

Rola oraz możliwości wykorzystania wywiadu jawnoźródłowego w zapewnianiu bezpieczeństwa Rzeczypospolitej Polskiej¹

The role and potential applications of open-source intelligence
in ensuring the security of the Republic of Poland

ANNA NASTUŁA

Autorka niezależna

 <https://orcid.org/0000-0002-2061-5067>

Abstrakt

Celem artykułu jest określenie znaczenia oraz możliwości wykorzystania wywiadu jawnoźródłowego (*open source intelligence*, OSINT) w zapewnianiu bezpieczeństwa państwa. W opracowaniu omówiono zagadnienia teoretyczne związane z charakterystyką OSINT, w tym jego metody i środki oraz prawne i pozaprawne aspekty jego wykorzystania. Przedstawiono również rozwój OSINT w Stanach Zjednoczonych, Wielkiej Brytanii oraz Izraelu. Następnie zaprezentowano wyniki badań empirycznych zrealizowanych w latach 2023–2024 z zastosowaniem metody indywidualnych wywiadów pogłębionych przeprowadzonych z 12 ekspertami z zakresu bezpieczeństwa oraz wywiadu jawnoźródłowego. Na podstawie dokonanej

¹ Artykuł powstał na podstawie rozprawy doktorskiej pt. *Znaczenie wywiadu jawnoźródłowego w bezpieczeństwie państwa* obronionej na Wojskowej Akademii Technicznej. Praca została nagrodzona w XV edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

analizy oraz wyników badań sformułowano wnioski i rekomendacje dotyczące możliwości wykorzystania wywiadu jawnoźródłowego w zapewnianiu bezpieczeństwa Rzeczypospolitej Polskiej.

Słowa kluczowe wywiad jawnoźródłowy, OSINT, bezpieczeństwo, informacje jawnoźródłowe, otwarte źródła informacji, cyberbezpieczeństwo

Abstract The aim of this article is to determine the significance and potential applications of open-source intelligence in ensuring state security. The paper discusses theoretical issues related to the characteristics of open-source intelligence, including its methods and means, as well as the legal and non-legal aspects of its use. It also presents the development of open-source intelligence in the United States, the United Kingdom, and Israel. Subsequently, the results of empirical research conducted in 2023–2024 are presented. The study employed the method of individual in-depth interviews carried out with twelve experts in the fields of security and OSINT. Based on the findings of the empirical research and the theoretical analysis undertaken, conclusions and recommendations were formulated regarding the possibilities of using open-source intelligence in ensuring the security of the Republic of Poland.

Keywords open-source intelligence, OSINT, security, open-source information, open sources, cybersecurity

Wprowadzenie

Rola i skala wykorzystania otwartych źródeł informacji systematycznie wzrasta. Wynika to z postępującej rewolucji w dziedzinie technologii informacyjnych, zwiększającej się transparentności procesów politycznych charakterystycznych dla państw demokratycznych oraz z procesów globalizacyjnych. Tym zjawiskom towarzyszy znaczny przyrost ilości informacji ze źródeł otwartych, ich zróżnicowanie oraz problem z ich analizą. W obliczu tych wyzwań zasadne staje się pytanie o rolę i znaczenie wywiadu jawnoźródłowego (*open source intelligence*, OSINT)², perspektywy jego rozwoju, a także – co najistotniejsze – możliwości zastosowania w celu zapewnienia bezpieczeństwa państwa.

² Wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego (przyp. red.).

Istotnym warunkiem bezpieczeństwa państwa jest dostęp do rzetelnych i aktualnych informacji, które stanowią jeden z jego strategicznych zasobów. Zmiany społeczno-komunikacyjne przyczyniły się do wzrostu znaczenia mediów społecznościowych jako przestrzeni wymiany informacji, kształtowania opinii publicznej oraz prowadzenia dyskursu politycznego. W konsekwencji decyzje w obszarze bezpieczeństwa państwa coraz częściej opierają się na informacjach pozyskiwanych ze źródeł otwartych, stanowiących podstawę OSINT. Wywiad jawnoźródłowy to zaplanowane i zorganizowane pozyskiwanie oraz przetwarzanie informacji, a następnie dystrybucja produktu analitycznego do określonej grupy odbiorców (decydentów) w ustalonej formie, zgodnie ze sprecyzowanym zapotrzebowaniem informacyjnym. Źródła OSINT są legalne oraz powszechnie dostępne, ale dostęp do niektórych może wymagać poniesienia nakładów.

Celem artykułu jest określenie znaczenia oraz możliwości wykorzystania wywiadu jawnoźródłowego w zapewnianiu bezpieczeństwa Rzeczypospolitej Polskiej. Przedstawione rozważania oparto na wynikach badań przeprowadzonych przez autorkę w ramach rozprawy doktorskiej pt. *Znaczenie wywiadu jawnoźródłowego w bezpieczeństwie państwa*.

Charakterystyka wywiadu jawnoźródłowego

W tradycyjnym ujęciu ukształtowanym w amerykańskiej terminologii wojskowo-wywiadowczej ze względu na rodzaj źródeł pozyskiwania informacji wyróżnia się pięć podstawowych dyscyplin wywiadowczych:

- 1) HUMINT (*human intelligence*) – wywiad osobowy (źródła osobowe),
- 2) SIGINT (*signals intelligence*) – wywiad elektromagnetyczny (źródła elektromagnetyczne),
- 3) IMINT (*imagery intelligence*) – wywiad obrazowy (źródła obrazowe),
- 4) MASINT (*measurement and signature intelligence*) – wywiad pomiarowo-badawczy (źródła badawczo-pomiarowe),
- 5) OSINT (*open source intelligence*) – wywiad jawnoźródłowy (otwarte źródła informacji).

Rozpoczęcie rozpoznania od eksploracji źródeł otwartych jest praktycznie zawsze uzasadnione oraz zazwyczaj prowadzi do obniżenia kosztów związanych z innymi kategoriami działalności wywiadowczej³. Eksperti bezpieczeństwa oceniają, że to właśnie informacje jawnoźródłowe pozyskiwane ze wszystkich możliwych ogólnie dostępnych źródeł składają się obecnie na ostateczny materiał

³ J. Konieczny, *Kryminalistyczny leksykon śledztwa*, Opole 2020, s. 336.

wywiadowczy⁴. Z tego względu zasadne jest postrzeganie wymienionych dyscyplin wywiadowczych jako nakładających się na siebie, a wywiadu jawnoźródłowego jako integralnej części wszystkich działań wywiadowczych⁵.

Wywiad jawnoźródłowy dostarcza kontekstu prowadzonego rozpoznania przez zapewnienie ogólnej wiedzy, która stanowi punkt wyjścia do określenia dalszych kierunków rozpoznania. Użyteczność OSINT wynika z możliwości szybkiego pozyskiwania informacji o rozległej tematyce. Istotną zaletą jest także to, że można zweryfikować i uzupełniać informacje o te uzyskiwane ze źródeł zamkniętych. Powszechny dostęp do źródeł otwartych umożliwia szybką reakcję na zdarzenia i skraca czas podejmowania decyzji na rzecz bezpieczeństwa. Wywiad jawnoźródłowy może dostarczać skondensowanych i precyzyjnych informacji, które pozwalają zweryfikować przyjęte założenia oraz stanowią wystarczającą podstawę do formułowania nowych hipotez analitycznych. Dodatkowym atutem takiego wywiadu jest łatwość wymiany i rozpowszechniania uzyskanej wiedzy między podmiotami odpowiedzialnymi za bezpieczeństwo. Ponadto pozwala on na prowadzenie analiz na bieżąco, co ma szczególne znaczenie w dynamicznie zmieniającym się środowisku bezpieczeństwa⁶.

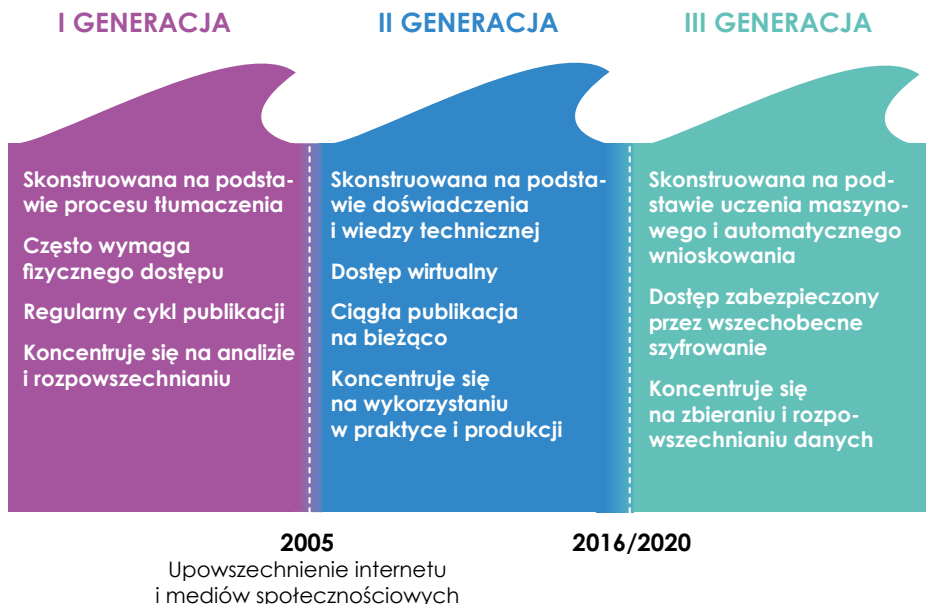
Rozwój globalnej sieci wpłynął na ewolucję wywiadu jawnoźródłowego. Wyodrębnienie kolejnych generacji OSINT jest powiązane z etapami rozwoju World Wide Web – Sieć 1.0, Sieć 2.0 i Sieć 3.0⁷. Każda z nich odzwierciedla zarówno postęp technologiczny, jak i zmieniające się potrzeby w zakresie pozyskiwania informacji jawnoźródłowych. Rysunek 1 przedstawia najważniejsze cechy kolejnych generacji OSINT.

