Przegląd Bezpieczeństwa Wewnętrznego
2024, nr 31, s. 119–151

https://doi.org/10.4467/20801335PBW.24.020.20797

ARTYKUŁ

Wywiad jawnoźródłowy w internecie – kategoryzacja i ewaluacja narzędzi wyszukiwawczych

Open source intelligence on the internet – categorisation and evaluation of search tools

DANIEL MIDER

Wydział Nauk Politycznych i Studiów Międzynarodowych,
Uniwersytet Warszawski
https://orcid.org/0000-0003-2223-5997

Abstrakt

Artykuł przedstawia kompleksową analizę i systematyczny przegląd narzędzi wyszukiwawczych stosowanych w wywiadzie jawnoźródłowym (*open source intelligence*, OSINT). Ewaluacji poddano trzy główne kategorie oprogramowania: systemy zintegrowane z systemem operacyjnym lub przeglądarką internetową, autonomiczne aplikacje oraz repozytoria odnośników do narzędzi specjalistycznych. Dokonano krytycznej ewaluacji reprezentatywnych egzemplifikacji z każdej kategorii, uwzględniając ich funkcjonalność, efektywność oraz ograniczenia. W toku analizy zidentyfikowano istotne luki w obecnym instrumentarium oraz sformułowano postulaty dotyczące potencjalnych kierunków rozwoju warsztatu operatora OSINT. Jako optymalny kierunek rozwoju wskazano otwarte, modularne narzędzia o niskim progu wejścia, pozwalające na aktywny udział społeczności w ich doskonaleniu i dostosowywaniu do indywidualnych potrzeb analityków. Przedstawione wyniki stanowią kompendium wiedzy dla naukowców, praktyków oraz entuzjastów OSINT.

Słowa kluczowe

wywiad jawnoźródłowy, OSINT, cyberbezpieczeństwo, wyszukiwanie w internecie

Abstract

This article presents a comprehensive analysis and systematic review of search tools used in Open Source Intelligence (OSINT). Three main categories of software were evaluated: systems integrated with operating platforms (OS) or web browsers, standalone applications, and repositories of links to specialized tools. A critical evaluation of representative examples from each category was conducted, taking into account their functionality, effectiveness, and limitations. The analysis identified significant gaps in the current OSINT toolset and formulated postulates regarding potential directions for the development of operators' methodologies. The optimal development direction should focus on open source, modular tools with a low entry barrier, enabling community participation in their refinement and customization for analysts' needs. The findings serve as a knowledge compendium for OSINT researchers, practitioners, and enthusiasts.

Keywords

open source intelligence, OSINT, cybersecurity, internet-based information retrieval

Wprowadzenie

Obserwowany jest bezprecedensowy, nieustanny wzrost wolumenu danych dostępnych w internecie, obejmujących informacje zarówno ustrukturyzowane, jak i nieustrukturyzowane[1]. Przyrost danych przyczynił się do powszechnego postrzegania zasobów globalnej sieci jako fundamentalnego źródła informacji oraz doprowadził do wykształcenia się i dynamicznego rozwoju metodyki pozyskiwania informacji znanej jako wywiad jawnoźródłowy (*open source intelligence*, OSINT)[2] lub biały

[1] Wolumen danych w internecie wzrósł z 4,4 zettabajta w 2013 r. do 6,6 zettabajta w 2014 r. W 2020 r. wyniósł 64,2 zettabajta, a prognozy na 2025 r. wskazują, że osiągnie 175–181 zettabajtów. To oznacza, że średni roczny wzrost jest na poziomie ok. 33%, a wolumen danych podwaja się co ok. 2,5 roku. Zob. D. Reinsel, J. Grantz, J. Rydning, *The Digitization of the World. From Edge to Core*, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf [dostęp: 28 VI 2024]; *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025*, Statista, czerwiec 2021 r., https://www.statista.com/statistics/871513/worldwide-data-created/ [dostęp: 28 VI 2024].

[2] Prawie wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje tej informacji za każdym razem. Informacja pojawia się jedynie w przypadku wyrazów obcych pochodzących z języka innego niż angielski (przyp. red.).

wywiad. Zaowocowało to szerokim wykorzystaniem OSINT w wielu dziedzinach: w cyberbezpieczeństwie, w wywiadzie gospodarczym, konkurencyjnym, politycznym i wojskowym, w dochodzeniach kryminalnych i ubezpieczeniowych, a także w różnych formach wsparcia organów ścigania oraz zarządzaniu ryzykiem. Coraz częściej podkreśla się wartość oraz legitymizację wykorzystania dowodów ze źródeł otwartych w międzynarodowych dochodzeniach karnych[3]. Istotną rolę w gromadzeniu elektronicznych dowodów przestępstw odgrywają niewielkie, wyspecjalizowane organizacje wykorzystujące źródła otwarte do dokumentowania zbrodni i dostarczania dowodów o wysokim stopniu wiarygodności. Na przykład ustalenia Bellingcat, wiodącej organizacji zajmującej się OSINT i dziennikarstwem śledczym, uznano za wystarczająco rzetelne, aby mogła je wykorzystać oficjalna komisja badająca sprawę zestrzelenia malezyjskiego samolotu wykonującego lot MH17[4]. W orzeczeniu Europejskiego Trybunału Praw Człowieka w sprawie Ukraina i Holandia przeciwko Rosji wśród dowodów przedstawionych przez prawników reprezentujących Ukrainę znajdowały się również ustalenia organizacji prowadzącej OSINT na takie tematy, jak: zaangażowanie Rosji w Ukrainie, losy MH17, transgraniczne ataki artyleryjskie oraz działania personelu rosyjskiej armii we wschodniej Ukrainie[5]. Skuteczność metodyki

---

[3] A. Mackinnon, *Bellingcat Can Say What U.S. Intelligence Can't*, Foreign Policy, 17 XII 2020 r., https://foreignpolicy.com/2020/12/17/bellingcat-can-say-what-u-s-intelligence-cant/ [dostęp: 28 VI 2024]; *Electronic evidence of war crimes. The role of journalists, media and social media*, webinar zorganizowany przez Group of Friends on the Safety of Journalists and Media Freedom in Strasbourg oraz Radę Europy, 25 XI 2022 r., https://www.coe.int/en/web/kyiv/-/electronic-evidence-of-war-crimes-and-the-role-of-journalists-media-and-social-media [dostęp: 28 VI 2024]; E. White, *Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism*, Cambridge University Press, 7 IX 2023 r., https://www.cambridge.org/core/journals/leiden-journal-of-international-law/article/closing-cases-with-opensource-facilitating-the-use-of-usergenerated-opensource-evidence-in-international-criminal-investigations-through-the-creation-of-a-standing-investigative-mechanism/981CEFF9D5AF80B6FD0A75BE6A1A384C [dostęp: 28 VI 2024].

[4] O. Matthews, *Fact Cats. The inside story of how it got the Skripal scoop*, The Spectator, 20 X 2018 r., https://www.spectator.co.uk/article/fact-cats/ [dostęp: 28 VI 2024]. Warto również wspomnieć o śledztwie dotyczącym ataku chemicznego w kwietniu 2017 r. w Chan Szajchun w Syrii, który doprowadził do śmierci ok. 100 osób. Bellingcat wykorzystał dane ze źródeł otwartych, takie jak: fotografie, nagrania wideo, dane meteorologiczne i relacje naocznych świadków, i zrekonstruował wydarzenia przed atakiem, w trakcie i po nim. Pozwoliło to zidentyfikować miejsce wystrzelenia rakiety oraz znaleźć dowody obciążające syryjskie siły rządowe. Raport Bellingcat zyskał uznanie ze względu na przejrzystość metodologii i możliwość weryfikacji przedstawionych dowodów przez osoby trzecie.

[5] E. Higgins, *How Open Source Evidence was Upheld in a Human Rights Court*, Bellingcat, 28 III 2023 r., https://www.bellingcat.com/resources/2023/03/28/how-open-source-evidence-was-upheld-in-a-human-rights-court/ [dostęp: 28 VI 2024]; *Case of Ukraine and the Netherlands v. Russia, 8019/16, 43800/14, 28525/20*, Archiwum Europejskiego Trybunału Praw Człowieka, 30 XI 2022 r., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-222889%22]} [dostęp: 28 VI 2024].

OSINT przyciąga uwagę ekspertów, a informacje zbierane przez cywilne, niezależne organizacje są wysoko oceniane i wykorzystywane przez specjalistów w zakresie wywiadu[6]. W dyskursie publicznym pojawiają się opinie funkcjonariuszy służb specjalnych, że organizacje zajmujące się wywiadem jawnoźródłowym na wielu polach przewyższają efektywnością tradycyjne służby wywiadowcze. Metodyka działań tych organizacji jest jednak zbyt innowacyjna, by zaakceptowali je decydenci[7]. Specjaliści sugerują ponadto, że jedna z organizacji (Bellingcat) stała się „największym koszmarem" Federacji Rosyjskiej wskutek systematycznego ujawniania informacji o jej działaniach wewnętrznych i poza granicami kraju[8]. Przytoczone stwierdzenia mają status anegdotyczny, odzwierciedlają jednak emocje ekspertów rozbudzane przez nowe zjawisko. Perspektywy finansowe również prezentują się imponująco – globalny rynek rozwiązań wywiadowczych OSINT dynamicznie rośnie. W 2022 r. jego wartość wyniosła 4219,56 mln dolarów, a prognozy wskazują, że do 2031 r. osiągnie wartość 7317,89 mln dolarów, co przekłada się na skumulowany roczny wskaźnik wzrostu we wskazanym okresie na poziomie 6,31%[9]. Wszechstronne wykorzystanie wywiadu jawnoźródłowego w tak wielu obszarach wynika z jego zdolności do skutecznego pozyskiwania, przetwarzania i analizy ogromnych ilości danych dostępnych publicznie, co przekłada się na wartościowe spostrzeżenia osiągane niewygórowanym kosztem. Rosnąca rola OSINT skłania do pogłębionej refleksji nad jego znaczeniem, potencjałem oraz wyzwaniami związanymi z jego stosowaniem.

Celem niniejszego artykułu jest kategoryzacja i ewaluacja wybranych narzędzi OSINT służących do wyszukiwania informacji. W artykule skupiono się wyłącznie

---

[6] A. Mackinnon, *Bellingcat Can Say…* Warto dodać, że wyniki analiz dostarczane przez społeczność OSINT pozwalają funkcjonariuszom wywiadów na bardziej swobodną dyskusję publiczną, bez obaw o ujawnienie źródeł lub metod pozyskiwania informacji.

[7] W oryginale: „I'd say they're way ahead of us on many things, (…) Bellingcat's methods are 'way too innovative for the great majority of lemmings in government (…)". Zob. O. Matthews, *Fact Cats…* Notabene, w 1996 r. komisja Aspina–Browna w USA zaleciła zmianę postawy Wspólnoty Wywiadowczej (Intelligence Community) wobec OSINT, podkreślając, że amerykańskie służby powoli wdrażają tę metodykę, a nie utworzono postulowanej National Open Source-Intelligence Agency jako 19. członka Wspólnoty Wywiadowczej.

[8] AFP, *How Bellingcat became Russia's 'biggest nightmare'*, France24, 7 IX 2022 r., https://www.france24.com/en/live-news/20220907-how-bellingcat-became-russia-s-biggest-nightmare [dostęp: 28 VI 2024].

[9] *Open Source Intelligence Market Size, Share, Growth, and Industry Analysis, By Type (Video Analytics, Text Analytics, Visualization Tool, Cyber Security, Web Analysis, Social Media Analysis, and Others), By Application (Private Sector, Public Sector and Other), Regional Insights, and Forecast to 2032*, Business Research Insights, marzec 2024 r., https://www.businessresearchinsights.com/market-reports/open-source-intelligence-market-109546 [dostęp: 28 VI 2024]. Por. *Open Source Intelligence Market Size, Share, Competitive Landscape and Trend Analysis Report, by Source, Technique and End User: Global Opportunity Analysis and Industry Forecast, 2020-2027*, Allied Market Research, maj 2020 r.

na rozwiązaniach otwartoźródłowych (*open source software*)[10], ponieważ dla każdego użytkownika są one dostępne do bezpośredniej analizy. Czyni je to głównym elementem w badaniach i praktyce OSINT. Narzędzia otwartoźródłowe powinny być pierwszym wyborem w analizie jawnoźródłowej z uwagi na ich powszechną dostępność oraz szerokie wsparcie społecznościowe. Dzięki tworzeniu kompleksowej mapy obszarów tematycznych w analizie jawnoźródłowej możliwe są nie tylko systematyzacja wiedzy, lecz także identyfikacja potencjalnych luk w oprogramowaniu i metodologii. Proces ten pozwala na wnioskowanie o możliwych brakach w tych narzędziach, szczególnie w kontekście zaspokajania różnych potrzeb informacyjnych. Taka ewaluacja może wskazywać na obszary wymagające dalszego rozwoju lub adaptacji.

