WOJSKOWA AKADEMIA TECHNICZNA
im. Jarosława Dąbrowskiego

ROZPRAWA DOKTORSKA
„ZNACZENIE WYWIADU JAWNOŹRÓDŁOWEGO W BEZPIECZEŃSTWIE PAŃSTWA”

mgr Anna Nastuła

Promotor: **prof. dr hab. Bogusław JAGUSIAK**

Warszawa 2025

SPIS TREŚCI

WSTĘP

Współcześnie bezpieczeństwo państwa w dużej mierze zależy od dostępu do rzetelnych i aktualnych informacji, które stanowią jedno z najważniejszych zasobów strategicznych. Informacje te, zarówno w kontekście cywilnym, jak i wojskowym, umożliwiają realizację zadań o charakterze ofensywnym i defensywnym na poziomach strategicznym, operacyjnym oraz taktycznym. Globalizacja oraz dynamiczny rozwój technologiczny, w tym sztucznej inteligencji oraz systemów satelitarnych, powodują, że dostęp do otwartych źródeł informacji nabiera coraz większego znaczenia, umożliwiając nie tylko skuteczniejszą ochronę przed potencjalnymi zagrożeniami, lecz także wyznaczając kierunki rozwoju stosunków międzynarodowych. Wskazuje to na zasadniczą rolę informacji w formowaniu współczesnych struktur politycznych oraz bezpieczeństwa państwa.

W związku z powyższym tematyka niniejszej rozprawy doktorskiej ma istotne znaczenie dla bezpieczeństwa. Celem pracy jest określenie znaczenia wywiadu jawnoźródłowego dla bezpieczeństwa państwa. W aspekcie praktycznym celem badań jest zidentyfikowanie możliwości wykorzystania wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa. Zakładanym rezultatem pracy są rekomendacje dotyczące usprawnienia wykorzystania wywiadu jawnoźródłowego na rzecz bezpieczeństwa państwa.

Praca składa się ze wstępu, sześciu rozdziałów, zakończenia, załączników: scenariusza wywiadu eksperckiego, transkrypcji przeprowadzonych wywiadów z ekspertami, zgód na publikację wywiadów oraz bibliografii, wykazu rysunków i tabel.

Rozdział pierwszy ma charakter ściśle teoretyczny i jednocześnie wprowadzający do dalszych części pracy. Po przedstawieniu uzasadnienia potrzeby podjęcia badań dokonano charakterystyki podstawowych pojęć występujących w pracy, tj. wywiadu jawnoźródłowego oraz bezpieczeństwa państwa. Następnie przedstawiono przedmiot i cel badań oraz problemy i hipotezy badawcze (główne i szczegółowe). Omówiono również organizację i przebieg badań. Rozdział ten kończy przegląd literatury przedmiotu z zakresu wywiadu jawnoźródłowego oraz nauk o bezpieczeństwie.

W rozdziale drugim podjęte zostały rozważania poświęcone charakterystyce wywiadu jawnoźródłowego oraz jego znaczeniu dla bezpieczeństwa państwa. W otwierającym ten rozdział podrozdziale przedstawiono cechy wywiadu

jawnoźródłowego oraz wyszczególniono jego generacje. Następnie scharakteryzowano klasyczny cykl wywiadowczy oraz przedstawiono schemat tego procesu dostosowany do wywiadu jawnoźródłowego. W kolejnych częściach rozdziału badawczemu oglądowi poddane zostały zagadnienia dotyczące pojęcia informacji jawnoźródłowych i ich cech oraz omówiono charakterystykę otwartych źródeł informacji i ich klasyfikację. W dalszej kolejności przedstawiono zagadnienia teoretyczne związane z pozyskiwaniem i analizą informacji jawnoźródłowych.

W rozdziale trzecim przeprowdzono analizę metod i środków stosowanych w wywiadzie jawnoźródłowym. Po dokonaniu ogólnego podziału metod pozyskiwania informacji jawnoźródłowych przedstawiono metody stosowane w cyfrowym wywiadzie jawnoźródłowym, ze szczególnym uwzględnieniem rekonesansu. Następnie zaprezentowano podział i charakterystykę środków technicznych oraz przegląd wybranych narzędzi, w tym narzędzi automatyzujących, stosowanych w wywiadzie jawnoźródłowym.

W rozdziale czwartym zamieszczono analizy poświęcone prawnym i pozaprawnym aspektom wykorzystania wywiadu jawnoźródłowego w bezpieczeństwie państwa. W początkowym fragmencie tego rozdziału przedstawiono aspekty prawne oraz etyczne dotyczące pozyskiwania i analizy informacji jawnoźródłowych. W dalszej kolejności dokonano charakterystyki aspektów metodologicznych, w tym związanych z naruszeniem cyklu wywiadowczego, występowaniem błędów poznawczych i językowych. Zaprezentowano aspekty techniczne oraz aspekty informacyjne mające bezpośredni wpływ na wykorzystanie wywiadu jawnoźródłowego w sektorze bezpieczeństwa.

W rozdziale piątym omówiono znaczenie, rolę oraz ewolucję wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa w wybranych krajach demokratycznych. Analizie i ocenie poddano rozwój wywiadu jawnoźródłowego w Stanach Zjednoczonych, w tym aspekty organizacyjne i prawne. Charakterystyka tego systemu wskazuje na jego rosnące znaczenie jako istotnego komponentu wspierającego działania na rzecz bezpieczeństwa państwa. Państwo to wytypowano ze względu na najbardziej rozbudowane formy pozyskiwania informacji jawnoródłowych. Następnie dokonano charakterystyki wywiadu jawnoźródłowego w Wielkiej Brytanii, gdzie ta forma działalności wywiadowczej ma najdłuższą udokumentowaną historię. Brytyjski model wyróżnia się rozwiniętymi procedurami oraz systemową integracją pozyskiwania i analizy informacji jawnoźródłowych w działaniach wywiadowczych

i policyjnych. Jego eksploracja umożliwia zidentyfikowanie historycznych uwarunkowań oraz ich wpływu na współczesne rozwiązania w zakresie wykorzystania wywiadu jawnoźródłowego na rzecz bezpieczeństwa państwa. W końcowej części rozdziału podjęto zagadnienia pojmowania i wykorzystania wywiadu jawnoźródłowego w Izraelu, którego działalność wywiadowcza uznawana jest za jedną z najlepszych na świecie. Charakterystyczne w tym ujęciu są innowacyjność, efektywność działań oraz ścisła współpraca między sektorem publicznym a prywatnym, które wspierają działania operacyjne i strategiczne w kontekście wyzwań bezpieczeństwa, przed jakimi staje Izrael. Wybór powyższych państw opiera się na ich reprezentatywnych podejściach do wywiadu jawnoźródłowego odzwierciedlających zróżnicowanie modeli organizacyjnych, prawnych i operacyjnych. Umożliwa to dokonanie wieloaspektowej analizy wykorzystania wywiadu jawnoźródłowego oraz sformułowanie wstępnych wniosków. Po pierwsze, w przedstawionych państwiach demokratycznych wywiad jawnoźródłowy charakteryzuje się zróżnicowaniem wynikającym ze specyfiki prawnej, geopolitycznej i kulturowej każdego z nich. Po drugie, jego efektywność zależy w dużym stopniu od integracji systemów wywiadowczych oraz współpracy z sektorem prywatnym. Po trzecie, doświadczenia analizowanych państw mogą stanowić podstawę do opracowania spójnych i efektywnych rozwiązań, które pozwolą na optymalizację wykorzystania wywiadu jawnoźródłowego na rzecz bezpieczeństwa państwa. Dalsze analizy oraz oceny tych modeli stanowią punkt wyjścia do pogłębionego badania zagadnień, umożliwiając ich odniesienie do specyficznych potrzeb i wyzwań związanych z wykorzystaniem wywiadu jawnoźródłowego w Polsce.

W początkowej części rozdziału szóstego dysertacji zawarto wyniki przeprowadzonych przez autorkę badań empirycznych, w tym charakterystykę grupy eksperckiej, wybranej m.in. pod względem charakteru i miejsca wykonywanej pracy, obszaru zainteresowań oraz doświadczenia zawodowego. Na podstawie zaprezentowanych we wcześniejszych rozdziałach wyników analiz teoretycznych oraz badań empirycznych sformułowano wnioski końcowe wynikające z pracy. W ostatniej części rozdziału przedstawiono rekomendacje dotyczące możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa.

Opracowanie to może znaleźć szczególne zastosowanie w działalności służb wywiadu i kontrwywiadu Rzeczypospolitej Polskiej, a także innych instytucji odpowiedzialnych za bezpieczeństwo państwa, takich jak Policja, Straż Graniczna czy Ministerstwo Obrony Narodowej. W obliczu współczesnych zagrożeń związanych

z działalnością służb specjalnych Federacji Rosyjskiej oraz jej sojuszników uwidacznia się konieczność konsolidacji oraz ujednolicenia współpracy zarówno na poziomie strukturalnym, jak i w zakresie bezpośrednich działań operacyjnych. Rekomendacje wynikające z przeprowadzonych badań mają na celu usprawnienie współpracy pomiędzy podmiotami oraz zwiększenie efektywności procesów decyzyjnych poprzez modernizację mechanizmów zarządzania informacjami jawnoźródłowymi, a także ograniczenie ryzyka błędów wynikających z ich interpretacji. W przypadku wdrożenia działania te mogłyby wspierać budowanie przewagi informacyjnej dzięki wczesnemu wykrywaniu potencjalnych zagrożeń, precyzyjnemu profilowaniu ryzyk oraz efektywniejszemu planowaniu operacji w obszarze bezpieczeństwa państwa.

Bieżąca polityka państwa, szczególnie w kontekście zagrożeń hybrydowych, wymaga redefinicji pojęć w zakresie ochrony informacji i cyberbezpieczeństwa, w tym wykorzystania informacji jawnoźródłowych. Na szczeblu centralnym konieczne jest uporządkowanie pojęć związanych z wywiadem jawnoźródłowym, co w istotny sposób poprawi wzajemną komunikację i współpracę poszczególnych jednostek organizacyjnych związanych z bezpieczeństwem Rzeczypospolitej Polskiej wykorzystujących bezpośrednio w swojej działalności wywiad jawnoźródłowy.

W aspekcie dokonanej analizy dla potrzeb niniejszej rozprawy doktorskiej istotny był wywiad jawnoźródłowy realizowany w obszarze bezpieczeństwa państwa.

Rozprawa doktorska została przygotowana na podstawie dogłębnej analizy literatury przedmiotu, obejmującej publikacje książkowe, artykuły naukowe, akty prawne, strategie bezpieczeństwa oraz materiały dostępne w Internecie. W pracy wykorzystano zarówno źródła polskie, jak i anglojęzyczne, w tym publikacje renomowanych wydawnictw naukowych, raporty organizacji międzynarodowych oraz artykuły z czasopism indeksowanych w międzynarodowych bazach danych. W niezbędnym zakresie poddano również analizie i ocenie materiały w innych językach, w szczególności dotyczące wykorzystania wywiadu jawnoźródłowego w Izraelu. Kompletny wykaz wykorzystanych źródeł został zamieszczony w bibliografii na końcu pracy. Scenariusz wraz z transkrypcjami wywiadów oraz zgodami na ich publikację stanowią załącznik do niniejszej dysertacji. Analizę przedstawioną w pracy uzupełniono rysunkami i tabelami, których wykaz zamieszczono w spisie treści.

W badaniach wykorzystano różnorodne metody badawcze, zarówno pierwszego, jak i drugiego rzędu. W trakcie analizy problematyki charakterystyki i ewolucji wywiadu jawnoźródłowego zastosowano metodę desk research oraz metodę

historyczno-porównawczą, polegającą na badaniu genezy oraz rozwoju zjawisk w kontekście historycznym. Zastosowanie tych metod umożliwiło identyfikację i ukazanie związków przyczynowo-skutkowych między wydarzeniami z przeszłości a współczesną sytuacją. Wykorzystano również metodę analizy instytucjonalno-prawnej, polegającą na szczegółowym badaniu aktów normatywnych tworzonych przez instytucje państwowe. Ponadto metody porównawcze, studium przypadku, wywiad ekspercki oraz metody teoretyczne, zastosowane w sposób komplementarny, pozwoliły na identyfikację podobieństw i różnic między procesami oraz instytucjami, a także na sformułowanie wniosków dotyczących zachodzących zjawisk i ich implikacji dla wywiadu jawnoźródłowego.

Zakończenie rozprawy doktorskiej zawiera podsumowanie całości przeprowadzonych badań. Odniesiono się w nim również do oceny stopnia realizacji celu badań, postawionej hipotezy oraz wskazanych problemów badawczych.

Wyrażam głęboką wdzięczność kadrze dydaktycznej Szkoły Doktorskiej Wojskowej Akademii Technicznej za inspirację oraz wsparcie, które znacząco przyczyniło się do rozwoju mojej pracy naukowej.

Serdecznie dziękuję ekspertom, z którymi miałam zaszczyt przeprowadzić wywiady w ramach niniejszej pracy naukowej. Ich cenne uwagi, wiedza oraz doświadczenie znacząco przyczyniły się do pogłębienia analizy, wzbogacenia merytorycznej części pracy oraz poszerzenia mojego spojrzenia na badane zagadnienie.

Szczególne słowa uznania oraz wdzięczności kieruję pod adresem Promotora – Pana prof. Bogusława Jagusiaka, którego merytoryczne wsparcie oraz wartościowe wskazówki okazały się nieocenione na każdym etapie tworzenia niniejszej pracy.

Szczególne podziękowania kieruję do Rodziców i Najbliższych, których pomoc, wsparcie, cierpliwość oraz niezachwiana wiara dały mi ogromną siłę do ukończenia tej dysertacji.

SPIS UŻYTYCH OZNACZEŃ I SKRÓTÓW

ACINT	rozpoznanie akustyczne (ang. *accoustic intelligence*)
ACPO	brytyjskie Stowarzyszenie Głównych Oficerów Policji Anglii, Walii i Irlandii Północnej (ang. *Association of Chief Police Officers*)
AFRINIC	Afrykańskie Centrum Informacji Sieciowej (ang. *African Network Information Centre*)
AI	sztuczna inteligencja (ang. *artificial intelligence*)
AIIP	Stowarzyszenie Niezależnych Profesjonalistów Informacji (ang. *The Association of Independent Information Professionals*)
Aman	Służba Wywiadu Wojskowego (Izrael)
APNIC	Centrum Informacyjne Sieci Azji i Pacyfiku (ang. *Asia-Pacific Network Information Centre*)
ARIN	Amerykański Rejestr Numerów Internetowych (ang. *American Registry for Internet Numbers*)
BBC	British Broadcasting Corporation
BEI	wywiad z wykorzystaniem biometrii (ang. *biometrics-enabled intelligence*)
CAI	komercyjnie dostępne informacje (ang. *commercially available information*)
CAST	Centrum Nauk Stosowanych i Technologii (ang. *Centre for Applied Science and Technology*)
CBNINT	rozpoznanie chemiczne i biologiczne (ang. *chemical and biological intelligence*)
CEH	certyfikat Certified Ethical Hacker
CENTRIC	centrum doskonalenia ds. przeciwdziałania terroryzmowi, aktywności obcych wywiadów i przestępczości zorganizowanej (ang. *Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research*)
CETaS	centrum badań politycznych *Centre for Emerging Technology and Security*
CIA	Centralna Agencja Wywiadowcza (ang. *Central Intelligence Agency*)
CIG	Centralna Grupa Wywiadowcza (ang. Central Intelligence *Group*)
COMINT	wywiad telekomunikacyjny (ang. *communications intelligence*)
COSPO	Biuro Programu Źródeł Otwartych Wspólnoty Wywiadowczej (ang. *Community Open Source Program Office*)

DARPA Agencja Zaawansowanych Projektów Badawczych Departamentu Obrony Stanów Zjednoczonych (ang. *Defense Advanced Research Projects Agency*)

DEWINT rozpoznanie broni wiązkowej (ang. *directed energy weapons intelligence*)

DOMEX wywiad z wykorzystaniem dokumentów i mediów (ang. *document and media exploitation*)

DOSIS ang. *Defence Open-Source Intelligence Service*

ELECTRO-OPTINT rozpoznanie elektro-optyczne (ang. *electro-optical intelligence*)

ELINT wywiad elektroniczny (ang. *electronic intelligence*)

EMPINT rozpoznanie impulsu elektromagnetycznego (ang. *electromagnetic pulse intelligence*)

FBIS Federalna Służba Informacji Radiowej (ang. *Federal Broadcast Information Service*)

FBMS Służba Monitoringu Nadawców Zagranicznych (ang. *Foreign Broadcast Monitoring Service*)

FEI wywiad umożliwiony analizą kryminalistyczną (ang. *forensic-enabled intelligence*)

FOCA pakiet oprogramowania typu open source FOCA (ang. *Fingerprinting Organizations with Collected Archives*)

FORD Departament Badań Ministerstwa Spraw Zagranicznych (ang. *Foreign Office Research Department*)

FRPS Służba Badań i Prasy Zagranicznej (ang. *Foreign Research and Press Service*)

GAN generatywne sieci współzawodniczące (ang. *generative adversarial networks*)

GEOINT wywiad geoprzestrzenny (ang. *geospatial intelligence*)

GIS system informacji geograficznej (ang. *geographic information system*)

GISP certyfikat *GIAC Information Security Professional*

GPS Globalny System Pozycjonowania (ang. *Global Positioning System*)

HTML język znaczników hipertekstowych (ang. *HyperText Markup Language*)

HUMINT rozpoznanie osobowe (ang. *human intelligence*)

I2P oprogramowanie I2P (ang. *Invisible Internet Protocol*)

IC Wspólnota Wywiadu (ang. *Intelligence Community*)

ICANN organizacja ICANN (ang. *Internet Corporation for Assigned Names and Numbers*)

IDI	indywidualne wywiady pogłębione (ang. *in-depth interviews*)
IMINT	rozpoznanie obrazowe (ang. *imagery intelligence*)
INCB	Izraelskie Krajowe Biuro ds. Cyberbezpieczeństwa (ang. *Israeli National Cyber Bureau*)
INCD	Izraelska Krajowa Dyrekcja ds. Cyberbezpieczeństwa (ang. *Israel National Cyber Directorate*)
INDEX	brytyjskia platforma wymiany informacji INDEX (ang. *Information and Data Exchange*)
INR	Biuro Departamentu Stanu USA ds. Wywiadu, Analiz i Prognoz Politycznych (ang. *Bureau of Intelligence and Research*)
IOSWG	Międzynarodowa Grupa Robocza ds. Otwartego Wywiadu (ang. *International Open Source Working Group*)
IP	protokół internetowy (ang. *Internet Protocol*)
IRINT	rozpoznanie podczerwieni (ang. *infrared intelligence*)
IT	technologia informacyjna (ang. *information technology*)
IoT	internet rzeczy (ang. *internet of things*)
KRS	Krajowy Rejestr Sądowy
LACNIC	Centrum Informacyjne Sieci Ameryki Łacińskiej i Karaibów (ang. *Latin American and Caribbean Internet Addresses Registry*)
LASINT	rozpoznanie laserowe (ang. *laser intelligence*)
MASINT	rozpoznanie pomiarowo-badawcze (ang. *measurement and signatures intelligence*)
MATINT	analiza materiałowa (ang. *materials intelligence*)
MI5	brytyjska Służba Bezpieczeństwa
MI6	brytyjska Tajna Służba Wywiadowcza
ML	uczenie maszynowe (ang. *machine learning*)
Mossad	Instytut ds. Wywiadu i Operacji Specjalnych (Izrael)
NATO	Organizacja Traktatu Północnoatlantyckiego
NCSA	Narodowy Urząd ds. Cyberbezpieczeństwa (ang. *National Cyber Security Authority*)
NLP	przetwarzanie języka naturalnego (ang. *natural language processing*)
NPCC	Krajowa Rada Szefów Policji w Wielkiej Brytanii (ang. *National Police Chief's Council*)
NUCINT	rozpoznanie nuklearne (ang. *nuclear intelligence*)

ODIN	Digital Investigations Network
ODNI	Biuro Dyrektora Wywiadu Narodowego (ang. *Office of the Director of National Intelligence*)
OPSEC	bezpieczeństwo operacyjne (ang. *operations security*)
OSC	Centrum Otwartych Źródeł (ang. *Open Source Center*)
OSD	dane jawnoźródłowe (ang. *open source data*)
OSE	Open Source Enterprise
OSIF	informacje jawnoźródłowe (ang. *open source information*)
OSINT	wywiad jawnoźródłowy (ang. *open-source intelligence*)
OSIS	Open Source Information System
OSS	Open Source System
PAI	publicznie dostępne informacje (ang. *publicly available information*)
RESINT	rozpoznanie oparte na badaniach (ang. *research-originating intelligence*)
RINT	rozpoznanie emisji ujawniającej (ang. *radiation intelligence*)
RIPE NCC	Centrum Koordynacyjne Europejskiej Sieci IP (fr. *Réseaux IP Européens Network Coordination Centre*)
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE z 2016 r., L 119.
RUSI	Royal United Services Institute
SCIP	Strategiczne Konsorcjum Specjalistów Wywiadu (ang. *Strategic Consortium of Intelligence Professionals*)
SEO	optymalizacja wyszukiwarek (ang. *search engine optimization*)
SI	sztuczna inteligencja
SIGINT	rozpoznanie radiowe i elektroniczne (ang. *signals intelligence*)
SOC	Security Operation Center
SOCMINT	rozpoznanie oparte na informacjach pozyskanych z mediów społecznościowych (ang. *social media intelligence*)
STIX	standard opisu i wymiany informacji o zagrożeniach STIX (ang. *Structured Threat Information eXpression*)
Szin Bet	Służba Bezpieczeństwa Ogólnego (Izrael)
TLD	domena najwyższego poziomu (ang. *top-level domain*)

TOR sieć TOR (ang. *The Onion Router*)

URI ujednolicony identyfikator zasobów (ang. *Uniform Resource Identifier*)

URINT rozpoznanie przypadkowej emisji ujawniającej (ang. *unintentional radiation intelligence*)

URL ujednolicony lokalizator zasobów (ang. *Uniform Resource Locator*)

VIRTUOSO projekt VIRTUOSO (ang. *Versatile Information Toolkit for end-Users Oriented Open-Source Exploitation*)

VPN wirtualna sieć prywatna

WAT Wojskowa Akademia Techniczna

1. METODOLOGICZNE PODSTAWY BADAŃ WŁASNYCH

1.1. Uzasadnienie podjęcia tematu

Zjawiska zachodzące we współczesnym świecie wskazują na jakościowo nową rolę, jaką informacja, procesy i systemy informacyjne zajmują w całym życiu społecznym, a zwłaszcza w sektorze bezpieczeństwa. Postęp technologiczno-informatyczny, jawność i przejrzystość procesów politycznych, charakterystyczne dla systemów demokratycznych, przemiany społeczne oraz związana z nimi większa dostępność informacji o życiu prywatnym osób, a także globalizacja, przyczyniły się do tego, że obecnie większość informacji jest dostępna publicznie, legalnie i w łatwy sposób.

Zachodzące zmiany społeczno-komunikacyjne zdynamizowały rozwój mediów społecznościowych takich jak Facebook, Twitter (obecnie platforma X), a także aplikacji mobilnych i portali internetowych, tworząc przestrzeń, w której użytkownicy mogą wchodzić w interakcje, dzielić się informacjami oraz wymieniać poglądy w czasie rzeczywistym. Platformy te nie tylko wspierają globalną komunikację, lecz także generują ogromne ilości danych, które mogą być analizowane i wykorzystywane na rzecz zapewnienia bezpieczeństwa państwa.

W rezultacie przeważająca większość podejmowanych decyzji, w tym również tych dotyczących bezpieczeństwa państwa, opiera się na informacjach jawnoźródłowych. Informacje te stanowią podstawę dla wywiadu jawnoźródłowego, zwanego również z języka angielskiego *open-source intelligence* (OSINT).

Istotą wywiadu jawnoźródłowego są zaplanowane i zorganizowane pozyskiwanie, przetwarzanie informacji oraz dystrybucja powstałego w tym procesie produktu analitycznego do określonej grupy odbiorczej (decydentów), zgodnie ze sprecyzowanym zapotrzebowaniem informacyjnym, w ustalonej formie. Informacje jawnoźródłowe mogą być pozyskiwane z rozwijających się otwartych cyfrowych źródeł informacji, takich jak media społecznościowe, otwarte bazy danych, platformy dzielenia się wiedzą, portale informacyjne, BodyNET[1] oraz internet rzeczy. Gromadzone są także z tradycyjnych otwartych źródeł, tj. publikacji drukowanych, raportów rządowych,

[1] BodyNET – bezprzewodowa sieć okolic ciała, inaczej sieć okolic ciała, która składa się z sensorów używanych do monitorowania sygnałów fizjologicznych człowieka na potrzeby spersonalizowanej opieki zdrowotnej. Źródło: *BodyNet Sensor System for Wearable Electronics*, Stanford University, https://techfinder.stanford.edu/technology/bodynet-sensor-system-wearable-electronics [dostęp: 14.05.2024].

dokumentacji prasowej oraz konferencji naukowych. Potencjał, który zawierają otwarte źródła informacji, stał się fundamentem działalności wywiadowczej dla służb i instytucji państwowych oraz podmiotów prywatnych.