⁴ W opracowaniu NATO wskazano, że ponad 80% informacji zawartych w końcowym materiale wywiadowczym może pochodzić ze źródeł otwartych. Jeden z przywołanych szacunków dotyczył wsparcia wywiadowczego w zakresie przeciwdziałania proliferacji. Zob. NATO, *Open Source Intelligence Reader*, February 2002, <https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf>, s. 17, 73 [dostęp: 27 III 2025]. W 2005 r. emerytowany wysoki rangą funkcjonariusz CIA William M. Nolte stwierdził, że 95–98% wszystkich informacji przetwarzanych przez społeczność wywiadowczą USA pochodzi ze źródeł otwartych. Zob. S.D. Gibson, *Open-Source Intelligence: A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, 2007, <https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/13574c5b-9ba2-4eea-8ef8-fd0d035cb6e8/content>, s. 93 [dostęp: 25 VI 2026].

⁵ M.M. Lowenthal, *OSINT the State of Art, The Artless State*, „Studies in Intelligence” 2001, t. 45, nr 3, s. 63.

⁶ S.D. Gibson, *Open Source Intelligence*, w: *The Routledge Companion to Intelligence Studies*, R. Dover, M.S. Goodman, C. Hillebrand (red.), London 2014, s. 127.

⁷ H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf, s. 39 [dostęp: 27 III 2025].



Rysunek 1. Generacje wywiadu jawnoźródłowego.

Źródło: opracowanie własne na podstawie: H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf, s. 40 [dostęp: 27 III 2025].

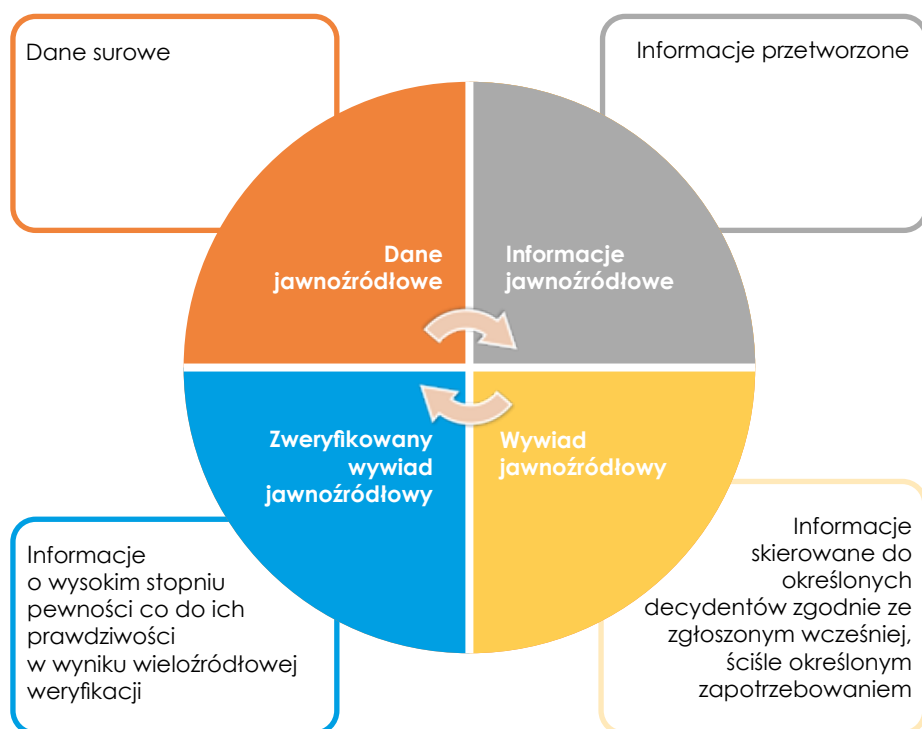
Pierwsza generacja OSINT była związana z rozwojem Sieci 1.0 w latach 90. XX w. Charakteryzowała się brakiem interaktywności oraz prostą, jednokierunkową komunikacją, której model można przyrównać do triady klasycznych mediów, tj. prasy, radia i telewizji. W tym okresie działalność wywiadowcza opierała się na gromadzeniu, monitorowaniu, analizie i rozpowszechnianiu informacji oraz tłumaczeniu materiałów zagranicznych.

Przejście do drugiej generacji OSINT nastąpiło wraz z rozwojem Sieci 2.0 i zmianą modelu komunikacji między właścicielami serwisów internetowych a ich użytkownikami. Wzrost interaktywności komunikacji oraz udziału użytkowników w tworzeniu treści sprzyjał dynamicznemu rozwojowi mediów społecznościowych i niemal ciągłej publikacji informacji. W rezultacie zwiększył się udział informacji jawnoźródłowych w prowadzonych działaniach wywiadowczych.

Trzecia generacja wywiadu jawnoźródłowego jest związana z rozwojem Sieci 3.0. Sieć ta, określana mianem semantycznej, umożliwia uczenie maszynowe i automatyczne wnioskowanie. Na tym etapie rozwoju OSINT szczególnego znaczenia nabierają również rozszerzona rzeczywistość (*augmented reality*) i psychometria,

a jednym z głównych wyzwań staje się upowszechnienie szyfrowania ograniczającego dostęp do informacji⁸.

Podstawowe pojęcia, takie jak dane jawnoźródłowe, informacje jawnoźródłowe, wywiad jawnoźródłowy oraz zweryfikowany wywiad jawnoźródłowy, oraz założenia dotyczące OSINT zostały opracowane przez amerykańskie służby specjalne i ekspertów zajmujących się działalnością rozpoznawczą współpracujących w ramach NATO. Proces przekształcania danych jawnoźródłowych w produkt wywiadowczy został przedstawiony na rysunku 2.



Rysunek 2. Proces przekształcania danych jawnoźródłowych w produkt wywiadowczy.

Źródło: opracowanie własne.

Dane jawnoźródłowe (*open source data*, OSD) to surowe dane pochodzące ze źródeł pierwotnych. Występują w formie drukowanej, przekazu radiowego i telewizyjnego, ustnych wypowiedzi publicznych lub w innych postaciach, m.in. fotografii,

⁸ Tamże, s. 40.

nagrań dźwiękowych i audiowizualnych, komercyjnych zobrazowań, prywatnej korespondencji. Dane te można klasyfikować ze względu na format na: ustrukturyzowane, częściowo ustrukturyzowane i nieustrukturyzowane.

Informacje jawnoźródłowe to dane pozyskane w pierwszym etapie, poddane odpowiedniemu przetworzeniu obejmującemu, w zależności od charakteru OSD, translację, transkrypcję, konwersję formatu, a także filtrowanie, korelację, grupowanie oraz interpretację. W wyniku integracji, oceny i analizy informacji, dokonywanych w celu odpowiedzi na konkretne zapytania, powstaje produkt wywiadowczy. Dodatkowym etapem jest wieloźródłowa weryfikacja produktu wywiadowczego przez funkcjonariuszy mających dostęp do informacji niejawnych, która pozwala ocenić stopień wiarygodności tego produktu. Wysoki poziom wiarygodności można osiągnąć również w przypadku informacji pochodzących z jawnego źródła, którego prawdziwość nie budzi wątpliwości. W ten sposób powstaje zweryfikowany produkt wywiadu jawnoźródłowego.

Źródła otwarte można klasyfikować według kanału przekazywania publicznie dostępnych informacji na: treści pozyskane z obserwacji, dokumenty i materiały drukowane, treści transmitowane przez media nadawcze oraz treści cyfrowe⁹.

Gromadzenie informacji przez obserwację polega na ich bezpośrednim pozyskiwaniu od osób fizycznych, grup osób lub podczas publicznych wydarzeń, oficjalnych kontaktów oraz obserwacji otoczenia. Umożliwia to uzyskanie aktualnych informacji niewystępujących jeszcze w sformalizowanych źródłach.

Dokumenty i materiały drukowane, obejmujące m.in. prasę, książki, raporty, dokumenty urzędowe oraz szarą literaturę, stanowią podstawowe źródło wiedzy faktograficznej i specjalistycznej, pozwalające na weryfikację oraz pogłębioną analizę informacji.

Media nadawcze, takie jak radio, telewizja oraz inne nieinternetowe publicznie dostępne transmisje, dostarczają informacji o charakterze społeczno-politycznym, gospodarczym i z dziedziny bezpieczeństwa, umożliwiając monitorowanie bieżących wydarzeń.

Publicznie dostępne treści cyfrowe obejmują wszelkie dane, które można pobierać i przetwarzać za pomocą urządzeń cyfrowych, niezależnie od ich formatu. Do tej kategorii treści należą strony internetowe, blogi, media społecznościowe oraz inne zasoby internetowe dostępne we wszystkich warstwach sieci, również w darknecie.

⁹ OSINT Foundation, *Mediums of Publicly Available Information*, Document Number: 20230304-01a, 4 III 2023 r., s. 2. Dokument jest dostępny na stronie: <https://www.osintfoundation.com/osint/Standards.asp> [dostęp: 25 VI 2026].