Sformułowano następujące pytania badawcze:

1. Jakie luki występują w obecnym zestawie narzędzi OSINT opartych na rozwiązaniach otwartoźródłowych oraz jakie kierunki rozwoju tych narzędzi są najbardziej oczekiwane?
2. Jakie są funkcjonalności i ograniczenia różnych narzędzi otwartoźródłowych wykorzystywanych w OSINT?
3. Jakie narzędzia otwartoźródłowe służące do prowadzenia OSINT są obecnie często wskazywane podczas szkoleń, w publikacjach instruktażowych oraz typowo występują w zbiorach autorskich?

Rozważania definicyjne

Pojęcie *open source intelligence* pojawiło się w praktyce amerykańskiej Wspólnoty Wywiadowczej, głównie Centralnej Agencji Wywiadowczej (Central Intelligence Agency, CIA) oraz Agencji Wywiadowczej Departamentu Obrony (Defense Intelligence Agency, DIA). W sferze cywilnej zaczęto go używać dopiero w latach 90. XX w.[11] Popularyzował je wówczas Robert David Steele, były oficer CIA, autor *The Open-Source Everything Manifesto: Transparency, Truth, and Trust*[12]. Pojęcie to jest przekładane na język polski za pomocą dwóch równoważnych terminów – „wywiad

[10] Zagadnienia związane z narzędziami odpłatnymi pozostają poza zakresem niniejszego artykułu, ponieważ są to produkty zamknięte, które mogą stwarzać zagrożenie dla operatorów OSINT. Charakter tych narzędzi jako „czarnych skrzynek" rodzi wątpliwości co do tego, czy tematyka bądź wyniki wyszukiwań podlegają rejestracji przez dostawcę, w sposób zarówno jawny, jak i niejawny. Tego rodzaju ryzyko może mieć poważne implikacje dla bezpieczeństwa i poufności działań analitycznych.

[11] A. Olcott, *Open Source Intelligence in a Networked World (Continuum Intelligence Studies)*, New York 2012, s. 87–88.

[12] R.D. Steele, *The Open-Source Everything Manifesto: Transparency, Truth, and Trust*, Berkeley 2012.

jawnoźródłowy" oraz „biały wywiad". Pomimo że metodę OSINT stosowano znacznie wcześniej, nadal brakuje systematycznych studiów historycznych poświęconych temu zagadnieniu, a dostępna wiedza ma często charakter anegdotyczny, szkicowy[13] i wymaga uporządkowania[14]. Zgodnie z arystotelesowską koncepcją pojęcie *open source intelligence* zostanie zdefiniowane przez wskazanie jego najbliższego rodzaju (łac. *genus proximum*), co umożliwi jego ulokowanie w szerszym kontekście. Najczęściej przywoływana kategoryzacja ma charakter normatywny, uwzględnia aspekty etyczne i prawne. A zatem termin „biały wywiad" rozumie się jako taki sposób gromadzenia danych, który nie budzi wątpliwości ani etycznych, ani prawnych. Według dostępnych danych aż 80% informacji pozyskiwanych współcześnie przez służby wywiadowcze i organizacje zajmujące się gromadzeniem danych pochodzi ze źródeł otwartych i jawnych. Jego przeciwieństwo – czarny wywiad obejmuje działania uznawane za nielegalne w danej jurysdykcji, często również nieetyczne. W zakres czarnego wywiadu wchodzą takie praktyki, jak: inwigilacja i infiltracja z wykorzystaniem podsłuchów, włamanie, kradzież informacji i tożsamości (w tym biometrycznych), łamanie zabezpieczeń kryptograficznych, a także zdobywanie informacji z wykorzystaniem m.in. szantażu i korupcji. Szacuje się, że za pomocą tych metod pozyskuje się ok. 5% informacji w ramach wywiadu politycznego i gospodarczego[15]. Pomiędzy białym a czarnym wywiadem sytuuje się kategoria szarego

[13] L. Block, *The long history of OSINT*, „Journal of Intelligence History" 2024, t. 23, nr 2, s. 95–109. https://doi.org/10.1080/16161262.2023.2224091; C. Colquhoun, *A Brief History of Open Source Intelligence*, Bellingcat, 14 VII 2016 r., https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ [dostęp: 28 VI 2024].

[14] Wartość źródeł otwartych została dostrzeżona w Stanach Zjednoczonych już w XVIII w. podczas rewolucji amerykańskiej. Jerzy Waszyngton czerpał informacje o sile brytyjskich wojsk i ich aktywności z publikacji prasowych. Z kolei podczas II wojny światowej wojska gen. George'a Pattona korzystały z map znajdujących się na stacjach paliw Michelin. Brytyjski rząd w 1939 r. zwrócił się do koncernu medialnego BBC z prośbą o utworzenie komercyjnego serwisu pod nazwą Digest of Foreign Broadcasts (obecnie BBC Monitoring), podsumowującego zagraniczną prasę i media radiowe. Po II wojnie światowej powszechnie powoływano zespoły analityczne oraz tworzono instytucje zajmujące się pozyskiwaniem informacji ze źródeł otwartych i ich analizą (czynili to: wschodnioniemiecka Stasi, Chińczycy, którzy powołali Instytut Informacji Naukowo-Technicznej, oraz Amerykanie wraz z Shermanem Kentem, historykiem, zwanym ojcem amerykańskiej szkoły wywiadowczej). Por. F. Schaurer, J. Störger, *Guide to the Study of Intelligence. The Evolution of Open Source Intelligence (OSINT)*, „The Intelligencer. Journal of U.S. Intelligence Studies" 2013, t. 19, nr 3, s. 53.

[15] Wskazany podział procentowy, odnoszący się do udziału wywiadu jawnoźródłowego w strukturze wywiadu politycznego i gospodarczego, ma charakter częściowo anegdotyczny. Bazuje głównie na szacunkach przedstawionych w publikacji Arthura S. Hulnicka, byłego oficera CIA oraz wykładowcy Boston University. Zob. A.S. Hulnick, *Fixing the Spy Machine. Preparing American Intelligence for the Twenty-First Century*, Westport 1999, s. 40–41. Współczesne istotne publikacje albo powielają te proporcje (np. S.C. Mercado, *Sailing the Sea of OSINT in the Information Age*, „Studies in Intelligence" 2004, t. 48, nr 3, s. 45–55), albo wskazują ogólnikowo na rosnącą rolę wywiadu

wywiadu, obejmująca działania, których nie można jednoznacznie zaklasyfikować w kategoriach legalności i etyczności. Chociaż, z założenia, te metody są legalne, to jednak sprzeczne z zasadami etycznymi, czy to uniwersalnymi, czy specyficznymi. Za egzemplifikacje szarego wywiadu mogą posłużyć inwigilacja w postaci obserwacji i monitoringu osób lub pojazdów, a także działania o charakterze socjotechnicznym, mające na celu manipulację i wyłudzenie informacji. Szacunki wskazują, że za pomocą metod szarego wywiadu pozyskuje się ok. 15% informacji wywiadowczych. Granica między legalnością a nielegalnością, a także między etycznością a nieetycznością bywa płynna i zależna od kontekstu kulturowego, społecznego i politycznego. W obiegu akademickim, wywiadowczym i publicystycznym jest rozpowszechnionych kilka definicji wywiadu jawnoźródłowego/białego wywiadu. Najczęściej jest przywoływana definicja CIA o charakterze ostensywnym, wskazująca, że OSINT to rodzaj wywiadu oparty na źródłach dostępnych legalnie dla dużego grona osób i obejmujący ich szeroki repertuar: media, literaturę, raporty pierwszego, drugiego i trzeciego sektora, fotografie satelitarne, mapy, dokumenty geodezyjne, dane geograficzne i meteorologiczne, a także informacje naukowe, technologiczne, przemysłowe oraz społeczne i demograficzne[16]. Definicję tę przyjmuje się jako roboczą, ze świadomością, że istnieją inne interpretacje[17].

Z perspektywy historycznej i technologicznej można wyróżnić trzy kumulatywne, chronologiczne etapy rozwoju wywiadu jawnoźródłowego: OSINT 1.0, OSINT 2.0 oraz OSINT 3.0. Pierwsze dwa współistnieją obok siebie, trzeci natomiast ma charakter częściowo prognozowany. W artykule autor rozpatruje je w kategoriach deskryptywnych ewolucji i rozwoju OSINT.

OSINT 1.0 – obejmuje wczesne lata 80. XX w., kiedy analitycy wywiadu osobiście przeszukiwali i „ręcznie" agregowali źródła informacji (przede wszystkim „analogowe", rzadziej zdigitalizowane), prowadząc wyszukiwanie i analizy z niewielkim wspomaganiem technologii informacyjnych (katalogów i baz danych oraz pierwszych sieci internetowych sprzed WWW, takich jak USENET, BBS czy FTP, oraz wczesnego WWW).

jawnoźródłowego (np. R.D. Steele, *Open source intelligence*, w: *Handbook of Intelligence Studies*, New York 2007, s. 129–147).

[16] *A Consumer's Guide to Intelligence*, Office of Public Affairs CIA, 1999 r., https://archive.org/details/consumersguide_tenet/mode/2up [dostęp: 28 VI 2024]. W przyjętej definicji świadomie pomija się kwestie związane z nakładaniem się i przecinaniem innych rodzajów wywiadów, np. IMINT, HUMINT, GEOINT, z tak rozumianym wywiadem jawnoźródłowym.

[17] Trafnymi definicjami białego wywiadu są również definicje: NATO (*NATO Open Source Intelligence Handbook v 1.2*, https://archive.org/details/NATOOSINTHandbookV1.2/page/n1/mode/2up [dostęp: 28 VI 2024]) oraz Marka M. Lowenthala (M.M. Lowenthal, *Intelligence: From Secrets to Policy*, Washington 2007).

OSINT 2.0 – związany z rozwojem internetu, przede wszystkim mediów społecznościowych (tzw. Sieć 2.0 i Sieć 2.5). W OSINT 2.0 analitycy korzystają z wyszukiwarek, agregatorów wiadomości, analiz sieci społecznościowych oraz z automatyzacji procesów[18]. W tym okresie – aktualnie trwającym – nie tylko nastąpił wzrost ilości dostępnych informacji, lecz także pojawił się ich nadmiar[19].

OSINT 3.0 – to najnowsza, częściowo antycypowana faza OSINT, w której wykorzystuje się narzędzia analityczne z zakresu big data, uczenia maszynowego i przetwarzania języka naturalnego, a także słabych sztucznych inteligencji. W OSINT 3.0 dominują zaawansowane algorytmy do przeszukiwania i analizowania w czasie rzeczywistym ogromnych ilości danych oraz do wyciągania wniosków. Eksploruje się ponadto obszar Web3 i metawersów, następuje także konwergencja OSINT i innych rodzajów wywiadu, m.in. *geospatial intelligence* (GEOINT), *human intelligence* (HUMINT), *measurement and signature intelligence* (MASSINT), *signals intelligence* (SIGINT). Niewykluczone, że jednym z przyszłych trendów będzie popularyzacja zdecentralizowanych, oddolnych struktur zespołów badaczy OSINT, funkcjonujących na zasadzie crowdsourcingu. Jest to obszar *in statu nascendi*[20].

Narzędzia wywiadu jawnoźródłowego

Klasyfikacja aktualnego oprogramowania służącego wywiadowi jawnoźródłowemu stanowi wyzwanie ze względu na heterogeniczność funkcji, zróżnicowanie metodologii oraz dynamiczny rozwój. Liczba i rodzaj możliwych sposobów eksploracji internetu są ograniczone, w związku z czym funkcje różnych programów nakładają się na siebie. Liczbę programów oraz innych narzędzi OSINT autor ocenia na ok. 1000–1200. Głównym problemem jest szybkie dezaktualizowanie się narzędzi – z przyczyn zarówno wewnętrznych (utrata motywacji przez zespół lub

[18] H.J. Williams, I. Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, RAND, 17 V 2018 r., https://www.rand.org/pubs/research_reports/RR1964.html [dostęp: 28 VI 2024].

[19] Por. K. Tylutki, *Informacja masowego rażenia – OSINT w działalności wywiadowczej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19, s. 166–192.