Rola i skala wykorzystania otwartych źródeł informacji systematycznie rośnie w wyniku postępującej rewolucji w dziedzinie technologii informacyjnych. Dynamiczny wzrost mocy obliczeniowej, umożliwiający przechowywanie i natychmiastowe przeszukiwanie dużych ilości danych, oraz globalizacja, ułatwiająca dostęp do różnorodnych źródeł informacji na całym świecie, dodatkowo zwiększają użyteczność i wartość danych jawnoźródłowych dla operacji wywiadowczych. Wraz ze spadkiem liczby reżimów autorytarnych na świecie rosną społeczne naciski na rozliczalność działań rządowych, uzyskiwaną poprzez zwiększoną transparentność i jawność życia publicznego. Zmiany te generują poszerzanie źródeł otwartych, łatwiejszy do nich dostęp, a tym samym możliwość szerszego prowadzenie wywiadu jawnoźródłowego.

Rozwój badań nad wywiadem jawnoźródłowym uległ znacznemu przyspieszeniu po atakach 11 września 2001 roku na World Trade Center. Zmiany geopolityczne, technologiczne i społeczne doprowadziły do modyfikacji polityki z „potrzeby wiedzy" na „odpowiedzialność za dostarczanie"[2], wynikającą z konieczności szerszego dzielenia się informacjami. Widoczne stało się też odejście od tajności jako głównego parametru działań wywiadowczych, na rzecz złożoności i kompleksowości przestrzeni informacyjnej. Było to również efektem zmiany postrzegania bezpieczeństwa w sferze legislacyjnej, zwłaszcza w odniesieniu do praw i wolności jednostki. Coraz bardziej upowszechniło się przekonanie, że bezpieczeństwo jest równie ważne jak prawa i wolności jednostki, które mogą być w związku z tym ograniczane. Nastąpiło dodatkowo odejście od koncepcji ścigania wyłącznie już dokonanych naruszeń prawa na rzecz działań prewencyjnych i analizy przygotowań do potencjalnych aktów terrorystycznych. Zaakcentowano konieczność proaktywnej postawy państwa poprzez podejmowanie działań w celu zapewnienia bezpieczeństwa obywateli oraz przeciwdziałania popełnianiu przestępstw o charakterze globalnym. Działania te zrównano w znaczeniu z prawem do wolności, które z tej przyczyny mogłyby być ewentualnie ograniczone. Efekt 11 września przesunął punkt uwagi na informacje pozyskiwane ze źródeł otwartych.

[2] M.M. Lowenthal, R.M. Clark, *The Five Disciplines of Intelligence Collection*, SAGE Publications, 2016, s. 14.

Wywiad jawnoźródłowy charakteryzuje się stosowaniem pasywnych metod gromadzenia informacji, które nie wymagają uwierzytelniania do uzyskania fizycznego dostępu czy cyfrowego logowania. Główne zalety wykorzystania informacji jawnoźródłowych obejmują ich ogólną dostępność, bogactwo dostępnych danych oraz relatywnie niskie koszty ich pozyskania. Jawność ułatwia ich gromadzenie i analizę oraz przyczynia się do przyspieszenia procesów decyzyjnych na rzecz bezpieczeństwa. Dodatkowo informacje jawnoźródłowe są często dostępne w czasie rzeczywistym, co umożliwia szybkie reagowanie i dostarczanie odpowiedzi na bieżące zapotrzebowanie[3]. Współcześnie w sektorze bezpieczeństwa to właśnie czas podejmowania decyzji staje się kluczowym czynnikiem warunkującym bezpieczeństwo i ciągłość działania. Wywiad jawnoźródłowy jest wykorzystywany przez służby specjalne, organy ścigania, podmioty administracji państwowej oraz sektora prywatnego, aby odpowiadać na kluczowe pytania wywiadowcze dla swoich decydentów.

Jednym z podstawowych imperatywów, które legitymizują istnienie państwa, jest zapewnienie jego bezpieczeństwa. Zgodnie z art. 5 Konstytucji Rzeczypospolitej Polskiej: „Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolność i prawa człowieka i obywatela oraz bezpieczeństwo obywateli”[4]. Osiągnięcie tego fundamentalnego celu jest możliwe wyłącznie za sprawą efektywnie funkcjonującego systemu instytucjonalnego, który integruje zarówno mechanizmy prawne, jak i działalność organów wykonawczych odpowiedzialnych za porządek publiczny i obronność. Zgodnie z artykułem 126 ust. 2 Konstytucji Prezydent odpowiedzialny jest za ochronę suwerenności i bezpieczeństwa państwa, a także za nienaruszalność i jedność jego terytorium. Konstytucyjna odpowiedzialność za utrzymanie bezpieczeństwa państwa spoczywa również na organach administracji rządowej oraz na Radzie Ministrów. Podmiotami odpowiedzialnymi za bezpieczeństwo państwa i jego sprawną organizację są: parlament, centralne i terenowe organy administracji rządowej oraz organy samorządu terytorialnego. Realizację tych zadań wykonują zgodnie z przepisami prawa: siły zbrojne, służby, straże, a także instytucje rządowe, odpowiedzialne za zapobieganie zagrożeniom, przeciwdziałanie im oraz zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego. Podstawą dla

[3] M.M. Lowenthal wskazuje, że dostarczenie informacji wywiadowczej na czas do decydenta politycznego jest ważniejsze niż czekanie, aż wpłynie każdy skrawek danych lub papier będzie nieskazitelny, czysty i we właściwym formacie. Zob. szerzej: M.M. Lowenthal, *From Secrets to Policy* (4th ed.), CQ Press, Washington 2009, s. 92.
[4] Konstytucja Rzeczypospolitej Polskiej (Dz.U. z 1997 r. nr 78, poz. 483), art. 5.

bezpieczeństwa państwa są zatem decyzje podejmowane przez te podmioty, a ich kluczową determinantą jest dostępność wysokiej jakości informacji, relewantnych dla danego problemu, dostarczonych w optymalnym czasie, które umożliwiają skuteczne zarządzanie.

Zgodnie z art. 11 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu[5] do służb specjalnych w Polsce zalicza się: Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne. Pozyskiwanie i analizowanie informacji w celu zapewnienia bezpieczeństwa państwa należy również do podmiotów działających na podstawie odpowiednich ustaw, tj. Policji, Straży Granicznej, Straży Marszałkowskiej, Żandarmerii Wojskowej, Służby Więziennej, Służby Ochrony Państwa, Krajowej Administracji Skarbowej.

Służby specjalne pozyskują informacje z wszystkich możliwych źródeł, w tym ogólnodostępnych. Rodzaj wykorzystanego źródła determinowany jest specyfiką i obszarem działania oraz tematem prowadzonego rozpoznania. Informacje jawnoźródłowe służą do potwierdzenia treści pochodzących z niejawnych baz danych oraz pozyskanych poprzez aktywność operacyjną. Materiał jawnoźródłowy wykorzystywany jest zarówno przez wywiad cywilny, jak i wojskowy do budowania tła informacyjnego, planowania i organizacji działań zmierzających do budowania legendy operacyjnej, a także tworzenia podstaw do podejmowania złożonych czynności operacyjnych w przeciwdziałaniu bieżącym, jak i ewentualnym przyszłościowym zagrożeniom. W polskich służbach specjalnych i administracji publicznej nie ma jednolitego modelu organizacyjnego prowadzenia analiz jawnoźródłowych. Struktury te różnią się w zależności od rodzaju służb oraz działalności organów państwowych. W wojskowych służbach specjalnych przyjęty został zdecentralizowany model prowadzenia analiz jawnoźródłowych poprzez ich delegowanie do wyodrębnionych departamentów, zarządów czy biur. Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego są odpowiedzialne za uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mających znaczenie dla obronności państwa, bezpieczeństwa, zdolności bojowych sił zbrojnych Rzeczypospolitej Polskiej oraz innych jednostek organizacyjnych Ministerstwa Obrony Narodowej. Struktura obu służb pozostaje niejawna.

[5] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2002 r. nr 74, poz. 676).

Agencja Wywiadu odpowiada za uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego. W Agencji Wywiadu jednostką organizacyjną odpowiedzialną za analizę informacji jest Departament Informacyjny, który przygotowuje opracowania analityczne dla władz Rzeczpospolitej Polskiej. Agencja Bezpieczeństwa Wewnętrznego zajmuje się pozyskiwaniem, analizowaniem, przetwarzaniem i przekazywaniem właściwym organom informacji, które mogą mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. W ramach Agencji Bezpieczeństwa Wewnętrznego działa Departament Informacji, Analiz i Prognoz (Departament VIII), wyodrębniony z Biura Ewidencji i Analiz (zwanego biurem E).

Centralne Biuro Antykorupcyjne jest odpowiedzialne za zwalczanie korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także działalności godzącej w interesy ekonomiczne państwa. W swoich działaniach wykorzystuje wywiad jawnoźródłowy do identyfikacji zagrożeń mogących naruszyć interes ekonomiczny państwa, umożliwiając tym samym odpowiednio wczesne, prewencyjne informowanie organów państwowych o wykrytych zagrożeniach oraz proponowanie środków zaradczych. Za przetwarzanie i analizowanie informacji w Centralnym Biurze Antykorupcyjnym odpowiada Departament Analiz. Z uwagi na katalog ustawowych uprawnień działania Centralnego Biura Antykorupcyjnego są bardziej zbliżone do organów policyjnych niż pracy wywiadowczej. Warunkuje to metodykę analizy oraz kategorie wykorzystywanych informacji jawnoźródłowych, a także determinuje ich szersze zastosowanie.

W ramach struktury Komendy Głównej Straży Granicznej funkcjonują Zarząd ds. Cudzoziemców oraz Biuro Analityczno-Informacyjne. W ramach prowadzonej działalności Komendy Głównej Policji istotne miejsce zajmuje Gabinet Komendanta Głównego Policji, do którego zadań należy między innymi koordynowanie przygotowania materiałów na posiedzenia komisji i podkomisji parlamentarnych oraz przygotowanie analiz dotyczących funkcjonowania policji na doraźne potrzeby kierownictwa. Dodatkowo funkcjonuje Główny Sztab Policji, którego zadanie stanowi gromadzenie i analizowanie informacji o bieżących zdarzeniach i zagrożeniach na terytorium kraju oraz podejmowanie działań zapobiegawczych i eliminujących ich wystąpienie.

Procesy zmian wywołane rozwojem technologii i sposobów komunikacji spowodowały istotną reorientację w działaniach organów ścigania. W ramach prowadzonych czynności działania prokuratury związane są ze zdobywaniem i analizowaniem informacji. Przewaga otwartych źródeł informacji w przestrzeni publicznej determinuje zainteresowanie nimi tych organów w celu wspierania walki z przestępczością. Zebrane i poddane analizie informacje jawnoźródłowe mogą stanowić podstawę do inicjowania czynności sprawdzających, wszczynania postępowań przygotowawczych oraz być wykorzystywane jako ewentualny materiał dowodowy w toczących się postępowaniach. Obecnie analiza materiałów jawnoźródłowych odgrywa podstawową rolę na każdym etapie postępowania karnego[6]. Pozyskiwanie i gromadzenie informacji jawnoźródłowych w swojej definicji nie jest formą pracy o charakterze niejawnym, jednak sposób i zakres ich wykorzystania powinien być objęty klauzulami pracy niejawnej. Wynika to z faktu, że ujawnienie kierunków zainteresowań operacyjnych lub działań rozpoznawczych organów ścigania może stanowić istotną przesłankę dla działań podejmowanych przez wrogie wobec Rzeczypospolitej Polskiej służby wywiadowcze. Z tego powodu szczególne znaczenie ma zapewnienie ochrony systemów teleinformatycznych, w których przetwarzane są dane wywiadowcze, w tym jawnoźródłowe, a także skuteczne zarządzanie ryzykiem w obszarze bezpieczeństwa informacji. Ochrona ta powinna obejmować szacowanie ryzyka bezpieczeństwa informacji, wdrożenie odpowiednich procedur kontroli przestrzegania przepisów dotyczących ochrony informacji oraz regularne audyty systemów informacyjnych. Zabezpieczenie materiałów jawnoźródłowych wymaga zdefiniowania jasnych procedur klasyfikacji oraz zarządzania dostępem do informacji w sposób, który ograniczy potencjalne nadużycia i zmniejszy ryzyko naruszenia bezpieczeństwa państwa. W kontekście walki z przestępczością oraz zapewnienia bezpieczeństwa, materiały jawnoźródłowe, choć powszechnie dostępne, nabierają charakteru strategicznego, kiedy zostają zintegrowane z działaniami operacyjnymi. Dlatego ich analiza i wykorzystanie powinny być objęte ścisłą kontrolą oraz podporządkowane regulacjom ochrony informacji niejawnych, co pozwoli na minimalizację ryzyka i zwiększenie efektywności działań organów ścigania.

[6] J.D. Pogorzelski, *Wykorzystanie otwartych źródeł informacji w pracy prokuratora,* [w:] W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Wydawnictwo C.H. Beck, Warszawa 2011, s. 195.

Policja pozyskuje i przetwarza informacje związane z ochroną bezpieczeństwa i porządku publicznego, w tym zapewnieniem spokoju w miejscach publicznych oraz w środkach publicznego transportu i komunikacji, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania. Straż Graniczna gromadzi i przetwarza informacje jawnoźródłowe zgodnie z delegacją ustawową w zakresie ochrony granic, państwowej kontroli ruchu granicznego, zapobiegania i przeciwdziałania nielegalnej migracji. W tym celu wykorzystuje zarówno systemy informatyczne, które umożliwiają automatyczne pozyskiwanie i analizę informacji dostępnych w otwartych źródłach, jak i w mniejszym zakresie tradycyjne systemy polegające na przetwarzaniu informacji pozyskanych bezpośrednio przez poszczególnych funkcjonariuszy. Wykorzystanie wywiadu jawnoźródłowego w działalności Straży Granicznej jest szczególnie istotne w kontekście identyfikacji zagrożeń związanych z nielegalną migracją, monitorowaniem ruchu transgranicznego oraz wykrywania potencjalnych działań zagrażających bezpieczeństwu granic.

Służba Ochrony Państwa odpowiada za działania związane z ochroną osób i obiektów oraz rozpoznanie, przeciwdziałanie i zwalczanie wszelkich form przestępstw skierowanych przeciwko przedstawicielom władz administracji rządowej oraz osobom wchodzącym w gremium delegacji państw obcych przebywającym na terytorium Rzeczypospolitej Polskiej. Ochrona ta obejmuje również inne osoby oraz obiekty ustawowo chronione ze względu na interes państwa, w tym placówki zagraniczne Rzeczypospolitej Polskiej. W ramach realizacji tych zadań Służba Ochrony Państwa prowadzi działania operacyjno-rozpoznawcze oraz przeprowadza analizy, w tym rozpoznanie jawnoźródłowe, niezbędne do wykonywania ustawowych obowiązków. Inne podmioty zajmujące się analizą informacji, w tym jawnoźródłowych dotyczących bezpieczeństwa państwa, to między innymi Rządowe Centrum Bezpieczeństwa, które odpowiada za zapewnienie obiegu informacji w całej administracji publicznej, w tym w ministerstwach, urzędach i służbach. W jego strukturze działa komórka analityczna – Biuro Analiz i Reagowania, składające się z Centrum Operacyjno-Analitycznego oraz Wydziału Polityki Informacyjnej.

Wywiad jawnoźródłowy w Polsce prowadzony jest w sposób zdecentralizowany przez różne organy administracji rządowej, co skutkuje powielaniem działań i obniżeniem efektywności ekonomicznej tych operacji. Taka struktura utrudnia kompleksową analizę pozyskanych informacji jawnoźródłowych. Poszczególne służby koncentrują się tylko na informacjach niezbędnych im do realizacji własnych zadań,

pomijając często szerszy kontekst zagrożeń oraz ich wzajemne powiązania. Dodatkowo rozbieżności terminologiczne i interpretacyjne, w tym wymienne stosowanie pojęć „wywiad jawnoźródłowy" i „biały wywiad", a także brak odpowiednich regulacji prawnych ograniczają skuteczność działań opartych na tej formie wywiadu. Pełne wykorzystanie potencjału wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa wymaga opracowania spójnych i kompleksowych rozwiązań systemowych, które umożliwią efektywną integrację oraz analizę informacji z otwartych źródeł.

Międzynarodowe organizacje aktywnie wykorzystują wywiad jawnoźródłowy do wspierania operacji prowadzonych na rzecz bezpieczeństwa. Działania Organizacji Traktatu Północnoatlantyckiego (NATO) oraz Komisji Europejskiej, w tym Wspólnego Centrum Badawczego, w zakresie pozyskiwania i analizowania informacji jawnoźródłowych stały się wzorem efektywnego prowadzenia wywiadu jawnoźródłowego. Tego typu inicjatywy umożliwiają szybsze reagowanie na sytuacje kryzysowe, wzmacnianie odporności infrastruktury krytycznej oraz skuteczne odpowiadanie na nowe wyzwania technologiczne oraz geostrategiczne.

Budowanie systemowej odporności, będące jednym z priorytetów wszystkich państw członkowskich Sojuszu Północnoatlantyckiego, wynika bezpośrednio z art. 3 Traktatu Północnoatlantyckiego. Przepis ten zobowiązuje państwa NATO do rozwijania zdolności indywidualnych i zbiorowych, co znajduje odzwierciedlenie w strategicznym wykorzystaniu wywiadu jawnoźródłowego oraz współpracy międzynarodowej w obliczu dynamicznie zmieniających się zagrożeń.

Wiele krajowych organów ścigania posiada specjalne jednostki analizy jawnoźródłowej. W Europie Interpol i Europol utworzyły komórki wywiadu jawnoźródłowego. W Stanach Zjednoczonych zarówno federalne, jak i lokalne agencje wywiadowcze oraz organy ścigania systematycznie wykorzystują wywiad jawnoźródłowy jako integralną część swoich działań, co umożliwia bardziej efektywne przeciwdziałanie zagrożeniom bezpieczeństwa.

Wymiana i współpraca w zakresie informacji jawnoźródłowych wspierają i doskonalą bezpieczeństwo państw współpracujących, umożliwiając bardziej efektywne przeciwdziałanie zagrożeniom oraz szybsze reagowanie na sytuacje kryzysowe.

Rozwój cyberprzestrzeni spowodował, że bezpieczeństwo państwa jest obecnie zależne od technologii i infrastruktury informatycznej.

Odporność państwa wzmacniana jest zarówno poprzez zastosowanie technologii

cyfrowych umożliwiających skuteczne reagowanie na sytuacje kryzysowe (tzw. odporność cyfrowa), jak i rozwój cyberodporności, która obejmuje zdolność do przeciwdziałania zagrożeniom w cyberprzestrzeni. Jednym z istotnych wymiarów bezpieczeństwa państwa pozostaje również odporność społeczna, ukierunkowana na przeciwdziałanie dezinformacji oraz zagrożeniom hybrydowym, w tym cyberatakom. Odporność tę wspierają działania takie jak rozwijanie kompetencji w zakresie bezpiecznego współużytkowania cyberprzestrzeni oraz fact-checking, czyli proces, który ma na celu zweryfikowanie pozyskanych informacji. Przykładem znaczenia tych działań jest rosyjska inwazja na Ukrainę, która wykroczyła poza domenę militarną, obejmując również wrogie działania w cyberprzestrzeni i operacje dezinformacyjne, stanowiące istotny element współczesnej sztuki wojennej.

Cyberprzestrzeń, jako wirtualna sieć powiazań elementów o charakterze technicznym, technologicznym i społecznym, uznana została za kolejne pole walki – obok lądu, morza, przestrzeni powietrznej i kosmicznej[7]. Działania w cyberprzestrzeni mogą wywoływać nie tylko zakłócenia w sferze wirtualnej, ale również skutki kinetyczne, co stanowi szczególne zagrożenie dla funkcjonowania obiektów infrastruktury krytycznej państwa. Wywiad jawnoźródłowy dostarcza podmiotom odpowiedzialnym za bezpieczeństwo państwa informacji umożliwiających podejmowanie działań prewencyjnych wobec zagrożeń takich jak sabotaż, szpiegostwo, terroryzm, przestępczość zorganizowana, działania ugrupowań ekstremistycznych czy dezinformacja. Możliwość pozyskiwania danych o zasięgu międzynarodowym przy znacznie niższych kosztach i mniejszym ryzyku oznacza, że informacje, które wcześniej były dostępne jedynie za pośrednictwem innych metod wywiadowczych, są teraz łatwiej osiągalne.

Kluczową przesłanką do podjęcia badań nad znaczeniem wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa jest aktualna potrzeba zarządzania bezpieczeństwem przez proaktywne pozyskiwanie i analizę informacji jawnoźródłowych. Pozyskiwanie wiedzy o złożonej rzeczywistości politycznej

[7] W polskim systemie prawnym cyberprzestrzeń została zdefiniowana w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r. nr 64, poz. 565) jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami. Tożsame definicje występują w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2002 r. nr 156, poz. 1301), ustawie z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. z 2002 r. nr 113, poz. 985) oraz ustawie z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 r. nr 62, poz. 558).

i społecznej stanowi priorytet, który warunkuje bezpieczeństwo państwa, zarówno wewnętrzne, jak i w relacjach międzynarodowych. Rzetelny produkt wywiadowczy optymalizuje procesy decyzyjne, zmniejszając niepewność i umożliwiając bardziej skuteczne reagowanie na nowe zagrożenia.

Uzasadnienie wyboru tematu dysertacji stanowi również potrzeba rekonceptualizacji wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa, biorąc pod uwagę dynamiczne zmiany technologiczno-informacyjne, rosnące upowszechnienie procesów generowania i dystrybucji informacji oraz rozwój metod i środków ich analizy. Do czynników, które wpłynęły na wybór tematu rozprawy, zalicza się też ograniczoną liczbę badań i podjętych analiz dotyczących tej problematyki.

Motywacją do podjęcia badań jest również doświadczenie autorki związane z pełnieniem funkcji inspektora ochrony danych osobowych w pionach bezpieczeństwa informacji oraz wykładowcy akademickiego z zakresu cyberbezpieczeństwa, technik wywiadu jawnoźródłowego oraz bezpieczeństwa informacji. Jako uczestnik międzynarodowych kursów w omawianym obszarze autorka dostrzega znaczącą potrzebę poszerzania wiedzy na temat niniejszej dysertacji w polskojęzycznej literaturze naukowej.

1.2. Charakterystyka podstawowych pojęć

W pracy występują dwa podstawowe pojęcia wymagające wyjaśnienia: „wywiad jawnoźródłowy" i „bezpieczeństwo państwa". W celu właściwego zrozumienia terminu „wywiad jawnoźródłowy" omówiono różne pojęcia jemu bliskoznaczne, takie jak „biały wywiad" i „wywiad otwarty". Natomiast „bezpieczeństwo państwa" wyjaśnione zostało w drodze analizy dwóch podstawowych terminów, które je tworzą, tj. „bezpieczeństwa" oraz „państwa".

W literaturze *intelligence studies* brakuje zgody odnośnie do jednoznacznej definicji samego pojęcia „wywiad". Jest on rozpatrywany najczęściej w trzech płaszczyznach jako wiedza, aktywność i organizacja[8]. Na potrzeby niniejszej dysertacji przyjęto określenie „wywiadu" jako działalności podmiotu polegającej na opracowaniu informacji, która stanowi wsparcie procesu decyzyjnego.

[8] M.A. Kamiński, *Ewolucja wywiadu jako instytucji państwa*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2021, s. 66–79.

Definicja wywiadu jawnoźródłowego kształtowała się na płaszczyźnie wojskowej oraz cywilnej. Było to wynikiem historycznego rozwoju otwartych źródeł informacji, zwiększenia ich ilości oraz dostępności, już nie tylko dla służb specjalnych, organów ścigania, sił zbrojnych, administracji publicznej, ale również dla sektora prywatnego. Na gruncie polskiej literatury przedmiotu istnieje dychotomia pojęciowa, w obrębie której zamiennie z pojęciem „wywiad jawnoźródłowy" funkcjonuje pojęcie „biały wywiad". Jedną z przyczyn takiego stanu rzeczy jest brak regulacji w ustawodawstwie polskim definiujących pozyskiwanie i analizę jawnoźródłową. Określenie „biały wywiad" zostało wprowadzone w celu zróżnicowania pozyskiwania informacji z otwartych źródeł od działalności wywiadowczej wykorzystującej źródła operacyjne, czyli tzw. czarnego wywiadu[9]. Rozwój otwartych źródeł informacji oraz postęp w zakresie ich technicznej analizy wygenerowały potrzebę uporządkowania pojęciowego. W zagranicznej literaturze przedmiotu, aktach legislacyjnych oraz wyróżnionych dyscyplinach wywiadowczych sformułowano pojęcie „wywiad jawnoźródłowy – OSINT", które stopniowo zaczęło przenikać do polskich opracowań dotyczących analizy informacji i służb specjalnych oraz wypierać sformułowanie „biały wywiad". W *Wielkim leksykonie tajnych służb świata* J. Larecki definiuje tę metodę pracy wywiadowczej w odniesieniu do źródła jako „wywiad ze źródeł jawnych", który polega na zbieraniu, gromadzeniu, studiowaniu i analizie zagranicznych materiałów, publikowanych oficjalnie lub ogólnie dostępnych. Określany jest również jako wywiad bezagenturalny, publiczny, jawny, pasywny oraz monitoring jawnych źródeł informacji[10].