Skuteczność OSINT zależy od właściwej identyfikacji źródeł, doboru odpowiednich metod analizy oraz krytycznej oceny wiarygodności pozyskanych informacji. Dynamiczny rozwój źródeł otwartych prowadzi do stopniowego zacierania granic między informacjami jawnymi i niejawnymi¹⁰. Wymaga to zmiany podejścia do klasyfikacji źródeł informacji oraz metod ich analizy, a także uwzględnienia nowych wyzwań prawnych i organizacyjnych.

Metody i środki OSINT w cyberprzestrzeni

Rzeczywisty rozwój nowoczesnych technologii znacznie zwiększył efektywność i precyzję pozyskiwania informacji ze źródeł otwartych. Przyjmując klasyfikację gromadzenia informacji opartą na czterech rodzajach wykorzystywanych źródeł otwartych (obserwacja, dokumenty drukowane, media nadawcze, treści cyfrowe) należy zaznaczyć, że obecnie wywiad jawnoźródłowy obejmuje zarówno tradycyjne metody pozyskiwania informacji, jak i zaawansowane rozwiązania oparte na automatyzacji, analizie dużych zbiorów danych oraz sztucznej inteligencji. We współczesnym wywiadzie jawnoźródłowym dominującą rolę odgrywają źródła internetowe.

Pozyskiwanie informacji z internetu może być realizowane zarówno manualnie, jak i automatycznie z użyciem specjalistycznych narzędzi i skryptów. Do charakterystycznych metod cyfrowego OSINT należą: monitorowanie, wyszukiwanie, techniczny footprinting, analiza mediów społecznościowych oraz web scraping.

Monitorowanie polega na ustrukturyzowanym i systematycznym śledzeniu w określonym czasie zmieniających się treści generowanych przez stałe źródło.

Wyszukiwanie obejmuje posłużenie się wyspecjalizowanym oprogramowaniem lub stronami internetowymi do eksploracji internetu w celu pozyskania informacji odpowiadających określonym potrzebom informacyjnym.

Techniczny footprinting, inaczej odtwarzanie śladów cyfrowych, jest procesem gromadzenia dostępnych informacji na temat systemów komputerowych, infrastruktury sieciowej, technologii, usług oraz podmiotów, do których należą. Dzięki technicznemu footprintingowi można odtworzyć techniczny i organizacyjny obraz badanego podmiotu, zidentyfikować jego zasoby cyfrowe oraz rozpoznać potencjalne podatności informacyjne na podstawie źródeł otwartych.

Analiza mediów społecznościowych pozwala na identyfikację treści, relacji, nastrojów, wzorców zachowań oraz dynamiki komunikacji w środowisku cyfrowym. Ten rodzaj analizy odgrywa istotną rolę w zarządzaniu sytuacjami kryzysowymi, ponieważ umożliwia monitorowanie procesów radykalizacji, identyfikację zagrożeń oraz

¹⁰ H.J. Williams, I. Blum, *Defining Second Generation...*, s. 37.

prognozowanie trendów wpływających na bezpieczeństwo. Informacje pozyskane z mediów społecznościowych są wykorzystywane do zwalczania przestępczości i terroryzmu – wspierają profilowanie kryminalne, w tym pośrednie szacowanie osobowości, opracowanie taktyki przesłuchania oraz typowanie kandydatów do roli agenta¹¹.

Web scraping polega na automatycznym pozyskiwaniu danych z zasobów internetowych i zapisywaniu ich w systemie plików lub bazie danych w celu późniejszego wyszukiwania, przetwarzania i analizy.

Metody pozyskiwania informacji można podzielić ze względu na poziom interakcji z obiektem rozpoznania na pasywne, półpasywne i aktywne¹². Wybór właściwej metody zależy od podmiotu prowadzącego rozpoznanie, celu i charakteru działań, rodzaju pozyskiwanych informacji oraz wymagań bezpieczeństwa operacyjnego (*operations security*) i powinien zostać określony już na etapie planowania. Metody półpasywne i aktywne wymagają interakcji z badanym obiektem lub jego infrastrukturą, dlatego wykraczają poza klasyczną definicję wywiadu jawnoźródłowego opartego na pozyskiwaniu informacji bez ingerencji w obiekt rozpoznania¹³. Rekonesans pasywny stanowi podstawową metodę prowadzenia wywiadu jawnoźródłowego, z uwagi na cel gromadzenia informacji wyłącznie ze źródeł otwartych oraz konieczność zachowania wysokich standardów etycznych i bezpieczeństwa prowadzonych działań.

Informacje jawnoźródłowe mogą być również kupowane od podmiotów komercyjnych lub ich pozyskanie może być zlecone w ramach outsourcingu. Często używa się do tego programów agentowych i botów. Rozwiązania te wymagają jednak zachowania odpowiednich standardów etycznych oraz zgodności z obowiązującymi przepisami.

Ze względu na metody pozyskiwania i przetwarzania informacji jawnoźródłowych można wyróżnić cztery główne kategorie narzędzi:

- 1) językowe i tekstowe (lingwistyczne),
- 2) geoprzestrzenne,
- 3) oparte na teorii sieci (sieciowe),
- 4) wykorzystujące kryminalistykę wizualną¹⁴.

Narzędzia lingwistyczne umożliwiają analizę dużych zbiorów danych tekstowych pochodzących z wielu źródeł i języków. Są one wykorzystywane do identyfikacji

¹¹ Zob. szerzej: J. Konieczny, *Kryminalistyczny leksykon...*, s. 145, 202–203.

¹² N.A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, New York 2018, s. 14.

¹³ W Izraelu, ze względu na różnice w normach prawnych oraz uwarunkowania społeczno-historyczne, część metod półpasywnych i aktywnych jest uznawana za element wywiadu jawnoźródłowego.

¹⁴ H. Akin Ünver, *Digital Open Source Intelligence and International Security: A Primer*, „Cyber Governance and Digital Democracy” 2018, nr 8, s. 8. <https://doi.org/10.13140/RG.2.2.16242.56000>.

słów kluczowych, analizy częstotliwości ich występowania oraz wnioskowania o cechach demograficznych, poglądach i zachowaniach autorów. Analiza sentymentu oraz analiza stanowiska pozwalają określić emocjonalny wydźwięk wypowiedzi, postawy oraz intencje badanych podmiotów. Coraz większą rolę odgrywa przetwarzanie języka naturalnego (*natural language processing*) oraz uczenie maszynowe, zapewniające automatyczną analizę wielojęzycznych i nieustrukturyzowanych zbiorów danych oraz identyfikację wzorców językowych.

Narzędzia geoprzestrzenne służą do pozyskiwania i analizy informacji lokalizujących osoby, obiekty i zdarzenia w przestrzeni geograficznej, wspierając rozpoznanie sytuacji politycznej, militarnej i kryzysowej. Podstawowe metody analizy geoprzestrzennej obejmują geotagowanie, geolokację, geownioskowanie oraz georeferencjonowanie¹⁵. Pozwalają one określać położenie obiektów, odtwarzać ich przemieszczanie oraz identyfikować zależności przestrzenne. W analizach są wykorzystywane systemy informacji geograficznej, dane GPS, zobrażenia satelitarne i lotnicze, LIDAR oraz informacje publikowane w mediach społecznościowych. Integracja danych geoprzestrzennych z innymi źródłami OSINT umożliwia monitorowanie konfliktów zbrojnych, migracji ludności, sytuacji kryzysowych oraz infrastruktury krytycznej, co zwiększa świadomość sytuacyjną oraz wspiera procesy decyzyjne w obszarze bezpieczeństwa państwa.

Narzędzia sieciowe opierają się na metodach analizy relacji między osobami, organizacjami, miejscami i innymi podmiotami. Umożliwia to identyfikację struktur społecznych oraz zależności występujących w badanych sieciach. W wywiadzie jawnoźródłowym są używane przede wszystkim do analizy mediów społecznościowych przez wyszukiwanie, mapowanie i ocenę relacji między użytkownikami z wykorzystaniem metod obliczeniowej analizy sieci oraz sztucznej inteligencji. Narzędzia sieciowe znajdują zastosowanie m.in. w identyfikacji sieci terrorystycznych i przestępczych, analizie kampanii dezinformacyjnych oraz rozpoznawaniu mechanizmów oddziaływania na grupy społeczne.

Narzędzia wykorzystujące kryminalistykę wizualną służą do ekstrakcji danych z plików graficznych i wideo, umożliwiają wykrywanie zmanipulowanych obrazów oraz przeprowadzenie analizy fotogrametrycznej. Ich znaczenie wzrosło wraz z rozwojem mediów społecznościowych i ewolucją komunikacji z tekstowej na opartą na mediach. W analizie materiałów wizualnych stosuje się m.in. analizę artefaktów, fotogrametrię, analizę metadanych, porównanie fotograficzne oraz analizę cyfrową, wspieraną danymi geoprzestrzennymi, zobrażeniami satelitarnymi i materiałami z dronów. Metody te umożliwiają weryfikację autentyczności obrazów i nagrań, wykrywanie manipulacji, geolokalizację zdarzeń oraz rekonstrukcję ich przebiegu,

¹⁵ H.J. Williams, I. Blum, *Defining Second Generation...*, s. 33.

dostarczając materiału o wartości dowodowej. Rozwiązania z zakresu kryminalistyki wizualnej są szeroko wykorzystywane w działaniach wywiadowczych, dochodzeniowych oraz dokumentowaniu naruszeń praw człowieka i konfliktów zbrojnych.