[20] A.W. Dorn, *United Nations Peacekeeping Intelligence*, w: *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (red.), Oxford 2010, s. 280; D. Mider, J. Garlicki, W. Mincewicz, *Pozyskiwanie informacji z Internetu metodą Google Hacking – biały, szary czy czarny wywiad?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 20, s. 68–91; K. Turaliński, *Wywiad gospodarczy i polityczny. Podręcznik dla specjalistów ds. bezpieczeństwa, detektywów i doradców gospodarczych*, Warszawa 2015, s. 31–33.

poszczególnych jego członków), jak i zewnętrznych (blokowanie określonych kanałów pozyskiwania informacji). Zasadniczo można wyróżnić trzy grupy narzędzi OSINT: podstawowe, czyli wyszukiwawcze; wspomagające, czyli analityczne i wizualizacyjne; oraz narzędzia bezpieczeństwa, które operatorowi OSINT zapewniają anonimowość lub fałszywą, lecz spójną tożsamość.

Narzędzia wyszukiwawcze OSINT obejmują większość narzędzi i metod wykorzystywanych w wywiadzie jawnoźródłowym. Wielu ekspertów utożsamia OSINT przede wszystkim z tymi narzędziami, gdyż umożliwiają one efektywne zbieranie informacji ze źródeł otwartych. Narzędzia te można podzielić na trzy główne kategorie: zintegrowane z systemem operacyjnym lub przeglądarką, samodzielne aplikacje wymagające rejestracji i konfiguracji oraz odnośniki do różnych zasobów OSINT, które użytkownik musi samodzielnie zainstalować i skonfigurować.

Narzędzia analityczne i wizualizacyjne OSINT odgrywają najważniejszą rolę w przetwarzaniu, analizie i wizualizacji danych zebranych ze źródeł otwartych. Pomagają w identyfikacji wzorców i trendów, umożliwiają tworzenie wykresów, map oraz innych form wizualizacji, co ułatwia interpretację danych.

Narzędzia bezpieczeństwa OSINT zapewniają ochronę podczas zbierania i analizowania danych ze źródeł otwartych. Obejmują one rozwiązania chroniące prywatność użytkownika (*privacy enhancing technologies*, PET) oraz narzędzia do wykrywania i unikania zagrożeń związanych z przetwarzaniem publicznie dostępnych informacji. Oprogramowanie to można skategoryzować z perspektywy ergonomii pracy operatora narzędzi OSINT.

Autorsko wyróżniono trzy grupy narzędzi wyszukiwawczych dających operatorowi zróżnicowane jakościowo doświadczenia (krzywa uczenia się, efektywność, elastyczność) oraz stwarzające rozmaite bariery (użytkowania i poznawcze).

1. **Oprogramowanie zintegrowane z systemem operacyjnym i/lub przeglądarką internetową**. Operator OSINT otrzymuje gotowy, bezpieczny produkt zawierający wiele narzędzi. Najczęściej są one już preinstalowane i wstępna konfiguracja umożliwia korzystanie z nich[21].
2. **Oprogramowanie samodzielne, instalowane lokalnie lub online** (serwer dostawcy). Zanim operator skorzysta z takiego narzędzia, najczęściej musi zarejestrować instalację, pozyskać klucze API (*application programming interface*) i skonfigurować narzędzia. Niekiedy są wymagane instalacje dodatkowego oprogramowania, np. SQL (*structured query language*).
3. **Odnośniki do oprogramowania i innych narzędzi OSINT**. Mogą one funkcjonować w postaci zakładek, arkuszy, stron www, innych typów list.

[21] Przegląd dotychczasowych rozwiązań wskazuje, że wybór bazowych platform dla zintegrowanych narzędzi OSINT jest starannie przemyślany, a kwestie bezpieczeństwa są uwzględniane ze szczegółami.

Analitykowi OSINT jest dostarczana lista klasyfikowanych i posegregowanych narzędzi. Otrzymuje on wyłącznie odnośniki. Instalację, konfigurację lub inne niezbędne czynności związane z korzystaniem z usługi musi wykonać sam.

Zostały przeanalizowane reprezentatywne programy w ramach każdej z trzech wymienionych grup.

Oprogramowanie OSINT zintegrowane z systemem operacyjnym i/lub przeglądarką internetową

To najmniej liczna grupa oprogramowania (dlatego omawiana obszernie), wymaga największego wkładu pracy dostawcy, a stosunkowo najmniejszego operatora OSINT. Jest to zbiór aktualnie rozwijanych rozwiązań. Omówione tu systemy zawierają narzędzia szerzej opisane w dalszych częściach artykułu.

Trace Labs (Crowdsourced Open Source Intelligence for Missing Persons) – to następca Linux Buscador[22]. Trace Labs (TL) zostało założone w Kanadzie w 2017 r. przez Adriana Korna, konsultanta ds. bezpieczeństwa, audytora, autora monografii z obszaru OSINT. Jest to organizacja non profit zajmująca się zbieraniem informacji na temat osób zaginionych, a Korn aktualnie pełni funkcję jej CEO. Trace Labs, będący jednym z czołowych projektów OSINT na świecie, znacznie zwiększa skuteczność poszukiwań. Dzięki wdrożeniu systemu crowdsourcingu angażuje globalną społeczność wolontariuszy do współpracy z organami ścigania i organizacjami zajmującymi się osobami zaginionymi. Celem jest wspieranie oficjalnych poszukiwań, a nie ich zastępowanie. Trace Labs OSINT wywodzi się z dystrybucji Kali Linux, a ten – z Debiana. System działa z wykorzystaniem maszyny wirtualnej, co jest elementem zapewniania bezpieczeństwa, a podano go w uniwersalnym (Oracle VB, VM Ware) formacie OVA (*open virtualization appliance*)[23].

[22] Trace Labs rozwijało niegdyś system operacyjny Linux Buscador, wykorzystywany przez wiele agencji rządowych, firm prywatnych i organizacji pozarządowych. Buscador zawierał liczne narzędzia związane z wywiadem cyfrowym, penetracją sieciową i monitorowaniem mediów społecznościowych. Zaprzestano jego rozwijania na rzecz Trace Labs OSINT i nie podano oficjalnych informacji na temat przyczyn rezygnacji. W jednym z wpisów na blogu Adrian Korn wskazał, że decyzja była podyktowana potrzebą stworzenia bardziej zaawansowanej dystrybucji, która lepiej odpowiadałaby potrzebom organizacji.

[23] Strona domowa projektu: https://www.tracelabs.org/initiatives/osint-vm. Pobieranie: tlosint-vm, w: https://github.com/tracelabs/tlosint-vm/releases [dostęp: 28 VI 2024]. Nie ma bezpośredniej możliwości uruchomienia systemu w najbezpieczniejszym środowisku, tj. Qemu/KVM. Konieczne jest wykonanie konwersji pliku .ova na .qcow2 lub kompilacja ze źródeł. System nie jest gotowy do użycia bezpośrednio po uruchomieniu, należy zainstalować narzędzia, korzystając z umieszczonego na pulpicie skryptu instalacyjnego (install-tools.sh). Dopiero wówczas jest uzyskiwana pełna funkcjonalność.

System bazowy Kali Linux znacznie zmodyfikowano przez wprowadzenie w pierwotnym produkcie licznych ograniczeń – spośród szerokiego repertuaru programów pozostawiono zaledwie kilka. Trace Labs OSINT zawiera jednak inne programy, takie jak: CherryTree, EyeWitness, ExifTool, Maltego, Metagoofil, OSR-Framework, Recon-ng, Spiderfoot, TheHarvester, TcpDump, Wireshark. Ponadto do projektu włączono dwie przeglądarki – Chromium oraz Firefox ESR, zaopatrzone w kilkaset odnośników służących wywiadowi jawnoźródłowemu[24]. Mocną stroną zbioru tych odnośników jest bogaty wybór oprogramowania używanego do wyszukiwania osób (główny cel TL) oraz numerów telefonów. Zwraca uwagę duża (jednak niewyczerpująca) liczba wyszukiwarek internetowych, przejrzyście pogrupowanych. Słabą stroną jest niedostatek odnośników kartograficznych oraz związanych z sieciami społecznościowymi spoza głównego nurtu, np. brakuje Fediverse – alternatywnego systemu mediów społecznościowych. Ponadto nie ma odwołań do sieci nakładkowych (m.in. The Onion Router – Tor, Invisible Internet Project – I2P, Lokinet), alternatywnych systemów domenowych (np. OpenNIC) oraz undergroundowych forów (imageboardów) i czatów. Dla początkującego użytkownika przeszkodą w użytkowaniu systemu będzie konieczność instalacji narzędzi i bibliotek z użyciem terminala. Dla zaawansowanego użytkownika istotnym ograniczeniem może być natomiast niemożność uruchomienia systemu bezpośrednio pod kontrolą najbezpieczniejszego hipernadzorcy, jakim jest Qemu/KVM. Należy jednak podkreślić przydatność tego narzędzia oraz to, że jest ono głównym z kompleksowych narzędzi OSINT. Z tych względów zostało ono omówione tak szeroko. Wskazane niedostatki wydają się ściśle powiązane z profilowaniem systemu na spełnianie specyficznych wymagań operacyjnych wynikających z misji poszukiwawczej. To usprawiedliwia pewne kompromisy w zakresie instalacji i bezpieczeństwa.

Tsurugi Linux[25] – to dystrybucja systemu operacyjnego GNU/Linux przeznaczonego do działań DFIR (*digital forensics and incident response*) oraz analizy złośliwego oprogramowania stworzona w 2019 r. przez zespół programistów i specjalistów ds. bezpieczeństwa z Japonii, Stanów Zjednoczonych, Wielkiej Brytanii, Niemiec i Australii. Liderem zespołu jest Mati Aharoni, wcześniej pracujący nad systemem operacyjnym Kali Linux (Backtrack), założyciel i CEO firmy Offensive

[24] Skategoryzowano je następująco: Company, Internet Scan, Email Search, Phone Number, People, Maps & Geography, Search, Social Media Tools, Social Networks, User Name Check, Collections, Broad Search Tools. Ponadto do przeglądarki Firefox dodano dwie praktyczne wtyczki – pierwsza umożliwia odczytywanie na głos stron internetowych w ponad 40 językach, druga usuwa elementy śledzące z odnośników internetowych. Wprowadzono także kilka innych wtyczek służących personalizacji przeglądarki.

[25] Tsurugi Linux, https://tsurugi-linux.org/index.php [dostęp: 28 VI 2024]. Tsurugi (剣) to japońskie słowo oznaczające 'miecz'.

Security. Przedsiębiorstwo ma swoją siedzibę w Stanach Zjednoczonych i jest finansowane ze sprzedaży narzędzi cyberbezpieczeństwa oraz z nieujawnianych dotacji prywatnych. System ten nie skupia się na oprogramowaniu OSINT, lecz zawiera narzędzia związane z bezpieczeństwem sieciowym, informatyką śledczą oraz odzyskiwaniem danych[26]. Z powodzeniem może konkurować z powszechnie znanym i wykorzystywanym w tym zakresie Kali Linux[27]. Tsurugi Linux opiera się na dystrybucji Ubuntu (w odmianie Long Term Support), co oznacza, że korzysta z jej stabilnych, długoterminowo wspieranych komponentów. Jądro systemu zawiera optymalizacje wspomagające pracę z narzędziami do odzyskiwania danych i analizy złośliwego oprogramowania. W cyklu rozwojowym ukazują się (zazwyczaj) każdego roku dwa wydania systemu. Narzędzie jest oferowane w różnych formatach – w jednym cyklu jako obraz ISO, w innym jako plik .ova. Powoduje to niekonsekwencję w formacie udostępnianych wydań. System jest zaprojektowany do działania zarówno w środowisku wirtualnym (na maszynie wirtualnej), jak i na sprzęcie fizycznym, gdyż można go zainstalować bezpośrednio na dysku twardym. W obu przypadkach instalacja nie nastręcza trudności i narzędzie jest od razu gotowe do działania. Jest to – niewątpliwie – narzędzie podwójnego zastosowania (*dual-use technology*), może bowiem służyć przedsięwzięciom legalnym i bezprawnym[28]. Wśród 16 grup narzędzi oferowanych przez Tsurugi Linux jedną poświęcono wywiadowi jawnoźródłowemu. Zawartość to kilkadziesiąt wyselekcjonowanych elementów – pojedynczych narzędzi, agregatorów oraz frameworków. Przeważająca część zbioru to takie, które działają w linii poleceń. Wartościową funkcją jest umiejscowiony na pulpicie OSINTSwitcher, umożliwiający przełączanie między porządkiem wyszukiwawczym na potrzeby cyberbezpieczeństwa a porządkiem

[26] Należy dodać, że obok Tsurugi Linux jest oferowane również inne oprogramowanie, jak Bento DFIR Portable Toolkit oraz Tsurugi Acquire. Bento DFIR to przenośny zestaw narzędzi zaprojektowany do wykorzystania w analizie śledczej i reagowaniu na incydenty bezpieczeństwa. Zestaw zawiera szeroką gamę narzędzi niezbędnych do przeprowadzania różnych operacji w ramach cyfrowej analizy śledczej, intuicyjnych i wygodnych w użyciu nawet dla średnio zaawansowanego użytkownika. Z kolei Tsurugi Acquire zostało stworzone z myślą o cyfrowej analizie śledczej i odzyskiwaniu danych. Jest to lekka, 32-bitowa wersja systemu, która pozwala na łatwe przeprowadzanie operacji związanych z pozyskiwaniem danych z różnych nośników pamięci. Wszystkie narzędzia są bezpłatne.