Termin „wywiad jawnoźródłowy" (ang. *open-source intelligence*, OSINT), zgodnie z nomenklaturą wywiadu amerykańskiego, odnosi się do określonego źródła informacji. Źródła wywiadowcze służą do wytwarzania nieprzetworzonych danych, które mogą być dalej przetwarzane podczas kolejnych etapów cyklu wywiadowczego w celu uzyskania materiału wywiadowczego. Biuro wywiadu Stanów Zjednoczonych definiuje wywiad jawnoźródłowy jako pozyskiwanie informacji z publicznie dostępnych źródeł, które są gromadzone, wykorzystywane i rozpowszechniane

[9] Zob. szerzej: T.R. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*, [w:] K. Liedel, P. Piasecka (red.), *Rola mediów w przeciwdziałaniu terroryzmowi*, Collegium Civitas Press, Warszawa 2009, s. 81 oraz G. Dobrowolski, W. Filipkowski, M. Kisiel-Dorohinicki, W. Rakoczy, *Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu*, [w:] L. Paprzycki, Z. Rau (red. nauk.), *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, Wyd. Wolters Kluwer, Warszawa 2009, s. 279.
[10] J.H. Larecki, *Wielki leksykon tajnych służb świata*, wyd. 2, Oficyna Wydawnicza RYTM Sp. z o.o., 2017, s. 945.

w określonym wymiarze czasowym odpowiednim odbiorcom w celu spełnienia konkretnych wymagań wywiadowczych[11]. Definicja zaproponowana w publikacjach Sojuszu Północnoatlantyckiego kładzie nacisk na ścisłe określenie zapotrzebowania, a przez to sprofilowanie podejmowanych działań wywiadowczych. Wywiad jawnoźródłowy rozumiany jest jako zaplanowane pozyskiwanie informacji, selekcjonowanie, wnioskowanie i ich dystrybucję do określonej grupy odbiorców, zgodnie z założeniami określonymi przez składającego zapytanie (ang. *request for information*, RFI). W wywiadzie jawnoźródłowym stosowane są zweryfikowane metody pracy wywiadowczej, których wynikiem jest jawnoźródłowy materiał wywiadowczy[12]. Wywiad jawnoźródłowy stanowi zatem zaplanowane działanie polegające na gromadzeniu informacji ze źródeł otwartych, czyli nieobjętych ochroną. Źródła OSINT-u w swej specyfice są jawne, legalne i ogólnodostępne, mimo, że w niektórych przypadkach mogą to być źródła wymagające opłaty za dostęp do usługi lub bazy danych. Takie też pojmowanie wywiadu jawnoźródłowego przyjęte zostało w niniejszej pracy.

W celu ukazania wartości i cech wywiadu jawnoźródłowego istotne jest jego umiejscowienie w środowisku różnorodnych rodzajów rozpoznania. W ujęciu procesowym ukształtowanym w amerykańskiej terminologii wojskowo-wywiadowczej wymienia się tradycyjnie pięć rodzajów rozpoznania wyróżnionych ze względu na metodę i źródło informacji oraz postawiony problem. Dyscypliny określane są według schematu zbudowanego z dwóch akronimów. Pierwszy wskazuje zakres przedsięwzięć, skoncentrowany wokół problemu, np. otwarte źródła informacji – *open-source*, drugi zaś pochodzi od terminu *intelligence*, tj. końcówka „INT" (OSINT – wywiad jawnoźródłowy). Wyróżnione dyscypliny to:

- **HUMINT** (ang. *human intelligence*) – rozpoznanie osobowe, polega na pozyskiwaniu informacji ze źródeł osobowych poprzez typowe działania wywiadowcze, rozpoznanie dyplomatyczne lub poprzez jawne kontakty z osobami, mogącymi udzielić informacji;
- **SIGINT** (ang. *signals intelligence*) – rozpoznanie radiowe i elektroniczne (wywiad radiowy i elektroniczny), polega na pozyskaniu i analizie informacji pochodzących ze środków łączności, radarów oraz urządzeń pomiarowych z wykorzystaniem

[11] Office of the Director of National Intelligence – United States of America, *U.S. National Intelligence – An Overview 2011*, 2011, https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf [dostęp: 18.11.2021].
[12] *NATO Open-Source Intelligence Handbook*, Norfolk 2001, s. 2.

zarówno odbiorników naziemnych, satelitów, jak i jednostek pływających oraz powietrznych. Wywiad radiowy i elektroniczny dzieli się na dwie specjalistyczne subdyscypliny: COMINT (ang. *communications intelligence* – wywiad telekomunikacyjny) oraz ELINT (ang. *electronic intelligence* – wywiad elektroniczny);

- **IMINT** (ang. *imagery intelligence*) – rozpoznanie obrazowe, polega na analizie i interpretacji technicznych, geograficznych danych zawartych w obrazach satelitarnych lub lotniczych, danych z radiolokatorów, przyrządów elektrooptycznych, pracujących w podczerwieni i termowizyjnych oraz innych urządzeń obrazujących[13]. W rozpoznawaniu obrazowym można wyróżnić: GEOINT (ang. *geospatial intelligence* – wywiad geoprzestrzenny);
- **MASINT** (ang. *measurement and signatures intelligence*) – rozpoznanie pomiarowo-badawcze, polega na analizie ilościowej i jakościowej danych pozyskanych z różnych źródeł za pomocą czujników pomiarowych w celu określenia cech specyficznych dla źródeł przechwytywanego sygnału. Można wyróżnić subdycypliny MASINT-u w zależności od obszaru rozpoznania[14]: RINT/URINT (ang. *unintentional radiation intelligence* – przypadkowej emisji ujawniającej), IRINT (ang. *infrared intelligence* – podczerwieni), ACINT (ang. *accoustic intelligence* – akustyczne), NUCINT (ang. *nuclear intelligence* – nuklearne), EMPINT (ang. *electromagnetic pulse intelligence* – impulsu elektromagnetycznego), CBINT/CBNINT (ang. *chemical and biological intelligence* – chemiczne i biologiczne), DEWINT (ang. *directed energy weapons intelligence* – broni wiązkowej), ELECTRO-OPTINT (ang. *electro-optical intelligence* – elektro-optyczne, w tym LASINT – (ang. *laser intelligence* – laserowe), MATINT (ang. *materials intelligence* – analiza materiałowa), oraz *spectroscopic intelligence* (analiza spektroskopowa) i *effluent/debris collection* (analiza zanieczyszczeń atmosferycznych);
- **OSINT** (ang. *open-source intelligence*) – rozpoznanie jawnoźródłowe, dotyczy danych pochodzących zarówno z publicznie dostępnych informacji, jak i innych

[13] Definicja de iure została formalnie zapisana w: 10 U.S.C. § 467: US Code – Section 467: *Definitions*, https://uscode.house.gov/, s. 198 [dostęp: 2.02.2023].
[14] K. Matela, *Wybrane aspekty systemów wywiadu, obserwacji i rozpoznania (ISR)*, „Wiedza Obronna" 2021, vol. 276, no. 3, s. 238–253 oraz Federation of American Scientists, Intelligence Resource Program, *Measurement and Signature Intelligence (MASINT)*, https://irp.fas.org/program/masint.htm [dostęp: 25.06.2023].

jawnych informacji o ograniczonym rozpowszechnianiu lub dostępie[15]. Jako subdyscyplinę wywiadu jawnoźródłowego klasyfikuje się **SOCMINT**[16] (ang. *social media intelligence*), czyli rozpoznanie oparte na informacjach pozyskanych z mediów społecznościowych w formie skanowania, pomiaru i analizy. SOCMINT umożliwia monitorowanie dynamiki i nastrojów społecznych, identyfikowanie potencjalnych zagrożeń oraz analizę działalności osób lub organizacji. Kolejną subdyscypliną wywiadu jawnoźródłowego jest rozpoznanie oparte na badaniach – **RESINT** (ang. *research-originating intelligence*)[17]. To forma wywiadu skupiona na analizie wielu różnorodnych zbiorów danych oraz raportów analitycznych, ich porównywaniu, wykrywaniu powiązań pomiędzy rozproszonymi danymi, porównywaniu oraz wykorzystywaniu efektu synergii zarówno pomiędzy poszczególnymi dyscyplinami wywiadowczymi, jak i źródłami danych.

Wraz z rozwojem technologii powstają nowe źródła informacji, które są przyczynkiem do wyodrębniania kolejnych dyscyplin wywiadowczych. Doktryna wywiadu armii amerykańskiej z 2018 roku wskazała cztery dyscypliny wspierające[18]:

1. **BEI** (ang. *biometrics-enabled intelligence*) – wywiad z wykorzystaniem biometrii, którego celem jest ustalenie tożsamości na podstawie danych biometrycznych;
2. **CYBER-INT** (ang. *cyber intelligence*) – wywiad z wykorzystaniem cyberprzestrzeni i pola elektromagnetycznego, którego celem jest pozyskanie wiedzy o zagrożeniach i podatnościach informatycznych systemów komunikacyjnych, dzięki czemu możliwe jest bardziej precyzyjne prognozowanie zagrożeń w cyberprzestrzeni oraz ostrzeganie, obniżanie poziomu ryzyka i wsparcie rozwiązań organizacyjnych i technologicznych wzmacniających cyberbezpieczeństwo;
3. **DOMEX** (ang. *document and media exploitation*) – wywiad z wykorzystaniem dokumentów i mediów;
4. **FEI** (ang. *forensic-enabled intelligence*) – wywiad umożliwiony analizą kryminalistyczną, prowadzony jest w celu ustalenia relacji między osobami, zdarzeniami, miejscami i przedmiotami.

[15] Department of the Army, *Complementary Intelligence Capabilities, Army Doctrine Publication (ADP 2-0) for Army Intelligence Activities*, rozdz. 4, 2018, s. 4–7, https://irp.fas.org/doddir/army/adp2_0.pdf [dostęp: 25.06.2023].
[16] A.N. Liaropoulos, *The Challenge of Social Media for the Intelligence Community*, „Journal of Mediterranean and Balkan Intelligence" 2013, nr 1(1), s. 6.
[17] A.D.M. Svendsen, *Introducing RESINT: A Missing and Undervalued "INT" in All-Source Intelligence Efforts*, „International Journal of Intelligence and CounterIntelligence" 2013, vol. 26, nr 4.
[18] Department of the Army, op. cit.

Narzędzia i metody pozyskiwania informacji w wymienionych wyżej kategoriach wywiadu były zbieżne z tymi wykorzystywanymi w wywiadzie jawnoźródłowymi m.in. przez otwarty dostęp samych źródeł. Sposób definiowania dyscyplin wywiadowczych jest istotny, gdyż decyduje o tym, jak informacje wywiadowcze są oceniane pod kątem wiarygodności i wagi przez analityków w całościowej analizie danych pozyskanych ze wszystkich źródeł (ang. *all source intelligence*). Jednakże podział pomiędzy dyscyplinami wywiadu nie jest jednoznaczny. Bardziej efektywnym i odzwierciedlającym schematem jest postrzeganie dyscyplin wywiadowczych jako nakładających się na siebie[19]. W wywiadzie jawnoźródłowym informacje, o ile tylko są publicznie dostępne, pozyskiwane są ze wszelkich możliwych źródeł, których podział stanowi podstawę do klasyfikacji dziedzin wywiadowczych. Zarówno w GEOINT, jak i OSINT pozyskiwane są dane obrazowe, np. poprzez satelity komercyjne, które zapewniają możliwości obrazowania z góry na poziomie porównywalnym z możliwościami historycznie dostępnymi jedynie dla służb specjalnych. Gromadzenie danych w mediach społecznościowych, obejmujące elektroniczne gromadzenie dużej liczby rekordów, które są przesiewane przy użyciu środków technicznych w celu identyfikacji interakcji lub komunikacji, może być celem zarówno wywiadu jawnoźródłowego, jak i SIGINT-u. W wywiadzie jawnoźródłowym informacje pozyskiwane są też ze źródeł osobowych (podobnie: HUMINT) poprzez analizę ekspercką czy konferencje. Działalność wywiadowcza oparta na otwartych źródłach stanowi integralną część wszystkich działań wywiadowczych. Na rysunku 1.1, z uwagi na różne cele wywiadowcze i charakter eksplorowanych źródeł, przedstawiano nakładający się charakter dyscyplin wywiadowczych.

Informacje jawnoźródłowe mogą być pozyskiwane w sposób pasywny, półpasywny i aktywny, w zależności od poziomu interakcji z obiektem rozpoznania. Metody półpasywne i aktywne wymagają pośredniego lub bezpośredniego zaangażowania, co może wiązać się z ingerencją w obiekt rozpoznania. Ze względu na tę specyfikę, klasyfikuje się je jako wykraczające poza klasyczną definicję wywiadu jawnoźródłowego, która zakłada brak interakcji z obiektem. Zbieranie pasywne określane jest natomiast w większości opracowań[20] jako charakterystyczne dla wywiadu

[19] M.M. Lowenthal, *OSINT the State of Art, The Artless State*, „Studies in Intelligence" 2001, vol. 45, no. 3, s. 63.
[20] Zob. szerzej: N.A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, Apress, 2018, s. 14–15. Pozostałe metody pozyskiwania informacji jawnoźródłowych, tj. półpasywne i aktywne, wiążą się m.in. z podejmowaniem działań niezgodnych

jawnoźródłowego, dlatego też w tym rozumieniu było ono używane w dalszej części pracy.

Rysunek 1.1. Nakładający się charakter dyscyplin wywiadowczych
Źródło: Oprac. na podstawie: H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, Rand Corporation, 2018, s. 9, https://www.rand.org/pubs/research_reports/RR1964.html [dostęp: 27.03.2025].

W sensie etymologicznym termin „bezpieczeństwo" wywodzony jest z łacińskiego słowa *sine cura*, co oznaczało stan „bez pieczy", stan spokoju i pewności. W okresie starożytnego Rzymu termin ten miał konotacje odnoszące się do politycznej stabilności. Współczesne definicje leksykalne rozszerzają to pojęcie, ujmując bezpieczeństwo jako stan pewności, spokoju, zabezpieczenia, braku zagrożenia oraz ochrony przed nim[21].

Bezpieczeństwo jest pojęciem interdyscyplinarnym, będącym przedmiotem zainteresowania m.in. ekonomii, prawa, politologii, nauki o stosunkach międzynarodowych czy psychologii. Każda z tych dziedzin wnosi unikatową perspektywę, poszerzając i pogłębiając zrozumienie bezpieczeństwa w różnych jego kontekstach. W ujęciu praktycznym, według byłego doradcy prezydenta Stanów Zjednoczonych ds. bezpieczeństwa narodowego Henry'ego Kissingera, bezpieczeństwo stanowi fundament wszystkiego, co czynimy[22]. Jest uznane jako jedna z centralnych kategorii antropocentrycznych, przez co ma charakter ponadczasowy. Tym samym rozumienie i dążenie do bezpieczeństwa odgrywają kluczową rolę w kształtowaniu polityk i strategii na każdym poziomie zarządzania, od lokalnego do globalnego.

---

z prawem, charakterystycznych dla przestępstw hackingu, phisingu, szpiegostwa, oszustwa czy kradzieży informacji. Ze względu na różnice w normach prawnych i społeczno-historycznych uwarunkowań tego typu metody, uznawane za wywiad jawnoźródłowy, stosowane są w Izraelu.

[21] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego*, Warszawa 2007, s. 27.

[22] H. Kissinger, Przemowa w Międzynarodowym Instytucie Studiów Strategicznych, Londyn 1975, cyt. za: J. Stańczyk, *Formułowanie kategorii pojęciowych bezpieczeństwa*, Wydawnictwo FNCE, 2017, s. 239.

Bezpieczeństwo jest jedną z podstawowych potrzeb człowieka. W takim ujęciu przedstawione zostało w połowie XX wieku przez Abrahama Maslowa na drugim poziomie piramidy potrzeb[23], tuż za potrzebami fizjologicznymi. Ryszard Zięba określa bezpieczeństwo jako potrzebę egzystencjalną, czyli związaną z istnieniem danego podmiotu[24]. Podobnie Roman Kuźniar podkreśla, że bezpieczeństwo stanowi pierwotną, egzystencjalną potrzebę jednostek, grup społecznych, wreszcie państw[25]. Bezpieczeństwo współcześnie pojmowane jest również jako naczelna potrzeba człowieka, oznacza stan spokoju, pewności, który daje brak poczucia zagrożenia[26]. Odnosi się zatem do stanu i pewności wolności od zagrożeń[27]. Bezpieczeństwo jako fundamentalna potrzeba człowieka stanowi również przedmiot szerokich analiz w literaturze zagranicznej. Barry Buzan definiuje bezpieczeństwo jako zasadniczy wymiar ludzkiej egzystencji, wskazując, że dotyczy ono ochrony przed zagrożeniami na poziomie jednostki, państwa i międzynarodowym[28]. Z kolei Paul D. Williams postrzega bezpieczeństwo jako niezbędny warunek egzystencji, wyróżniając dwie filozofie jego rozumienia: pierwszą, opartą na akumulacji siły, oraz drugą, traktującą bezpieczeństwo jako rezultat praw człowieka i sprawiedliwości[29].

Pojęcie państwa ewoluowało wraz ze zmianą poglądów na temat jego charakteru, funkcji i przeznaczenia. Temat ten podejmowany był przez największych prawników i filozofów od czasów starożytności. Platon określał państwo jako organizm społeczny, który pozwala na zharmonizowanie działania klas ludzkich w jedną całość, rządzący się cnotą sprawiedliwości i porządku w wykonywaniu obowiązków[30]. Arystoteles postrzegał państwo zarówno jako wspólnotę terytorialną i organizacyjną,

[23] Piramida Maslowa, znana również jako hierarchia potrzeb Maslowa, jest modelem psychologicznym zaproponowanym przez Abrahama Maslowa w jego pracy z 1943 roku pt. *A Theory of Human Motivation*. Model ten przedstawia potrzeby ludzkie w formie piramidy, z najbardziej podstawowymi potrzebami na dole, a bardziej złożonymi na górze. Na najniższym poziomie znajdują się potrzeby fizjologiczne, takie jak jedzenie, woda i schronienie. Kolejny poziom to potrzeby bezpieczeństwa, obejmujące ochronę fizyczną i stabilność finansową. Trzeci poziom to potrzeby społeczne, w tym uczucie przynależności i miłości. Czwarty poziom to potrzeby uznania, takie jak szacunek, uznanie i poczucie własnej wartości. Na szczycie piramidy znajduje się samorealizacja, czyli dążenie do realizacji własnego potencjału i osobistych aspiracji. Zob. A. Maslow, *A Theory of Human Motivation*, „Psychological Review" 1943, vol. 50, s. 370–396.
[24] R. Zięba, *O tożsamości nauk o bezpieczeństwie*, „Zeszyty Naukowe AON" 2012, nr 1(86), s. 8.
[25] R. Kuźniar, *Między polityką a strategią*, Wydawnictwo PWN, Warszawa 1994, s. 176.
[26] J. Czaputowicz, *Bezpieczeństwo międzynarodowe. Współczesne koncepcje*, Wydawnictwo PWN, Warszawa 2012, s. 22.
[27] R. Zięba, *Pojęcie i istota bezpieczeństwa państwa w stosunkach międzynarodowych*, „Sprawy Międzynarodowe" 1989, nr 10, s. 49.
[28] B. Buzan, O. Waever, J. de Wilde, *Security: A New Framework for Analysis*, Boulder 1998, s. 5–6.
[29] P.D. Williams, *Security Studies: An Introduction*, [w:] P.D. Williams (ed.), *Security Studies: An Introduction*, London–New York 2008, s. 5–10.
[30] Zob. szerzej: Platon, *Państwo*, t. 1, Wydawnictwo PWN, Warszawa 1994, s. 170–175.

obejmującą swym zakresem działania ogół członków zamieszkujących dane terytorium, w którym powinno panować prawo mające zapewnić poddanym sprawiedliwość i dobro. Państwo, jego zdaniem, jest wspólnotą różnych grup ludzi niezbędną do jego istnienia[31]. W *Słowniku języka polskiego* „państwo" określane jest jako zorganizowana politycznie społeczność zamieszkująca określone terytorium, mająca swój rząd i swoje prawa[32].

Pojęcie państwa stanowi przedmiot analiz we współczesnej literaturze polskiej i zagranicznej. Wśród koncepcji ukazujących integracyjną wizję społeczeństwa i państwa szczególne znaczenie ma teoria Georga Jelinka, definiująca państwo jako jedność terytorium, ludności i władzy suwerennej[33]. Jego trójelementowa koncepcja ukształtowała dominujący model definiowania państwowości, który pozostaje istotnym punktem odniesienia, zwłaszcza w doktrynie prawa międzynarodowego. Zbliżone podejście prezentuje Hans Kelsen, definiując państwo jako porządek prawny organizujący stosunki społeczne i sprawujący nad nimi suwerenną władzę[34]. W jego ujęciu nie jest ono jedynie organizacją polityczną, lecz przede wszystkim systemem norm, które regulują funkcjonowanie społeczeństwa i stanowią podstawę jego struktury. Z kolei Max Weber wskazywał, że zasadniczym wyróżnikiem państwa jest monopol na stosowanie legalnej przemocy na określonym terytorium, co odróżnia je od innych organizacji społecznych i politycznych[35]. We współczesnych teoriach podkreśla się znaczenie efektywnych instytucji oraz rządów prawa jako fundamentów stabilności państwa. Francis Fukuyama wskazuje, że jego trwałość państwa zależy nie tylko od suwerenności i władzy, lecz także od zdolności instytucji do skutecznego działania oraz zapewnienia porządku społecznego[36].

Kolejne definicje prezentują pojmowanie państwa w kontekście rozważań nad jego bezpieczeństwem. Ryszard Wróblewski postrzega państwo jako organizację polityczną wielkiej grupy społecznej nierozdzielnie związaną z określonym terytorium, na którym rozciąga się jego władza i obowiązujące prawa przez nią stanowione[37].

[31] Zob. szerzej: Arystoteles, *Polityka*, t. 7, Wydawnictwo PWN, Warszawa 1964, s. 303.
[32] Hasło „państwo", [w:] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/szukaj/państwo.html [dostęp: 26.05.2023].
[33] G. Jelinek, *Ogólna nauka o państwie*, Wydawnictwo F. Hoesicka, Warszawa 1921, s. 50.
[34] H. Kelsen, *General Theory of Law and State,* The Lawbook Exchange, Ltd., Clark, New Jersey 2007, s. 183–185.
[35] M. Weber, *Racjonalność, władza, odczarowanie*, Wydawnictwo Poznańskie, Poznań 2011, s. 266.
[36] F. Fukuyama, *Budowanie państwa. Władza i ład międzynarodowy w XXI wieku,* Rebis 2005, s. 44–55.
[37] R. Wróblewski, *Podstawowe pojęcia z dziedziny polityki bezpieczeństwa, strategii i sztuki wojennej*, AON, Warszawa 1993, s. 9.

Zygmunt Ziembiński i Sławomira Wronkowska definiują państwo jako organizację polityczną wyposażoną w suwerenną władzę, zarówno terytorialną i taką, do której przynależność ma charakter sformalizowany[38]. W formułowanych definicjach państwa, zarówno w literaturze polskiej jak i zagranicznej, pojawiają się elementy wspólne, które są konieczne dla jego powstania i istnienia, tj. ludność, terytorium, władza najwyższa, suwerenność oraz określone prawo. Zasadne jest zatem przyjęcie definicji uwzględniającej te podstawowe atrybuty.

W polskiej literaturze przedmiotu brakuje powszechnie uznanej interpretacji bezpieczeństwa w odniesieniu do państwa czy narodu, tym samym niejednokrotnie terminy te są utożsamiane i używane zamiennie[39]. Termin „bezpieczeństwo narodowe" (ang. *national security*) został zaadaptowany w polskiej nauce z doktryny anglosaskiej, bez uwzględnienia odmiennego pojęcia „naród" w państwach kontynentalnych i anglosaskich. Na gruncie anglosaskim „naród" oznacza wspólnotę wszystkich obywateli, niezależnie od ich przynależności etnicznej i kulturowej (tzw. polityczna koncepcja narodu) i jest zrównany z państwem. Tymczasem w podejściu kontynentalnym „naród" jest wspólnotą ludzi, których połączyły wspólna kultura, język, historia, tradycja, symbole, religia (tzw. kulturowa koncepcja narodu). Należy również zwrócić uwagę, że w formułowanych definicjach państwa jego elementami są społeczeństwo, terytorium i władza. Państwo ma wymiar instytucjonalny i może być zamieszkiwane przez kilka narodów, których może nie łączyć wspólna kultura. Naród stanowi element składowy państwa, koniecznym do jego istnienia. Dlatego też należy przyjąć, że pojęcia „bezpieczeństwo narodowe" i „bezpieczeństwo państwa" nie są tożsame, a w pracy doktorskiej autorka posługuje się terminem „bezpieczeństwo państwa".