Rozwój technologii informacyjnych, automatyzacji i sztucznej inteligencji znacznie zwiększył efektywność oraz precyzję wywiadu jawnoźródłowego. Umożliwił gromadzenie i automatyczną analizę ogromnych zbiorów danych, skrócił czas opracowania produktów wywiadowczych oraz podniósł ich wartość analityczną. Zintegrowane wykorzystanie różnych narzędzi OSINT ułatwia wzajemne uzupełnianie i weryfikację pozyskanych informacji, dzięki czemu można otrzymać pełniejszy i bardziej wiarygodny obraz analizowanego zjawiska. Efektywność ich użycia zależy jednak nie tylko od możliwości technologicznych, lecz także od wiedzy i praktycznych umiejętności analityka oraz właściwego doboru metod i narzędzi.

Prawne i pozaprawne aspekty wywiadu jawnoźródłowego

Wywiad jawnoźródłowy funkcjonuje w środowisku prawnym, które nie zostało dotychczas kompleksowo uregulowane ani na szczeblu krajowym, ani międzynarodowym. Brak jednoznacznych regulacji prowadzi do rozbieżności interpretacyjnych oraz zróżnicowanych praktyk stosowania OSINT. Może to ograniczać jego skuteczność i jednocześnie zwiększać ryzyko zagrożeń dla bezpieczeństwa państwa. Choć istotą OSINT jest wykorzystywanie informacji pochodzących z publicznie dostępnych źródeł, to ich agregacja za pomocą nowoczesnych narzędzi może prowadzić do identyfikacji osób fizycznych, tzw. efekt mozaiki. Powoduje to wyzwania w zakresie ochrony prywatności i danych osobowych. Aspekty prawne dotyczą również ochrony praw autorskich oraz baz danych, które mogą obejmować wykorzystywane materiały jawnoźródłowe. Dodatkowe aspekty wynikają z rosnącej roli prywatnych podmiotów prowadzących działalność OSINT, których aktywność wpływa na dotychczasowy model zarządzania informacją wywiadowczą. Kolejnym zagadnieniem jest pozyskiwanie informacji wykraczających poza zakres postawionego zapytania, co może prowadzić do naruszenia przepisów prawa oraz norm etycznych dotyczących ochrony prywatności i godności jednostki.

Rozproszenie regulacji prawnych sprawia, że normy etyczne pełnią funkcję uzupełniającą wobec prawa, wyznaczając granice pozyskiwania i analizy informacji. Automatyzacja procesów gromadzenia i analizy dużych zbiorów danych (Big Data) zwiększa znaczenie tych standardów, jednak ich dobrowolny charakter nie zapewnia skutecznego ograniczania powstających zagrożeń. Zarówno w praktyce, jak i w literaturze przedmiotu jest akcentowana pilna potrzeba opracowania spójnych

ram etycznych dla prowadzenia wywiadu jawnoźródłowego przez podmioty państwowe i prywatne¹⁶.

Inne pozaprawne czynniki, które wpływają na OSINT, to uwarunkowania metodologiczne oraz techniczne. Obejmują one m.in. zakłócenia cyklu wywiadowczego, błędy poznawcze analityków, problemy językowe oraz ograniczenia infrastruktury technicznej i bezpieczeństwa operacyjnego.

Informacje jawnoźródłowe, ze względu na swoją dostępność oraz łatwość rozpowszechniania, są szczególnie podatne na manipulacje. Najpoważniejsze zagrożenia dla wywiadu jawnoźródłowego stanowią dezinformacja i propaganda, których celem jest świadome zniekształcanie rzeczywistości, kształtowanie postaw odbiorców oraz wpływanie na procesy decyzyjne. Rozwój mediów cyfrowych oraz technologii informacyjnych znacznie zwiększył skuteczność tych działań, umożliwiając szybkie rozpowszechnianie fałszywych narracji oraz ich dostosowywanie do określonych grup odbiorców. Propaganda pełni obecnie funkcję nie tylko perswazyjną, lecz także mobilizacyjną oraz służy kształtowaniu narracji społeczno-politycznych. Dezinformacja stała się jednym z podstawowych elementów wrogich operacji informacyjnych prowadzonych zarówno przez państwa, jak i podmioty niepaństwowe. Jej celem jest destabilizacja sytuacji politycznej, społecznej i gospodarczej oraz osłabianie zaufania do instytucji państwa. Współczesne technologie, w tym sztuczna inteligencja, umożliwiają tworzenie zaawansowanych form manipulacji, takich jak fake newsy i deepfaki, których wykrywanie staje się coraz większym wyzwaniem analitycznym.

Jednocześnie wywiad jawnoźródłowy odgrywa istotną rolę w wykrywaniu i analizie kampanii dezinformacyjnych oraz propagandowych. Skuteczne przeciwdziałanie manipulacjom informacyjnym wymaga jednak posłużenia się nowoczesnymi technologiami wspierającymi analizę OSINT oraz podnoszenia kompetencji analityków i odporności społeczeństwa na dezinformację.

Rozwój wywiadu jawnoźródłowego w Stanach Zjednoczonych, Wielkiej Brytanii i Izraelu

Analiza doświadczeń Stanów Zjednoczonych, Wielkiej Brytanii oraz Izraela w zakresie wykorzystania wywiadu jawnoźródłowego na rzecz bezpieczeństwa państwa pozwala zidentyfikować dotychczasowe kierunki rozwoju OSINT w państwach

¹⁶ Etycznym aspektem wywiadu jawnoźródłowego były poświęcone międzynarodowe projekty badawcze, np. The Versatile InfoRmation Toolkit for end-Users oriented Open Sources explOitation (VIRTUOSO, 2010–2013), The Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organized crime (CAPER, 2011–2014), The Maritime Integrated Surveillance Awareness (MARISA, 2017–2020).

demokratycznych o wysoko rozwiniętych instytucjach bezpieczeństwa oraz wieloletniej praktyce w posługiwaniu się informacjami jawnoźródłowymi.

Początki zinstytucjonalizowanego wywiadu jawnoźródłowego w USA sięgają okresu II wojny światowej, kiedy utworzono Służbę Monitoringu Nadawców Zagranicznych (Foreign Broadcast Monitoring Service), którą 26 lipca 1942 r. przekształcono w Federalną Służbę Informacji Radiowej (Federal Broadcast Information Service). Instytucja ta odpowiadała za monitorowanie, tłumaczenie i analizę zagranicznych informacji pochodzących ze źródeł otwartych. W kolejnych latach rozwój OSINT wspierały m.in. Wydział Dokumentacji Zagranicznej (Foreign Documents Division) oraz Federalny Wydział Badawczy Biblioteki Kongresu (Federal Research Division). Reformy przeprowadzone po zakończeniu zimnej wojny¹⁷ oraz po zamachach z 11 września 2001 r.¹⁸ miały przełomowe znaczenie i doprowadziły do utworzenia Open Source Center, a następnie Open Source Enterprise funkcjonującego w strukturach Centralnej Agencji Wywiadowczej (Central Intelligence Agency).

W marcu 2024 r. opublikowano Strategię OSINT Wspólnoty Wywiadowczej Stanów Zjednoczonych na lata 2024–2026¹⁹, określającą kompleksową wizję, priorytety i kierunki dalszego rozwoju wywiadu jawnoźródłowego oraz działania ukierunkowane na wzmocnienie jego roli w systemie wywiadowczym. Cele strategii ujęto w czterech kluczowych obszarach:

1. Koordynacja pozyskiwania danych ze źródeł otwartych oraz rozszerzenie ich udostępniania.
2. Ustanowienie zintegrowanego zarządzania zasobami informacji jawnoźródłowych.

¹⁷ Raport Komisji do spraw Ról i Możliwości Wspólnoty Wywiadowczej Stanów Zjednoczonych (Commission on the Roles and Capabilities of the United States Intelligence Community, potocznie: komisja Aspina-Browna) z 1996 r. zawierał rekomendacje dotyczące reformy amerykańskiej Wspólnoty Wywiadowczej. Autorzy raportu podkreślili znaczenie informacji jawnoźródłowych oraz konieczność dostosowania działalności wywiadowczej do złożonych i wielowymiarowych zagrożeń. Zob. szerzej: *Preparing for the 21st Century: An Appraisal of U.S. Intelligence: Report of the Commission on the Roles and Capabilities of the United States Intelligence Community*, „American Intelligence Journal” 1995, t. 16, nr 2/3, s. 11–17.

¹⁸ Na potrzebę reformy struktury wywiadowczej Stanów Zjednoczonych, w tym utworzenia podmiotu odpowiedzialnego za wywiad jawnoźródłowy, wskazywała Narodowa Komisja ds. Ataków Terrorystycznych na Stany Zjednoczone (The National Commission on Terrorist Attacks Upon the United States, potocznie: komisja 9/11) w swoim raporcie opublikowanym w 2004 r. Zob. *The 9/11 Commission Report*, <https://www.9-11commission.gov/report/911Report.pdf> [dostęp: 15 VI 2026].

¹⁹ United States Intelligence Community, *IC OSINT Strategy 2024–2026. The INT of First Resort: Unlocking the Value of OSINT*, https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf [dostęp: 15 VI 2026].

3. Rozwój innowacji w zakresie OSINT w celu tworzenia nowych zdolności analitycznych i operacyjnych.
4. Kształcenie specjalistów oraz doskonalenie metodologii wywiadu jawno-źródłowego²⁰.

Strategia stanowi istotny etap instytucjonalizacji OSINT, wzmacniając jego integrację z działalnością Wspólnoty Wywiadowczej Stanów Zjednoczonych (United States Intelligence Community) oraz potwierdzając jego znaczenie dla procesów analitycznych i decyzyjnych.