[27] Przewaga systemu Tsurugi Linux nad Kali Linux polega na tym, że Tsurugi został wyposażony w zaawansowany moduł analizy śledczej, obejmujący zarówno artefakty z chmury, fotografie, obrazy systemów, jak i inne artefakty cyfrowe. Ponadto oferuje wszechstronny zestaw narzędzi do analizy śledczej kryptowalut.

[28] Por. National Research Council, *Computers at Risk: Safe Computing in the Information Age*, Washington 1991; J. Forge, *A Note on the Definition of "Dual Use"*, „Science and Engineering Ethics" 2010, t. 16, nr 1, s. 111–118. Wydaje się, że w związku z tym twórcy mogli podjąć decyzję o wprowadzeniu do systemu elementów potencjalnie służących deanonimizowaniu użytkowników.

wyszukiwawczym na potrzeby OSINT, co ułatwia operatorowi pracę. W Tsurugi Linux podstawą do pracy OSINT jest zmodyfikowana przeglądarka Mozilla Firefox, nosząca nazwę OSINTBrowser. Wyposażono ją w odnośniki do 11 grup narzędzi OSINT[29], dodano również ok. 30 wtyczek (*extensions*) o różnym przeznaczeniu – od bezpieczeństwa, po OSINT. Najbardziej obszerne są listy narzędzi służących do lokalizacji geograficznej (mapy lotnicze, satelitarne i inne sposoby geolokalizacji) oraz śledzenia transportu lotniczego, morskiego i kolejowego. Wartościowe dodatki to zbiór odnośników do narzędzi analitycznych OSINT oraz zbiór agregujących informację zakładek, dotyczących skanowania/monitorowania częstotliwości radiowych i radiofonii[30]. Słabą stroną jest niewielka liczba wyszukiwarek internetowych (jest ich zaledwie kilkanaście). Wybór przeglądarki Firefox ograniczył możliwości wykorzystania wielu specjalistycznych wtyczek, które są dostępne w bardziej zasobnej rodzinie opartej na silniku Blink (Chrome, Chromium, Brave, MS Edge). Zrezygnowano także z implementacji bookmarkletów[31] oraz autorskich wtyczek. Tsurugi Linux ma ponadto braki w następujących obszarach analizy: sieci nakładkowe (ma skrajnie małą liczbę narzędzi do eksploracji Tor), alternatywne media społecznościowe oraz alternatywne systemy domenowe. Należy jednak podkreślić jego unikatowość w kontekście możliwości specyficznych zastosowań.

Wiele innych systemów operacyjnych służących testom penetracyjnym również ma moduły zawierające narzędzia przeznaczone do OSINT[32]. Są to narzędzia podwójnego zastosowania.

BlackArch Linux[33] – to system operacyjny zainicjowany w 2013 r. przez zespół entuzjastów cyberbezpieczeństwa działających na zasadzie wolontariatu. Projekt jest finansowany głównie z dobrowolnych datków przekazywanych przez użytkowników i społeczność, przeznaczanych na pokrycie kosztów hostingu, utrzymania nazwy domeny, serwerów lustrzanych oraz sprzętu testowego. BlackArch

---

[29] Skategoryzowano je następująco: Resources, Geo Based Searches, Metadata, Socials, P2P, Transport, Date-Time, Website analysis, Search engine, Radio, Commercial Registries.

[30] Są to np. SDR.hu – portal internetowy, który umożliwia dostęp do zdalnych odbiorników radiowych SDR (*software defined radio*) na całym świecie. Użytkownicy mogą za pomocą przeglądarki słuchać odbiorników SDR z różnych lokalizacji, w szerokim zakresie częstotliwości radiowych i kontrolować te odbiorniki. Broadcastify to platforma internetowa umożliwiająca słuchanie transmisji radiowych prowadzonych na żywo.

[31] Bookmarklet to niewielki, lekki skrypt JavaScript zapisany jako zakładka w przeglądarce internetowej. Umożliwia wykonywanie zadań na bieżącej stronie www bez konieczności instalowania wtyczek lub rozszerzeń.

[32] Warto zwrócić uwagę, że rok 2013 był punktem zwrotnym dla oprogramowania związanego z bezpieczeństwem IT ze względu na potrzebę modernizacji istniejących narzędzi, rosnące znaczenie cyberbezpieczeństwa (vide: sprawa Edwarda Snowdena) oraz rozwój społeczności *open source*.

[33] BlackArch, https://blackarch.org/index.html [dostęp: 28 VI 2024].

bazuje na dystrybucji Arch Linux, dzięki czemu wykorzystuje zasady reguły KISS (*keep it simple, stupid*), której istotą jest osiąganie najwyższej wydajności w połączeniu z wygodą użytkowania. Dystrybucja jest dostępna zarówno w pełnej wersji ISO, oferującej różnorodne menedżery okien, jak i w wersji „Slim" ze środowiskiem graficznym XFCE. System rekomenduje się średnio zaawansowanym użytkownikom, obeznanym z Arch Linux. BlackArch to kompleksowe rozwiązanie do testów penetracyjnych oraz badań z zakresu cyberbezpieczeństwa, zawierające imponującą liczbę blisko 3000 narzędzi ukierunkowanych na bezpieczeństwo IT, w tym eksploatację, analizę śledczą, testy penetracyjne, inżynierię wsteczną, analizę sieci i wiele innych[34]. Wśród szerokiej gamy narzędzi znajdują się również te przeznaczone do zadań OSINT, ale nie stworzono dla nich osobnej kategorii[35].

ParrotOS Security[36] – został publicznie wydany 10 kwietnia 2013 r. przez Lorenza Faltrę, lidera zespołu oraz głównego dewelopera (tj. twórcę). System wywodzi się z forum społecznościowego Frozenbox, również stworzonego przez Faltrę. ParrotSec jest spółką interesu społecznego (*community interest company*)[37] zarejestrowaną w Wielkiej Brytanii, z siedzibą w Palermo we Włoszech. ParrotOS Security jest systemem *open source*, finansowanym głównie z darowizn społeczności i wolontariuszy. Oparty na Debianie, gałęzi *testing*, stosuje model *rolling release*. Jest to dystrybucja do testowania penetracyjnego, badań nad bezpieczeństwem, analizy śledczej, inżynierii wstecznej i kryptografii. System może być uruchamiany na serwerach, komputerach stacjonarnych, laptopach, maszynach wirtualnych oraz urządzeniach IoT (Internet of Things, pol. internet rzeczy), m.in. Raspberry Pi. Oferuje ponad 600 narzędzi, w tym do pełnego szyfrowania dysku oraz ochrony prywatności (Tor i AnonSurf). Atutem jest tryb *forensic mode*, który zapobiega automatycznemu montowaniu urządzeń pamięci masowej, chroniąc wrażliwe dane przed modyfikacją. Jest używany przez agencje rządowe i organy ścigania. W odrębnej zakładce ma skromne zasoby menu OSINT, gdzie znajdują się takie programy, jak: Censys, cloud-enum, emailharvester, inspy, instalooader – Instagram OSINT tool, Maltego, sherlock, Shodan oraz TheHarvester[38].

---

[34] Zbiór narzędzi jest dostępny pod adresem: https://blackarch.org/tools.html.

[35] Narzędzia te zostały skategoryzowane według ich przeznaczenia. Obejmują m.in.: eksploatację (186 narzędzi), skanery (313 narzędzi), aplikacje webowe (310 narzędzi), łamanie haseł (169 narzędzi) oraz analizę śledczą (129 narzędzi).

[36] ParrotOS Security, https://www.parrotsec.org [dostęp: 28 VI 2024].

[37] Jedna z form prawnych brytyjskich przedsiębiorstw społecznych (przyp. red.).

[38] Na wzmiankę zasługuje cloud-enum – narzędzie do enumeracji i analizy zasobów w chmurze, takich jak buckets S3 czy instancje EC2, oraz narzędzia do analizy kont na Instagramie – inspy i instaloader.

Kali Linux[39] – zadebiutował na rynku w marcu 2013 r., jest to następca BackTrack Linux. Rozwój i utrzymanie tej dystrybucji leży w gestii firmy Offensive Security, która czerpie zyski z organizowania certyfikowanych szkoleń i kursów, takich jak renomowany Offensive Security Certified Professional. Jako kompleksowe narzędzie dla profesjonalistów z dziedziny bezpieczeństwa Kali Linux zawiera ponad 600 preinstalowanych narzędzi. Wśród nich znajduje się również skromna zakładka OSINT Analysis, obejmująca takie narzędzia, jak: Maltego, SpiderFoot oraz TheHarvester. Kali Linux działa na licznych platformach, w tym maszynach wirtualnych. Cechuje go duża częstotliwość aktualizacji, precyzja i estetyka wykonania.

W dystrybucjach Linuxa ukierunkowanych na cyberbezpieczeństwo, takich jak: BlackArch, Kali oraz Parrot, narzędzia OSINT stanowią integralną część arsenału, chociaż ich liczba i wyeksponowanie nie dorównują innym kategoriom. Wyjątkiem jest Kali Linux, który wyróżnia się na tle pozostałych systemów, gdyż oferuje zakładkę przeznaczoną dla narzędzi OSINT. Analiza narzędzi w opisanych dystrybucjach pozwala zauważyć, że uniwersum cyberbezpieczeństwa i OSINT się przenikają, dzieląc wspólne instrumenty.

CAT (Cyberuniverse Analysis Tool)[40] – polski zbiór narzędzi OSINT w postaci funkcjonalnie zintegrowanej z przeglądarką Brave[41]. CAT powstał, ponieważ było potrzebne narzędzie lekkie, szybkie w instalacji i użytkowaniu, zdolne do działania w każdym środowisku i na dowolnej maszynie, częściowo zanonimizowane i niewskazujące na działalność służb. Prace nad nim rozpoczęły się w czerwcu 2021 r. Do 2024 r. nie powstała jeszcze wersja, która by w pełni satysfakcjonowała twórców. Narzędzie jest wykorzystywane w śledztwach o charakterze detektywistycznym, sprawdzeniach KYC oraz wyszukiwaniach akademickich, dydaktyce i szkoleniach OSINT. CAT jest udostępniany na licencji ♡Copyheart[42]. Tworzeniu narzędzia przyświecały następujące cele: łagodna krzywa uczenia się (łatwość użytkowania po krótkim przeszkoleniu), szybkość instalacji (instalacja w kwadrans), wygoda (integracja wszystkich narzędzi w jednej przeglądarce), uniwersalność (wszechstronne zastosowanie w różnych śledztwach i badaniach), jurysdykcja (polska; aktualnie brak podobnych rozwiązań), skalowalność

[39] Kali Linux, https://www.kali.org [dostęp: 28 VI 2024]. Nazwa pochodzi od hinduskiej bogini Kali, potocznie kojarzonej z siłą i mocą.

[40] Narzędzie dostępne na prośbę skierowaną via e-mail: d.mider@uw.edu.pl.

[41] Nawiązuje koncepcyjnie do przeglądarki Oryon OSINT stworzonej przez polskiego infobrokera Marcina Mellera. Narzędzie to przestało być aktualizowane w 2017 r. Zob. https://sourceforge.net/projects/oryon-osint-browser/ (uwaga: wersja z 6 IV 2017 r.).

[42] N. Paley, *Copying is an act of love. Please copy and share*, https://copyheart.org [dostęp: 28 VI 2024].

(jednoczesna praca wielu użytkowników, tworzenie wersji), elastyczność (kompatybilność z różnymi systemami, ograniczona zmiana cyfrowego odcisku palca – *digital fingerprint*), rekonfigurowalność (dostosowanie narzędzi, zmiana funkcjonalności i wyglądu), modularność (łatwe dodawanie i usuwanie elementów), otwartoźródłowość i darmowość (bezpłatne, otwarte narzędzia, lokalne działanie), uwzględnienie aspektów społeczno-kulturowych i językowych (eksploracja subkultur, słowniki socjolektów), względna anonimowość (ok. 1500–2000 użytkowników), anonimowość w zespole (współpraca bez ujawniania tożsamości). Każdy z tych celów został co najmniej częściowo zrealizowany. Narzędzie nie jest jednak wolne od wad. Po pierwsze, nie wszystkie wtyczki i odnośniki są audytowane, co stwarza realne, chociaż niskie ryzyko inwigilacji (przeglądarka Brave, uznawana za jedną z najbezpieczniejszych, znacznie poprawia bezpieczeństwo). Po drugie, użycie głównie otwartoźródłowych i darmowych narzędzi może ograniczać dostęp do niektórych danych. Po trzecie, aktualnie CAT jest rozwijany przez jedną osobę i z wykorzystaniem środków własnych.