Bezpieczeństwo państwa definiowane jest jako system wartości, które stanowią o jego istocie wraz z zespołem środków zabezpieczających[40]. Jest precyzowane jako zapewnienie integralności terytorialnej, suwerenności, swobody wyboru drogi

[38] Z. Ziembiński, S. Wronkowska, *Państwo i inne struktury społeczne*, [w:] M. Zmierczak, S. Wronkowska (red.), *Kompendium wiedzy o społeczeństwie, państwie i prawie*, PWN, Warszawa–Poznań 1993, s. 54.
[39] Zob. szerzej: K.A. Wojtaszczyk, *Bezpieczeństwo państwa – konceptualizacja pojęć*, [w:] A. Materska-Sosnowska, K.A. Wojtaszczyk (red.), *Bezpieczeństwo państwa. Wybrane problemy*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2009, s. 11; J. Gierszewski, *Wokół uniwersum nauk o bezpieczeństwie*, Difin, Warszawa 2022, s. 38.
[40] M. Brzeziński, *Rodzaje bezpieczeństwa państwa*, [w:] S. Sulowski, M. Brzeziński (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa 2009, s. 35.

politycznej ora warunków umożliwiających osiągniecie dobrobytu i rozwoju[41]. Bezpieczeństwo państwa manifestuje się poprzez dwa fundamentalne wymiary: bezpieczeństwo wewnętrzne i bezpieczeństwo zewnętrzne[42]. Bezpieczeństwo wewnętrzne odnosi się do zagadnień i relacji wewnątrz struktury państwa, które gwarantują jego istnienie i prawidłowy rozwój. Bezpieczeństwo wewnętrzne obejmuje: bezpieczeństwo publiczne, porządek publiczny i bezpieczeństwo ustrojowe[43]. Bezpieczeństwo zewnętrzne dotyczy relacji międzynarodowych oraz interakcji z innymi podmiotami suwerennymi. Bezpieczeństwo zewnętrzne jest pojmowane jako zdolność państwa do obrony i ochrony przed wszelkimi zewnętrznymi zagrożeniami militarnymi i pozamilitarnymi. Obejmuje takie elementy jak obrona integralności terytorialnej, niezależności politycznej oraz życia ludności[44].

Różne metody interpretacji bezpieczeństwa państwa formułują to pojęcie w takich kategoriach jak wartość, proces i stan. Bezpieczeństwo jest wartością, o którą należy ciągle zabiegać, uwzględniając zmiany wewnątrz i na zewnątrz państwa. Traktowane jako proces obejmuje zbiór zróżnicowanych działań, które mają na celu neutralizację zagrożeń uniemożliwiających osiągnięcie kluczowych celów państwa. Stan bezpieczeństwa narodowego określany jest każdorazowo przez analizę stosunku między potencjałem obronnym a poziomem występujących zagrożeń[45]. Efektywne zarządzanie bezpieczeństwem państwa wymaga zintegrowanego podejścia, które uwzględnia zarówno wewnętrzne, jak i zewnętrzne aspekty bezpieczeństwa, a także potrzebę adaptacji do zmieniającego się globalnego środowiska i pojawiających się nowych zagrożeń.

Dynamiczne zmiany technologiczne, rozwój cyberprzestrzeni i nowych form komunikacji, globalizacja, obejmująca zarówno aspekty gospodarcze, polityczne, społeczne, jak i informacyjne, generują nowego rodzaju zagrożenia. Rozszerzanie katalogu szans i zagrożeń powoduje systematyczne poszerzanie zakresu przedmiotowego koncepcji bezpieczeństwa[46]. Efektem jest ewolucyjne przechodzenie

[41] J. Czaputowicz, *Kryteria bezpieczeństwa międzynarodowego – aspekty teoretyczne*, [w:] S. Dębski, B. Górska-Winter (red.), *Kryteria bezpieczeństwa międzynarodowego państwa*, PISM, Warszawa 2003, s. 35.
[42] Zob. szerzej: N. Moch, *Bezpieczeństwo państwa*, [w:] J. Itrich-Drabarek, A. Misiuk, S. Mitkow, P. Bryczek-Wróbel (red.), *Encyklopedia bezpieczeństwa narodowego*, Wydział Bezpieczeństwa, Logistyki i Zarządzania. Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Dom Wydawniczy i Handlowy ELIPSA, Warszawa 2023, s. 72–73.
[43] M. Brzeziński, *Rodzaje bezpieczeństwa państwa*…, op. cit., s. 41.
[44] Ibidem, s. 38–39.
[45] K.A. Wojtaszczyk, *Bezpieczeństwo państwa – konceptualizacja pojęć*…, op. cit., s. 12.
[46] J. Stańczyk, *Formułowanie kategorii pojęciowych*…, op. cit., s. 245.

od bezpieczeństwa jednowymiarowego, ukierunkowanego na zagrożenia militarne, na bezpieczeństwo państwa w wielowymiarowej postaci. Realizacja zadań państwa, zarówno w sferze wewnętrznej, jak i zewnętrznej, współcześnie warunkowana jest dostępem do informacji. Zwiększenie ilości źródeł informacji i samych informacji oraz kanałów informacyjnych generuje nowe potrzeby po stronie podmiotów państwowych odnośnie do narzędzi i metod koniecznych do prowadzenia analiz. Współcześnie jednym z zasadniczych źródeł pozyskiwania informacji ważnych dla zapewnienia bezpieczeństwa państwa są źródła otwarte[47]. Istotne są zatem zarówno wiedza, jak i kompetencje podmiotów uprawnionych do podejmowania decyzji na rzecz bezpieczeństwa państwa w zakresie wywiadu jawnoźródłowego. W dobie globalizacji i postępu technologicznego wywiad jawnoźródłowy stał się istotnym elementem wszystkich działań wywiadowczych, a jego efektywność zależy zarówno od dostępu do nowoczesnych technologii jak i od umiejętności analitycznych.[48] Jednak, jak wskazują badacze zajmujący się tym obszarem[49], skuteczne wykorzystanie wywiadu jawnoźródłowego wymaga jego integracji z innymi formami wywiadu, co stanowi wyzwanie organizacyjne i operacyjne dla podmiotów odpowiedzialnych za bezpieczeństwo państwa.

1.3. Przedmiot i cel badań

W ramach przyjętego tematu rozprawy określony został **przedmiot badań**, którym jest **wywiad jawnoźródłowy realizowany w obszarze bezpieczeństwa państwa.**

Studia wywiadowcze odgrywają coraz istotniejszą rolę w naukach o bezpieczeństwie, zarówno w perspektywie teoretycznej, metodologicznej, epistemologicznej, jak i prakseologicznej. Skoncentrowane są na kompleksowej analizie danych wywiadowczych oraz ich efektywnym zastosowaniu w procesach zarządzania bezpieczeństwem państwa. Rozwój studiów wywiadowczych związany jest z postępem technologicznym oraz rosnącymi możliwościami wykorzystania

[47] B. Jagusiak, P. Żukowski, *Zagrożenia procesów informacyjnych w systemie bezpieczeństwa państwa. Zagadnienia wybrane*, Wojskowa Akademia Techniczna, Warszawa 2019, s. 56.
[48] S.D. Gibson, *Open source intelligence*, [w:] R. Dover, M.S. Goodman, C. Hillebrand (eds.), *The Routledge Companion to Intelligence Studies*, London 2014, s. 127–130.
[49] E.A. Jardins, *Open Source Intelligence*, [w:] M.M. Lowenthal, R.M. Clark, *The Five Disciplines of Intelligence Collection*, SAGE Publications, 2015, s. 8–10; M. Phytian, *Beyond the Intelligence Cycle?*, [w:] M. Phytian (ed.), *Understanding the Intelligence Cycle*, Routledge, London–New York 2013, s. 18–19.

różnorodnych źródeł informacji, w tym źródeł dostępnych publicznie. Problematyka związana z wywiadem jawnoźródłowym staje się coraz bardziej złożona z uwagi na nieustannie rosnącą liczbę otwartych źródeł, powszechną dostępność informacji, brak przejrzystych regulacji prawnych dotyczących analizy danych z tych źródeł, trudności w ocenie ich wiarygodności oraz szybki rozwój technologii i narzędzi analitycznych, które jednocześnie zwiększają zarówno możliwości, jak i wyzwania w ich przetwarzaniu oraz interpretacji.

Podmiotem badań są przedstawicielstwa zajmujące się realizacją zadań związanych z bezpieczeństwem państwa.

Badania społeczne mogą służyć wielu celom, jednak zasadniczo można wyróżnić trzy główne[50]:

- eksplorację;
- opis;
- wyjaśnienie.

Na ich podstawie można wyróżnić dwa kluczowe cele badawcze: teoretyczny, którego istotą jest pogłębiona analiza i zrozumienie badanego zagadnienia, oraz praktyczny, ukierunkowany na opracowanie i implementację metod umożliwiających zastosowanie wyników badań w praktyce.

Głównym **celem badań w aspekcie poznawczym jest określenie znaczenia wywiadu jawnoźródłowego dla bezpieczeństwa państwa.**

Głównym **celem praktycznym badań jest zidentyfikowanie możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa.**

1.4. Problemy i hipotezy badawcze

Praca ma charakter teoretyczno-empiryczny. Główny problem badawczy, wynikający ze zidentyfikowanego przedmiotu oraz celu badań, zawiera się w pytaniu: **Jakie znaczenie ma wywiad jawnoźródłowy w zapewnieniu bezpieczeństwa państwa?**

Rozwiązanie głównego problemu badawczego wymaga sprecyzowania problemów o charakterze szczegółowym, ujętych w następujących pytaniach:

[50] E. Babbie, *Badania społeczne w praktyce*, Wydawnictwo Naukowe PWN, Warszawa 2005, s. 110.

1. Jaka jest istota i znaczenie wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa?
2. W jakim zakresie dostępne metody i środki prowadzenia wywiadu jawnoźródłowego wpływają na bezpieczeństwo państw?
3. Jakie prawne i pozaprawne aspekty wpływają na prowadzenie wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa?
4. Jakie są dotychczasowe kierunki prowadzenia wywiadu jawnoźródłowego na rzecz bezpieczeństwa w wybranych państwach demokratycznych?

W odniesieniu do postawionych problemów badawczych sformułowano następującą główną hipotezę badawczą:

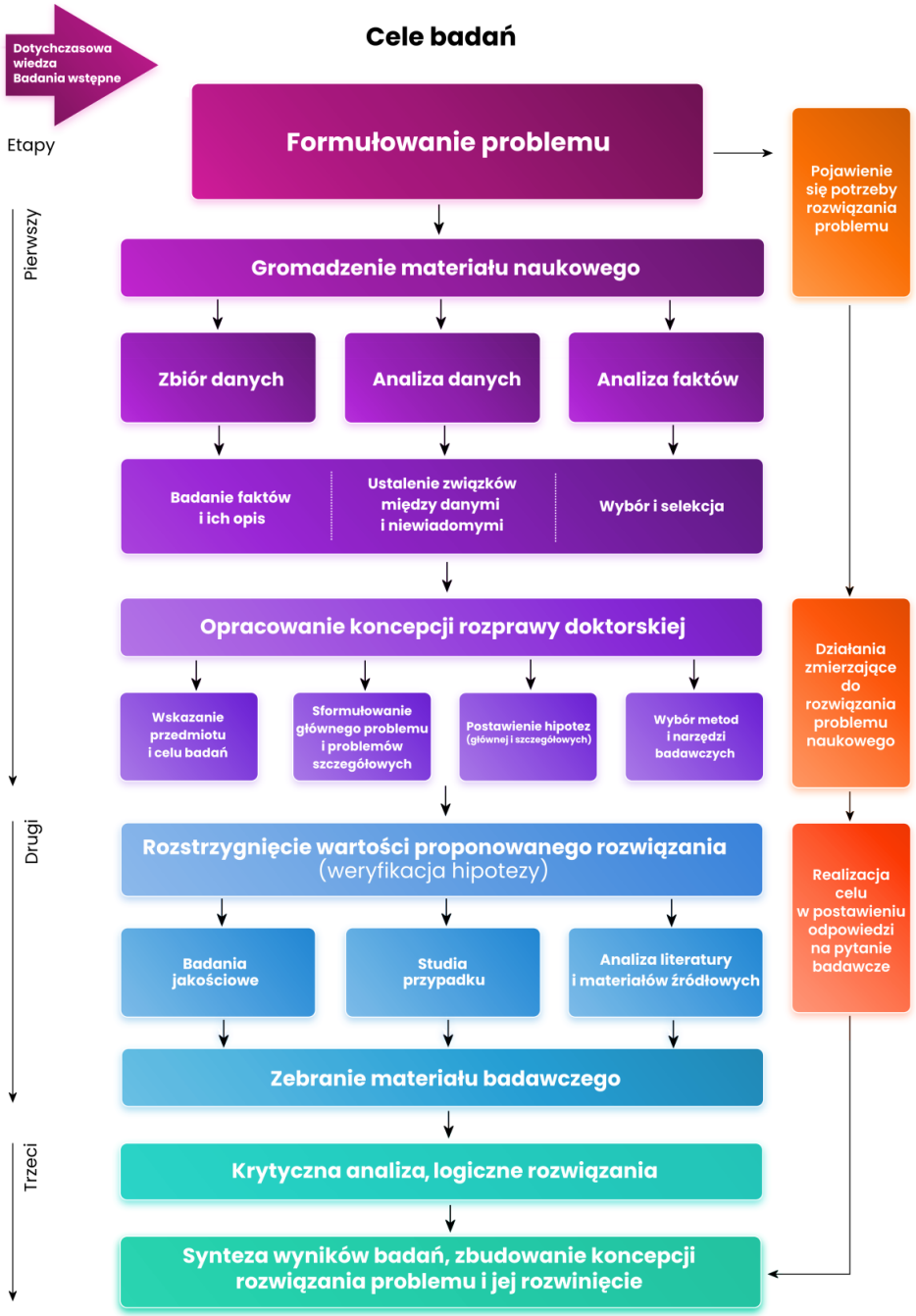
Dynamiczny rozwój otwartych źródeł informacji oraz technologii związanych z możliwością pozyskiwania i masowej dystrybucji informacji, a także coraz szersze wykorzystanie nowych technologii do pozyskiwania i analizy informacji jawnoźródłowych powodują wzrost możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa. Informacje dostarczone w wyniku działań wywiadu jawnoźródłowego: a) uzupełniają informacje pozyskane drogą operacyjną, b) skracają czas konieczny do podjęcia decyzji, przez co c) poprawiają jakość i skuteczność działań ofensywnych i defensywnych państwa.

Na podstawie problemów szczegółowych sformułowano następujące hipotezy szczegółowe:

1. Dynamiczny rozwój otwartych źródeł informacji oraz technologii związanych z pozyskiwaniem i przetwarzaniem informacji jawnoźródłowych zwiększa potencjał wykorzystania wywiadu jawnoźródłowego w sektorze bezpieczeństwa państwa.
2. Założyć można, że nowe technologie umożliwiają efektywne pozyskiwanie informacji jawnoźródłowych, przez co zwiększają precyzję i skracają czas analizy informacji jawnoźródłowych.
3. Uwarunkowania prawne oraz pozaprawne, jak etyczne, metodologiczne, techniczne oraz informacyjne, mają wpływ na wywiad jawnoźródłowy.
4. Wywiad jawnoźródłowy prowadzony jest w celu zwiększenia zdolności defensywnych i ofensywnych w wybranych państwach demokratycznych.

1.5. Organizacja i przebieg badań

Przyjęty proces badawczy, rozumiany jako całościowy schemat działań, które naukowcy podejmują w celu wytworzenia wiedzy[51], składał się z trzech etapów badań: wstępnych, właściwych oraz badań końcowych (rys. 1.2).



Rysunek 1.2. Schemat procesu badawczego rozprawy
Źródło: Opracowanie własne.

[51] Ch. Frankfort-Nachmias, D. Nachmias, *Metody badawcze w naukach społecznych*, Zysk i S-ka, Poznań 2001, s. 36.

Etap badań wstępnych zapoczątkowany został przez pojawienie się sytuacji problemowej. Na tym etapie zgromadzono informacje niezbędne do opracowania koncepcji badań. Zastosowano następujące metody teoretyczne: analizę i krytykę piśmiennictwa (celem dokonania oceny źródeł i literatury przedmiotu), syntezę oraz interpretację logiczną, co umożliwiło sformułowanie wniosków koniecznych do realizacji kolejnych etapów badań. Efektem tego etapu prac było przygotowanie koncepcji rozprawy doktorskiej poprzez wskazanie przedmiotu oraz celu prowadzonych badań, sformułowanie głównego problemu badawczego oraz problemów szczegółowych, postawienie hipotezy głównej i hipotez roboczych, jak również wybór metod i technik wraz z narzędziami badawczymi.

Na etapie badań właściwych zastosowano metody badań jakościowych poprzez przeprowadzenie indywidualnych wywiadów pogłębionych z ekspertami zajmującymi się wywiadem jawnoźródłowym. Podjęte działania, obok pogłębionej analizy literatury przedmiotu i materiałów źródłowych w zakresu teorii wywiadu jawnoźródłowego oraz bezpieczeństwa państwa, umożliwiły zebranie pełniejszego materiału badawczego.

W etapie badań końcowych skoncentrowano się na opracowaniu wyników badań i ich syntezie, udzieleniu odpowiedzi na główny i szczegółowe problemy badawcze oraz weryfikacji hipotezy badawczej. Etap ten, po przeprowadzonej redakcji pracy, zakończyło powstanie ostatecznej wersji rozprawy.

Przeprowadzone badania, ulokowane w obszarze interdyscyplinarnych nauk o bezpieczeństwie, miały charakter teoretyczno-empiryczny.

Do zweryfikowania I hipotezy wykorzystano krytyczną analizę literatury przedmiotu, dzięki której wzbogacono wiedzę teoretyczną związaną z funkcjonowaniem wywiadu jawnoźródłowego w obszarze bezpieczeństwa państwa. Stosując podejście normatywne, odwołano się do artykułów naukowych i prac zbiorowych oraz monografii naukowych. Przeprowadzono również badanie dokumentów i aktów prawnych. Zastosowane metody teoretyczne to: analiza, synteza, abstrahowanie, porównanie i uogólnienie, klasyfikowanie oraz wnioskowanie.

Do zweryfikowania II i III hipotezy badawczej zastosowano następujące metody: krytyczną analizę literatury przedmiotu, *desk research* oraz metody teoretyczne. W trakcie badań nad aspektami prawnymi i pozaprawnymi prowadzenia wywiadu jawnoźródłowego zastosowano również analizę instytucjonalno-prawną polegającą na studiowaniu oraz analizowaniu aktów prawnych regulujących ramy

jawności i dostępności informacji oraz funkcjonowanie służb oraz organów administracji publicznej wykorzystujących wywiad jawnoźródłowy.

Do zweryfikowania IV hipotezy zastosowano krytyczną analizę literatury przedmiotu i badanie dokumentów, analizę porównawczo-historyczną oraz metody teoretyczne: analizę, syntezę, indukcję, dedukcję, porównywanie, uogólnienie oraz wnioskowanie. Powyższe techniki badawcze miały na celu dostarczenie wiedzy na temat podobieństw i różnic między sposobem wykorzystania wywiadu jawnoźródłowego oraz kierunków jego prowadzenia na rzecz bezpieczeństwa w wybranych państwach demokratycznych.

W celu zweryfikowania hipotezy I, II, III i IV wykorzystano metodę badań jakościowych, do których zalicza się wywiad ekspercki[52]. Cele metod jakościowych to:

- dostarczenie nowych hipotez;
- dostarczenie nowych informacji o badanym zjawisku oraz dostarczanie informacji o nowej jakości;
- pomoc w lepszym zrozumieniu działania analizowanych zagadnień;
- pogłębienie istniejącej wiedzy[53].

Wywiad ekspercki przeprowadzony został na celowo dobranej próbie badawczej. Do grupy respondentów wybrano osoby posiadające duży dorobek zawodowy oraz profesjonalną lub ekspercką wiedzę na temat wywiadu jawnoźródłowego w sektorze bezpieczeństwa państwa. Zastosowanym narzędziem badawczym był *Scenariusz wywiadu z ekspertami wykorzystującymi wywiad jawnoźródłowy w swojej pracy zawodowej.* Zadawane respondentom pytania dotyczyły faktów bądź stosunku do nich oraz próby prognozowania możliwości wykorzystania wywiadu jawnoźródłowego w działaniach ofensywnych i defensywnych państwa. W badaniach przeprowadzono 12 wywiadów eksperckich, respondentami byli: funkcjonariusze (służby specjalne, Policja, Straż Graniczna, Jednostka Wojskowa GROM, Wojska Obrony Terytorialnej, Wojska Obrony Cyberprzestrzeni),

[52] „Metody jakościowe charakteryzuje indywidualne podejście do respondenta, niewielka skala badań, stosowanie niezestandaryzowanych narzędzi badawczych oraz szczególna rola badacza, który wchodzi z badanym w interakcję. Badacz dokonuje też subiektywnej interpretacji uzyskanych wyników. Najczęściej metodom jakościowym przypisuje się techniki badawcze oparte na wywiadzie (spontaniczny wywiad narracyjny, swobodny wywiad nieukierunkowany, wywiad ekspercki, wywiad zogniskowany, wywiad pogłębiony, wywiad grupowy) oraz obserwacji (obserwacja uczestnicząca lub nieuczestnicząca, jawna lub ukryta)". Zob. S. Górski, *O metodach badawczych w naukach społecznych*, [w:] A. Czupryński, B. Wiśniewski, J. Zboina (red.), *Nauki o bezpieczeństwie. Wybrane problemy badań*, Wydawnictwo CNBOP-PIB, 2017, s. 63.

[53] J. Gierszewski, A. Pieczywok, *Metodologiczne podstawy badania problemów bezpieczeństwa*, Wydawnictwo Difin, Warszawa 2020, s. 102.

funkcjonariusz administracji rządowej (Ministerstwo Cyfryzacji), naukowiec zajmujący się problematyką związaną z wywiadem i bezpieczeństwem państwa (profesor uczelni) oraz dziennikarz-detektyw, były dyrektor Biura Analiz i Informacji.

W obrębie problemów badawczych posłużono się również metodami prognozowania, których wypadkową stanowi prognoza wpływu wywiadu jawnoźródłowego na rozwój bezpieczeństwa państwa. Transdyscyplinarność badań oraz różnorodność wykorzystanych metod badawczych powoduje, że pluralizm metodologiczny, a tym samym zastosowanie metodologii mieszanej może skutkować uzyskaniem bardziej precyzyjnych wyników obarczonych mniejszym ryzykiem błędu. Zastosowane metody nie wykluczają się, lecz wzajemnie komplementarnie oddziałują, wzbogacając perspektywę badawczą i zwiększając rzetelność uzyskanych wyników.

W ramach przeprowadzonych badań przyjęto, że zmienną zależną jest bezpieczeństwo państwa, natomiast zmienną niezależną jest wywiad jawnoźródłowy.

Przyjęty w rozprawie przedmiot badań charakteryzuje się wieloaspektowością, złożonością oraz zmiennością odnośnie do zakresu i szybkości zachodzących zjawisk, co generuje określone ograniczenia badawcze.

Po pierwsze, dynamika zmian technologicznych w pozyskiwaniu i analizie jawnoźrodłowej oraz szybkie przeobrażenia przestrzeni informacyjnej powodują, że przedmiot podjętych badań ulega ciągłej ewolucji. Dodatkowo możliwa jest dezaktualizacja przedstawionych narzędzi oraz metod pozyskiwania i analizy informacji z otwartych źródeł. Wpływ prowadzonych badań na podmiot i przedmiot bezpieczeństwa państwa zawężony jest czasowo do lat 2020-2024.

Po drugie, w literaturze przedmiotu brakuje publikacji na temat wykorzystania informacji jawnoźródłowych w pracy operacyjnej oraz zestawień i danych statystycznych na ten temat. Założono więc, że badania będą obejmowały ogólnodostępne dokumenty i publikacje. Dodatkowo informacje dotyczące metod i narzędzi służących do pozyskiwania i analizy informacji jawnoźródłowych są rozproszone, zarówno w literaturze naukowej, publikacjach eksperckich (stricte technicznych), jak również w materiałach dostępnych w źródłach internetowych. Dysproporcja w literaturze na rzecz tych ostatnich powoduje konieczność ich każdorazowej weryfikacji pod kątem rzetelności.

Po trzecie, wywiad jawnoźródłowy prowadzony przez organy bezpieczeństwa i organy ściągania państwa, ma charakter niejawny, przez co uzyskanie informacji o metodologii prowadzonego rozpoznania jest utrudnione lub wręcz niemożliwie.

1.6. Analiza literatury przedmiotu

Analiza literatury stanowi fundament wszelkich badań naukowych, umożliwiając przeprowadzenie szczegółowej analizy i krytyki piśmiennictwa (analiza krytyczna), oraz analizy i krytyki źródeł. Istotną częścią niniejszej pracy badawczej była weryfikacja literatury przedmiotu przeprowadzona na wstępnym etapie określania problemu badawczego i kontynuowana aż do finalizacji dysertacji.

W przeprowadzonej analizie odniesiono się do artykułów, prac zbiorowych i monografii naukowych oraz aktów prawnych i raportów. Tematyka rozprawy, podejmująca zagadnienia osadzone w dynamicznie rozwijającym się środowisku cyfrowym, wiązała się również z koniecznością analizy selektywnie dobranych źródeł internetowych. Literatura poddana interpretacji została w całości zamieszczona w bibliografii niniejszej pracy.

Do opracowania rozdziału metodologicznego pracy wykorzystano literaturę dotyczącą metod i narzędzi badawczych oraz opracowania, które pozwoliły na zdefiniowane podstawowych pojęć będących przedmiotem dysertacji. W pierwszej grupie znalazły się takie publikacje jak: A. Kołodziejczyk, M. Marciniak, J. Adamkiewicz, *Poradnik metodologiczny dla dyplomantów kierunków bezpieczeństwo narodowe i obronność państwa WAT,* Wojskowa Akademia Techniczna, Warszawa 2023; Ch. Frankfort-Nachmias, D. Nachmias, *Metody badawcze w naukach społecznych,* Zysk i S-ka, Poznań 2001 oraz J. Gierszewski, A. Pieczywok, *Metodologiczne podstawy badania problemów bezpieczeństwa*, Wydawnictwo Difin, Warszawa 2020.