Ewolucja wywiadu jawnoźródłowego w USA doprowadziła do jego formalizacji i profesjonalizacji oraz ugruntowania jego roli w działalności wywiadowczej.

Rozwój wywiadu jawnoźródłowego w Wielkiej Brytanii ma najdłuższą udokumentowaną historię spośród analizowanych państw. Istotną rolę w jego rozwoju odegrała działalność utworzonego w 1939 r. BBC Monitoring, odpowiedzialnego za monitorowanie, tłumaczenie i analizę zagranicznych źródeł informacji. Po zakończeniu II wojny światowej elementem brytyjskiego systemu bezpieczeństwa stała się współpraca międzynarodowa realizowana w ramach sojuszu Five Eyes²¹, umożliwiająca wymianę informacji jawnoźródłowych oraz koordynację działań wywiadowczych. Wywiad jawnoźródłowy znajduje zastosowanie również w działalności brytyjskiej policji oraz służb specjalnych, takich jak Służba Bezpieczeństwa (Security Service, MI5) i Tajna Służba Wywiadowcza (Secret Intelligence Service, MI6). Wspiera zapobieganie terroryzmowi, zwalczanie przestępczości oraz przeciwdziałanie zagrożeniom hybrydowym.

Zasady wykorzystywania informacji jawnoźródłowych przez organy ścigania w Wielkiej Brytanii określiła Krajowa Rada Szefów Policji (National Police Chiefs' Council). W swoich wytycznych wskazuje ona m.in. na konieczność przestrzegania przepisów prawa, proporcjonalność działań oraz poszanowanie prawa do prywatności i ochrony danych osobowych²². Z kolei brytyjskie Ministerstwo Obrony (Ministry of Defence) ujęło OSINT w doktrynie działalności wywiadowczej, definiując go jako informacje wywiadowcze pochodzące z informacji

²⁰ Tamże, s. 1.

²¹ Five Eye (Sojusz Pięciorga Oczu) – partnerstwo wywiadowcze Stanów Zjednoczonych, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii, którego podstawę stanowiło brytyjsko-amerykańskie porozumienie zawarte 5 marca 1946 r. Współpraca obejmuje wymianę informacji pozyskiwanych w ramach różnych dyscyplin wywiadowczych, w tym wywiadu jawnoźródłowego.

²² J. Housego, *NPCC Guidance on Open Source Investigation/Research*, April 2015, <https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/workforce-coordination-committee/2023/061-2023-07-published-npcc-guidance-osint---reserach.pdf>, s. 4–5 [dostęp: 14 VIII 2026].

publicznie dostępnych oraz innych informacji jawnych o ograniczonym dostępie lub rozpowszechnianiu²³.

Współpraca z sektorem prywatnym i środowiskiem akademickim, realizowana m.in. za pośrednictwem OSINT Hub działającego w ramach CENTRIC²⁴, sprzyja rozwojowi nowoczesnych narzędzi, kompetencji oraz innowacyjnych metod pozyskiwania i analizy informacji jawnoźródłowych. Uzupełnieniem tego modelu jest działalność wyspecjalizowanych organizacji pozarządowych i podmiotów prywatnych, takich jak Association of British Investigators oraz UK OSINT Community, promujących rozwój kompetencji, standardów oraz dobrych praktyk w zakresie OSINT. Z kolei osiągnięcia Bellingcat i BBC potwierdziły znaczenie wywiadu jawnoźródłowego w dokumentowaniu konfliktów zbrojnych, naruszeń praw człowieka oraz przeciwdziałaniu dezinformacji, m.in. w związku z agresją Rosji na Ukrainę²⁵.

Brytyjski model wywiadu jawnoźródłowego wyróżnia się podejściem łączącym rozwój aspektów organizacyjnych i legislacyjnych, współpracę międzynarodową oraz wykorzystanie potencjału sektora prywatnego i środowiska akademickiego.

Działalność wywiadowcza Izraela jest uznawana za jedną z najskuteczniejszych na świecie. Jednocześnie analiza izraelskiego modelu wykorzystania OSINT stanowi wyzwanie badawcze ze względu na ograniczoną dostępność oficjalnych informacji. To ograniczenie wynika z geopolitycznych i historycznych uwarunkowań państwa, a także możliwości celowego kształtowania przekazu oraz zniekształcania w ramach działań dezinformacyjnych informacji dostępnych w źródłach otwartych.

Analiza programu szkoleniowego dla europejskich służb wywiadowczych uruchomionego przez Mossad w 2021 r. wskazuje, że wywiad jawnoźródłowy jest intensywnie wykorzystywany w działalności operacyjnej izraelskiego wywiadu²⁶. Program podkreśla znaczenie integracji informacji jawnoźródłowych z danymi pochodzącymi z innych źródeł wywiadowczych, rozwoju nowoczesnych metod

²³ Ministry of Defence, *Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations*, 3rd Edition, August 2011, <https://www.yumpu.com/en/document/read/5888415/jdp-2-00-3rd-edition-understanding-and-intelligence-support-to-/3>, s. 2–12, pkt 227 [dostęp: 14 VIII 2026].

²⁴ OSINT Hub. *CENTRIC open source intelligence hub*, CENTRIC, <https://centric-research.co.uk/projects/osint-hub> [dostęp: 15 VI 2026].

²⁵ A. Janjeva, A. Harris, J. Byrne, *The Future of Open-Source Intelligence for UK National Security*, 2022, https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf, s. 11 [dostęp: 25 VI 2026].

²⁶ *Mossad trains European intel agents in open source spy tools analysis*, Intelligence Online, 20 VII 2022 r., <https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra> [dostęp: 18 VI 2026].

gromadzenia i analizy informacji oraz współpracy izraelskiego wywiadu z sektorem prywatnym.

Zarówno Shin Bet odpowiedzialna za bezpieczeństwo wewnętrzne, jak i Aman, czyli wywiad wojskowy, traktują OSINT jako uzupełnienie informacji pozyskiwanych z innych źródeł wywiadowczych. Przykładem skutecznego zastosowania analizy komunikacji prowadzonej za pośrednictwem mediów społecznościowych i komunikatorów internetowych było udaremnienie zamachów planowanych przez Al-Kaidę na ambasadę USA w Tel Awiwie oraz na Międzynarodowe Centrum Konferencyjne w Jerozolimie²⁷.

W ramach Amanu funkcjonuje jednostka 8200, która specjalizuje się w SIGINT. W jej strukturach utworzono komórkę Hatzav odpowiedzialną za wywiad jawnoźródłowy. Ewolucja mediów społecznościowych doprowadziła do rozszerzenia działalności Hatzav z monitorowania tradycyjnych mediów arabskich na analizę informacji publikowanych w czasie rzeczywistym w serwisach internetowych. Miało to znaczenie zarówno taktyczne, ponieważ umożliwiało monitorowanie informacji dotyczących konkretnych operacji, jak i strategiczne, gdyż pozwalało na analizę nastrojów społecznych. Hatzav rozwijał specjalistyczne narzędzia analityczne oraz model szkolenia oparty na kompetencjach językowych, znajomości mediów społecznościowych i umiejętnościach informatycznych. W 2021 r. Hatzav został zlikwidowany, a jego zadania rozproszone. Przeciwnicy tej decyzji krytykowali nadmierne poleganie na technicznych metodach pozyskiwania informacji kosztem analiz prowadzonych przez wyspecjalizowanych analityków OSINT.

Doświadczenia związane z wojną, która rozpoczęła się 7 października 2023 r., doprowadziły do odtworzenia Hatzav oraz odbudowy zdolności służb w zakresie wywiadu jawnoźródłowego. Decyzja o reaktywacji jednostki potwierdziła, że OSINT stanowi odrębną i komplementarną wobec pozostałych dyscyplin wywiadowczych formę rozpoznania. Nie są w stanie jej zastąpić zaawansowane rozwiązania technologiczne i sztuczna inteligencja, które nie uchwycą np. niuansów językowych i kulturowych, takich jak kontekst polityczny, uwarunkowania społeczne czy pamięć instytucjonalna²⁸.

Z analizy porównawczej rozwoju i wykorzystania wywiadu jawnoźródłowego w Stanach Zjednoczonych, Wielkiej Brytanii i Izraelu wynika, że wszystkie te państwa dostrzegają rosnące znaczenie informacji pochodzących ze źródeł otwartych

²⁷ M. Ginsburg, T. Staff, *Al-Qaeda planned to blow up US Embassy in Tel Aviv, Jerusalem convention center*, The Times of Israel, 22 I 2014 r., <https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/> [dostęp: 25 IV 2024].

²⁸ A. Bohbot, *IDF revives disbanded Hatzav intelligence unit amid regional threats*, The Jerusalem Post, 22 VI 2025 r., <https://www.jpost.com/israel-news/defense-news/article-858491> [dostęp: 25 VI 2026].

oraz ich istotny wpływ na bezpieczeństwo. Różnice są widoczne zarówno na płaszczyźnie definicyjnej, jak i w sposobie postrzegania wywiadu jawnoźródłowego. Stany Zjednoczone i Wielka Brytania koncentrują się na równoległym rozwoju jego aspektów organizacyjnych i legislacyjnych, podczas gdy w Izraelu OSINT pełni funkcję jedynie wspomagającą, jako element naprowadzający do podejmowania złożonych działań operacyjnych.