Do CAT zaimplementowano następujące narzędzia, usługi i rozwiązania: ponad 700 miejsc i narzędzi online, ponad 130 wtyczek, ponad 20 bookmarkletów[43], ponad 270 wyszukiwarek, ponad 100 miejsc Deep Web & Darknet, ponad 60 polskich baz/wyszukiwarek/miejsc, ponad 50 narzędzi bezpieczeństwa/anonimizacji (*going grey*), ponad 40 narzędzi do stalkingu/doxingu w social mediach, ponad 30 narzędzi Imagery/Map Intelligence, ponad 30 narzędzi Crypto/Blockchain Intelligence, ponad 20 narzędzi edukacyjnych, ponad 20 narzędzi do weryfikacji fake news, ponad 10 stron wyciekowych, ponad 10 alternatywnych social mediów, 8 kombajnów OSINT. Ponadto: fora hakerskie, przetwarzanie danych, analiza danych, warezownie, narzędzia *privacy enhancing technologies*, *operations security* (OpSec); automatyczną obsługę sieci Tor, IPFS (InterPlanetary File System) wraz z Unstoppable Domains; skrypty do ukrytych polskich imageboardów (Karachan oraz Wilchan, w tym odnośniki do ukrytych „elitarnych" boardów); komplet danych dostępu do sieci nakładkowych Hyphanet, Lokinet oraz do Alternative Top Level Domains (ATLD).

Kilka elementów wyróżnia CAT na tle istniejących rozwiązań OSINT. Po pierwsze, uznano za niezbędne wdrożenie kompletu źródeł dotyczących Polski. Większość zasobów społeczności OSINT charakteryzuje się globalnym lub euroatlantyckim zasięgiem. Kraje doświadczające napięć geopolitycznych lub podejmujące kontrowersyjne działania również są przedmiotem intensywnej analizy OSINT. Wiedza globalnej społeczności OSINT o Europie Środkowo-Wschodniej, szczególnie o Polsce, jest jednak limitowana. W Polsce istnieją

[43] Systematycznie zamienianych na wtyczki własne.

liczne, niezauważane na świecie zasoby umożliwiające prowadzenie białego wywiadu gospodarczego i osobowego. Po drugie, Deep Web i Darknet[44] zazwyczaj znajdują się na pograniczu zainteresowania operatorów OSINT. Na ogół są one kojarzone (w świadomości społecznej i przez publicystów) z działalnością niezgodną z prawem, w tym z nielegalnym pozyskiwaniem informacji, co jest częściowo błędnym mniemaniem. Drugim problemem jest ograniczanie się analityków OSINT wyłącznie do jednej sieci, mianowicie Tor, podczas gdy funkcjonuje ich jeszcze kilka, chociaż mniejszych[45]. Kilku uczonych podkreśla znaczenie Deep Web i Darknet dla OSINT, ale nie są to głosy powszechnie znane. Ponadto analitycy traktują te zjawiska zawężająco i ograniczają eksplorację OSINT do pozyskiwania informacji o przestępcach i przestępstwach w celu zwalczania tychże[46]. W CAT zaimplementowano wiele narzędzi wyszukiwawczych w tym zakresie. Po trzecie, wywiad naukowy (*science intelligence*, SCINT) odgrywa ważną rolę zarówno w państwowym, jak i komercyjnym sektorze wywiadowczym[47]. Opiera się głównie na źródłach otwartych i obejmuje proces akwizycji oraz analizy informacji naukowych w celu optymalizacji procesów decyzyjnych, strategii innowacyjnych i polityki naukowej. Szczególne znaczenie ma tu szara literatura (*grey literature*), definiowana jako materiały informacyjne i publikacje nieobjęte tradycyjnymi kanałami komercyjnego wydawnictwa, która pomimo trudności w indeksacji i dostępie dostarcza unikalnych danych i wniosków. Z tego względu CAT integruje w swoich działaniach zarówno tradycyjne źródła naukowe, jak i szarą literaturę. Po czwarte, wyszukiwarki są najpowszechniejszym, a jednocześnie najbardziej nieumiejętnie wykorzystywanym narzędziem wyszukiwania danych[48].

---

[44] Pojęcia te zostały wyjaśnione w: D. Mider, *Mappa Mundi ukrytego Internetu. Próba kategoryzacji kanałów komunikacji i treści*, „PTINT Praktyka i Teoria Informacji Naukowej i Technicznej" 2015, t. 23, nr 1, s. 3–16.

[45] To nieporozumienie usiłują wyjaśnić autorzy: V. Ciancaglini i in., *Deep Web and Cybercrime: It's Not All About TOR*, Trend Micro, 12 XI 2014 r., https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/deep-web-and-cybercrime-its-not-all-about-tor [dostęp: 28 VI 2024].

[46] Por. M. Bazzell, *Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information*, Charleston 2018; M. Chertoff, T. Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, https://www.cigionline.org/static/documents/gcig_paper_no6.pdf [dostęp: 28 VI 2024].

[47] P. Maddrell, *Spying on Science: Western Intelligence in Divided Germany 1945–1961*, Oxford 2006; *Wyniki pracy wywiadu naukowo-technicznego MSW PRL 1971–1989*, M. Sikora (oprac.), Katowice–Warszawa 2019; H. Nasheri, *Economic Espionage and Industrial Spying*, Cambridge 2004; K. Turaliński, *Wywiad gospodarczy i polityczny*…

[48] Problem ten dostrzeżono już wcześniej. Zob. E. Hargittai, A. Hinnant, *Digital Inequality: Differences in Young Adults' Use of the Internet*, „Communication Research" 2008, t. 35, nr 5, s. 602–621. https://doi.org/10.1177/0093650208321782. Nadal wydaje się on aktualny. Zob. K. Abramczuk,

Wyszukiwarka Google może być rozpatrywana w kategoriach najłatwiejszego w użyciu narzędzia hakerskiego[49]. Wprowadzenie tego obszaru OSINT wynika wprost z ujmowania internetu jako zbiornika danych[50]. Należy zwrócić także uwagę, że najpopularniejsza wyszukiwarka Google jest nie tyle używana, ile wręcz nadużywana przez użytkowników, którzy nie dostrzegają innych globalnych, lokalnych lub specjalistycznych wyszukiwarek internetowych[51]. Takie wyszukiwarki są liczne, pokrywają inny obszar, niż czyni to Google. Uwzględniono je w CAT, w tym wyszukiwarki oraz narzędzia wykorzystujące duże modele językowe (*large language models*, LLM). Po piąte, wycieki dokumentów rządowych i korporacyjnych stanowią istotny obszar analizy OSINT. Szybka identyfikacja, dostęp oraz ewaluacja tych materiałów mają decydujące znaczenie dla zainteresowanych instytucji, aktorów politycznych i całych społeczeństw. Fenomen sygnalistów (*whistleblowers*), chociaż obecny już w erze przedinternetowej, zyskał na znaczeniu wraz z rozwojem technologii cyfrowych[52]. Przykłady takie jak działania Daniela Ellsberga, Chelsea Manning czy Edwarda Snowdena pokazują skalę i wpływ tego zjawiska na współczesną geopolitykę i dyskurs publiczny. Internet umożliwił powstanie wyspecjalizowanych platform i kanałów dystrybucji wycieków informacji. Dla operatorów OSINT źródła te stanowią krytyczny element w procesie pozyskiwania i analizy danych i dlatego ujęto je w CAT. W ramach kompleksowego podejścia do analizy jawnoźródłowej uwzględniono dodatkowe obszary tematyczne. Zakres ten obejmuje analizę kryptowalut i blockchainów w kontekście OSINT, jak również źródła otwarte na potrzeby wywiadu gospodarczego, w tym *corporate intelligence*, *financial intelligence* oraz *trade intelligence*. Ponadto włączono źródła kartograficzne istotne dla OSINT oraz wyszukiwarki treści związanych z ludzką seksualnością. Integracja tych zróżnicowanych domen badawczych umożliwia wieloaspektowe podejście do analizy jawnoźródłowej.

M. Kąkol, A. Wierzbicki, *How to Support the Lay Users Evaluations of Medical Information on the Web?*, w: *Human Interface and the Management of Information: Information, Design and Interaction*, S. Yamamoto (red.), Cham 2016, s. 3–13. https://doi.org/10.1007/978-3-319-40349-6_1.

[49] Por. D. Mider, *Sztuka wyszukiwania w Internecie – autorski przegląd wybranych technik i narzędzi*, „Studia Politologiczne" 2019, t. 54, s. 191–229; D. Mider, J. Garlicki, W. Mincewicz, *Pozyskiwanie informacji z Internetu metodą Google Hacking*…

[50] M. Bazzell, *OSINT Techniques: Resources For Uncovering Online Information*, [bmw] 2023.

[51] *Market share of leading desktop search engines worldwide from January 2015 to January 2024*, Statista, 2024 r., https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/ [dostęp: 28 VI 2024].

[52] P. Rosenzweig, T.J. McNulty, E. Shearer, *Whistleblowers, Leaks, and the Media: The First Amendment and National Security*, Chicago 2015.

Należy dodać kilka słów na temat wyboru nośnika, tj. przeglądarki Brave. Po przeanalizowaniu przeglądarek internetowych Brave została wybrana jako optymalna, gdyż wyróżnia się wysokim poziomem prywatności i bezpieczeństwa. Potwierdzają to testy autora artykułu przeprowadzone za pomocą BrowserAudit[53] i PrivacyTests[54]. Istotnym atutem Brave jest otwartoźródłowość, a bezpieczeństwo jest dodatkowo wzmacniane przez program *bug bounty*. Przeglądarka cechuje się uniwersalnością – jest kompatybilna z różnymi systemami operacyjnymi. Wykorzystanie silnika Blink pozwala na dostęp do szerokiej gamy rozszerzeń, co zwiększa funkcjonalność narzędzia. Za rozwój Brave odpowiada zespół doświadczonych specjalistów, na czele z Brendanem Eichem, twórcą języka JavaScript. Stanowi to rekomendację bezpieczeństwa. Ponadto Brave Software opiera swój model biznesowy na innowacyjnym systemie tokenów BAT (*basic attention token*). Eliminuje to konieczność monetyzacji danych użytkowników.

Oprogramowanie OSINT samodzielne, instalowane lokalnie lub online

Jest to grupa oprogramowania OSINT stosunkowo najliczniejsza i o najszerszych zastosowaniach. Trudno wskazać, kto zapoczątkował zwyczaj dzielenia się zasobami, gdyż nie są prowadzone systematyczne studia na temat historii globalnej społeczności wywiadu jawnoźródłowego. Można jednak wymienić Arno Reusera. Jest on „bibliotekarzem wywiadowczym" i jednym z pionierów OSINT. Jego prace sięgają lat 90. XX w. Stworzył bibliotekę wywiadowczą na stronie Reuser's Information Services (RIS) zawierającą zasoby OSINT. Strona nie jest już dostępna, RIS zaś przekształcił się w przedsiębiorstwo konsultingowe. Należy wspomnieć również o Michaelu Bazzellu, znanym pionierze i popularyzatorze OSINT. Przez blisko dwie dekady pracował on w rozmaitych jednostkach federalnych i lokalnych organów ścigania USA. Jego zasoby są szeroko rozpoznawane, jako jedne z pierwszych w tej dziedzinie. Bazzell jest autorem wielu książek o tematyce OSINT oraz kontrinwigilacji w internecie. Prowadzi popularny podcast *The Privacy, Security, & OSINT Show*, a także jest twórcą IntelTechniques[55], platformy z narzędziami i szkoleniami dla profesjonalistów OSINT. W artykule przeanalizowano najlepsze, najczęściej wykorzystywane i przez to reprezentatywne oprogramowania.

Maltego[56] – zostało opracowane przez firmę Paterva założoną w 2007 r. lub 2008 r. (źródła różnie podają) w Republice Południowej Afryki przez Roelofa Temmingha, eksperta ds. cyberbezpieczeństwa, wywiadu informacyjnego i analizy

[53] BrowserAudit, https://browseraudit.com [dostęp: 28 VI 2024].

[54] PrivacyTests, https://privacytests.org [dostęp: 28 VI 2024].

[55] IntelTechniques, https://inteltechniques.com [dostęp: 28 VI 2024].