Do analizy pojęcia bezpieczeństwo państwa wykorzystano m.in. następujące opracowania: J. Stańczyk, *Formułowanie kategorii pojęciowej bezpieczeństwa,* Wydawnictwo FNCE, Poznań 2017; B. Jagusiak, P. Żukowski, *Zagrożenia procesów informacyjnych w systemie bezpieczeństwa państwa*, Wojskowa Akademia Techniczna, Warszawa 2019; K.A. Wojtaszczyk, A. Materska-Sosnowska, *Bezpieczeństwo państwa*, ASPRA-JR, Warszawa 2009; J. Gierszewski, *Wokół uniwersum nauk o bezpieczeństwie*, Difin, Warszawa 2022, J. Itrich-Drabarek, A. Misiuk, S. Mitkow, P. Bryczek-Wróbel, *Encyklopedia Bezpieczenstwa Narodowego,* Wydział Bezpieczeństwa, Logistyki i Zarządzania Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego, Dom Wydawniczy ELIPSA, Warszawa 2023. Natomiast do określeniu pojęcia wywiad jawnoźródłowy posłużyły takie publikacje jak: Mark M. Lowenthal, *OSINT the State of*

Art, The Artless State, „Studies in Intelligence" 2001, vol. 45, nr 3; H.J. Williams, I. Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, Rand Corporation, 2018; Warszawa 2017; K. Matela, *Wybrane aspekty systemów wywiadu, obserwacji i rozpoznania (ISR)*, Wiedza Obronna, 2021. Skorzystano również z dokumentów opracowanych przez Sojusz Północnoatlantycki: *NATO Open Spurce Intelligence Handbook*, 2001; *NATO Open Source Reader*, 2002; *Intelligence Exploitation of the Internet*, 2002; *Słownik terminów i definicji NATO*, 2019, które były pomocne również przy opracowaniu rozdziału drugiego i trzeciego.

W zakresie charakterystyki roli i znaczenia wywiadu jawnoźródłowego należy wyróżnić publikację H.J. Williams, I. Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, Rand Corporation, 2018, która w sposób kompleksowy przedstawia zarówno teoretyczne, jak i praktyczne aspekty pozyskiwania oraz analizy informacji jawnoźródłowych. Korzystano również z literatury amerykańskiej dotyczącej działalności wywiadowczej, w której odnaleźć można odniesienia do rozpatrywanego problemu badawczego: R. Dover, M.S. Goodman, C. Hillebrand, *Routledge Companion to Intelligence Studies*, Routledge 2014; R.M. Clark, *Intelligence Analysis. A Target-Centric Approach*, Fourth edition, SAGE, 2013; J. Mena, *Investigative Data Mining for Security and Criminal Detection*, Butterworth Heinemann, 2013; J. Richards, *The Art and Science of Intelligence Analysis*, OXFORD University Press, Oxford 2010 oraz M. Lowenthal, *Intelligence, From secrets to policy*, Fith edition, SAGE. Wśród polskich opracowań znaczącym wkładem w problematykę wywiadu jawnoźródłowego jest publikacja K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Difin, 2011. Wykorzystano również inne źródła, w tym: W. Filipkowski, W. Modrzejowski, *Biały wywiad. Otwarte źródła informacji-wokół teorii i praktyki*, C.H. Beck, 2011; B. Saramk, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej. Historia, praktyka, perspektywy*, Uniwersytet Warszawski Wydział Dziennikarstwa i Nauk Politycznych, Warszawa 2015 oraz M. Minkina, *Sztuka wywiadu w państwie współczesnym*, Oficyna Wydawnicza RYTM, Warszawa 2022.

W kontekście metodologicznych aspektów prowadzenia wywiadu jawnoźródłowego, szczególnie w zakresie analizy informacji, istotnym dziełem jest praca Jerzego Koniecznego pt. *Analiza informacji w dziedzinie bezpieczeństwa państwa*, wydana przez Agencję Bezpieczeństwa Wewnętrznego w Warszawie w 2014 roku. W obszarze analizy informacji za wielce przydatne dla powstania niniejszej dysertacji

należy uznać prace polskich autorów, takie jak: J. Oleński, *Ekonomika Informacji. Metody*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2003; W. Fehler, *Podstawy bezpieczeństwa informacyjnego*, Wydawnictwo Naukowe UPH, Siedlce 2021 oraz P. Zaskórski, W. Zaskórski, *Big-Data systems in improving modern organizations*, „Nowoczesne Systemy Zarządzania" 2017, z 12, nr 2, WAT, Warszawa. Dodatkowo wnioski czerpano na podstawie publikacji autorstwa Krzysztofa Liedla, Pauliny Piaseckiej oraz Tomasza R. Aleksandrowicza, w tym były to: *Analiza informacji. Teoria i praktyka*, Difin, Warszawa 2011; *Analiza informacji w zarządzaniu bezpieczeństwem*, Difin, Warszawa 2013 oraz *Analiza informacji w działaniu*, Difin, Warszawa 2012.

Wybór literatury, w szczególności zagranicznej, na temat metod i narzędzi wykorzystywanych w wywiadzie jawnoźródłowym jest obszerny. Podstawę wiedzy w tym zakresie stanowiły następujące opracowania: M. Bazzell, *Open Source Intelligence Techniques. Resources for searchning and analyzing online information*, Sixth Edition, 2018 oraz N.A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools. A practical Guide to Online Intelligence*, Apres, 2018. W odniesieniu do charakterystyki środków i metod wywiadu jawnoźródłowego cenną literaturą okazują się publikacje z zakresu bezpieczeństwa defensywnego oraz technologii informacyjnych, w tym P. Hrabiec-Hojda, J. Trzeciakowska, *Google Hacking, Infomedia Group*, Kraków 2019; R. Messier, *Kali Linux. Testy bezpieczeństwa. Testy penetracyjne i etyczne hakowanie*, Helion, Gliwice 2019; L. Brothesrton, M. Hickey, J. Arcuri, *Warsztat Hakera. Testy penetracyjne i inne techniki wykrywania podatności*, Helion, 2022 oraz V.K. Velu, *Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite*, wydanie 4, Helion S.A., 2023. Poza opracowaniami monograficznymi w analizie uwzględniono także artykuły naukowe zawierające istotne uwagi na temat metod i narzędzi stosowanych w wywiadzie jawnoźródłowym, w tym: D. Mider, *Sztuka wyszukiwania w Internecie – autorski przegląd wybranych technik i narzędzi*, „Studia Politologiczne" 2019, t. 54. Cennym źródłem był również raport A. Unvera, *Digital Open Source Intelligence and International Security*: A Primer, EDAM Research Reports – Cyber Governance and Digital Democracy 2018.

W rozdziale czwartym przedstawiono prawne i pozaprawne aspekty prowadzenia wywiadu jawnoźródłowego, w tym zagadnienia związane z prawnymi ograniczeniami pozyskiwania informacji jawnoźródłowych, ich etycznym wykorzystaniem oraz technicznymi i metodologicznymi aspektami, które wpływają na

zdolność pozyskiwania i analizy informacji ze źródeł otwartych.

W odniesieniu do aspektów prawnych korzystano z dokumentów źródłowych w postaci aktów prawnych oraz strategii, a także takich publikacji jak: D.E. Pozen, *The Mosaic Theory the Mosaic Theory, National Security, and the Freedom of Information Act*, „Yale Law Journal" 2005, vol. 115, no. 3; A.F. Westin, *Privacy and Freedom*, „Washington and Lee Law Review" 1968, vol. 25, no. 1, M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni*, Wolters Kluwer, Warszawa 2019. W zakresie analizy realizacji prawa do prywatności w kontekście wywiadu jawnoźródłowego uwzględniono również jego odniesienia do stosowania w praktyce zawarte w publikacji C. Cuijpers, *Legal aspects of open source intelligence – Results of the VIRTUOSO project*, „Computer Law & Security Review" 2013, vol. 29, no. 6.

Przy opracowaniu aspektów etycznych odniesiono się w szczególności do: *Berkeley Protocol on Digital Open Source Investigations*, HR/PUB/20/2, Nowy York i Genewa 2022. Skorzystano również z publikacji: J. Richards, *The Art and Science of Intelligence Analysis*, Oxford University Press, 2010; M. Michalik, *Społeczne przesłanki, swoistość i funkcje etyki zawodowej*, [w:] A. Sarapata (red.), *Etyka zawodowa*, Warszawa 1971, M. Herman, *Ethics in Intelligence after September 2001*, „Intelligence and National Security" 2004, 19. W zakresie analizy raportowania obywatelskiego znaczące ustalenia dostarczyły raporty amerykańskiej agencji rządowej DARPA (Darpa Network Challenge Project Report 2010, Defense Advanced Research Projects Agency) oraz A. Mukhopadhyay, S. Venkatagiri, K. Luther, *OSINT Research Studios: A Flexible Crowdsourcing Framework to Scale Up Open Source Intelligence Investigations*, „Proceedings of the ACM on Human Computer Interaction" 2024, 8, CSCW1, Article 105. W części dotyczącej deontologii podmiotów prowadzących rozpoznanie jawnoźródłowe za przydatne należy uznać kodeksy etyki zawodowej, które stanowią istotne odniesienie standardów etycznych obowiązujących w wywiadzie jawnoźródłowym.

Wiele istotnych ustaleń w odniesieniu do kwestii aspektów metodologicznych wywiadu jawnoźródłowego dostarczyły wspomniane już publikacje J. Koniecznego, a także: Heuer Jr., *Psychology of Intelligence Analysis, Center For The Study Of Intelligence*, Central Intelligence Agency, 1999; R. Johnston, *Analytic Culture in the U.S. Intelligence Community. An Ethnographic Study*, DC, Washington 2005 oraz A. Tversky, D. Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, „Science, New Series" 1974, vol. 185, no. 4157.

Przy przedstawieniu aspektów technicznych skorzystano w literatury zawartej w rozdziale trzecim oraz takich publikacji jak G. Szpor, K. Czaplicki, *Internet. Analityka danych*, Wydawnictwo C. H. Beck, Warszawa 2019 i R. Baker, *Prawdziwa głębia OSINT*, Helion, 2024. W odniesieniu do bezpieczeństwa operacyjnego skorzystano z dokumentu FAS Intelligence Resource Program, *Operations Security Intelligence Threat Handbook* oraz wytycznych zawartych w *Operations Security Guide (2011), RCC dokument 600-11*, opracowanych przez Range Commanders Council (U.S. Army White Sands Missile Range).

Za przydatne do opracowania kwestii informacyjnych należy uznać takie publikacje jak V. Volkoff, *Psychosocjotechnika, dezinformacja, oręż wojny*, Wydawnictwo Antyk, Komorów 1999, T.R. Aleksandrowicz, *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*, Difin, Warszawa 2021 oraz J.H. Larecki, *Wielki leksykon służb tajnych świata*, Oficyna Wydawnicza RYTM, Warszawa 2017.

Rozdział piąty przedstawia wywiad jawnoźródłowy w Stanach Zjednoczonych, Izraelu i Wielkiej Brytanii. W tym zakresie wykorzystano źródła: S. Marrin, *Revisiting Intelligence and Policy*, Routladge 2014; J. Buckley, *Managing Intelligence. A Guide for Law Enforcement Professionals*, CRC Press, 2014; B. Akhar, P. Saskia Bayerl, F. Sampson, *Open Source Intelligence Investigation. From Strategy to Implementation*, Springer 2016; T. Forminicki, *Wywiad i kontrwywiad jako kluczowe komponenty walki informacyjnej*, Instytu Informacji, Warszawa 2020; L. Wiszniewski, *Rola i znaczenie analizy informacji wywiadowczej w zapewnianiu bezpieczeństwa państwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22 (12). W kontekście analizy wykorzystania wywiadu jawoźródłowego w brytyjskich strukturach bezpieczeństwa oraz jego rosnącej roli w procesie podejmowania decyzji strategicznych szczególnie istotnym źródłem był raport przygotowany przez ekspertów Royal United Services Institute (RUSI) oraz Centre for Emerging Technology and Security (CETaS) – The Future of Open-Source Intelligence for UK National Security (A. Janjeva, A. Harris, J. Byrne, Royal United Services Institute for Defence and Security Studies, 2022). Wiele wartościowych ustaleń w odniesieniu do przedmiotowych kwestii zaczerpnięto ze stron internetowych służb wywiadowczych, w tym witryn Centralnej Agencji Wywiadowczej (ang. *Central Intelligence Agency*, CIA), brytyjskiej Służby Bezpieczeństwa (MI5), a także izraelskich instytucji odpowiedzialnych za działalność wywiadowczą i analityczną, takich jak Instytut ds. Wywiadu i Operacji Specjalnych (Mossad), Służby Wywiadu

Wojskowego (Aman) oraz Służby Bezpieczeństwa Ogólnego (Szabak). Ponadto istotne informacje pozyskano z oficjalnych dokumentów i strategii dotyczących wykorzystania wywiadu jawnoźródłowego, w tym U.S. Intelligence Community OSINT Strategy 2024–2026, dokumentów brytyjskiego Stowarzyszenia Głównych Oficerów Policji Anglii, Walii i Irlandii Północnej (ang. *Association of Chief Police Officers,* ACPO) oraz Krajowej Rady Szefów Policji (ang. *National Police Chief's Council*, NPCC), aktów prawnych regulujących działalność śledczą w Wielkiej Brytanii oraz izraelskich strategii cyberbezpieczeństwa.

Analiza literatury przedmiotu pozwoliła na stwierdzenie, że opublikowane materiały mają głównie charakter przyczynkowy. Dodać należy, że w literaturze polskiej brakuje opracowań w sposób systematyczny i kompleksowy prezentujących zagadnienia wywiadu jawnoźródłowego. Specyfika obszaru badań powoduje, że większość materiałów dotyczących operacyjnej pracy podmiotów wykorzystujących wywiad jawnoźródłowy, zarówno w literaturze krajowej, jak i obcojęzycznej, pozostaje niejawna. Ciężar dostępnych opracowań skupia się na technicznym aspekcie pozyskiwania i analizy jawnoźródłowej, z uwagi na tożsamość tematyki z aspektami technicznymi cyfrowego bezpieczeństwa defensywnego, w tym przeprowadzaniem testów bezpieczeństwa oraz testów penetracyjnych. Kwerenda literatury wskazuje na dysproporcję związaną z brakiem wyeksponowania zagadnień dotyczących wpływu roli i znaczenia wywiadu jawnoźródłowego na bezpieczeństwo państwa. Niniejsza rozprawa ma stanowić uzupełnienie tej luki badawczej.

1.7. Podsumowanie

Istota podjętej problematyki badań zawarta została w rozdziale pierwszym, w którym dokonano szczegółowej charakterystyki podstawowych pojęć będących przedmiotem prowadzonych badań, takich jak bezpieczeństwo państwa oraz wywiad jawnoźródłowy. W celu realizacji badań przyjęto podejście teoretyczno-empiryczne. Zastosowane metody teoretyczne badań to: analiza, synteza, indukcja, dedukcja, porównanie, uogólnienie oraz wnioskowanie. Zastosowane metody empiryczne – jakościowe to: analiza treści, ocena i krytyka, piśmiennictwa, analiza instytucjonalno-prawna (dogmatyczna), analiza historyczno-porównawcza oraz indywidualny wywiad pogłębiony. W zakresie metod jakościowo-ilościowych zastosowano badanie dokumentów urzędowych, studia przypadku oraz badania *desk research*.

Przedmiotem badań dysertacji jest wywiad jawnoźródłowy realizowany w obszarze bezpieczeństwa państwa. Na podstawie sformułowanego przedmiotu badań wyróżniono cel teoretyczny, który stanowi określenie znaczenia wywiadu jawnoźródłowego dla bezpieczeństwa państwa, oraz cel praktyczny, wyrażający się w scharakteryzowaniu możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa.

Główny problem badawczy w pracy to odpowiedź na pytanie: *Jakie znaczenie ma wywiad jawnoźródłowy w zapewnieniu bezpieczeństwo państwa*? Do tak postawionego problemu przyjęto hipotezę główną, zgodnie z którą dynamiczny rozwój otwartych źródeł informacji oraz technologii związanych z możliwością pozyskiwania i masowej dystrybucji informacji, a także coraz szersze wykorzystanie nowych technologii do pozyskiwania i analizy informacji jawnoźródłowych powodują wzrost możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa.W szczególności założono, że informacje dostarczone w wywniku działań wywiadu jawnoźródłowego uzupełniają informacje pozyskane drogą operacyjną, przyczyniają się do skrócenia czasu koniecznego do podjęcia decyzji oraz poprawiają jakość i skuteczność działań państwa zawrówno w wymiarze ofensywnym, jak i defensywnym.

W tab. 1.1 zaprezentowano zestawienie szczegółowych problemów badawczych i hipotez oraz zastosowanych metod badawczych.

W rozdziale pierwszym, po omówieniu elementów metodologicznych, zaprezentowano organizację badań, opisując poszczególne etapy ich realizacji.

Ostatni element stanowiła analiza literatury przedmiotu. Szczególny nacisk położono na dobór literatury uwzględniającej najnowsze badania i teorie w dziedzinie bezpieczeństwa oraz wywiadu jawnoźródłowego, które według autorki miały kluczowe znaczenie dla realizacji niniejszej dysertacji.

Tabela 1.1. Zestawienie szczegółowych problemów badawczych i hipotez oraz zastosowanych metod badawczych

Problem badawczy	**Hipoteza**	**Metody badawcze**
Jaka jest istota i znaczenie wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa?	Dynamiczny rozwój otwartych źródeł informacji oraz technologii związanych z pozyskiwaniem i przetwarzaniem informacji jawnoźródłowych zwiększa potencjał wykorzystania wywiadu jawnoźródłowego w sektorze bezpieczeństwa państwa.	badania literaturowe, metody teoretyczne, *desk research*, wywiad ekspercki
W jakim zakresie dostępne metody i środki prowadzenia wywiadu jawnoźródłowego wpływają na bezpieczeństwo państw?	Założyć można, że nowe technologie umożliwiają efektywne pozyskiwanie informacji jawnoźródłowych, przez co zwiększają precyzję i skracają czas analizy informacji jawnoźródłowych.	badania literaturowe, metody teoretyczne, *desk research*, wywiad ekspercki
Jakie prawne i pozaprawne aspekty wpływają na prowadzenie wywiadu jawnoźródłowego na rzecz bezpieczeństwa państwa?	Uwarunkowania prawne oraz pozaprawne, jak etyczne, metodologiczne, techniczne oraz informacyjne, mają wpływ na wywiad jawnoźródłowy.	studia przypadku, badania literaturowe, badanie dokumentów urzędowych, *desk research*, wywiad ekspercki
Jakie są dotychczasowe kierunki prowadzenia wywiadu jawnoźródłowego na rzecz bezpieczeństwa w wybranych państwach demokratycznych?	Wywiad jawnoźródłowy prowadzony jest w celu zwiększenia zdolności defensywnych i ofensywnych w wybranych państwach demokratycznych.	studia przypadku, badania literaturowe, badanie dokumentów urzędowych, *desk research*, wywiad ekspercki

Źródło: Opracowanie własne.

2. CHARAKTERYSTYKA WYWIADU JAWNOŹRÓDŁOWEGO

Rozważania w niniejszym rozdziale koncentrują się na analizie istoty i znaczenia wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa. Nadrzędnym zamierzeniem tej części jest opracowanie teoretycznego ujęcia zagadnienia i systematyzacja podstawowych pojęć, które posłużą jako podstawa do dalszej analizy. W ramach tej części pracy podjęto próbę odpowiedzi na pierwsze szczegółowe pytanie badawcze: *Jaka jest istota i znaczenie wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa*? Zakres badań obejmuje kwestie definicyjne, w tym cechy i generacje wywiadu jawnoźródłowego, klasyczny cykl wywiadowczy, a także pojęcie, klasyfikację i właściwości informacji jawnoźródłowych. Ponadto analizie poddane zostaną pojęcie oraz klasyfikacja otwartych źródeł informacji, ich specyfika oraz etapy pozyskiwania informacji jawnoźródłowych. Szczególnie istotnym elementem badań w tym rozdziale są zagadnienia związane z opracowywaniem i interpretacją informacji jawnoźródłowych, w tym oceną wiarygodności źródeł oraz metodami analizy, które umożliwiają ich skuteczne wykorzystanie w procesach decyzyjnych. W podsumowaniu rozdziału przedstawiona zostanie odpowiedź o charakterze teoretycznym na postawione pierwsze szczegółowe pytanie badawcze, uwzględniająca wyniki przeprowadzonej analizy. Stanowić to będzie punkt wyjścia do dalszych badań empirycznych oraz kompleksowej konkluzji w tym zakresie.

2.1. Cechy i generacje wywiadu jawnoźródłowego

Przemiany społeczne wynikające z rewolucji informacyjnej oraz postęp technologiczny znacząco wpłynęły na metodykę działań podmiotów odpowiedzialnych za bezpieczeństwo państwa, w tym na metody pracy operacyjnej. Eksperci wywiadu szacują, że większość informacji, które składają się na ostateczny materiał wywiadowczy, pochodzi ze źródeł otwartych[54]. Informacje jawnoźródłowe uzupełniają wiedzę uzyskaną innymi metodami pracy operacyjnej, a w przypadku ich pozytywnej weryfikacji mogą przyczynić się do podjęcia działań wyprzedzających w zakresie

[54] Organizacja Traktatu Północnoatlantyckiego szacuje, że 80% informacji zawartych w materiałach wywiadowczych opracowanych na potrzeby kontroli zbrojeń i proliferacji broni dostępnych jest w źródłach otwartych (NATO, *Open Source Intelligence Reader*, Norfolk, VA: Intelligence Branch, 2002). W 2005 roku były zastępca dyrektora Centralnego Wywiadu W.M. Nolte stwierdził, że 95–98% wszystkich informacji przetwarzanych przez społeczność wywiadowczą USA pochodzi ze źródeł otwartych (S.D. Gibson, *Open-Source Intelligence (OSINT): A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, Appendices: Interview EUROPOL 4, 2007, https://dspace.lib.cranfield.ac.uk/handle/1826/6524 [dostęp: 22.01.2023]).

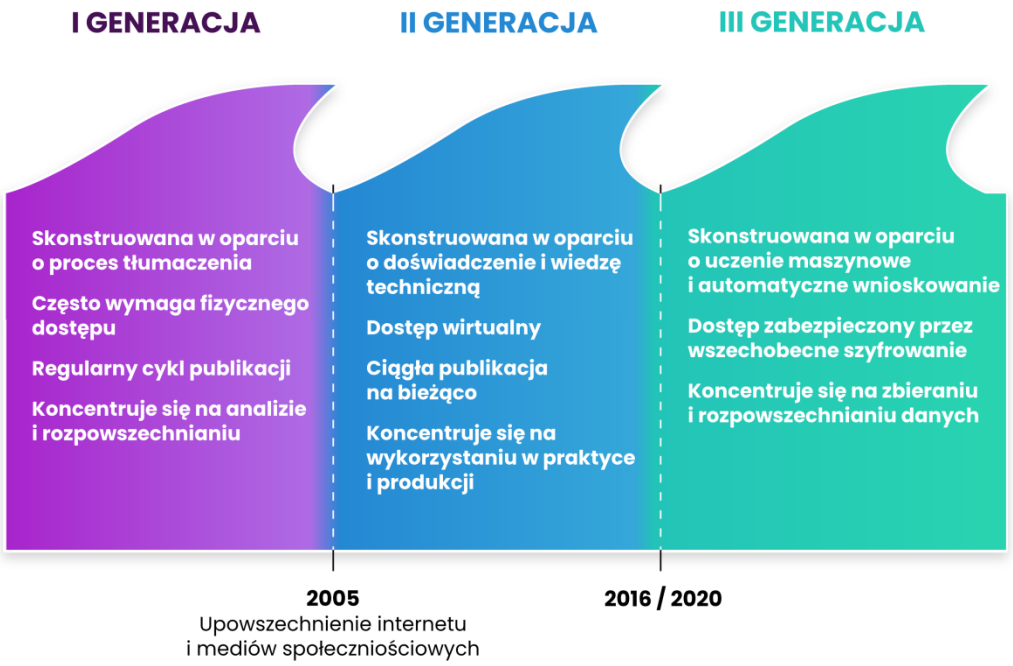
bezpieczeństwa. Ze względu na rosnące możliwości wywiadu jawnoźródłowego rozpoczęcie rozpoznania od eksploracji źródeł otwartych jest praktycznie zawsze uzasadnione[55]. Można wyróżnić takie cechy wywiadu jawnoźródłowego jak[56]:

1. dostarczenie kontekstu prowadzonego rozpoznania poprzez zapewnienie ogólnej wiedzy, „tła" badanego problemu, która stanowi punkt wyjścia do określenia dalszych kierunków rozpoznania. Ilość oraz różnorodność pozyskanych informacji wpływają na uzyskanie trafnej odpowiedzi poprzez dostarczenie szerszego kontekstu społecznego, kulturowego religijnego, ekonomicznego itp.;
2. użyteczność, wynikająca z możliwości szybkiego i tematycznie obszernego pozyskiwania informacji. Wykorzystanie wywiadu jawnoźródłowego przed zastosowaniem innych form gromadzenia danych zazwyczaj prowadzi do obniżenia ich kosztów[57];
3. wsparcie w dokonywaniu ewaluacji informacji uzyskiwanych ze źródeł zamkniętych oraz ich uzupełnienie. Wykorzystanie wywiadu jawnoźródłowego jako integralnej części opracowanego materiału wywiadowczego zapewnia decydentowi wiedzę z całości dostępnych źródeł;
4. lokalizacja źródeł otwartych na „pierwszej" linii informowania, przez co skraca się czas podejmowania decyzji. Dostęp do szczegółowych informacji jawnoźródłowych może zaspokoić potrzeby organizacji, eliminując konieczność korzystania z kosztownych, osobowych lub technicznych źródeł informacji wykorzystywanych w pracy operacyjnej służb;
5. dostarczenie informacji skondensowanych i dokładnych, które mogą zakończyć badaną sytuację decyzyjną lub być wystarczającą podstawą do formułowania nowych hipotez w prowadzonych analizach wywiadowczych;
6. komunikacyjność, czyli łatwiejsze rozpowszechnianie uzyskanej wiedzy w stosunku do dystrybucji informacji, co umożliwia również wymianę informacji zarówno pomiędzy służbami, jak i podmiotami prywatnymi zajmującymi się pozyskiwaniem informacji[58];

[55] J. Konieczny, *Kryminalistyczny leksykon śledztwa*, Wydawnictwo Uniwersytetu Opolskiego, Opole 2020, s. 336.
[56] S.D. Gibson, *Open source intelligence*, op. cit., 2014, s. 127.
[57] J. Konieczny, *Kryminalistyczny leksykon*…, op. cit., s. 335.
[58] H. Minas, *Can the Open-Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the Twenty-First Century*, RIEAS, 2010, s. 33–34, https://rieas.gr/publications/1119-harris-minas-can-the-open-source-intelligence-emerge-as-an-indispensable-discipline-for-the-intelligence-community-in-the-21st-century-rieas-research-paper-no-139-january-2010 [dostęp: 27.03.2025].