Jednocześnie we wszystkich analizowanych państwach obserwuje się intensywny rozwój i wykorzystanie nowoczesnych technologii, w tym sztucznej inteligencji i Big Data, co wiąże się z koniecznością dalszych inwestycji w infrastrukturę technologiczną oraz rozwój metod analitycznych. Technologie te znajdują zastosowanie odpowiednio w rozwoju narzędzi OSINT w Stanach Zjednoczonych, działaniach policyjnych i monitorowaniu zagrożeń wewnętrznych w Wielkiej Brytanii oraz integracji wywiadu jawnoźródłowego z operacjami cyberbezpieczeństwa w Izraelu.

Kolejną wspólną cechą jest rozproszenie działań i odpowiedzialności w zakresie wywiadu jawnoźródłowego między podmioty publiczne. Prowadzi to do ograniczonej współpracy między instytucjami, niedostatecznego finansowania potrzeb operacyjnych oraz zróżnicowania poziomu dostępu i metod gromadzenia danych.

Istotnym obszarem wymagającym dalszego rozwoju pozostają kompetencje w zakresie wywiadu jawnoźródłowego, przy czym w Stanach Zjednoczonych i Wielkiej Brytanii nadal są dostrzegane braki w analizie, selekcji, integracji i dystrybucji informacji jawnoźródłowych w całym cyklu wywiadowczym. Izrael rozwija te kompetencje we współpracy z sektorem prywatnym, obejmującej transfer wiedzy, technologii oraz działalność szkoleniową.

We wszystkich omówionych państwach jako kierunek rozwoju jest wskazywane wzmocnianie współpracy międzynarodowej zarówno w ramach sojuszy takich jak Five Eyes, jak i partnerstw z sektorem prywatnym, które służą wymianie informacji, koordynacji działań, rozwojowi nowoczesnych technologii oraz poprawie zdolności wywiadowczych i cyberbezpieczeństwa.

Przeprowadzona analiza wskazuje, że Stany Zjednoczone, Wielka Brytania oraz Izrael systematycznie zwiększają wykorzystanie wywiadu jawnoźródłowego, wzmacniając tym samym swoje zdolności w zakresie działań zarówno defensywnych, jak i ofensywnych.

Wykorzystanie OSINT a możliwości państwa w zakresie przeciwdziałania zagrożeniom. Wyniki badań

Celem badań przeprowadzonych przez autorkę w ramach przygotowywania rozprawy doktorskiej było pozyskanie jakościowych informacji umożliwiających

identyfikację zależności między wykorzystaniem wywiadu jawnoźródłowego a możliwościami państwa w zakresie przeciwdziałania zagrożeniom wewnętrznym i zewnętrznym. Zamierzeniem było również uzyskanie prognoz dotyczących kierunków rozwoju metod oraz środków technicznych stosowanych do pozyskiwania i analizy informacji jawnoźródłowych w celu zapewniania bezpieczeństwa państwa.

Badanie było realizowane od grudnia 2023 r. do kwietnia 2024 r., co pozwoliło na zachowanie względnie stałych warunków badawczych w odniesieniu do zarówno prawnych i pozaprawnych aspektów wykorzystania wywiadu jawnoźródłowego, uwarunkowań geopolitycznych, jak i stosowanych metod oraz środków technicznych używanych w rozpoznaniu prowadzonym z wykorzystaniem źródeł otwartych. Zastosowano metodę indywidualnych wywiadów pogłębionych (*in-depth interviews*). Do udziału w badaniu zaproszono 12 ekspertów wybranych według określonych kryteriów. Były to osoby mające specjalistyczną wiedzę oraz bogate doświadczenie zawodowe w obszarze bezpieczeństwa i OSINT. Część z nich uczestniczyła po 1990 r. w tworzeniu komórek organizacyjnych zajmujących się wywiadem jawnoźródłowym w Polsce. Wśród respondentów znaleźli się byli oraz czynni zawodowo funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego, Policji, Straży Granicznej, Jednostki Wojskowej GROM, Wojsk Obrony Terytorialnej oraz Wojsk Obrony Cyberprzestrzeni, przedstawiciel administracji rządowej zatrudniony w Departamencie Cyberbezpieczeństwa Ministerstwa Cyfryzacji, naukowiec zajmujący się problematyką wywiadu i bezpieczeństwa państwa, detektyw oraz dziennikarz śledczy pełniący wcześniej funkcję dyrektora w biurze analiz i informacji. Narzędziem badawczym był *Scenariusz wywiadu z ekspertami wykorzystującymi wywiad jawnoźródłowy w swojej pracy zawodowej*, obejmujący 11 pytań dotyczących doświadczeń respondentów związanych z wykorzystaniem OSINT oraz oceny jego znaczenia dla bezpieczeństwa państwa.

Eksperci konsekwentnie akcentowali, że wywiad jawnoźródłowy odgrywa istotną rolę w zapewnianiu bezpieczeństwa państwa, wspierając procesy decyzyjne na wszystkich poziomach zarządzania, od lokalnego po międzynarodowy. Integracja informacji jawnoźródłowych z informacjami operacyjnymi na wczesnym etapie analizy zwiększa zrozumienie problemu oraz skuteczność planowania działań. Respondenci podkreślali również, że rozwój technologii informacyjnych oraz zmieniające się środowisko bezpieczeństwa systematycznie podnoszą znaczenie OSINT, przy czym jego potencjał nie jest w pełni wykorzystywany, zwłaszcza w obszarze wspierania rozwoju gospodarczego i strategicznego państwa.

Uczestnicy badania przewidują, że zastosowanie nowoczesnych technologii, w tym sztucznej inteligencji oraz zaawansowanych narzędzi Big Data, doprowadzi do dalszego rozwoju i poprawy efektywności wykorzystania wywiadu jawnoźródłowego w sektorze bezpieczeństwa. Automatyzacja procesów pozyskiwania i analizy

informacji jawnoźródłowych, wspierana przez algorytmy uczenia maszynowego, pozwala na szersze, a przede wszystkim ciągle monitorowanie źródeł otwartych. Tym samym możliwe się staje skrócenie czasu niezbędnego do przetwarzania informacji, co podnosi zdolność identyfikacji i oceny zagrożeń oraz przyczynia się do szybszego reagowania na nie. Narzędzia oparte na sztucznej inteligencji usprawniają analizę tekstu, obrazu, dźwięku oraz innych treści multimedialnych, identyfikację wzorców, zależności i trendów, a także analizę mediów społecznościowych. Eksperti podkreślili, że w zakresie metod wykorzystywanych w OSINT szczególnego znaczenia nabierają analiza predykcyjna, analiza semantyczna oraz analiza sieci społecznościowych. Jednocześnie integracja metod i narzędzi OSINT umożliwia prowadzenie wieloaspektowej analizy informacji pochodzących z różnych źródeł i zwiększa możliwości identyfikacji zależności, wykrywania zagrożeń oraz wspierania procesów decyzyjnych w obszarze bezpieczeństwa państwa.

Analiza tych wypowiedzi wskazuje, że prawne i pozaprawne uwarunkowania prowadzenia wywiadu jawnoźródłowego mają istotny wpływ na jego skuteczność, przy czym największym wyzwaniem pozostaje manipulacja informacją, w tym działania dezinformacyjne, propaganda, fake newsy oraz smog informacyjny. Agregacja i przetwarzanie informacji jawnoźródłowych, mimo ich legalnego pozyskania, mogą prowadzić do identyfikacji osób fizycznych, co rodzi istotne wyzwania prawne i etyczne w obszarze ochrony prywatności i danych osobowych. Na efektywność wykorzystania OSINT wpływają ponadto czynniki technologiczne, ekonomiczne i organizacyjne, w szczególności ograniczony dostęp do specjalistycznych narzędzi, wysokie koszty ich wdrażania oraz niewystarczająca współpraca między instytucjami. Istotną barierę stanowi również niedostateczny poziom kompetencji analitycznych, brak doświadczenia, predyspozycji psychologicznych oraz specjalistycznych szkoleń funkcjonariuszy.

Na podstawie przeprowadzonych wywiadów można stwierdzić, że jednym z głównych kierunków rozwoju wywiadu jawnoźródłowego w państwach demokratycznych jest wzmocnienie międzynarodowej współpracy oraz wymiany informacji z państwami sojuszniczymi. Kooperacja międzynarodowa przyczynia się do zwiększenia zdolności państw do identyfikowania i oceny globalnych zagrożeń, takich jak terroryzm, cyberataki czy dezinformacja, przez co wspiera procesy decyzyjne w obszarze bezpieczeństwa. Skuteczność tej współpracy wymaga stosowania jednolitych standardów bezpieczeństwa, przestrzegania zasad etycznych oraz obowiązujących regulacji prawnych. Jednocześnie eksperci podkreślali, że współpraca międzynarodowa wymaga zachowania szczególnej ostrożności oraz starannej selekcji udostępnianych materiałów, aby nie ujawniać sojusznikom informacji mogących wskazywać na słabe strony państwa, zwłaszcza w sytuacji

zmieniających się uwarunkowań geopolitycznych i zróżnicowanych priorytetów poszczególnych sojuszników.

Wnioski i rekomendacje dla Rzeczypospolitej Polskiej

Coraz większa liczba informacji jawnoźródłowych oraz dynamiczny rozwój technologii informacyjnych powodują systematyczny wzrost znaczenia wywiadu jawnoźródłowego jako integralnego elementu procesów wywiadowczych. Zastosowanie nowoczesnych technologii zwiększa wydajność pozyskiwania, przetwarzania i analizy informacji jawnoźródłowych, jednocześnie skracając czas reakcji na zagrożenia.