[56] Maltego, https://www.maltego.com [dostęp: 28 VI 2024].

danych. Jest to jedno z najbardziej popularnych i cenionych narzędzi OSINT używanych przez agencje rządowe i wojskowe[57] oraz firmy prywatne na całym świecie[58]. Nacisk położono na przejrzysty interfejs użytkownika, dający pogłębiony przegląd informacji. Maltego jest jednym z najwygodniejszych, najbardziej intuicyjnych i estetycznych narzędzi. Ma charakter zintegrowany, instaluje się je na dysku twardym komputera i korzysta z serwera producenta (wersja darmowa oraz tańsze wersje odpłatne[59]) lub z własnego serwera (w tym przypadku tematyka wyszukiwań jest dla producenta niewidoczna). Maltego ewoluowało od prostego narzędzia służącego do mapowania powiązań biznesowych do zaawansowanego oprogramowania OSINT. Nie jest otwartoźródłowe, jednak zostało omówione ze względu na powszechność jego użytkowania. Fundamentem działania jest triada ściśle powiązanych elementów: encji (*entities*), kolekcji (*collections*) oraz transformacji (*transforms*), których synergia umożliwia efektywne wyszukiwanie i przetwarzanie danych. Encje, stanowiące elementarne jednostki informacji (np. osoba, witryna internetowa, adres IP), tworzą podstawowy budulec systemu. Kolekcje, będące zbiorami skorelowanych encji (np. pracownicy przedsiębiorstwa, konta e-mail w domenie), wprowadzają wymiar strukturalny. Natomiast transformacje, czyli zautomatyzowane procesy przetwarzające encje (np. geolokalizacja na podstawie adresu IP, ekstrakcja danych WHOIS), odpowiadają za przepływ i wzbogacanie informacji. Rezultatem współdziałania tych komponentów jest przejrzysty graf powiązań, oferujący perspektywę holistyczną. Odrębny aspekt funkcjonalności narzędzia stanowią transformacje niezintegrowane z Maltego (wtyczki). Są to rozszerzenia, które można szybko i łatwo uruchomić, aby umożliwić użytkownikowi natychmiastowe wykonywanie zadań analitycznych. Bogaty zbiór wtyczek (obecnie nieco ponad 80), których lista jest prezentowana na ekranie powitalnym (*home*) aplikacji, jest dostępny na zróżnicowanych warunkach – począwszy od nieograniczonego i intuicyjnego użytkowania (*click-and-run unlimited*), przez opcje darmowe, aczkolwiek wymagające uzyskania klucza API, aż po subskrypcyjne, wiążące się z opłatami. Poprzez wtyczki Maltego integruje wiele znanych narzędzi służących OSINT[60]. Wśród wtyczek o nieograniczonym dostępie uwagę przykuwa m.in. Maltego Regex Transform (Maltego Technologies), która umożliwia ekstrakcję dopasowanych obiektów z witryn internetowych z zastosowaniem wyrażeń

[57] Są to m.in.: Europol, FBI, NATO, policja w Wielkiej Brytanii, Scotland Yard.

[58] Na przykład przedsiębiorstwa konsultingowe i audytowe, jak: Deloitte, EY, KPMG, PwC, oraz zajmujące się cyberbezpieczeństwem, jak: Mandiant, Palantir, Recorded Future.

[59] W tym przeznaczona dla instytucji rządowych Maltego Government/Military.

[60] Są to m.in. eksploratory blockchainów, oprogramowanie do wyszukiwania adresów e-mail – Hunter czy systemy śledzenia online statków powietrznych i morskich.

regularnych. Kolejną wtyczką jest Loginsoft OSINT, wykrywająca numery telefonów i pozyskująca metadane. Obecna jest także grupa wtyczek wspomagająca identyfikację powiązań i relacji. LittleSis (Maltego Technologies) umożliwia identyfikację relacji między osobami w sferze biznesu i administracji państwowej (głównie w USA). OCCRP Aleph (Maltego Technologies) pozwala na przeszukiwanie rejestrów przedsiębiorstw, dokumentów, danych dotyczących zamówień publicznych, sankcji, wycieków, artykułów prasowych i innych zasobów, dzięki czemu stanowi jedno z najlepszych źródeł dla dziennikarzy śledczych. Social Links CE (Social Links Inc.) daje możliwość pozyskiwania danych z wyszukiwarek IoT. Wayback Machine (Maltego Technologies) umożliwia eksplorację ponad 439 mld zarchiwizowanych stron internetowych. Maltego ma również pewne ograniczenia. W umiarkowanym stopniu dba o bezpieczeństwo użytkownika, gdyż nie tylko wymaga rejestracji i uwierzytelniania, lecz także przetwarza zapytania na własnych serwerach. Dane osobowe są udostępniane dodatkowym modułom i wtyczkom. Maltego jest kosztownym narzędziem, jeśli użytkownik chce korzystać z wszystkich funkcjonalności (subskrypcja). Użytkowanie darmowej wersji wiąże się z limitami (maksymalnie 12 wyników). Ponadto Maltego koncentruje się głównie na aspektach informatycznych i pomija kontekst kulturowy i społeczny.

OSRFramework (Open Sources Research Framework)[61] – to potężny zestaw narzędzi do zadań OSINT, stworzony w 2015 r. przez Félixa Brezę i Yaizę Rubio, hiszpańskich badaczy cyberbezpieczeństwa. Ten zbiór bibliotek i skryptów, napisanych głównie w Pythonie, automatyzuje proces gromadzenia i analizy publicznie dostępnych informacji. Modularną architekturę OSRFramework, pozwalającą na rozszerzanie i dostosowywanie do konkretnych potrzeb, cechuje dobra integracja z innymi narzędziami OSINT. Najważniejsze funkcje to: sprawdzanie dostępności i istnienia nazwy użytkownika na różnych platformach, zbieranie informacji o adresach e-mail, wyszukiwanie informacji o osobie lub temacie, o domenach, o numerach telefonów, a także tworzenie kompleksowego profilu osoby oraz generowanie raportów z zebranych danych. Wady OSRFramework to: stroma krzywa uczenia się, zależność od zewnętrznych API, potencjalne problemy z prywatnością oraz możliwość generowania fałszywych pozytywów w wynikach wyszukiwań.

SpiderFoot[62] – narzędzie powstało w 2012 r., udostępniono je na licencji GNU General Public License v2.0, a jego twórcą jest Steve Micallef, specjalista ds. bezpieczeństwa i programista. Zostało opracowane na potrzeby rozpoznania w zakresie cyberbezpieczeństwa oraz OSINT. Koncentruje się na pozyskiwaniu informacji o domenach,

[61] OSRFramework, https://github.com/i3visio/osrframework [dostęp: 28 VI 2024].

[62] SpiderFoot, https://github.com/smicallef/spiderfoot – wersja instalowana [dostęp: 28 VI 2024], https://login.hx.spiderfoot.net/ – wersja online (HX) [dostęp: 28 VI 2024].

adresach IP, sieciach, eksploracji blockchainów, certyfikatów SSL/TLS, a w ograniczonym stopniu dokonuje przeszukiwania mediów społecznościowych, forów dyskusyjnych oraz Darknetu (pod kątem wycieków). Składa się z ponad 200 różnych narzędzi. Działa online (w okrojonej wersji darmowej oraz pełnej odpłatnej na zasadzie subskrypcji) lub jako oprogramowanie instalowane lokalnie (starsza wersja). Wersja online nosi nazwę SpiderFoot HX. Niewątpliwą wadą jest to, że oprogramowanie jest przeznaczone przede wszystkim dla specjalistów w zakresie cyberbezpieczeństwa, a nie białego wywiadu. To narzędzie odpłatne, a przedmiot zainteresowania operatorów OSINT jest widoczny dla dostawcy oprogramowania (wersja HX).

Recon-ng[63] – powstał w 2013 r., jego twórcą jest Tim Tomes, znany również jako LaNMaSteR53. Narzędzie zostało napisane w języku Python, działa jako framework, w którym użytkownicy korzystają z różnych modułów do zbierania i analizowania danych:

- Recon – służy do zbierania informacji z zewnętrznych źródeł, takich jak: wyszukiwarki, bazy danych WHOIS, media społecznościowe itp.;
- Reporting – moduły przeznaczone do tworzenia raportów;
- Exploitation – badanie potencjalnych luk w zabezpieczeniach, na potrzeby białego wywiadu jest mniej przydatne;
- Import/Export – moduły do importowania i eksportowania danych.

Jest to narzędzie otwartoźródłowe, udostępniane na licencji BSD 3-Clause New/Revised. Większość modułów Recon-ng jest bezpłatna, lecz niektóre mogą korzystać z zewnętrznych usług lub API wymagających płatnego dostępu. Trzeba mieć na uwadze możliwość wykorzystania limitów pobierania danych, a ponadto Recon-ng funkcjonuje wyłącznie w systemach GNU/Linux. Narzędzie działa w terminalu i wymaga specyficznego języka poleceń.

TheHarvester[64] – pozwala na zbieranie informacji na temat domen, adresów e-mail, nazw użytkowników, nazw hostów i adresów IP. Został stworzony przez Christiana Martorella w 2007 r. i jest utrzymywany przez zespół Edge Security. To narzędzie *open source* (licencja GPLv3) dostępne do użytku na własnym komputerze. Umożliwia wyszukiwanie z użyciem: wyszukiwarek internetowych (Google, Bing, Baidu), serwisów społecznościowych (LinkedIn, Twitter), WHOIS, rejestrów certyfikatów SSL/TLS, DNS. Działa w terminalu i wymaga nauczenia się specyficznego języka poleceń. Jest przeznaczony dla osób radzących sobie z Bashem/Pythonem/systemami GNU/Linux.

[63] Recon-ng, https://github.com/lanmaster53/recon-ng [dostęp: 28 VI 2024].

[64] TheHarvester, https://github.com/laramies/theHarvester [dostęp: 28 VI 2024].

FOCA (Fingerprinting Organizations with Collected Archives)[65] – narzędzie internetowe zaprojektowane do celów wywiadu jawnoźródłowego. Po raz pierwszy pojawiło się w 2009 r., zostało stworzone przez hiszpańską firmę ElevenPaths specjalizującą się w cyberbezpieczeństwie. Wydane na licencji GNU (FOCAFree). Służy głównie do wyszukiwania metadanych i informacji ukrytych w skanowanych dokumentach. Dokumenty można skanować online lub lokalnie. Umożliwia identyfikację informacji wrażliwych, takich jak: struktura sieci, dane użytkowników (imiona, nazwiska, webonimy), dane techniczne i wersje oprogramowania. Nie ma własnej wyszukiwarki, proces pozyskiwania dokumentów odbywa się za pomocą Google, Bing i DuckDuckGo. Program zasadniczo służy do skanowania dokumentów Microsoft Office/Open Office, pdf, AdobeInDesign oraz svg. Może również działać w postaci wtyczki, co zaimplementowano w przeglądarce CAT. Wady FOCA to: konieczność instalacji serwera SQL, częściowa odpłatność (FOCAPro), wysoki próg wejścia, stroma krzywa uczenia się, brak aktualizacji od dwóch lat oraz ograniczenie wyłącznie do analizy metadanych.

Odnośniki do oprogramowania i innych narzędzi OSINT

Jest to zróżnicowana i liczna grupa. Właściwie każdy operator OSINT dysponuje własnym zbiorem odnośników. Wskazano zbiory charakteryzujące się największą liczebnością zgromadzonych odnośników lub popularnością wśród badaczy.

Bellingcat's Online Investigation Toolkit[66] – zbiór narzędzi do badań i weryfikacji informacji w internecie opracowany przez Bellingcat. Zestaw ten przyjmuje formę arkusza MSExcel, zawierającego 14 zakładek z logicznie pogrupowanymi odnośnikami, opatrzonymi nazwami i komentarzami dotyczącymi przeznaczenia oraz reguł użycia poszczególnych narzędzi. Główny nacisk położono na media społecznościowe i rejestry. Pomimo starannej organizacji forma arkusza Excel nie sprzyja ergonomii pracy. Wśród ograniczeń należy wymienić: brak aktualizacji od czerwca 2023 r., stosunkowo niewielką liczbę narzędzi do eksploracji imageboardów, brak adresów forów dyskusyjnych oraz narzędzi eksploracji Darknetu. Arkusz spełnia wyłącznie funkcję pośrednika – kieruje do zewnętrznych narzędzi, bez ich osadzenia. Zauważalny jest brak rejestrów informacji dotyczących Europy Środkowo-Wschodniej i Federacji Rosyjskiej. To jednak zbiór, który powinien posiadać w swoim zasobniku każdy analityk OSINT.

[65] FOCA, https://github.com/ElevenPaths/FOCA [dostęp: 28 VI 2024].

[66] Bellingcat's Online Investigation Toolkit, https://heystacks.com/doc/612/bellingcats-online-investigation-toolkit-bitlybcat (arkusz kalkulacyjny) [dostęp: 28 VI 2024].

