom z niewielką wiedzą o obsłudze środowiska Linux. Środowisko pentesterów z dezaprobatą wyraża się o tym systemie, który *sensu stricto* jest czystą wersją Ubuntu Linux, urozmaiconą wbudowanymi dodatkowymi aplikacjami, takimi jak Maltego, Recon-ng, Creepy, Spiderfoot, TheHarvester czy Sublist3r. M. Bazzell w książce odpowiada jednak, iż takie było jego główne zadanie – utworzenie systemu lekkiego, przyjemnego w obsłudze, czyli systemu „dla każdego" oraz możliwego do postawienia na wirtualnej platformie[6]. Dodatkowy atut to fakt, że Buscador Linux jest jedną z niewielu platform, która bardzo płynnie współpracuje z komputerami Mac firmy Apple. Dokładny opis instalacji (zarówno wirtualnej maszyny, jak i stabilnego systemu lub bootowanego z pendriva) oraz opis obsługi systemu pozwalają na przeprowadzenie skomplikowanych operacji przez każdego, nawet z niewielkim doświadczeniem w informatyce.

Open Source Intelligence Techniques nie jest monografią *stricte* naukową. Brakuje w niej przypisów i odniesień do materiałów źródłowych. M. Bazzell nie jest jednak pracownikiem akademickim, lecz byłym pracownikiem służb, osobą z bardzo dużym doświadczeniem i chęcią podzielenia się nim. Prosty w użyciu język, duża liczba grafik oraz obszerne – czasami aż nazbyt – tłumaczenia problemów pozwalają traktować publikację jako poradnik w zakresie prowadzenia białego wywiadu. Autor po kolei pokazuje czytelnikowi, jak przejść całą drogę prawidłowo prowadzonego dochodzenia.

W rozdziale 1 znajdziemy więc wskazówki, jak bezpiecznie przygotować swój komputer przed przystąpieniem do pracy. Znajdują się tam szczegółowe techniki konfiguracji przeglądarek internetowych oraz proponowane ustawienia bezpieczeństwa sieci. Jest to element niezwykle ważny, gdyż umożliwiający zachowanie w miarę możliwości anonimowość w Internecie. W kolejnych rozdziałach umieszczone zostały szczegółowe opisy działania oraz metody użycia narzędzi śledczych, w zdecydowanej większości stworzonych przez autora. Umożliwiają one korzystanie z wielu aplikacji i stron służących do prowadzenia dochodzeń w usystematyzowany, łatwy sposób. Każdy rozdział poświęcony jest osobnemu źródłu informacji. Tak więc w czwartym znajduje się omówienie narzędzi śledczych służących do inwigilacji użytkowników Facebooka, a w piątym Twittera. Dalej opisane są między innymi narzędzia do przeszukiwań Internetu pod względem nazwy użytkownika (rozdz. 9), maila (rozdz. 8, 10) czy numeru telefonu[7] (rozdz. 11) lub adresu IP[8] (rozdz. 17). Rozdział 18 przybliża metody przeszu-

[6] Dzięki czemu z łatwością można kontrolować cały ruch wychodzący oraz przepuszczać go przez bramki proxy czy VPN.

[7] Działa wyłącznie z numerami zarejestrowanymi w krajach Ameryki Północnej.

[8] By odnaleźć omawiane narzędzia, należy na stronie https://inteltechniques.com kliknąć w zakładkę „Tools" (dostęp: 16.12.2018). Dostęp do nich

kiwania rządowych baz danych, jednak wyłącznie tworzonych i prowadzonych przez administrację USA. W rozdziale 19 autor omawia stosowane przez siebie inne aplikacje śledcze, w większości oparte na licencji *open source* i dostępne dla każdego[9]. Dalsza część powstała wraz z szóstym wydaniem i znajduje się w niej opis najnowszych metod śledczych stosowanych przez M. Bazzella, a często niesłusznie pomijanych w dochodzeniach ze względu na ich „młodzieżowy" charakter, pozorną nieprzydatność, jak i niedawne uruchomienie usług. W rozdziale 21 znajdziemy narzędzie wiążące nazwę użytkownika SnapChata z numerem telefonu czy wskazówki, do czego może się przydać aplikacja randkowa Tinder w zaawansowanych indagacjach śledczych. W rozdziale 24 autor porządkuje metody dochodzeniowe oraz proponuje gotowe schematy badań w zależności od posiadanych danych.