Uwarunkowania prawne i pozaprawne wpływają na skuteczność OSINT. Jednym z największych wyzwań w tym obszarze pozostaje dezinformacja, której efektywne przeciwdziałanie wymaga zintegrowania działań technologicznych, organizacyjnych, prawnych oraz edukacyjnych. Brak jednolitych regulacji oraz niejednoznaczność podstawowych pojęć mogą prowadzić do niepewności prawnej i rozbieżności interpretacyjnych, co zmniejsza skuteczność wywiadu jawnoźródłowego. Warunkiem jego optymalnego wykorzystania jest więc wdrożenie rozwiązań prawnych, organizacyjnych i technicznych, które zapewnią spójność działań podmiotów odpowiedzialnych za bezpieczeństwo państwa.

Wywiad jawnoźródłowy odgrywa istotną rolę we wspieraniu procesów decyzyjnych w obszarze bezpieczeństwa państwa przez identyfikację i ocenę zagrożeń oraz budowanie świadomości sytuacyjnej. Jednocześnie współpraca i wymiana informacji z państwami sojuszniczymi, sektorem prywatnym oraz środowiskiem akademickim może prowadzić do sprawniejszego monitorowania globalnych zagrożeń, standaryzacji metod analitycznych oraz poprawy jakości produktów wywiadowczych.

Na podstawie wniosków z analizy teoretycznej oraz badań empirycznych autorka sformułowała rekomendacje dotyczące usprawnienia wykorzystania wywiadu jawnoźródłowego na rzecz bezpieczeństwa RP. Ich wdrożenie mogłoby poprawić współpracę między podmiotami odpowiedzialnymi za bezpieczeństwo państwa, zwiększyć efektywność zarządzania informacjami jawnoźródłowymi oraz ograniczyć ryzyko błędów wynikających z ich interpretacji. W konsekwencji byłoby możliwe zwiększenie zdolności państwa do wczesnego wykrywania i oceny zagrożeń, skuteczniejsze planowanie działań w obszarze bezpieczeństwa oraz lepsze wykorzystanie informacji jawnoźródłowych w procesach decyzyjnych. Rekomendacje, które mogłyby stanowić również element dalszej modernizacji struktur bezpieczeństwa, obejmują cztery obszary.

1. Uporządkowanie w polskim systemie prawnym pojęć związanych z wywiadem jawnoźródłowym

Zdefiniowanie podstawowych pojęć związanych z wywiadem jawnoźródłowym pozwoli na ograniczenie rozbieżności interpretacyjnych oraz precyzyjne określenie zakresu pozyskiwania i analizy informacji jawnoźródłowych. W konsekwencji zmniejszy się ryzyko naruszenia przepisów dotyczących ochrony danych osobowych, prawa do prywatności, praw autorskich oraz innych regulacji sektorowych. Wprowadzenie odpowiednich regulacji prawnych zapewni przejrzystość funkcjonowania wywiadu jawnoźródłowego oraz stworzy podstawy do opracowania jednolitych procedur, standardów i dobrych praktyk w zakresie prowadzenia działań OSINT, co przyczyni się do jego standaryzacji i profesjonalizacji. Spójne ramy prawne zwiększą zaufanie do wyników analiz OSINT oraz możliwości ich wykorzystania w procesach decyzyjnych. Stworzą również warunki do bezpiecznego wdrażania narzędzi bazujących na nowoczesnych technologiach, w tym sztucznej inteligencji, w analizie informacji jawnoźródłowych. Dostosowanie regulacji do norm międzynarodowych usprawni również współpracę międzynarodową w omawianym obszarze.

Ta rekomendacja jest zgodna z kierunkami rozwoju wywiadu jawnoźródłowego w Stanach Zjednoczonych oraz Wielkiej Brytanii, gdzie równolegle doskonalą się aspekty organizacyjne oraz legislacyjne.

2. Stworzenie Zespołu Koordynacyjnego ds. Wywiadu Jawnoźródłowego

Zespół podlegający bezpośrednio Prezesowi Rady Ministrów i skupiający przedstawicieli służb specjalnych oraz agencji rządowych zapewniłby koordynację działań państwa w obszarze wywiadu jawnoźródłowego. Jego funkcjonowanie przyczyniłoby się do przyspieszenia procesów pozyskiwania i analizy informacji jawnoźródłowych, wyeliminowania dublowania działań, poprawy ekonomiki operacji oraz optymalizacji wykorzystania zasobów. Opracowywanie spójnych produktów analitycznych, opartych na informacjach jawnoźródłowych pozyskiwanych przez różne podmioty, zwiększyłoby kompleksowość analiz oraz zdolność państwa do identyfikowania działań dezinformacyjnych i przeciwdziałania im.

Do zadań zespołu należałoby inicjowanie, koordynowanie oraz monitorowanie działań podejmowanych przez organy administracji rządowej w zakresie wywiadu jawnoźródłowego. Zespół realizowałby zadania związane z opracowywaniem i przekazywaniem danych wyjściowych oraz analiz jawnoźródłowych służbom specjalnym, podmiotom odpowiedzialnym za bezpieczeństwo państwa, w tym Prezydentowi Rzeczypospolitej Polskiej, Prezesowi Rady Ministrów, marszałkom Sejmu i Senatu, Radzie Ministrów według rozdzielnika, ministrowi koordynującemu służby specjalne, szefom poszczególnych służb, a także społeczeństwu. Zespół

przygotowywałyby również przeznaczone dla społeczeństwa analizy jawnoźródłowe w formie komunikatów, raportów lub cyklicznych opracowań analitycznych, udostępniane z uwzględnieniem wymogów bezpieczeństwa państwa. W ten sposób wspierałby przeciwdziałanie dezinformacji.

Istotnym obszarem jego działalności byłaby organizacja współpracy międzynarodowej w zakresie wywiadu jawnoźródłowego oraz przygotowywanie zbiorczych analiz związanych z zagrożeniami dla Polski i państw sojuszników. Do kompetencji tej grupy należałoby również opracowywanie projektów standardów etycznych, procedur prowadzenia OSINT oraz wytycznych dotyczących narzędzi wykorzystywanych do pozyskiwania i analizy informacji. Ponadto zespół przygotowywałby propozycje usprawnienia metod i narzędzi stosowanych przez podmioty publiczne oraz monitorował kierunki działań dezinformacyjnych i źródła otwarte wykorzystywane do ich generowania i rozpowszechniania.

Przedstawiona rekomendacja koresponduje z rozwiązaniami przyjętymi w *Strategii OSINT Wspólnoty Wywiadowczej Stanów Zjednoczonych na lata 2024–2026*²⁹, w której podkreślono znaczenie centralnej koordynacji, wspólnych standardów oraz integracji działań w obszarze wywiadu jawnoźródłowego.

3. Stworzenie rządowej platformy wymiany informacji jawnoźródłowych jako wspólnej przestrzeni do wyszukiwania, łączenia i promowania materiałów jawnoźródłowych

Utworzenie scentralizowanej rządowej platformy OSINT zapewni wszystkim podmiotom odpowiedzialnym za bezpieczeństwo państwa dostęp do wspólnej przestrzeni pozyskiwania, integracji i udostępniania informacji jawnoźródłowych. Zwiększy to efektywność wymiany tych informacji między podmiotami odpowiedzialnymi za bezpieczeństwo państwa, usprawni ich współpracę i wymianę dobrych praktyk. Krótszy czas identyfikacji zagrożeń i opracowywania materiałów analitycznych poprawi z kolei efektywność procesów decyzyjnych oraz zracjonalizuje wykorzystanie zasobów kadrowych, technicznych i finansowych. Zintegrowana platforma OSINT umożliwi ponadto prowadzenie kompleksowych analiz z uwzględnieniem szerszego kontekstu zagrożeń oraz zależności między nimi, wykraczających poza zakres zadań realizowanych przez poszczególne służby.

Rekomendacja ta znajduje potwierdzenie w rozwiązaniach wdrażanych w Stanach Zjednoczonych i Wielkiej Brytanii. Zarówno amerykańska koncepcja wspólnych platform OSINT powiązanych ze scentralizowanym, wielodomenowym katalogiem informacji dostępnych publicznie i komercyjnie³⁰, jak i brytyjska platforma

²⁹ United States Intelligence Community, *IC OSINT Strategy 2024–2026...*

³⁰ Tamże, s. 3.

INDEX³¹ opierają się na centralizacji zasobów, zapewnieniu interoperacyjności systemów oraz stworzeniu wspólnej przestrzeni do gromadzenia i wymiany informacji jawnoźródłowych, raportów oraz narzędzi OSINT. Rozwiązania te zmierzają do wyeliminowania dublowania działań prowadzonych przez poszczególne instytucje, ujednolicenia standardów analitycznych oraz zintensyfikowania wykorzystania nowoczesnych technologii, takich jak uczenie maszynowe i zaawansowane metody analityczne, w procesach analizy informacji. Ich implementacja stanowi ważny punkt odniesienia przy projektowaniu polskich rozwiązań systemowych w zakresie wywiadu jawnoźródłowego.

4. Utworzenie Inkubatora Innowacji Wywiadu Jawnoźródłowego

Celem inicjatywy jest rozwój współpracy między administracją publiczną, sektorem prywatnym, środowiskiem akademickim oraz społeczeństwem obywatelskim w zakresie wywiadu jawnoźródłowego. Jej efektem byłaby wymiana wiedzy i doświadczeń, rozwój innowacyjnych metod i narzędzi OSINT oraz budowanie trwałych relacji wspierających bezpieczeństwo RP.