OSINT Framework[67] – to strona www zawierająca interaktywną mapę sklasyfikowanych odnośników do narzędzi i stron OSINT. Zbudowana w formie grafu, zapewnia łatwy dostęp do potrzebnego narzędzia. Twórcą OSINT Framework jest Justin Nordine, specjalista w zakresie bezpieczeństwa informacji. Projekt został zainicjowany w 2015 r. jako narzędzie dla społeczności zajmującej się bezpieczeństwem, wywiadem i analizą informacji. Znany i często używany w społeczności OSINT. Istnieje polski odpowiednik o nazwie Otwarte Źródła bazujący na kodzie Nordine'a. Uzupełnia on dane o te dotyczące Polski[68]. Dostawca strony zbudował ją w JavaScript, niewykluczone, że zbiera ona cyfrowy odcisk palca operatora OSINT. Wiele informacji w Otwartych Źródłach jest nieaktualnych.

Malfrats OSINT Map[69] – stworzona przez Malfrats Industries, jest kontynuatorem OSINT Framework. Powstała w wyniku działań niezadowolonych badaczy, którzy zauważyli brak aktualizacji w OSINT Framework. Malfrats OSINT Map zawiera 18 kategorii, w tym zakładkę umożliwiającą prowadzenie śledztw OSINT w obszarze sił i działań zbrojnych. Dodatkowo oferuje takie kategorie, jak narzędzia do analizy sieci, monitorowania Dark Webu i inne. Platforma ma jednak wady. Są one związane z jej bezpieczeństwem (JavaScript).

MetaOSINT Chart[70] – to efekt pięcioletniej pracy TropChauda, profesjonalnego badacza i analityka zajmującego się białym wywiadem. Projekt stanowi bezpłatną i otwartą agregację narzędzi i zasobów, mającą na celu wsparcie osób początkujących w prowadzeniu dochodzeń OSINT. Tym, co wyróżnia MetaOSINT, jest innowacyjna forma prezentacji danych w postaci wykresu bąbelkowego (*bubble chart*), w którym wielkość pęcherzyków odzwierciedla popularność danego narzędzia wśród operatorów OSINT, mierzoną liczbą wskazań respondentów. Zbiór danych MetaOSINT powstał na podstawie ankiety przeprowadzonej przez autora projektu, obejmującej niemal 30 list narzędzi i zasobów OSINT, zawierających blisko 5000 linków źródłowych.

Awesome OSINT For Everything[71] – skategoryzowany, obszerny zbiór odnośników, który obejmuje praktycznie wszystkie aspekty OSINT. Zawiera narzędzia do analizy sieci, wyszukiwania informacji, analizy mediów społecznościowych i inne, często nieznane szerzej narzędzia. Wyróżnia go uwzględnienie narzędzi AI

[67] OSINT Framework, https://osintframework.com [dostęp: 28 VI 2024].

[68] Otwarte Źródła, https://osintframework.pl [dostęp: 28 VI 2024].

[69] Malfrats OSINT Map, https://map.malfrats.industries [dostęp: 28 VI 2024].

[70] MetaOSINT Chart, https://metaosint.github.io/learn-more [dostęp: 28 VI 2024].

[71] Awesome OSINT For Everything, https://github.com/Astrosp/Awesome-OSINT-For-Everything [dostęp: 28 VI 2024].

(*artificial intelligence*) oraz wybranych narzędzi do generowania tymczasowych fałszywych tożsamości w internecie.

The Ultimate OSINT Collection[72] – to kompleksowa kolekcja narzędzi OSINT z różnorodnymi kategoriami, takimi jak: analiza sieci, wyszukiwanie osób, analiza mediów społecznościowych i inne. Przyjazna dla początkujących badaczy.

Istnieje wiele zbiorów tego typu, których zakres i treść w dużej mierze się pokrywają[73].

Podsumowanie i wnioski

W artykule dokonano kategoryzacji i ewaluacji wybranych narzędzi OSINT służących do wyszukiwania informacji, ze szczególnym uwzględnieniem rozwiązań otwartoźródłowych. Najważniejsze wydaje się wskazanie ograniczeń popularnych narzędzi wyszukiwawczych w kontekście zakresu i obszaru ich zastosowania. Obserwuje się, że w badaniach OSINT niedostateczną wagę przykłada się do aspektów bezpieczeństwa. Często zakłada się, że wystarczy korzystać z maszyny wirtualnej z bezpieczną dystrybucją GNU/Linux, jak Whonix lub Linux Tails[74], względnie przestrzegać zaleceń użycia wirtualnych sieci prywatnych (*virtual private network*, VPN). Takie podejście wydaje się i błędne, i niepraktyczne. Zaawansowane systemy GNU/Linux ukierunkowane na bezpieczeństwo mogą być nieefektywne ze względu na przekierowywanie połączeń przez sieć Tor, której węzły wyjściowe są identyfikowane i często blokowane przez liczne usługi, w tym narzędzia OSINT. Charakterystyczny cyfrowy odcisk palca komputera z zainstalowaną bezpieczną dystrybucją GNU/Linux może podpowiadać wyszukiwanemu, że jest on przedmiotem zainteresowania operatora OSINT. Warto przypomnieć, że już 15 lat temu cyberprzestępcy

[72] The Ultimate OSINT Collection, https://start.me/p/DPYPMz/the-ultimate-osint-collection [dostęp: 28 VI 2024].

[73] Bogate zbiory to: OSINT4All (https://start.me/p/L1rEYQ/osint4all), OSINT Tools Lorando Bodo (https://start.me/p/7kxyy2/osint-tools-curated-by-lorand-bodo), Nixintel's OSINT Resource List (https://start.me/p/rx6Qj8/nixintel-s-osint-resource-list) oraz Verification Toolset Julii Bayer (https://start.me/p/ZGAzN7/verification-toolset). Warto korzystać z bibliotek narzędzi Freedomlab (https://www.freedomlab.io/tools-for-hrds) oraz zbiorów Haystack (https://heystacks.com, są tam dostępne nie tylko narzędzia i bazy OSINT).

[74] W kontekście prowadzenia wywiadu jawnoźródłowego systemy takie jak Linux Tails (https://tails.net) i Linux Whonix (https://www.whonix.org), mimo wysokiego poziomu bezpieczeństwa, mogą generować pewne ograniczenia funkcjonalne. Warto rozważyć wykorzystanie mniej znanych dystrybucji, np. Kodachi Linux (https://www.digi77.com/linux-kodachi/), Qubes OS (https://www.qubes-os.org) czy tworzony Subgraph OS (https://subgraph.com/sgos/download/index.en.html), które oferują balans między bezpieczeństwem a swobodą działań wywiadowczych.

wykorzystywali techniki inwigilacji w celu monitorowania działań funkcjonariuszy prowadzących przeciwko nim dochodzenia. Przykładem jest grupa przestępcza Bayrob, która zajmowała się sprzedażą nieistniejących pojazdów na platformie e-Bay. Członkowie grupy stosowali zaawansowane metody śledzenia i kontroli, aby uzyskać przewagę nad organami ścigania zaangażowanymi w prowadzone śledztwa[75]. Adresy serwerów VPN są również identyfikowalne, a niektóre usługi mogą je blokować. W badaniach OSINT rzadko rekomenduje się i praktykuje wykorzystanie prywatnych serwerów proxy, które zapewniają największe możliwości ukrycia się wśród użytkowników sieci. Jednocześnie brakuje dogłębnej analizy kwestii dotyczących pozostawiania cyfrowych odcisków palców oraz narzędzi umożliwiających swobodne kształtowanie tego aspektu tożsamości internetowej[76]. W literaturze brakuje również pogłębionej refleksji nad relacją między bezpieczeństwem a możliwościami wyszukiwania, gdy zwiększenie poziomu bezpieczeństwa często ogranicza potencjał poszukiwań. Nierzadko bezkrytycznie przyjmuje się zamknięte i komercyjne narzędzia OSINT i ignoruje to, że sam analityk staje się obiektem obserwacji dostawcy oprogramowania, a część wyników dochodzenia może być temu dostawcy znana. W związku z tym autor artykułu zdecydowanie rekomenduje wykorzystanie narzędzi będących w autonomicznym posiadaniu operatora OSINT. Istotnym problemem jest nierównowaga między pozyskiwaniem informacji a ich analizą. Na peryferiach zainteresowań specjalistów OSINT często pozostają kwestie związane z analityką wywiadowczą oraz zagadnienia dotyczące błędów poznawczych, heurystyki i szumu informacyjnego. Paradygmaty analizy oraz świadomość możliwości popełnienia błędów poznawczych to bardzo ważne zagadnienia, równie istotne jak narzędzia. Każdy analityk wywiadu jawnoźródłowego powinien mieć te tematy opanowane. Kolejnym wyzwaniem jest świadomy dobór narzędzi wspomagających analizę oraz wizualizację wyników OSINT. Obserwuje się, że badacze, podążając za trendem, ograniczają się do otwartego oprogramowania, np. otwartoźródłowego CherryTree[77] lub komercyjnego Hunchly[78]. Alternatywnie sięgają po rozwiązania dostępne online, takie jak Visual Investigative Scenarios (VIS)[79].

---

[75] United States Court of Appeals, *United States of America v. Bogdan Nicolescu; Radu Miclaus,* https://www.opn.ca6.uscourts.gov/opinions.pdf/21a0231p-06.pdf [dostęp: 28 VI 2024].

[76] Analityk OSINT może dostrzec użyteczność takich narzędzi, jak przeglądarka internetowa Dolphin{Anty} (https://dolphin-anty.com/en/), która umożliwia swobodne kształtowanie cyfrowego odcisku palca, czy zestaw zaawansowanych ustawień konfiguracyjnych Ghacks dla przeglądarki Firefox, stworzony w celu poprawy prywatności, bezpieczeństwa i wydajności. Istnieje wiele innych rozwiązań różniących się zakresem i treścią, a ich przegląd mógłby stanowić przedmiot odrębnego artykułu.

[77] CherryTree, https://www.giuspen.com/cherrytree [dostęp: 28 VI 2024].

[78] Hunchly, https://www.hunch.ly [dostęp: 28 VI 2024].

[79] VIS, https://vis.occrp.org [dostęp: 28 VI 2024].

Przy wyborze narzędzi również pomija się kwestie bezpieczeństwa, a programy komercyjne lub usługi online mogą być przedmiotem inwigilacji. Zauważalny jest brak wyczerpującego przeglądu dostępnego oprogramowania pod kątem jego wpływu na bezpieczeństwo i poufność prowadzonych analiz OSINT[80]. Kolejny problem to marginalne zastosowanie metod ilościowych. Dominują analizy jakościowe lub oparte na potocznym wnioskowaniu. Istotne jest również zwrócenie uwagi na nowe technologie, które mogą okazać się przełomowe w dziedzinie OSINT, zwłaszcza na duże modele językowe, określane mianem generatywnej AI. Narzędzia te mogą być wykorzystywane zarówno do wyszukiwania informacji, jak i do ich przetwarzania oraz analizy. Znaczne rozproszenie środowiska twórców oprogramowania OSINT może być oceniane ambiwalentnie. Mnogość narzędzi o zbliżonych funkcjach i krótkim cyklu istnienia, kończącym się komercjalizacją lub porzuceniem projektu, utrudnia wybór optymalnego rozwiązania. Narzędzia komercyjne, mimo wygody użytkowania, mogą ograniczać perspektywę poznawczą analityka OSINT i budzić wątpliwości co do prywatności. Optymalnym rozwiązaniem wydaje się otwarte, modularne narzędzie o niskim progu wejścia i łagodnej krzywej uczenia się, umożliwiające szerokiemu gronu użytkowników aktywny udział w rozwoju oprogramowania i dostosowanie go do indywidualnych potrzeb.

Na podstawie przeprowadzonych analiz i rozważań można antycypować dwa potencjalne scenariusze rozwoju OSINT 3.0: pozytywny i negatywny.

Scenariusz pozytywny zakłada wzrost integracji narzędzi OSINT z systemami operacyjnymi i przeglądarkami, co zwiększyłoby wygodę użytkowania oraz poziom bezpieczeństwa operacyjnego. Przykłady takie jak Trace Labs czy CAT sugerują, że przyszłość OSINT może opierać się na głębszej integracji, umożliwiającej preinstalację i konfigurację narzędzi w bezpiecznych środowiskach. Przewidywany jest także rozwój zaawansowanych mechanizmów analizy i wizualizacji danych, takich jak: interaktywne mapy powiązań, zaawansowane grafy sieci społecznościowych oraz dynamiczne modele predykcyjne. Oczekiwać można również rozwoju narzędzi przeznaczonych do eksploracji specyficznych przestrzeni internetowych, w tym dark webu, metawersów, zdecentralizowanych sieci i blockchainów. Istotnym elementem może być automatyzacja procesów z wykorzystaniem sztucznej inteligencji, co zwiększy wydajność operacji OSINT i umożliwi lepsze zarządzanie dużymi zbiorami danych.