7. możliwość prowadzenia czynności analitycznych niemal na bieżąco w stosunku do przebiegu relewantnych faktów.

Historyczny i technologiczny rozwój globalnej sieci doprowadził do zmian w przepływach informacyjnych, czyniąc wywiad jawnoźródłowy bardziej złożonym, zarówno pod względem dostępnych źródeł, jak i stosowanych metod oraz narzędzi. Ta znacząca transformacja bezpośrednio wpłynęła na sposób działania wywiadu jawnoźródłowego. Wydaje się zatem celowe wyróżnienie kolejnych generacji OSINT-u, przyjmując za momenty graniczne etapy rozwoju World Wide Web, tj. Sieć 1.0, Sieć 2.0 i Sieć 3.0[59]. Kolejne stopnie rozwoju sieci korespondują z jednej strony z postępem technologicznym, z drugiej zaś są odpowiedzią na ciągle rosnące potrzeby w zakresie ułatwienia procesu pozyskiwania żądanych przez użytkowników informacji. Na rysunku 2.1 przedstawiono wybrane cechy charakterystyczne generacji OSINT oraz możliwości kolejnych wyzwań i kierunków ich rozwoju.



Rysunek 2.1. Generacje wywiadu jawnoźródłowego

Źródło: Opracowanie własne na podstawie: H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, Rand Corporation, 2018, s. 40, https://www.rand.org/pubs/research_reports/RR1964.html [dostęp: 27.03.2025].

[59] H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, Rand Corporation, 2018, s. 39, https://www.rand.org/pubs/research_reports/RR1964.html [dostęp: 27.03.2025].

Sieć 1.0, która pojawiła się w latach 90. XX wieku, charakteryzowała się prostotą i brakiem interaktywności. Witryny Sieci 1.0 mają statyczny charakter[60], a ich treści są generowane i kontrolowane przez twórców, co ogranicza aktywność użytkowników do biernego odbioru informacji. Taki model komunikacji można przyrównać do triady mediów klasycznych, tj. prasy, radia i telewizji. W tym okresie praca wywiadowcza stanowiła domenę służb specjalnych, a informacje pozyskane z Sieci 1.0 były dodatkiem do informacji pochodzących z prasy drukowanej, radia, telewizji i szarej literatury. Analiza wywiadowcza opierała się głównie na zbieraniu informacji, ich monitorowaniu, rozpowszechnianiu oraz tłumaczeniu materiałów zagranicznych. Takie działania wyróżniaj pierwszą generację OSINT-u.

Rozwój technologiczny, wsparty potrzebą zmiany paradygmatu interakcji między właścicielami serwisów a ich użytkownikami, przyczynił się do powstania w 2004 roku Sieci 2.0[61]. Charakteryzuje się ona zwiększoną interaktywnością i partycypacją użytkowników w tworzeniu treści. Ten etap rozwoju sieci spowodował przesunięcie punktu ciężkości działań wywiadowczych i zwiększył udział informacji jawnoźródłowych w prowadzonych operacjach.

Przejście do Sieci 2.0 rozpoczyna rozwój mediów społecznościowych, takich jak Facebook, YouTube, Twitter, które w czasie rzeczywistym mogą dostarczyć informacje dla wywiadu jawnoźródłowego. Począwszy od Sieci 2.0, kiedy zasadniczo wzrosła ilość przesyłanych danych, rozpoczyna się druga generacja OSINT-u[62].

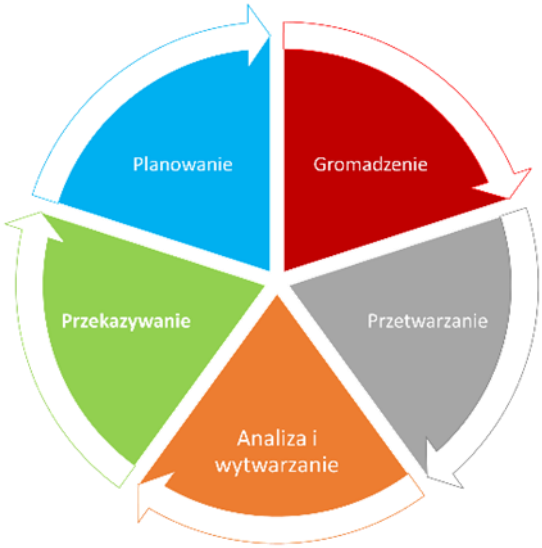
Dalsza ewolucja technologiczno-społeczna doprowadziła do powstania w 2016 roku Sieci 3.0, określanej też jako „sieć współpracy" czy „sieć semantyczna"[63]. Sieć 3.0 wykorzystuje sieci neuronowe, algorytmy genetyczne oraz inne zaawansowane technologie, które umożliwiają tworzenie rozbudowanych, semantycznie powiązanych baz danych, dostępnych dla aplikacji innych niż standardowe przeglądarki internetowe. Tak znacząca zmiana paradygmatu wymiany informacji jest podstawą do wyodrębnienia trzeciej generacji OSINT-u, której wyzwaniem są m.in. przepływy

[60] T. Berners-Lee, R. Cailliau, R. Luotonen, A. Nielsen, A. Secret, *The World-Wide Web*, „Communications of the ACM" 1994, vol. 37, no. 8, s. 76–82, http://dx.doi.org/10.1145/179606.179671 [dostęp: 3.03.2021].
[61] D. Benito-Osorio, M. Peris-Ortiz, C.R. Armengot, A.C. Colino, *Web 5.0: the future of emotional competences in higher education*, „Global Business Perspectives" 2013, vol. 1, no. 3, s. 274–287, https://doi.org/10.1007/s40196-013-0016-5 [dostęp: 1.02.2021].
[62] H.J. Williams, I Blum, *Defining Second Generation*…, op. cit., s. 2.
[63] J. Markoff, *Entrepreneurs See a Web Guided by Common Sense*, „The New York Times" 2006, https://www.nytimes.com/2006/11/12/business/12web.html [dostęp: 1.02.2021].

informacyjne oparte na uczeniu maszynowym, powszechne szyfrowanie danych, rozszerzona rzeczywistość oraz psychometria[64].

2.2. Klasyczny cykl wywiadowczy

Cykl wywiadowczy stanowi strukturę mnemotechniczną ukazującą przebieg poszczególnych działań wywiadowczych jako proces. Elementami tego procesu są: planowanie, zbieranie danych, przetwarzanie, analiza i wytwarzanie oraz przekazywanie (rys. 2.2).



Rysunek 2.2. Klasyczny cykl wywiadowczy
Źródło: Opracowanie własne.

Klasyczny cykl wywiadowczy modelowany jest jak proces produkcyjny, w którym wymagania dotyczące działalności wywiadowczej ze strony podmiotów zainteresowanych generują aktywność wywiadowczą. W wyniku tego procesu powstaje produkt wywiadowczy – informacja, która staje się podstawą do doskonalenia lub dostosowania wymagań w kolejnym cyklu. Takie ujęcie jest prezentowane jako adekwatne do wszelkiego rodzaju prowadzonej, również instytucjonalnie, działalności rozpoznawczej i określane mianem „klasycznego". Schemat ten ma zastosowanie do wywiadu jawnoźródłowego, choć w zestawieniu szczegółowym może mieć inną konfigurację, zależną od stopnia zaangażowania podmiotów zajmujących się pozyskiwaniem danych i ich analizą. Inne proponowane modele akcentują etapy

[64] H.J. Williams, I. Blum, *Defining Second Generation*…, op. cit., s. 40.

gromadzenia i analizy informacji, przy czym liczba etapów jest ograniczona do trzech[65] lub rozszerzona do siedmiu[66].

Pierwszym etapem klasycznego cyklu wywiadowczego jest planowanie. Obejmuje ono określenie problemu decyzyjnego poprzez wskazanie wymagań i celów dla działań rozpoznawczych, zaplanowanie działań i metod wywiadowczych oraz określenie środków finansowania. Definiowanie problemu w analizie wywiadowczej rozpoczyna się od odpowiedzi na pytania dotyczące czasu (na kiedy jest oczekiwany rezultat?), odbiorcy (kto jest finalnym użytkownikiem informacji?), celu (jaki jest cel prowadzonej analizy?), formy produktu wywiadowczego (w jakiej formie należy przekazać produkt wywiadowczy?) oraz tła procesu (jakie są faktyczne pytania, tło postawionego problemu)[67]. Efektywny przebieg tego etapu warunkuje zgodność produktu wytworzonego z produktem żądanym. Jest to uzależnione od jakości współpracy pomiędzy decydentem a analitykiem, doskonaleniem procesu poprzez doprecyzowanie stawianych pytań oraz dochowaniem analitycznej uczciwości[68].

Zbieranie danych polega na przemyślanym pozyskiwaniu danych, które są niezbędne do opracowania dokumentu wywiadowczego, rozpoczynając od identyfikacji potencjalnie użytecznych informacji, a kończąc na retencji zgromadzonego materiału. Organizacja pozyskiwania danych warunkowana jest ustaleniami dokonanymi w fazie planowania. Wymaga celowego i sprawnego zarządzania wzajemnymi powiązaniami osób i urządzeń uczestniczących w procesach gromadzenia informacji, ustalonych reguł i ich współdziałania[69].

Przetwarzanie informacji polega na tworzeniu nowych informacji na podstawie wcześniej zgromadzonych i zapisanych na materialnych nośnikach danych, wyrażonych w określonym języku w ramach konkretnego procesu informacyjnego[70]. Przetwarzanie informacji obejmuje zmianę formy pozyskanych wcześniej danych na jednolitą, niezależnie od źródła ich pochodzenia. Proces ten obejmuje translację, transkrypcję i agregację danych, które mogą występować w różnych sekwencjach czasowych. Translacja polega na przekształceniu informacji wyrażonych w jednym języku na informację wyrażoną w innym języku. Transkrypcja to dokładna konwersja mowy lub

[65] J. Ratcliffe, *Intelligence-Led Policing*, Routledge, London 2016, s. 110.
[66] Central Intelligence Agency, *Factbook on Intelligence*, https://irp.fas.org/cia/product/facttell/index.html [dostęp: 1.02.2021].
[67] R.M. Clark, *Intelligence Analysis. A Target-Centric Approach*, Sage, 2013, s. 21–22.
[68] J. Nicoll, *Task Definition*, [w:] J.H. Ratcliffe (red.), *Strategic Thinking in Criminal Intelligence*, The Federation Press, Sydney 2009, s. 67.
[69] J. Oleński, *Ekonomika informacji. Metody*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2003, s. 72.
[70] Ibidem, s. 90.

materiałów audiowizualnych na formę tekstową. Proces agregacji danych może składać się z redukcji lub reorganizacji danych. Kolejny etap przetwarzania stanowi integracja, w ramach której analizowane informacje są selekcjonowane i łączone w całość w toku tworzenia kolejnego komunikatu[71].

Analiza informacji polega na nadawaniu sensu zgromadzonym danym poprzez ich zestawienie, ocenę wiarygodności, interpretację i syntezę, z uwzględnieniem kontekstu. Obejmuje również prawidłowe wnioskowanie dotyczące ich użyteczności. Ocena wiarygodności odnosi się zarówno do rzetelności źródła informacji, jak i samych informacji. Efektem procesu analizy jest wytworzenie dokumentu wywiadowczego lub rekordu w bazie danych.

Ostatni etap klasycznego cyklu wywiadowczego, tj. przekazywanie, polega na rozpowszechnianiu raportu wywiadowczego lub udostępnieniu rekordu w bazie danych decydentom. Ta czynność kończy klasyczny cykl wywiadowczy. Przekazany wynik może być też wykorzystany na potrzeby kolejnej analizy w innym zakresie.

Z punktu widzenia analizy systemowej proponowane modele cyklu wywiadowczego nie ukazują w sposób kompleksowy złożoności zachodzących procesów. Nie pozwalają również na określenie, „kto" i „co" mogą wpłynąć na zakończenie poszczególnego etapu cyklu. Proponowany model w ujęciu systemowym oparty jest na schemacie[72]:

wejście –> proces –> wyjście

Taka struktura modelu przedstawia zarówno proces analityczny, czynniki wpływające na końcowy produkt wywiadowczy, jak i wpływ zmian zachodzących na dowolnym etapie cyklu na pozostałe elementy modelu.

W ujęciu analizy systemowej budowa modelu wywiadowczego wymaga identyfikacji poszczególnych etapów procesu, estymacji parametrów oraz uwzględnienia ryzyka i niepewności decyzyjnej. Proces ten obejmuje analizę celu rozpoznania, identyfikację ograniczeń, ocenę funkcji systemu oraz opracowanie modelu decyzyjnego, ze szczególnym uwzględnieniem zależności między jego elementami oraz

[71] NATO Standardization Office, *AAP-6: Słownik terminów i definicji NATO*, NATO, 2017, s. 250, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf [dostęp: 5.02.2024].
[72] R. Johnston, *Analytic Culture in the U.S. Intelligence Community. An Ethnographic Study*, Washington, DC, 2005, s. 47 i nast.

ich wpływu na efektywność działań[73]. Jego istotnym elementem jest stały dialog pomiędzy decydentem a analitykiem**.** Przedstawienie cyklu wywiadowczego w kategoriach analizy systemowej jest przydatne w procesie definiowania i unikania błędów analitycznych[74].

W warunkach dynamicznych zmian technologicznych i środowiska informacyjnego założenia w zakresie prowadzenia działalności wywiadowczej ulegają przeobrażeniom, a sam klasyczny cykl wywiadowczy postrzegany jest jako propedeutyczny schemat działania[75]. W ujęciu klasycznym decydent inicjuje cykl, który zatacza koło według wyznaczonego schematu. W praktyce mechanizm współdziałania podmiotów pozyskujących i wykorzystujących informacje jawnoźródłowe jest dynamiczny. Interakcje pomiędzy poszczególnymi wyróżnionymi etapami mogą zachodzić w dowolnym momencie cyklu[76]. W obszarze bezpieczeństwa państwa wynika to również z charakterystyki działania i zadaniowania służb informacyjnych, gdzie jedynym z obowiązków jest przekazywanie informacji o zagrożeniach również w przypadkach braku wcześniejszego ich ujęcia na liście celów informacyjnych. Poszczególne etapy cyklu w wywiadzie jawnoźródłowym są uszczegółowione z uwagi na specyfikę otwartych źródeł informacji. W tabeli 2.1 przedstawiono zestawienie działań w tych etapach.

W zarządzaniu informacją wykorzystywaną na potrzeby przygotowywania decyzji – fazy poprzedzające wskazane w klasycznym ujęciu cyklu są istotne dla merytorycznej i metodologicznej prawidłowości przebiegu analizy wywiadowczej.

[73] Zob. szerzej: P. Sienkiewicz*, Analiza systemowa. Podstawy i zastosowania*, Wydawnictwo BELLONA, Warszawa 1994, s. 36 i nast.
[74] T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Editions Spotkania, Warszawa 2016, s. 71.
[75] J. Konieczny (red.), *Analiza informacji w służbach policyjnych i specjalnych*, Wydawnictwo C.H. Beck, Warszawa 2012, s. 11.
[76] W wywiadzie jawnoźródłowym w dowolnym momencie cyklu wywiadowczego może dojść do ponownego ustalenia zakresu (ang. *scoping*) informacji, które powinny zostać pozyskane poprzez zredefiniowanie wymagań i ponowne ukierunkowanie zapytań. Jeśli wynikiem procesu ustalenia zakresu jest ich zmiana, dochodzi do przerwania etapu przetwarzania, a cały cykl wywiadowczy zainicjowany jest od początku. Ustalenie zakresu pozwala na uniknięcie błędów i doprecyzowanie prowadzonych działań. Por. szerzej: R. Baker, *Prawdziwa głębia OSINT. Odkryj wartość danych Open Source Intelligence*, Helion, Gliwice 2024, s. 69.

Tabela 2.1. Zestawienie działań w poszczególnych etapach cyklu wywiadu jawnoźródłowego

Etap cyklu wywiadowczego	**Działania**
Planowanie	• określenie problemu decyzyjnego • określenie zbioru źródeł • określenie kryteriów wyszukiwania danych/informacji • wybór oraz zaplanowanie środków i metod pozyskiwania i przetwarzania informacji
Gromadzenie	• identyfikacja potencjalnie użytecznych informacji • techniczne zebranie i transfer materialnych nośników • zorganizowanie danych • retencja danych/informacji
Przetwarzanie	• tagowanie danych i informacji • indeksowanie źródła • korelowanie, klasyfikowanie, grupowanie • podział, selekcja • translacja, transkrypcja • generowanie nowej informacji • agregacja (redukcja, reorganizacja danych) • integracja
Analiza	• autentykacja • ocena wiarygodności • kontekstualizacja • analiza zgromadzonych danych i informacji
Przekazywanie	• przekazanie opracowanego materiału do określonego podmiotu, w określonym czasie i formie

Źródło: Opracowanie własne.

2.3. Pojęcie i klasyfikacji informacji jawnoźródłowych

2.3.1. Pojęcie danych i informacji jawnoźródłowych oraz ich cechy

Podstawowymi pojęciami zdefiniowanymi zarówno przez amerykańskie służby specjalne, jak i przez ekspertów oraz praktyków współpracujących w ramach publikacji Sojuszu Północnoatlantyckiego są: **dane jawnoźródłowe** (ang. *open source data*, OSD), **informacje jawnoźródłowe** (ang. *open source information*, OSIF), **wywiad jawnoźródłowy** (ang. *open source intelligence*, OSINT) oraz **zweryfikowany wywiad jawnoźródłowy** (ang. *validated open source intelligence*)[77]. Na rysunku 2.3 zaprezentowano wizualizację przetwarzania danych w wywiadzie jawnoźródłowym.

[77] *NATO Open-Source Intelligence Handbook*, op. cit., s. 2.

Rysunek 2.3. Przetwarzanie danych w wywiadzie jawnoźródłowym
Źródło: Opracowanie własne.

Dane jawnoźródłowe to dane w stanie „surowym", które pochodzą z pierwotnego źródła, w postaci drukowanej, z nośników telewizyjnych, radiowych, wystąpień publicznych, stron internetowych (np. komercyjne zdjęcie satelitarne, zapisy elektroniczne, audycje obrazujące poglądy osób publicznych). Pozyskane dane można sklasyfikować ze względu na ich format na: dane ustrukturyzowane, częściowo ustrukturyzowane i dane nieustrukturyzowane. Dane ustrukturyzowane są uporządkowane według podstawowego modelu danych w sposób umożliwiający niezawodną identyfikację poszczególnych stwierdzeń, faktów oraz ich wszystkich składników. Dane nieustrukturyzowane nie mają z góry zdefiniowanego modelu danych albo nie są zorganizowane w z góry określony sposób. Dane częściowo ustrukturyzowane mogą zawierać obie formy powyżej opisanych danych. W tabeli 2.2 przedstawiono przykłady danych ustrukturyzowanych, częściowo ustrukturyzowanych i nieustrukturyzowanych.

Tabela 2.2. Przykłady ustrukturyzowanych, częściowo ustrukturyzowanych i nieustrukturyzowanych danych jawnoźródłowych

Dane ustrukturyzowane	**Dane częściowo ustrukturyzowane**	**Dane nieustrukturyzowane**
Bazy danych, modele danych	formaty XML/JSON	bez struktury, dowolny tekst
Bazy danych pozyskane za zgodą	API mediów społecznościowych	strony internetowe, blogi, fora internetowe, wikis
Listy wyborcze	otwarte dane (np. dane pochodzące z administracji publicznej)	raporty, publikacje akademickie
Dane statystyczne	Google / interfejsy API wyszukiwania Bing	książki
Geonazwy, badanie uzbrojenia	kanały RRS	dokumenty Word
	arkusze	media
		zdjęcia satelitarne
		widok ulicy
		zawartość głębokiego/czarnego Internetu

API – interfejs oprogramowania aplikacji; JSON (ang. *JavaScript Object Notation*) – lekki format wymiany danych komputerowych; RSS (ang. *Really Simple Syndication*) – format wymiany danych umożliwiający subskrypcję i automatyczne pobieranie treści ze stron internetowych; XML (ang. *Extensible Markup Language*) – język znaczników i format pliku do przechowywania, przesyłania i rekonstrukcji dowolnych danych.

Źródło: Opracowanie na podstawie: H. Gibson, *Acquisition and Preparation of Data for OSINT Investigations*, [w:] B. Akhgar, P. Saskia Bayerl, F. Sampson, *Open-Source Intelligence Investigation. From strategy to Implementation*, Springer, 2016, s. 74.

Na tym etapie wraz z danymi pozyskiwane są również metadane. Metadane to strukturalne informacje, które pomagają w opisie, wyjaśnianiu, lokalizowaniu oraz zarządzaniu zasobami informacji, a także ułatwiają ich odnajdywanie i wykorzystywanie[78]. Metadane dostarczają informacji umożliwiających uporządkowanie zebranych danych, a ich jakość bezpośrednio wpływa na możliwość wyszukiwania i wykorzystania zasobów. Na gruncie polskiego piśmiennictwa dane jawnoźródłowe są dzielone na dane wymierne i dane opisowe. Dane wymierne prezentują określoną wartość, identyfikują obiekty, miejsca, osoby oraz zjawiska. Dane opisowe prezentują jakość danych wymiernych, ich cechy, właściwości oraz czynności bezpośrednio związane z aktywnością podmiotów wyrażonych przez te dane[79]. Efektem przetworzenia zebranych danych jawnoźródłowych jest powstanie informacji jawnoźródłowej.

[78] NISO, *Understanding Metadata*, 2017, https://www.niso.org/publications/understanding-metadata-2017 [dostęp: 7.06.2022].
[79] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011, s. 51.

Informacje jawnoźródłowe to zinterpretowane dane, które zostały zebrane w pierwszym etapie (OSD), a następnie przygotowane poprzez ich zgrupowanie i wstępną analizę. Dane zawarte w tych informacjach podlegają procesom wstępnej ewaluacji, z uwzględnieniem czasu publikacji informacji i ich zawartości, dlatego możliwa jest ich prezentacja decydentowi[80]. W zależności od charakteru danych przetwarzanie obejmuje translację, transkrypcję, konwersję formatu, dodatkowo filtrowanie, korelację, klasyfikację, grupowanie oraz interpretacje podanych danych. W wyniku integracji, oceny i analizy wykonanej w celu rozwiązania konkretnego zapytania powstaje **produkt wywiadowczy**.

Dodatkowym etapem opisanym w podręczniku NATO jest zweryfikowanie informacji jawnoźródłowych przy użyciu innych metod pracy wywiadowczej przez pracowników wywiadu posiadających dostęp do informacji niejawnych. Za zweryfikowany jawnoźródłowy materiał wywiadowczy (ang. *validated OSINT*) jest uznawana również informacja pochodząca ze źródła, co do którego autentyczności i wiarygodności nie ma żadnych wątpliwości[81].