Model ten umożliwiłby wykorzystanie wiedzy i doświadczenia byłych funkcjonariuszy służb z praktyką operacyjną oraz ekspertów z zakresu nowoczesnych technologii, którzy tworzyliby kadrę inkubatora. Synergia ich kompetencji sprzyjałaby rozwojowi innowacyjnych rozwiązań w obszarze wywiadu jawnoźródłowego.

Współpraca z sektorem prywatnym otwierałaby drogę do pozyskiwania nowoczesnych technologii oraz bezpiecznego outsourcingu wybranych procesów związanych z pozyskiwaniem i analizą informacji, przy jednoczesnej optymalizacji kosztów dzięki współfinansowaniu badań, rozwojowi technologii i innowacyjnych projektów.

Do podstawowych zadań Inkubatora Innowacji Wywiadu Jawnoźródłowego należałoby tworzenie nowych technologii i narzędzi oraz rozwijanie metod wykorzystywanych w wywiadzie jawnoźródłowym, w tym rozwój algorytmów wspierających analizę informacji jawnoźródłowych. Istotnym obszarem jego działalności, wynikającym z interdyscyplinarności OSINT, powinno być również pozyskiwanie kadr o różnicowanych kompetencjach zawodowych i doświadczeniach. Inkubator odpowiadałby również za organizację szkoleń i działań edukacyjnych skierowanych zarówno do funkcjonariuszy służb specjalnych i pracowników jednostek sektora finansów publicznych, jak i do społeczeństwa. Ponadto jego zadaniem byłaby organizacja konferencji i sympozjów na szczeblu rządowym i samorządowym oraz rozwijanie współpracy

³¹ J. Hugill, *Introducing INDEX – A cross-government digital information and data exchange*, PUBLIC, 18 X 2021 r., <https://www.public.io/blog-post/introducing-index-a-cross-government-digital-information-and-data-exchange> [dostęp: 25 VI 2026].

z sektorem prywatnym, ośrodkami akademickimi i instytucjami badawczymi w celu wspólnego opracowywania innowacyjnych rozwiązań w obszarze OSINT.

Zasadność utworzenia takiego inkubatora potwierdzają doświadczenia Izraela, gdzie powołano CyberSpark Innovation Arena. Jest to wspólne przedsięwzięcie izraelskiej administracji publicznej, środowiska akademickiego oraz sektora przemysłowego ukierunkowane na rozwój innowacji i współpracy w obszarze cyberbezpieczeństwa³². Inicjatywa ta pokazuje, że integracja potencjału administracji, nauki i przemysłu sprzyja rozwojowi kapitału ludzkiego, transferowi wiedzy i technologii oraz wzmacnianiu zdolności państwa w zakresie pozyskiwania i analizy informacji jawnoźródłowych.

Podsumowanie

Procesy wywiadowcze są ściśle związane z informacją, technologią oraz zmieniającym się środowiskiem bezpieczeństwa. Rosnąca liczba źródeł otwartych, dostępnych niejednokrotnie w czasie rzeczywistym, umożliwia szybsze reagowanie i dostarczanie odpowiedzi na bieżące potrzeby informacyjne decydentów. Współcześnie czas podejmowania decyzji jest jednym z podstawowych czynników warunkujących poziom bezpieczeństwa oraz zachowanie ciągłości działania. Informacje zdobyte w wyniku działań wywiadu jawnoźródłowego nie tylko uzupełniają informacje pozyskane drogą operacyjną, lecz także przyczyniają się do skrócenia czasu koniecznego do podjęcia decyzji. Zwiększa to skuteczność działań państwa w wymiarach defensywnym i ofensywnym.

Przedstawione uwarunkowania wskazują na potrzebę zmiany sposobu postrzegania roli OSINT przez podmioty odpowiedzialne za bezpieczeństwo państwa oraz modelu współpracy w zakresie wymiany informacji jawnoźródłowych między służbami i organami administracji publicznej. Wdrożenie kompleksowych rozwiązań systemowych umożliwiających dobrą integrację, analizę i wykorzystanie informacji pochodzących ze źródeł otwartych może się przyczynić do poprawy skuteczności prowadzonych działań i ich ekonomicznej efektywności przez ograniczenie kosztów pozyskiwania informacji.

Znaczenie wywiadu jawnoźródłowego będzie systematycznie wzrastać wraz z postępującą cyfryzacją życia oraz wzrostem ilości danych w źródłach otwartych.

³² *Prime Minister Announces National Cyber Hub*, Americans for Ben-Gurion University, 28 I 2014 r., <https://americansforbgu.org/prime-minister-announces-national-cyber-hub/> [dostęp: 27 VI 2026]; *Cyberspark*, World Economic Forum, <https://www.weforum.org/organizations/cyberspark/> [dostęp: 27 VI 2026].

W obliczu coraz bardziej złożonych zagrożeń dla bezpieczeństwa Polski zapotrzebowanie na wiarygodne i zweryfikowane informacje nigdy nie było większe. Dlatego wyzwaniem staje się pełne wykorzystanie potencjału wywiadu jawnoźródłowego dla obrony RP oraz jej strategicznych interesów.

Bibliografia

Akın Ünver H., *Digital Open-Source Intelligence and International Security: A Primer*, „Cyber Governance and Digital Democracy” 2018, nr 8. <https://doi.org/10.13140/RG.2.2.16242.56000>.

Gibson S.D., *Open Source Intelligence*, w: *The Routledge Companion to Intelligence Studies*, R. Dover, M.S. Goodman, C. Hillebrand (red.), London 2014.

Hassan N.A., Hijazi R., *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, New York 2018.

Konieczny J., *Kryminalistyczny leksykon śledztwa*, Opole 2020.

Lowenthal M.M., *OSINT the State of Art, The Artless State*, „Studies in Intelligence” 2001, t. 45, nr 3, s. 61–66.

Preparing for the 21st Century. An Appraisal of U.S. Intelligence. Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, „American Intelligence Journal” 1995, t. 16, nr 2/3, s. 11–17.

Źródła internetowe

Bohbot A., *IDF revives disbanded Hatzav intelligence unit amid regional threats*, The Jerusalem Post, 22 VI 2025 r., <https://www.jpost.com/israel-news/defense-news/article-858491> [dostęp: 25 VI 2026].

Cyberspark, World Economic Forum, <https://www.weforum.org/organizations/cyberspark/> [dostęp: 27 VI 2026].

Gibson S.D., *Open-Source Intelligence: A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, 2007, <https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/13574c5b-9ba2-4eea-8ef8-fd0d035cb6e8/content> [dostęp: 25 VI 2026].

Ginsburg M., Staff T., *Al-Qaeda planned to blow up US Embassy in Tel Aviv, Jerusalem convention center*, The Times of Israel, 22 I 2014 r., <https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/> [dostęp: 25 IV 2024].

Hugill J., *Introducing INDEX – A cross-government digital information and data exchange*, PUBLIC, 18 X 2021 r., <https://www.public.io/introducing-index-a-cross-government-digital-information-and-data-exchange/> [dostęp: 25 VI 2026].

Janjeva A., Harris A., Byrne J., *The Future of Open-Source Intelligence for UK National Security*, 2022, https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf [dostęp: 25 VI 2026].

Mossad trains European intel agents in open-source spy tools analysis, Intelligence Online, 20 VII 2022 r., <https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra> [dostęp: 18 VI 2026].

OSINT Hub CENTRIC open course intelligence hub, CENTRIC, <https://centric-research.co.uk/projects/osint-hub> [dostęp: 15 VI 2026].

Prime Minister Announces National Cyber Hub, Americans for Ben-Gurion University, 28 I 2014 r., <https://americansforbgu.org/prime-minister-announces-national-cyber-hub/> [dostęp: 27 VI 2026].

The 9/11 Commission Report, <https://www.9-11commission.gov/report/911Report.pdf> [dostęp: 15 VI 2026].

Williams H.J., Blum I., *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf [dostęp: 27 III 2025].

Inne dokumenty

Housego J., *NPCC Guidance on Open Source Investigation/Research*, April 2015, <https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/workforce-coordination-committee/2023/061-2023-07-published-npcc-guidance-osint---reserach.pdf> [dostęp: 14 VIII 2026].

Ministry of Defence, *Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations*, 3rd Edition, August 2011, <https://www.yumpu.com/en/document/read/5888415/jdp-2-00-3rd-edition-understanding-and-intelligence-support-to-3> [dostęp: 14 VIII 2026].

NATO, *Open Source Intelligence Reader*, February 2002, <https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf> [dostęp: 27 III 2025].

OSINT Foundation, *Mediums of Publicly Available Information*, Document Number: 20230304-01a, 4 III 2023 r. Dokument jest dostępny na stronie: <https://www.osintfoundation.com/osint/Standards.asp> [dostęp: 25 VI 2026].

United States Intelligence Community, *IC OSINT Strategy 2024–2026. The INT of First Resort: Unlocking the Value of OSINT*. https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf [dostęp: 15 VI 2026].

Dr Anna Nastuła

Doktor nauk o bezpieczeństwie (Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego w Warszawie), prawnik, certyfikowany audytor wiodący ISO/IEC 27001 oraz AQAP 2110:2016 i ISO 9001:2015. Inspektor ochrony danych, obsługuje podmioty publiczne i prywatne. Prowadzi szkolenia i warsztaty na temat ochrony danych osobowych i cyberbezpieczeństwa. Prelegentka podczas konferencji krajowych i międzynarodowych. Autorka publikacji naukowych z zakresu prawa i cyberbezpieczeństwa.

Kontakt: anna.nastula@arkadiapolska.com