Głównym celem przyświecającym autorowi od pierwszego wydania pracy było – jak sam wskazuje we wstępie – umożliwienie przeprowadzania śledztw również osobom niespecjalizującym się w informatyce, takim jak pracownicy administracji publicznej czy prywatnych korporacji (uczestnicy jego szkoleń). Niewątpliwie ten cel został osiągnięty. Monografia w prosty sposób przybliża nawet bardziej zaawansowane metody śledcze i czyni je zrozumiałymi. Zastanawiający jest dla mnie jednak klucz doboru opisywanych narzędzi. W książce brakuje opisu działań aplikacji zawartych między innymi w autorskim systemie Buscador Linux, jak na przykład Maltego, ponadto należy wspomnieć praktyczne pominięcie opisu kombajnów takich jak SpiderFoot czy Harvester[10]. Wszystkie trzy służą do przeprowadzania ukierunkowanych na dany cel dochodzeń, zgodne są więc z założeniem przyjętym przez M. Bazzella, iż OSINT to zdobywanie wiedzy o osobie w realnym świecie przy pomocy danych pozostawionych w tym wirtualnym. Brak użycia tych aplikacji przyczynić się może do niekompletności wyników badań.

Sądzę jednak, iż powyższa publikacja w znacznym stopniu przyczynia się do rozwoju OSINT. Choć w Internecie znaleźć można dużo artykułów i dokumentów traktujących o otwartych źródłach informacji, mało który jest na tyle kompletny, by przeprowadzić czytelnika krok po kroku po drabinie dochodzeniowej. Ubolewać można, iż wśród światowych autorów brak jest polskich naukowców. Nie ma woli poszerzania wiedzy dotyczącej białego wywiadu w Internecie. Istniejące publikacje, jak ta Krzysztofa Liedela i Tomasza Serafina[11] oraz praca zbio-

jest w większości darmowy lub możliwe jest skorzystanie z wersji Trail.

9 Między innymi w te narzędzia wyposażony został Buscador Linux.

10 Usprawiedliwić autora może fakt, iż dwie ostatnie wymienione aplikacje w niektórych państwach, w pewnych konfiguracjach, przekraczają granice dopuszczone normami prawnymi. Przez to niedoświadczony użytkownik narazić się może na konsekwencje prawne.

11 K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011.

rowa pod redakcją Wojciecha Filipkowskiego i Wiesława Mądrzejowskiego[12], choć bardzo cenne, są już w dużej mierze nieaktualne i wymagają ponownej edycji. Nie zostały one również przetłumaczone na język angielski, przez co grupę odbiorców zawężono wyłącznie do polskich badaczy. *Open Source Intelligence Techniques* to odpowiednia publikacja zarówno dla osób zaczynających swoją przygodę z OSINT, jak i tych bardziej zaawansowanych. Z pewnością każdy znajdzie tu coś interesującego dla siebie.

Streszczenie

Informacja jest złotem XXI wieku. Czy Michael Bazzell w swojej książce *Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information* (2018) uczy, jak ją zdobywać? W niniejszej recenzji zawarto odpowiedź na to pytanie, wraz z obiektywnym spojrzeniem na całą publikację. We wstępie przedstawiona została biografia autora, wraz z jego doświadczeniem oraz wpływem na rozwój OSINT-u, czyli pozyskiwania informacji ze źródeł otwartych. W dalszej części recenzent opisuje rozwiązania proponowane swoim czytelnikom przez M. Bazzella. Pod koniec ocenie poddany został cel pracy, trafność argumentacji oraz orientacja autora w najnowszym dorobku reprezentowanej przez niego dziedziny, a także język i logika formułowanych wypowiedzi. Krytykę kończy syntetyczne podsumowanie omawianych wad i zalet oraz wyraźna opinia o recenzowanym dziele.

Bartosz Biderman

Michael Bazzell, Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information

In the 21st century, information is golden. The question is whether in his book entitled *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information* Michael Bazzell teaches us how to get it? This review answers this question by providing an objective overview on the publication. The introduction contains certain biographical information on the author, including information on his experience and its impact on the development of the open-source intelligence (OSINT). Next, the reviewer goes on to describe the solutions that M. Bazzell proposes to his readers, followed by the assessment of the work's goal and reasoning, the author's familiarity with the recent studies in the field, as well as the language of and the logic behind the statements. The review ends with a summary of the strengths and weaknesses of the publication and a clear view on the work.

Key words: *OSINT, white hat, data broker, intelligence assessment*

[12] W. Filipowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Warszawa 2012.