Najistotniejsze cechy informacji, zależne od parametrów technicznych i organizacyjnych systemów informacyjnych, to aktualność, relewantność, przyswajalność, kompletność oraz wiarygodność[82]. Informację uznaje się za aktualną, gdy jej zapis, dostępny w danej chwili, opisuje w dopuszczalnych granicach błędów teraźniejszy stan pewnych, interesujących zjawisk. Relewantność oznacza, że informacja nie zawiera elementów, które są zbędne z punktu widzenia użytkownika. Informację uważa się za przyswajalną, gdy bez dodatkowych przekształceń formy jej prezentacji istnieje możliwość jej wykorzystania. Kompletność oznacza zawartość rzeczywistych informacji o stanie rzeczy w danej wiadomości. Wiarygodność informacji znaczy, że istnieje określony stopień pewności, że jest to informacja prawdziwa lub ścisła. Powyższy katalog cech informacji może zostać uzupełniony[83] o dokładność, rozumianą jako precyzyjne sformułowanie treści oraz jej dostosowanie do poziomu wiedzy odbiorcy. Istotna jest również spójność, czyli wewnętrzna zgodność informacji, jej logiczna ciągłość oraz jednolitość w zakresie prezentacji i przekazu, co eliminuje sprzeczności i umożliwia jej efektywne wykorzystanie. Kolejnym atrybutem informacji jest adekwatność formy, oznaczająca, że sposób jej przedstawienia

[80] Ibidem.
[81] *NATO Open-Source Intelligence Handbook*, op. cit., s. 3.
[82] P. Sienkiewicz, *Analiza systemowa*…, op. cit. s. 146–147.
[83] K. Liderman, *Bezpieczeństwo informacyjne. Nowe wywzania*, PWN SA, Warszawa 2017, s. 16.

minimalizuje ryzyko błędnej interpretacji, ułatwia przyswojenie treści i wspiera skuteczność w procesach decyzyjnych.

Wszystkie te elementy, stanowiące kryteria jakości informacji, determinują jej przydatność w procesach decyzyjnych dotyczących bezpieczeństwa państwa. W analizach prowadzonych w tym obrszarze istotne jest więc pozyskiwanie informacji wartościowych, użytecznych i mających wysoką jakość.

Dla procesu decyzyjnego istotne jest, aby pozyskane informacje jawnoźródłowe posiadały cechę użyteczności. Jest to właściwość wyrażająca wpływ informacji na trafność podejmowanych decyzji, a co za tym idzie – skuteczność zarządzania[84]. Każda informacja, która zmniejsza niepewność w podejmowaniu decyzji, jest informacją użyteczną. Relacja pomiędzy użytecznością informacji a jej jakością wyraża się w wartości informacji. Dane, które powinien zawierać komunikat, by być użytecznym dla decydentów, dotyczą istoty, lokalizacji przestrzennej i czasowej problemu, najistotniejszych przyczyn jego powstania, jego aktualnych i potencjalnych skutków oraz stopnia zrutynizowania problemu[85].

Pojęcie informacji jawnoźódłowych ewoluuje, będąc odzwierciedleniem zmian technologicznych i społecznych, które wpływają na powstawanie i rozwój nowych, otwartych źródeł informacji. Ich specyfika wywodzi się bezpośrednio ze źródła, z którego pochodzą.

2.3.2. Otwarte źródła informacji

Każda informacja ma swoje **źródło.** Źródłem informacji jest podmiot, który ją tworzy, przechowuje i przekazuje[86]. Podział źródeł informacji nie jest prosty jako, że współcześnie poszczególne ich kategorie silnie się przenikają. Otwarte źródła informacji wyróżniają się cechami, które są przeciwieństwem wywiadu opartego na pracy operacyjnej. W tabeli 2.3 przedstawiono cechy wywiadu opartego na niejawnych i jawnych źródłach.

[84] T. Jemioło, P. Sienkiewicz, *Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analiza zagrożeń i ryzyka*, t. 1, *Raport z badań*, AON, Warszawa 2004, s. 173.
[85] Ibidem, s. 184.
[86] K. Liedel, T. Serafin, *Otwarte źródła informacji*…, op. cit., s. 57.

Tabela 2.3. Cechy wywiadu opartego na niejawnych i jawnych źródłach informacji

Otwarte źródła informacji	**Operacyjne źródła wywiadowcze**
Otwarty dostęp	ograniczony dostęp
Niedrogi	kosztowny
Nieznana wiarygodność	znana wiarygodność
Brak zależności	istnieją zależności
Brak struktury	określona struktura
Niskie ryzyko	wysokie ryzyko
Niskie zagrożenie wtargnięcia	wysokie zagrożenie wtargnięcia
Jawne	niejawne

Źródło: *NATO Open-Source Intelligence Reader*, 2002, s. 86.

Źródła informacji dzielone są na jawne i niejawne. Źródła jawne to źródła powszechnie dostępne. Źródła niejawne charakteryzowane są z uwagi na podmiot pozyskujących informacje w sposób skryty (działania służb operacyjnych). Są to informacje agenturalne, dane z satelitów szpiegowskich, obserwacja towarzysząca, nasłuch elektromagnetyczny.

Źródła informacji dzielone są również na otwarte i zamknięte. Cechą charakterystyczną źródeł zamkniętych jest ograniczony dostęp i brak możliwości ich dowolnego wykorzystania. Źródła otwarte nie są objęte żadną formą ochrony – można z nich korzystać legalnie i bez ograniczeń. Określenie źródła otwartego zostało doprecyzowane w nomenklaturze amerykańskiego wywiadu. To osoba albo inny podmiot, który dostarcza informacji nieobjętej ochroną prywatności lub niechronionej przed upublicznieniem[87]. Źródła otwarte można podzielić według kryterium dostępności na źródła ogólnie dostępne, o ograniczonej dostępności i źródła relatywnie niedostępne[88]. Do pierwszej kategorii zalicza się źródła, z których pozyskanie informacji nie wymaga szczególnych kwalifikacji. Są to mass media, Internet i dostępne darmowe bazy danych, wydawnictwa branżowe i specjalistyczne, spisy wokand sądowych. Dostęp do źródeł o ograniczonej dostępności wymaga poniesienia określonych nakładów, np. poprzez wykupienie dostępu do bazy danych. Przykładami drugiej kategorii źródeł są Zakład Ubezpieczeń Społecznych (ZUS), firmy ubezpieczeniowe, urzędy celne, komornicy, raporty Najwyższej Izby Kontroli (NIK). Źródła relatywnie niedostępne, inaczej operacyjne, to źródła, do których dostęp jest możliwy poprzez wykorzystanie metod niejawnych.

[87] National Open Source Enterprise, op. cit., F 1-4, za: K. Liedel, T. Serafin, *Otwarte źródła informacji*…, op. cit., s. 50.
[88] T.R. Aleksandrowicz, *Podstawy walki*…, op. cit., s. 73–74.

Ogólnie dostępne źródła informacji można podzielić na pierwotne, wtórne i pochodne[89]. Źródła pierwotne zawierają oryginalny opis spostrzeżeń, obserwacji, procesów oraz badań. Zalicza się do nich m.in.: bazy danych, hurtownie danych, wyszukiwarki, Krajowy Rejestr Sądowy (KRS), bazy przedsiębiorców, notowania giełdowe, rejestry pojazdów, polisy i szkody ubezpieczeniowe, europejską wyszukiwarkę prawników oraz wszelkie dane statystyczne. Źródła wtórne gromadzą, przetwarzają i publikują informacje pochodzące ze źródeł pierwotnych. Dzielą się one na wystąpienia publiczne (np. debaty, wykłady itp.), dokumenty publiczne (np. fotografie, rysunki, dokumenty drukowane, archiwa, książki, gazety itp.), transmisje publiczne (np. radio, telewizja) oraz Internet (np. komunikatory, zawartość stron internetowych, usługi internetowe). Źródła pochodne natomiast to zasoby informacyjne innych procesów lub systemów informacyjnych wykorzystywane w danym procesie jako źródło informacji[90]. Przykładami są informacje rozpowszechniane przez media, systemy informacji podatkowej, celnej, bankowej.

Z uwagi na różnorodność otwartych źródeł informacji OSINT stanowi dziedzinę interdyscyplinarną, w której istotne jest zarówno wykorzystanie nowych technologii do poznania i oceny zjawisk, ale także szerokiej wiedzy z zakresu filologii, językoznawstwa, bibliotekoznawstwa, językoznawstwa czy historii.

2.3.3. Klasyfikacja otwartych źródeł informacji

Jednoznaczna klasyfikacja otwartych źródeł informacji jest trudna z uwagi na przenikanie się ich poszczególnych kategorii oraz nakładanie dyscyplin wywiadowczych. Otwarte źródła informacji stanowią osoby (lub inne podmioty) dostarczające informacji nieobjętych ochroną oraz wszystkie jawne nośniki informacji i urządzenia umożliwiające dostęp do danych. Otwarte źródła informacji można podzielić ze względu na rodzaj kanału, jakim są przekazywane informacje publicznie dostępne, na:

- treści pozyskane z obserwacji;
- dokumenty papierowe;
- treści transmitowane w radiu i telewizji;
- treści cyfrowe[91].

[89] J. Oleński, *Ekonomika informacji. Podstawy*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2001, s. 49.
[90] Ibidem, s. 49–55.
[91] OSINT Foundation, *Mediums of Publicly Available Information*, 2023, Document Number: 20230304-01a, s. 2, https://www.osintfoundation.com/osint/Standards.asp [dostęp: 4.03.2023].

Gromadzenie informacji jawnoźródłowych poprzez obserwację ma charakter doświadczalny. Informacje jawnoźródłowe pozyskiwane są bezpośrednio od osób fizycznych lub grup osób, które w różnej formie, m.in. za pośrednictwem spotkań naukowych, dyplomatycznych, debat eksperckich, wydarzeń publicznych, demonstracji, dostarczają informacji niewystępujących jeszcze w sformalizowanych źródłach. Poza tymi formami informacje jawnoźródłowe mogą być gromadzone w ramach oficjalnych kontaktów politycznych, zarówno krajowych, jak i międzynarodowych, obejmujących działalność dyplomatów, attaché wojskowych, przedstawicieli handlowych oraz instytucji wojskowych i kulturalnych [92]. Interakcje te umożliwiają pozyskiwanie informacji dotyczących polityki zagranicznej, strategii obronnych, relacji gospodarczych oraz współpracy międzynarodowej. Informacje jawnoźródłowe mogą być też pozyskiwane w drodze obserwacji informacji utrwalonych na środkach materialnych, takich jak znaki czy transparenty[93].

Dokumentem jest zarejestrowana informacja w formie właściwej dla danego miejsca i czasu bez względu na jej fizyczną formę albo cechy[94]. Do tej grupy otwartych źródeł informacji należą: prasa, książki, materiały promocyjne, dokumenty badawcze, dokumenty rządowe, raporty przedsiębiorców i organizacji, instrukcje, mapy oraz szara literatura. Upowszechnienie drukowanych źródeł informacji zwiększyło ich dostępność, powodując wzrost znaczenia informacji ogólnodostępnych[95]. Prasa jest jednym z najstarszych środków masowego przekazu, pełniącym funkcje informacyjne, opiniotwórcze, kontrolne w stosunku do działań aparatu władzy oraz konsolidujące daną grupę odbiorców. Rodzaj prasy jest wyodrębniany na podstawie kryteriów: częstotliwości ukazywania się (dzienniki, tygodniki, miesięczniki itd.), nakładu (niskonakładowa, masowa), zasięgu (lokalna, regionalna, ogólnokrajowa, międzynarodowa), wydawcy i właściciela (rządowa, partyjna, niezależna, naukowa), światopoglądu (konserwatywna, liberalna, socjalistyczna), tematyki (kulturalno-społeczna, sportowa, ekonomiczna), adresata (młodzieżowa, kobieca, dla mężczyzn), jakości (dzienniki prestiżowe, czasopisma opinii, prasa bulwarowa, sensacyjna), funkcji

[92] A. Kozera, A. Żebrowski, *Agentura wywiadu i kontrwywiadu II Rzeczypospolitej Polskiej uczestnikiem walki informacyjne. Wybrane aspekty,* [w:] H. Ćwięk, M. Siewier (red.), *Wywiad i kontrwywiad a bezpieczeństwo Polski odrodzonej po 1918 roku*, ABW i IPN, Warszawa 2019, s. 203.
[93] Ibidem, s. 3.
[94] K. Liedel, T. Serafin, *Otwarte źródła informacji*…, op. cit., s. 62.
[95] A. Wojciulik, *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków*, [w:] W. Filipkowski, W. Mądrzejewski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, C.H. Beck, Warszawa 2012, s. 46.

społecznych (informacyjna, publicystyczna, ogłoszeniowa)[96]. W prasie mogą być publikowane również informacje niejawne, dotyczące bezpieczeństwa państwa, które są przekazywane przez sygnalistów.

Źródłem wiedzy specjalistycznej jest również „szara literatura" (ang. *grey literature*). Są to publikacje niekontrolowane przez komercyjnych wydawców, przez co trudniejsze do zidentyfikowania i pozyskania niż publikacje tradycyjne. Szara literatura wydawana jest na wszystkich poziomach: rządu, nauki, biznesu i przemysłu[97]. Tradycyjnie szara literatura oznacza drukowane książki i czasopisma, a szare informacje rozciągają się na inne rodzaje mediów[98]. Szara literatura kolportowana jest w ograniczonej liczbie egzemplarzy do konkretnego, ograniczonego kręgu użytkowników. To dokumenty o ograniczonym upublicznieniu, takie jak sprawozdania i raporty naukowe, techniczne, ekonomiczne, społeczne i inne, powstające w instytucjach publicznych i prywatnych, materiały konferencyjne niepublikowane i niedostępne za pośrednictwem handlowych sieci księgarskich, różnego rodzaju normy i zalecenia techniczne, tłumaczenia niepublikowane oraz inne rodzaje wypowiedzi pisemnych, udostępniane wąskiemu gronu odbiorców[99]. Istotną cechą szarej literatury jest jej aktualność, dokumenty nieoficjalne są publikowane szybciej niż formalne publikacje. Kolejną cechę stanowi jej kompletność, gdyż informacje zawarte w tego typu publikacjach są bardzo zwięzłe, szczegółowe i konkretne. Szara literatura zawiera informacje unikatowe, które nie trafiają do profesjonalnych wydawców. Informacje pozyskane z szarej literatury mogą potwierdzić twierdzenia wywodzone z innych pozyskanych informacji.

Jednym z efektywnych źródeł w wywiadzie jawnoźródłowym są raporty przygotowane przez wywiadownie gospodarcze, szczególnie w kontekście oceny ryzyka działalności gospodarczej. Wywiadownie te gromadzą dane z otwartych źródeł, tworząc szczegółowe analizy dotyczące wiarygodności firm oraz oferując różnorodne usługi, w tym rankingi firm, analizy branżowe i wsparcie przy windykacji[100]. Raporty

[96] Hasło „prasa", [w:] Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/prasa;3961726.html [dostęp: 4.03.2023].
[97] S. Cisek, *Szara literatura jako źródło informacji biznesowej. Zarys problematyki*, „EBIB Elektroniczny Biuletyn Informacyjny Bibliotekarzy" 2002, nr 11 (40), http://www.ebib.pl/2002/40/cisek.php [dostęp: 4.03.2023].
[98] M.H. Soule, R.P. Ryan, *Grey Literature. Technical Briefing*, [w:] *NATO Open-Source Intelligence Reader*, 2002, s. 24.
[99] Zob. E. Childress, E. Jul, *Going Gray: Gray Literature and Metadata*, „Journal of Internet Cataloging" 2003, vol. 6, no. 3, s. 3–6.
[100] P. Niemczyk, *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu",* „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5), s. 147–166.

wywiadowni dostarczają zwięzłych informacji, które można wykorzystać jako punkt wyjścia do wstępnej interpretacji danych i wskazania najważniejszych kierunków dalszych badań. Skracają one czas prowadzonych analiz jawnoźródłowych, co przyspiesza cały proces rozpoznania jawnoźródłowego.

Kolejnym wyróżnionym otwartym źródłem informacji są media nadawcze, czyli nieinternetowe transmisje sygnału lub transmisje przez publicznie dostępne głośniki, do których dostęp występuje w czasie nadawania. Media nadawcze obejmują zarówno analogowe, jak i cyfrowe transmisje drogą bezprzewodową, satelitarną oraz kablową. Przykłady źródeł transmisji to telewizja, radio, krótkofalarstwo oraz głośniki (np. wiadomości nadawane na ulicach). Radio i telewizja, określane jako mass media, charakteryzuje duża dostępność, szybkość i aktualność przekazu oraz bardzo szeroki kontekst informowania. Tematyka kanałów informacyjnych, zarówno radiowych, jak i telewizyjnych, oscyluje pomiędzy informacjami społeczno-politycznymi i finansowo-gospodarczymi. Systematycznie nadawane są najnowsze wydarzenia, po blokach informacyjnych transmitowane są filmy dokumentalne, programy publicystyczne, rozmowy z ekspertami czy analizy bieżącej sytuacji politycznej, społecznej i gospodarczej. Radio i telewizja dostarczają informacji, które mogą być istotne dla działań na rzecz bezpieczeństwa[101].

Publicznie dostępne kanały cyfrowe obejmują wszelkie dane, które można pobierać, przetwarzać i przechowywać za pośrednictwem urządzeń cyfrowych, niezależnie od ich formatu – czy są to teksty, obrazy, dźwięki, nagrania wideo czy immersyjne środowiska wirtualne. Przykłady mediów cyfrowych obejmują blogi, strony internetowe, posty w mediach społecznościowych, pliki komputerowe oraz e-booki. W miarę rozwoju nowych technologii dane pozyskane z pozostałych publicznie dostępnych kanałów są przekształcane do formy cyfrowej, co zwiększa ich dostępność i umożliwia łatwiejszą analizę w ramach wywiadu jawnoźródłowego.

Internet jako źródło informacji może być analizowany na dwóch poziomach: jako pierwotne źródło informacji, obejmujące serwisy społecznościowe, blogi, vlogi czy serwisy aukcyjne, oraz jako wtórne repozytorium, gromadzące dane z różnych otwartych kanałów informacyjnych. Jako otwarte źródło Internet dostarcza wielu aktualnych, łatwo dostępnych danych w różnych formatach. Pozyskiwanie informacji ze źródeł internetowych to – zgodnie z terminologią wywiadowczą – *Digital Network*

[101] K. Radwaniak, *Biały wywiad w Policji. Pozyskiwanie i analiza informacji ze źródeł otwartych*, [w:] J. Konieczny (red.), *Analiza informacji w służbach*…, op. cit., s. 94.

Intelligence. Unikatową cechą Internetu jest możliwość szybkiej interakcji między użytkownikami za pomocą mediów społecznościowych. Największą grupę w tym obszarze stanowią portale społecznościowe, a sposób pozyskiwania z nich informacji klasyfikowany jest jako subdyscyplina wywiadu jawnoźródłowego, czyli SOCMINT (ang. *social media intelligence*). Kolejne wyróżnione serwisy społecznościowe to serwisy networkingowe, branżowe, kontentowe, dziennikarstwa obywatelskiego, fora dyskusyjne, blogi i mikroblogi oraz repozytoria[102].

W zasobach cyfrowych publikowane są również dokumenty (rejestry publiczne, ewidencje, sprawozdania, informacje finansowe i organizacyjne), które stanowią źródło wiedzy o podmiotach i instytucjach zobligowanych przepisami prawa do ich udostępniania. Jawność życia publicznego wpływa na ilość publicznie dostępnych informacji.

Zasoby Internetu można podzielić na trzy warstwy. Pierwsza (ang. *surface web*, inna nazwa: *clearnet, index web*) określana jest jako sieć zindeksowana. W procesie indeksowania każdy zasób jest kategoryzowany, co oznacza, że jeśli strona internetowa nie posiada prowadzących do niej linków, umieszczonych na innej stronie internetowej, robot wyszukiwarki jej nie odnajdzie[103]. Znacznie większą częścią Internetu stanowi głęboka, ukryta sieć (ang. *deep web, hidden web, invisible web*), która nie jest dostępna w drodze zwykłego wyszukiwania poprzez przeglądarki internetowe. Głęboka sieć jest najdynamiczniejszą rozwijającą się częścią Internetu, zawierającą informacje specjalistyczne[104]. Zawartość głębokiej sieci nie jest celowo ukryta. Lokalizacja treści w tej części World Wide Web jest często konsekwencją ograniczeń wynikających z możliwości technicznych w popularnych wyszukiwarkach, takich jak autoryzacja dostępu, niepowiązanie treści, zawartość skryptów czy zmieniającą się treść strony z uwagi na odpowiedzi przesyłane na konkretne zapytania. W zasobach głębokiej sieci zawarte są m.in. strony wyspecjalizowanych agencji rządowych, specjalistyczne bazy danych, zawartość światowych bibliotek, publikacje i raporty naukowe, dokumenty rządowe, archiwa materiałów źródłowych i referencyjnych, szara literatura, bazy teleadresowe, słowniki, encyklopedie, wzory oraz grafiki. Treści te cechuje wysoka jakość i profesjonalizm, często bowiem powstają one z inicjatywy ekspertów

[102] M. Karciarz, M. Dutko, *Informacja w Internecie*, Wydawnictwo PWN, Warszawa 2010, s. 16–17.
[103] C. Sherman, G. Price, *The Invisible Web: Uncovering Sources Search Engines Can't See*, „Library Trends" 2003, vol. 52, no. 2, s. 282–298.
[104] M.K. Bergman, *The Deep Web: Surfacing Hidden Value*, „Journal of Electronic Publishing" 2001, vol. 7, no. 1, s. 2.

i specjalistów w danej dziedzinie[105]. Najgłębszą warstwą sieci głębokiej jest Dark Web (czarny Internet) inaczej Darknet. Jej treść jest celowo ukryta i niedostępna dla popularnych wyszukiwarek. Dzielenie się zasobami na tym poziomie sieci jest anonimowe (adresy IP nie są publicznie udostępniane). W czarnym internecie istnieje wiele sieci, w których treści dostępne są poprzez połączenia powstałe dzięki specjalnemu oprogramowaniu, takiemu jak: I2P (ang. *Invisible Internet Protocol*), GNUnet oraz sieć TOR (ang. *The Onion Router*). Zasoby Darknetu są często wykorzystywane do nielegalnych działań, takich jak handel bronią, narkotykami, fałszywymi dokumentami, prowadzenie cyberataków, cyberterroryzm oraz pranie pieniędzy. Monitorowanie Darknetu w ramach wywiadu jawnoźródłowego umożliwia skuteczniejsze identyfikowanie i neutralizowanie potencjalnych zagrożeń dla bezpieczeństwa państwa.

W związku z rozwojem kolejnych generacji OSINT-u zasadne jest przyjęcie podziału wywiadu jawnoźródłowego na cyfrowy (gdzie otwartym źródłem informacji jest Internet) i tradycyjny (obejmujący pozostałe źródła informacji). Taki podział determinują również metody i środki pozyskiwania informacji jawnoźródłowych.

2.4. Etapy pozyskiwania informacji jawnoźródłowych

Pozyskiwanie informacji jawnoźródłowych polega na zbieraniu danych surowych, które pojawią się w fazie generowania treści w określonych miejscu, czasie, technologii i języku. W procesie gromadzenia informacji można wyodrębnić jego aspekt materialny (gromadzenie surowych danych na materialnych nośnikach informacji) oraz aspekt semiotyczny (gromadzenie ciągów znaków danego języka)[106]. Aspekty te są w pełni zintegrowane i ściśle ze sobą związane. Pozyskiwanie informacji jawnoźródłowych wymaga szczegółowej organizacji, ustalenia reguł postępowania na każdym z zaplanowanych etapów procesu oraz określenia systemu wzajemnych powiązań osób i uczestniczących w nim urządzeń. Określenie poszczególnych etapów procesu gromadzenia informacji zwiększa efektywność, redukuje koszty oraz prowadzi do uzyskania bardziej precyzyjnych rezultatów. Pozyskiwanie danych jawnoźródłowych obejmuje:

- identyfikację potencjalnie użytecznych informacji;

[105] J. Devine, F. Egger-Sider, *Beyond Google: The Invisible Web in the Academic Library*, „The Journal of Academic Librarianship" 2004, vol. 30, s. 265–269.
[106] J. Oleński, *Ekonomika informacji. Metody*, op. cit., s. 71.

- zebranie (proces techniczny) oraz transfer materialnych nośników informacji z miejsc generowania do miejsc, w których są gromadzone;
- kontrolę kompletności jakości materialnych nośników danych;
- kontrolę kompletności i jakości zebranych informacji;
- zorganizowanie gromadzonych informacji;
- przechowywanie zgromadzonych informacji.

Identyfikacja potencjalnie użytecznych informacji wymaga uzyskania od decydentów wyraźnych lub ogólnych wskazówek, które pozwolą na precyzyjne określenie rodzaju danych, które mają być zgromadzone, oraz ustalenie odpowiadających im priorytetów organizacyjnych. Kluczową rolę odgrywa krytyczne i twórcze myślenie decydentów wyznaczających kierunek analizy. Trafność identyfikacji wpływa na proces analizy jawnoźródłowej, tj. dostarczenia odpowiedzi na pytania „co?" (co się wydarzyło, co wiemy na określony temat, co jeszcze należałoby wiedzieć) i „co z tego?" (jakie są następstwa powstałej sytuacji, jak je rozumieć, interpretować, co może wydarzyć się w przyszłości, jakie decyzje należy podjąć)[107]. Biorąc pod uwagę liczbę miejsc pozyskiwania i przechowywania informacji, można wyróżnić następujące rodzaje procesów informacyjnych, ujęte w tabeli 2.4.

Tabela 2.4. Rodzaje procesów informacyjnych z uwzględnieniem liczby miejsc generowania i przechowywania informacji

Typ procesu	**Liczba miejsc generowania informacji (M)**	**Liczba miejsc przechowywania informacji (N)**	**Przykład**
1 : 1	M = 1	N = 1	karta katalogowa w bibliotece
M : 1	M > 1	N = 1	komentarze w mediach społecznościowych zbierane w bazie danych do analizy sentymentu
1 : N	M = 1	N > 1	wiadomość e-mail wysyłana do wielu odbiorców
M : N	M > 1	N > 1	rozliczenia międzybankowe

Źródło: Opracowanie własne na podstawie: J. Oleński, *Ekonomika informacji. Metody*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2003, s. 73–74.