[80] Warto zwrócić uwagę na Trilium (https://github.com/zadam/trilium), które wydaje się spełniać postulaty sformułowane w artykule. To otwarte oprogramowanie, działające na komputerze użytkownika, zapewniające kontrolę nad poufnością danych, oferujące zestaw funkcji wspomagających gromadzenie i wizualizację śledztwa OSINT.

Scenariusz negatywny przewiduje tendencję do fragmentacji narzędzi OSINT. Zamiast konsolidacji funkcji możliwe są rosnąca specjalizacja i rozproszenie narzędzi, co zwiększy złożoność pracy operatorów OSINT. Narzędzia mogą stać się bardziej skomplikowane i mniej intuicyjne. Ograniczy to ich dostępność, zwłaszcza dla nowych użytkowników, i będzie prowadzić do spadku efektywności. Możliwa jest także rosnąca zależność od komercyjnych narzędzi i baz danych. Zanik otwartych i darmowych rozwiązań może skłonić użytkowników do korzystania z płatnych narzędzi, co zwiększy kontrolę dostawców oprogramowania nad dostępem do danych i jednocześnie zawęzi możliwości operacyjne mniejszych organizacji i niezależnych badaczy.

Podsumowując, przyszłość rozwoju narzędzi OSINT pozostaje nierozstrzygnięta. Z jednej strony, możliwe są pozytywne zmiany związane z integracją, automatyzacją oraz rozwojem zaawansowanych funkcji analitycznych. Z drugiej, istnieje ryzyko fragmentacji, skomplikowania użytkowania oraz rosnącej komercjalizacji, co może negatywnie wpłynąć na dostępność i funkcjonalność narzędzi OSINT.

Bibliografia

Abramczuk K., Kąkol M., Wierzbicki A., *How to Support the Lay Users Evaluations of Medical Information on the Web?*, w: *Human Interface and the Management of Information: Information, Design and Interaction*, S. Yamamoto (red.), Cham 2016, s. 3–13. https://doi.org/10.1007/978-3-319-40349-6_1.

Bazzell M., *Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information,* Charleston 2018.

Bazzell M., *OSINT Techniques: Resources For Uncovering Online Information*, [bmw] 2023.

Block L., *The long history of OSINT*, „Journal of Intelligence History" 2024, t. 23, nr 2, s. 95–109. https://doi.org/10.1080/16161262.2023.2224091.

Dorn A.W., *United Nations Peacekeeping Intelligence*, w: *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (red.), Oxford 2010, s. 275–295.

Forge J., *A Note on the Definition of "Dual Use"*, „Science and Engineering Ethics" 2010, t. 16, nr 1, s. 111–118.

Hargittai E., Hinnant A., *Digital Inequality: Differences in Young Adults' Use of the Internet*, „Communication Research" 2008, t. 35, nr 5, s. 602–621. https://doi.org/10.1177/0093650208321782.

Hulnick A.S., *Fixing the Spy Machine. Preparing American Intelligence for the Twenty-First Century*, Westport 1999.

Lowenthal M.M., *Intelligence: From Secrets to Policy*, Washington 2007.

Maddrell P., *Spying on Science: Western Intelligence in Divided Germany 1945–1961*, Oxford 2006.

Mercado S.C., *Sailing the Sea of OSINT in the Information Age*, „Studies in Intelligence" 2004, t. 48, nr 3, s. 45–55.

Mider D., *Mappa Mundi ukrytego Internetu. Próba kategoryzacji kanałów komunikacji i treści*, „PTINT Praktyka i Teoria Informacji Naukowej i Technicznej" 2015, t. 23, nr 1, s. 3–16.

Mider D., *Sztuka wyszukiwania w Internecie – autorski przegląd wybranych technik i narzędzi*, „Studia Politologiczne" 2019, t. 54, s. 191–229.

Mider D., Garlicki J., Mincewicz W., *Pozyskiwanie informacji z Internetu metodą Google Hacking – biały, szary czy czarny wywiad?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 20, s. 68–91.

Nasheri H., *Economic Espionage and Industrial Spying*, Cambridge 2004.

National Research Council, *Computers at Risk: Safe Computing in the Information Age*, Washington 1991.

Olcott A., *Open Source Intelligence in a Networked World (Continuum Intelligence Studies)*, New York 2012.

Open Source Intelligence Market Size, Share, Competitive Landscape and Trend Analysis Report, by Source, Technique and End User: Global Opportunity Analysis and Industry Forecast, 2020–2027, Allied Market Research, maj 2020 r.

Rosenzweig P., McNulty T.J., Shearer E., *Whistleblowers, Leaks, and the Media: The First Amendment and National Security*, Chicago 2013.

Schaurer F., Störger J., *Guide to the Study of Intelligence. The Evolution of Open Source Intelligence (OSINT)*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2013, nr 3, s. 53–56.

Steele R.D., *Open source intelligence*, w: *Handbook of Intelligence Studies*, New York 2007, s. 129–147.

Steele R.D., *The Open-Source Everything Manifesto: Transparency, Truth, and Trust*, Berkeley 2012.

Turaliński K., *Wywiad gospodarczy i polityczny. Podręcznik dla specjalistów ds. bezpieczeństwa, detektywów i doradców gospodarczych*, Warszawa 2015.

Tylutki K., *Informacja masowego rażenia – OSINT w działalności wywiadowczej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19, s. 166–192.

Wyniki pracy wywiadu naukowo-technicznego MSW PRL 1971–1989, M. Sikora (oprac.), Katowice–Warszawa 2019.

Źródła internetowe

A Consumer's Guide to Intelligence, Office of Public Affairs CIA, 1999 r., https://archive.org/details/consumersguide_tenet/mode/2up [dostęp: 28 VI 2024].

AFP, *How Bellingcat became Russia's 'biggest nightmare'*, France24, 7 IX 2022 r., https://www.france24.com/en/live-news/20220907-how-bellingcat-became-russia-s-biggest-nightmare [dostęp: 28 VI 2024].

Awesome OSINT For Everything, https://github.com/Astrosp/Awesome-OSINT-For-Everything [dostęp: 28 VI 2024].

Bellingcat's Online Investigation Toolkit, https://heystacks.com/doc/612/bellingcats-online-investigation-toolkit-bitlybcat (arkusz kalkulacyjny) [dostęp: 28 VI 2024].

BlackArch, https://blackarch.org/index.html [dostęp: 28 VI 2024].

BrowserAudit, https://browseraudit.com [dostęp: 28 VI 2024].

CherryTree, https://www.giuspen.com/cherrytree [dostęp: 28 VI 2024].

Chertoff M., Simon T., *The Impact of the Dark Web on Internet Governance and Cyber Security*, https://www.cigionline.org/static/documents/gcig_paper_no6.pdf [dostęp: 28 VI 2024].

Ciancaglini V. i in., *Deep Web and Cybercrime: It's Not All About TOR*, Trend Micro, 12 XI 2014 r., https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/deep-web-and-cybercrime-its-not-all-about-tor [dostęp: 28 VI 2024].

Colquhoun C., *A Brief History of Open Source Intelligence*, Bellingcat, 14 VII 2016 r., https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ [dostęp: 28 VI 2024].

Electronic evidence of war crimes. The role of journalists, media and social media, webinar zorganizowany przez Group of Friends on the Safety of Journalists and Media Freedom in Strasbourg oraz Radę Europy, 25 XI 2022 r., https://www.coe.int/en/web/kyiv/-/electronic-evidence-of-war-crimes-and-the-role-of-journalists-media-and-social-media [dostęp: 28 VI 2024].

FOCA, https://github.com/ElevenPaths/FOCA [dostęp: 28 VI 2024].

Higgins E., *How Open Source Evidence was Upheld in a Human Rights Court*, Bellingcat, 28 III 2023 r., https://www.bellingcat.com/resources/2023/03/28/how-open-source-evidence-was-upheld-in-a-human-rights-court/ [dostęp: 28 VI 2024].

Hunchly, https://www.hunch.ly [dostęp: 28 VI 2024].

IntelTechniques, https://inteltechniques.com [dostęp: 28 VI 2024].

Kali Linux, https://www.kali.org [dostęp: 28 VI 2024].

Mackinnon A., *Bellingcat Can Say What U.S. Intelligence Can't*, Foreign Policy, 17 XII 2020 r., https://foreignpolicy.com/2020/12/17/bellingcat-can-say-what-u-s-intelligence-cant/ [dostęp: 28 VI 2024].

Malfrats OSINT Map, https://map.malfrats.industries [dostęp: 28 VI 2024].

Maltego, https://www.maltego.com [dostęp: 28 VI 2024].

Market share of leading desktop search engines worldwide from January 2015 to January 2024, Statista, 2024 r., https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/ [dostęp: 28 VI 2024].

Matthews O., *Fact Cats. The inside story of how it got the Skripal scoop*, The Spectator, 20 X 2018 r., https://www.spectator.co.uk/article/fact-cats/ [dostęp: 28 VI 2024].

MetaOSINT Chart, https://metaosint.github.io/learn-more [dostęp: 28 VI 2024].

NATO Open Source Intelligence Handbook v 1.2, https://archive.org/details/NATOOSINTHandbookV1.2/page/n1/mode/2up [dostęp: 28 VI 2024].

Open Source Intelligence Market Size, Share, Growth, and Industry Analysis, By Type (Video Analytics, Text Analytics, Visualization Tool, Cyber Security, Web Analysis, Social Media Analysis, and Others), By Application (Private Sector, Public Sector and Other), Regional Insights, and Forecast to 2032, Business Research Insights, marzec 2024 r., https://www.businessresearchinsights.com/market-reports/open-source-intelligence-market-109546 [dostęp: 28 VI 2024].

OSINT Framework, https://osintframework.com [dostęp: 28 VI 2024].

OSRFramework, https://github.com/i3visio/osrframework [dostęp: 28 VI 2024].

Otwarte Źródła, https://osintframework.pl [dostęp: 28 VI 2024].

Paley N., *Copying is an act of love. Please copy and share*, https://copyheart.org [dostęp: 28 VI 2024].

ParrotOS Security, https://www.parrotsec.org [dostęp: 28 VI 2024].

PrivacyTests, https://privacytests.org [dostęp: 28 VI 2024].

Recon-ng, https://github.com/lanmaster53/recon-ng [dostęp: 28 VI 2024].

Reinsel D., Grantz J., Rydning J., *The Digitization of the World. From Edge to Core*, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-data-age-whitepaper.pdf [dostęp: 28 VI 2024].

SpiderFoot, https://github.com/smicallef/spiderfoot [dostęp: 28 VI 2024].

SpiderFoot, https://login.hx.spiderfoot.net [dostęp: 28 VI 2024].

The Ultimate OSINT Collection, https://start.me/p/DPYPMz/the-ultimate-osint-collection [dostęp: 28 VI 2024].

TheHarvester, https://github.com/laramies/theHarvester [dostęp: 28 VI 2024].

Trace Labs, https://www.tracelabs.org/initiatives/osint-vm [dostęp: 28 VI 2024].

Tsurugi Linux, https://tsurugi-linux.org/index.php [dostęp: 28 VI 2024].

VIS, https://vis.occrp.org [dostęp: 28 VI 2024].

Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025, Statista, czerwiec 2021 r., https://www.statista.com/statistics/871513/worldwide-data-created/ [dostęp: 28 VI 2024].

White E., *Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism*, Cambridge University Press, 7 IX 2023 r., https://www.cambridge.org/core/journals/leiden-journal-of-international-law/article/closing-cases-with-opensource-facilitating-the-use-of-usergenerated-opensource-evidence-in-international-criminal-investigations-through-the-creation-of-a-standing-investigative-mechanism/981CEFF9D5AF80B6FD0A75BE6A1A384C [dostęp: 28 VI 2024].

Williams H.J., Blum I., *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, RAND, 17 V 2018 r., https://www.rand.org/pubs/research_reports/RR1964.html [dostęp: 28 VI 2024].

Orzecznictwo

Case of Ukraine and the Netherlands v. Russia, 8019/16, 43800/14, 28525/20, Archiwum Europejskiego Trybunału Praw Człowieka, 30 XI 2022 r., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-222889%22]} [dostęp: 28 VI 2024].

United States Court of Appeals, *United States of America v. Bogdan Nicolescu; Radu Miclaus*, https://www.opn.ca6.uscourts.gov/opinions.pdf/21a0231p-06.pdf [dostęp: 28 VI 2024].

Dr hab. Daniel Mider

Adiunkt na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Specjalizuje się w problematyce wywiadu jawnoźródłowego w internecie, kryptoaktywów, cyberprzestępczości, socjologii internetu i socjologii przemocy politycznej.

Kontakt: d.mider@uw.edu.pl