[107] J. Konieczny, *Bezpieczeństwo państwa a bezpieczeństwo biznesu. Studium metodologiczne*, „Bezpieczeństwo: teoria i praktyka" 2015, nr 4, s. 21.

Każdy z wymienionych typów procesów informacyjnych wymaga dostosowanej do swojej specyfiki organizacji, jak i wymagań technologicznych. Dotyczy to w szczególności procesów typu M:1 i M: N, w których występuje bardzo duża liczba miejsc pozyskiwania informacji i względnie duża liczba miejsc ich gromadzenia w ostatnim z wymienionych typów. Sprawna realizacja tych procesów wymaga rozległych i bezpiecznych sieci teleinformatycznych, wyposażenia w odpowiedni sprzęt i oprogramowanie, a także opracowania standardów postępowań oraz przeszkolonych specjalistów.

Techniczne zebranie informacji wymaga dostępu do urządzeń technicznych dostosowanych do zbierania odpowiednich materialnych nośników informacji. Ujednolicenie pod względem technicznym wchodzących informacji, wyodrębnienie danych oraz przypisanie im konkretnych tagów ma na celu usprawnienie kolejnych etapów analizy. Sposób oznaczenia danych może ułatwiać ich wyszukiwanie w przyszłości. Specjalne systemy zarządzania heterogenicznymi źródłami danych powinny być zaprojektowane zgodnie ze specyfikacją wymagań prowadzonej analizy jawnoźródłowej. Ich zadaniem jest harmonizowanie danych z różnych, niezależnych źródeł w jedną, spójną reprezentację, ujednolicającą reguły dostępu do zbioru wykorzystanych źródeł danych, niezależnie od technologicznych i koncepcyjnych różnic między systemami zarządzania tymi źródłami danych[108]. Wyodrębnione dane organizowane są w zbiory o określonej strukturze i formie technicznej według kryterium znaczenia faktów, precyzji odpowiedzi na postawione problemy analityczne, kategorii logicznych, użyteczności do analizy, rodzaju źródła i jego wiarygodności, co umożliwia zidentyfikowanie luk w wiedzy oraz formułowanie potrzeby w zakresie dalszego gromadzenia informacji[109]. Ostatni etap procesu pozyskiwania informacji danych i informacji jawnoźródłowych stanowi ich przechowywanie zgodnie z normami prawnymi dotyczącymi retencji danych.

Biorąc pod uwagę czas gromadzenia informacji, można wyróżnić trzy jego elementy: tryb (sposób), częstotliwość i czas, które zostały ujęte w tabeli 2.5.

[108] B. Szafrański, *Analiza danych w warunkach niepewności źródeł danych*, [w:] G. Szpor, K. Czaplicki (red.), *Internet. Analityka danych*, Wydawnictwo C.H. Beck, Warszawa 2019, s. 75.
[109] J.E. Long, *Systems Analysis: A Tool to Understand and Predict Terrorist Activities*, Vienna 2002 (prezentacja, slajd nr VTC 1-3 oraz VTC 1-4), za: M. Minkina, *Sztuka wywiadu w państwie współczesnym*, Oficyna Wydawnicza RYTM, Warszawa 2022, s. 197.

Tabela 2.5. Gromadzenie informacji – aspekty temporalne

ASPEKTY	RODZAJE
TRYB	• tryb ciągły: systemy automatycznej rejestracji procesów technologicznych, systemy informatyczne (logi zdarzeń), media nadawcze • tryb cykliczny: raporty dzienne sprzedaży, serwisy informacyjne, czasopisma • tryb alertowy: nadzwyczajne sytuacje (wypadek, katastrofa) • tryb jednorazowy: jednorazowe gromadzenie informacji (spisy powszechne)
CZĘSTOTLIWOŚĆ	• konkretny punkt czasowy, w którym określone dane powinny być zebrane • konkretny punkt czasowy, do którego informacje powinny być zebrane • punkt czasu, po którym informacje mogą być gromadzone • przedział czasu, w którym informacje powinny lub mogą być zbierane, określony punktami czasowymi początkowym oraz końcowym • przedział czasu o określonej długości, bez ustalenia punktów początku i końca.
CZAS	• czas minimalny: najkrótszy możliwy czas gromadzenia informacji w określonych warunkach prawnych, organizacyjnych, technicznych i ekonomicznych. • czas dopuszczalny: czas, po upływie którego informacja traci swoją użyteczność i nie może być wykorzystana w dalszych fazach przetwarzania • czas maksymalny: maksymalny czas gromadzenia określonego zbioru informacji w danym procesie przetwarzania, po upływie którego dalsze gromadzenie informacji staje się zbyteczne z uwagi na ograniczenia organizacyjne czy techniczne

Źródło: Opracowanie własne na podstawie: J. Oleński, *Ekonomika informacji. Metody*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2003, s. 74-79.

Przed zebraniem informacji należy jednoznacznie określić tryb ich pozyskiwania oraz dopuszczalny czas gromadzenia danych. Wymagania te powinny być uwzględnione przy organizacji oraz alokacji zasobów ludzkich i finansowych potrzebnych do gromadzenia informacji. Optymalny czas gromadzenia danych powinien być wyznaczony dla każdego procesu informacyjnego i uwzględniony w planie prowadzonej analizy jawnoźródłowej.

Zarówno w fazie gromadzenia, jak i przetwarzania informacji jawnoźródłowych może być konieczna translacja, która zachodzi w sytuacjach, gdy następuje zmiana nośnika materialnego oraz gdy informacje są wykorzystywane przez osoby posługujące

się innym językiem niż użyty do ich wygenerowania. Błędy w translacji w fazie gromadzenia informacji są trudne do wykrycia i mogą wpływać na jakość dalszej analizy, dlatego też wdrażane są mechanizmy zapewniające poprawność tego procesu w celu zachowania integralności i dokładności danych. Przykłady takich mechanizmów obejmują automatyczne narzędzia do tłumaczenia oraz systemy weryfikacji danych przez ekspertów językowych.

Ostatnim elementem etapu gromadzenia informacji jawnoźródłowych jest przechowywanie zebranego materiału. W systemach technicznych i społecznych informacje przechowywane są na specjalnych urządzeniach technicznych, dostosowanych do cech fizycznych materialnych nośników informacji. Podstawowymi nośnikami informacji są papier oraz różne rodzaje nośników magnetycznych. Najnowszą kategorią są nośniki o charakterze technicznym, w postaci cyfrowej, ale zarazem niematerialnym, umożliwiające gromadzenie informacji w wielkich ilościach i ich natychmiastowe rozpowszechnienie. Postęp technologiczny determinuje przechowywanie informacji w formie cyfrowej, a w konsekwencji przekształcanie informacji z formy niecyfrowej na cyfrową. Przechowywanie materiałów cyfrowych regulowane jest przepisami o prawnej ochronie treści cyfrowych[110]. Podobnie retencja danych uregulowana jest w normach prawnych dotyczących przetwarzania zarówno danych osobowych, jak i nieosobowych. Przechowywanie treści cyfrowych powinno obejmować wierne przekazywanie informacji na nośniki materialne oraz ich przechowywanie w sposób zapewniający integralność, dostępność, poufność i kontrolę nad alokacją zasobów.

Przechowywanie pozyskanych informacji jawnoźródłowych z uwagi na czas ich planowanej dostępności można podzielić na krótko i długoterminowe. Przechowywanie krótkoterminowe polega na utrzymywaniu zasobów informacyjnych w czasie w sposób zapewniający ich integralność oraz potwierdzenie autentyczności. Przechowywanie długoterminowe obejmuje działania polegające na zagwarantowaniu długoterminowej cyfrowej użyteczności zasobów, w tym ich ochrony i zabezpieczenia. Integralnym procesem długoterminowego przechowywania treści cyfrowych jest aktualizacja zasobów informacyjnych w celu ich optymalizacji. Aktualizacja obejmuje ochronę

[110] Treści cyfrowe są to dane, na podstawie których za pomocą odpowiedniego oprogramowania i sprzętu można po przetworzeniu uzyskać informację. Przykładem takich danych są wszelkie informacje zawarte w formie plików elektronicznych, takich jak książki elektroniczne (e-booki, audiobooki), programy komputerowe, aplikacje na urządzenia mobilne, pliki z muzyką, filmami oraz zdjęciami – zob. K. Chałubińska-Jentkiewicz, *Prawna ochrona treści cyfrowych*, Wolters Kluwer, Warszawa 2022, s. 23.

sprzętu, nośników materialnych oraz aktualizację formatów przechowywania w celu zapewnienia dostępności zasobów informacyjnych przy użyciu aktualnych urządzeń. W procesie aktualizacji ważne są też optymalizacja organizacji zasobów danych, metod i technik wyszukiwania w celu zapewnienia dostępu do zasobów informacyjnych oraz usuwanie informacji uznanej za zbędną, wprowadzanie nowej informacji, uznanej za potrzebną, i zastępowanie informacji, która utraciła aktualność, informacją nową[111].

Właściwości elementów cyfrowych przechowywanych na nośnikach materialnych obejmują ich autentyczność, dostępność, tożsamość, trwałość, zdolność do świadczenia usług i zrozumiałość[112]. Autentyczność oznacza, że pochodzenie lub zawartość danych opisujących obiekt pozostają niezmienione od momentu pobrania elementu cyfrowego. Dodatkowo ewentualne jego modyfikacje muszą zostać udokumentowane. Dostępność oznacza, że zasób informacyjny jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie oraz zapewnienie prawa własności intelektualnej do użycia. Tożsamość odnosi się do możliwości zidentyfikowania i odróżnienia elementu cyfrowego m.in. poprzez zarejestrowanie go za pomocą identyfikatora. Trwałość oznacza, że sekwencje bitów elementu cyfrowego zostały zapisane w bazie w sposób nieulotny, są nienaruszone, możliwe do przetworzenia i odzyskania. Zdolność do świadczenia usług odnosi się do zdolności ludzi lub maszyn do używania lub interakcji z elementem cyfrowym przy użyciu odpowiedniego sprzętu i oprogramowania. Zrozumiałość odnosi się do zdolności określonych użytkowników do interpretacji, zrozumienia i użycia elementu cyfrowego w analizie jawnoźródłowej.

Metody zabezpieczania zebranych treści cyfrowych różnią się w zależności od celu wykorzystania surowych danych. Treści mające potencjalną wartość dowodową wymagają precyzyjnego zabezpieczenia w sposób zapewniający możliwość ich procesowego wykorzystania. Do tego celu dane cyfrowe powinny być gromadzone w ich natywnym formacie lub w stanie jak najbardziej zbliżonym do oryginału formatu, a wszelkie zmiany i przekształcenia muszą być udokumentowane. Zabezpieczanie treści cyfrowych w celu ich wykorzystania w analizie jawnoźródłowej na rzecz bezpieczeństwa również podlega tym samym warunkom.

[111] J. Oleński, *Ekonomika informacji. Metody*, op. cit., s. 89.
[112] *Berkeley Protocol on Digital Open-Source Investigations*, HR/PUB/20/2, Nowy Jork–Genewa 2022, s. 60–61.

2.5. Analiza jawnoźródłowa

Na etapie analizy dochodzi do zmiany pozyskanej i opracowanej informacji w informacje wywiadowcze poprzez ich integrację, autentykację, ocenę wiarygodności oraz kontekstualizację[113].

Autentykacja/uwierzytelnienie informacji (ang. *authenticating information*) to proces weryfikacji prawdziwości zebranych danych, którego celem jest zapewnienie, że informacje są autentyczne, pochodzą od deklarowanych źródeł i nie zostały zmienione. Proces ten obejmuje analizę metadanych, potwierdzenie oryginalności materiałów (takich jak dokumenty i inne pliki) oraz sprawdzenie zgodności z innymi niezależnymi źródłami. Autentykacja jest szczególnie istotna w przypadku danych pochodzących z mediów społecznościowych, gdzie użytkownicy mogą ukrywać swoją prawdziwą tożsamość lub dostarczać fałszywe informacje na swój temat. W takich przypadkach proces autentykacji staje się bardziej złożony ze względu na możliwość manipulowania informacjami i trudność w weryfikacji tożsamości użytkowników. Z kolei w przypadku informacji instytucjonalnych, takich jak artykuły uznanych redakcji czy raporty rządowe, autentykacja jest zazwyczaj prostsza, ponieważ źródła te mają na ogół dobrze znaną reputację i ustalone struktury publikacji, co ułatwia weryfikację ich wiarygodności i pochodzenia[114].

Ocena wiarygodności to proces, podczas którego ocenie podlegają zarówno wiarygodność informacji, jak i wiarygodność źródła informacji. Są to powiązane ze sobą elementy. Wdrożenie standardów priorytetowania, oceny wiarygodności oraz potwierdzania źródeł i informacji zwiększa prawdopodobieństwo, że przedstawione ostateczne dane wywiadowcze będą cechować się wysoką niezawodnością. Priorytetyzacja może być przyznawana na podstawie wcześniej określonych kryteriów, takich jak poszukiwanie informacji dotyczących konkretnej osoby lub miejsca, gdzie wszelkie wzmianki o tych podmiotach otrzymują wyższy priorytet. Priorytetyzacja może być również oparta na częstotliwości pojawiania się danej informacji, co umożliwia szybkie reagowanie na potencjalnie fałszywe treści i zapobieganie ich dalszemu rozpowszechnianiu.

Istnieją różne metody oceny wiarygodności źródła informacji, biorąc pod uwagę jego pochodzenie, niezawodność (inaczej: rzetelność) oraz częstotliwość generowania

[113] H.J. Williams, I. Blum, *Defining Second Generation*…, op. cit., s. 17.
[114] Ibidem, s. 18.

danych. Każde otwarte źródło informacji charakteryzuje się innymi parametrami i podatnościami na manipulację treścią. Kryteria oceny wiarygodności źródeł otwartych opracowane przez Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych zakładają ocenę źródeł informacji i ujęte są w sześciopunktową skalę oceny. Kategoria „wiarygodne" (A) obejmuje źródła charakteryzujące się pełną autentycznością, wiarygodnością i zdolnością do dostarczania dokładnych i rzetelnych informacji oraz historią całkowitej wiarygodności, kolejne kategorie to źródła: „zazwyczaj wiarygodne" (B), „prawie wiarygodne" (C), „zazwyczaj niewiarygodne" (D), „niewiarygodne" (E) oraz „nie można ocenić" (F) – oznaczające brak podstaw do oceny wiarygodności źródła. Inne wprowadzone kryterium stanowi częstotliwość dostarczania przez źródło informacji na określony temat. Kolejnym wyróżnionym kryterium oceny wiarygodności otwartych źródeł informacje jest częstotliwość dostarczania informacji na temat określonych zagadnień. Źródła mogą być klasyfikowane jako „stały dostawca" (dostarczające regularnie informacje), „częsty dostawca" (dostarczające informacje często, ale nie zawsze), „ograniczony dostawca" (dostarczające informacje sporadycznie) lub „nowy lub nieznany dostawca" (pierwszy raz dostarczające informacje na dany temat)[115].

Innymi sposobami oceny wiarygodności otwartych źródeł informacji oraz uzyskanych z nich danych są metody stosowane przez Departament Armii Stanów Zjednoczonych[116]. W tabeli 2.6 zaprezentowano ocenę wiarygodności źródeł otwartych, obejmującą zakresem od A (wiarygodne) do F (nie można ocenić). Źródło wykorzystywane po raz pierwszy otrzymuje ocenę F, która nie oznacza niewiarygodności, lecz wskazuje na brak wcześniejszych doświadczeń analityków z tym źródłem, co uniemożliwia ocenę jego wiarygodności.

[115] M.M. Lowenthal, R.M. Clark, *The Five Disciplines*…, op. cit., 2015, s. 32.
[116] *ATP 2-22.9: Open-Source Intelligence*, DC: Headquarters, Department of the Army, Waszyngton, 2012, s. 2–8.

Tabela 2.6. Ocena wiarygodności otwartych źródeł informacji

Kategoria	Opis
Niezawodne	Brak wątpliwości co do autentyczności, wiarygodności lub kompetencji; historia całkowitej niezawodności.
Zazwyczaj niezawodne	Niewielkie wątpliwości co do autentyczności, wiarygodności lub kompetencji; zazwyczaj dostarcza wiarygodne informacje.
Dość niezawodne	Wątpliwości co do autentyczności, wiarygodności lub kompetencji; dostarczało wiarygodne informacje w przeszłości.
Zazwyczaj niewiarygodne	Znaczące wątpliwości co do autentyczności, wiarygodności lub kompetencji; dostarczało wiarygodne informacje w przeszłości.
Niewiarygodne	Brak autentyczności, wiarygodności lub kompetencji; historia nieprawdziwych informacji.
Nie można ocenić	Brak podstaw do oceny wiarygodności źródła.

Źródło: *ATP 2-22.9: Open-Source Intelligence*, DC: Headquarters, Department of the Army, Waszyngton 2012, s. 2–8.

W tabeli 2.7 przedstawiono ocenę wiarygodności informacji na podstawie ich zgodności z innymi źródłami, logiczności oraz wewnętrznej spójności.

Tabela 2.7. Ocena wiarygodności informacji jawnoźródłowych

Kategoria	Opis
Potwierdzona	Potwierdzona przez inne niezależne, renomowane źródła; logiczna sama w sobie; zgodna z innymi informacjami na ten temat.
Prawdopodobna	Niepotwierdzona; logiczna sama w sobie; zgodna z innymi informacjami na ten temat.
Możliwa	Niepotwierdzona; w miarę logiczna sama w sobie; zgodna z niektórymi innymi informacjami na ten temat.
Wątpliwa	Niepotwierdzona; możliwa, ale nielogiczna; brak innych informacji na ten temat.
Mało prawdopodobna	Niepotwierdzona; nielogiczna sama w sobie; sprzeczna z innymi informacjami na ten temat.
Nie można ocenić	Brak podstaw do oceny prawdziwości informacji.

Źródło: *ATP 2-22.9: Open-Source Intelligence*, DC: Headquarters, Department of the Army, Waszyngton 2012, s. 2-8.

NATO stosuje sześciostopniową skalę oceny otwartych źródeł informacji – *NATO Admiralty Code* – do oceny wiarygodności źródeł oraz rzetelności samych informacji[117]. Ocena ta opiera się częściowo na subiektywnym osądzie analityka oraz doświadczeniu z wcześniejszymi informacjami dostarczonymi przez to samo źródło, a w przypadku danych uzyskanych za pomocą sensorów – na wiedzy dotyczącej

[117] NATO, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, AJP-2, wyd. A, wersja 2, NATO Standardization Office, 2016.

dokładności konkretnego systemu sensorów. System ten składa się z dwóch niezależnych skal: jednej – dla wiarygodności źródła i drugiej – dla wiarygodności informacji. Wiarygodność źródła ocenia się w skali od A do F, gdzie A oznacza „całkowicie wiarygodne" źródło, niebudzące wątpliwości co do autentyczności, rzetelności lub reputacji, zaś F oznacza, że nie można ocenić wiarygodności źródła z powodu braku odpowiednich danych. Natomiast wiarygodność informacji oceniana jest w skali od 1 do 6, gdzie 1 oznacza „potwierdzone przez niezależne źródła", a 6 – „niemożność oceny wiarygodności". Rozdzielenie ocen na dwie skale umożliwia bardziej precyzyjne i niezależne ocenianie, zapewniając, że ocena przypisana do wiarygodności źródła nie wpływa na ocenę wiarygodności informacji – ani odwrotnie.

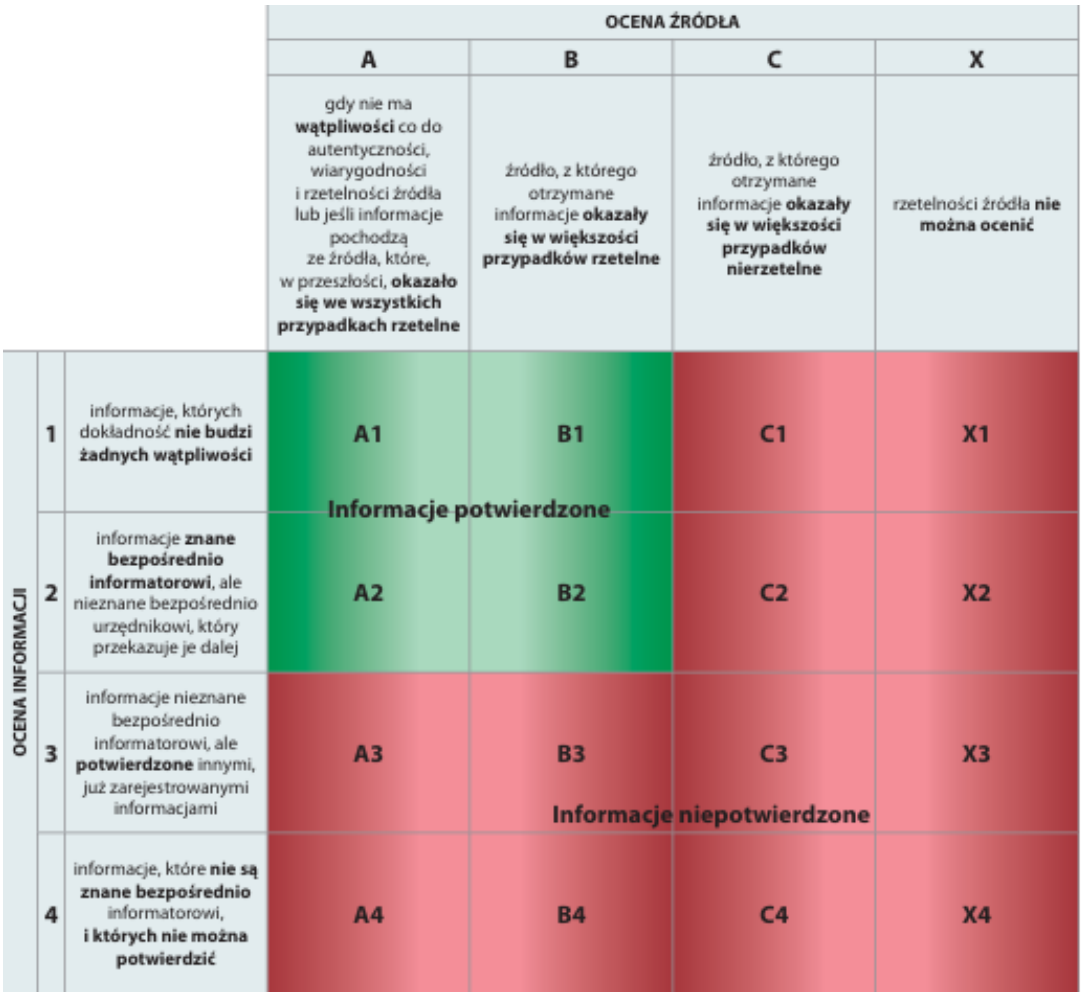
W przypadku źródeł niecyfrowych ocena ich wiarygodności jest prostsza niż w przypadku źródeł cyfrowych, a szczególnie trudna w kontekście treści z mediów społecznościowych. Miarą wiarygodności jest ustalenie czy informacje są godne zaufania, co oznacza, że zostały dostarczone bez intencji wprowadzenia w błąd, oraz czy źródło miało wiarygodny dostęp do tych danych. Oceniając wiarygodność źródła, należy również uwzględnić jego historię, tj. czy w przeszłości dostarczało potwierdzone i wiarygodne informacje. Przykładowo bardziej wiarygodna jest informacja przekazana przez placówkę dyplomatyczną niż przez anonimowe źródło w mediach społecznościowych, które nie ma potwierdzonej historii dostarczania rzetelnych danych. Podobnie wydawnictwa o ustalonej reputacji zazwyczaj charakteryzują się wysokim prawdopodobieństwem przekazywania sprawdzonych i wiarygodnych informacji oraz zachowują transparentność w kwestii swoich źródeł. Natomiast tabloidy lub wydawnictwa o niższej reputacji mogą być mniej wiarygodne ze względu na tendencję do manipulowania informacjami, aby wywrzeć wpływ na odbiorców. W przeciwieństwie do mediów informacyjnych media społecznościowe zazwyczaj dostarczają informacje pochodzące bezpośrednio od pierwotnego nadawcy. Jednak oryginalność tych informacji może być wątpliwa, zwłaszcza w przypadku retweetów, repostów czy działań botów, które mogą ukrywać rzeczywiste intencje pierwotnego autora. Nawet jeśli relacjonowane jest wydarzenie, którego świadkiem był pierwotny nadawca, pozostaje kwestia zaufania do przekazywanej relacji, zwłaszcza gdy brakuje pełnej wiedzy na temat kontekstu, w jakim znajdował się nadawca, jego ewentualnych uprzedzeń oraz poziomu wiedzy fachowej. Innym sposobem oceny wiarygodności

informacji jest weryfikacja przez potwierdzenie[118]. Im więcej źródeł potwierdza te same twierdzenia lub dostarcza zgodne informacje, tym większe jest prawdopodobieństwo ich prawdziwości. Na przykład im więcej świadków zdarzenia zgadza się co do jego przyczyn, przebiegu oraz skutków, tym większe prawdopodobieństwo uzyskania dokładnego obrazu wydarzeń. Przeprowadzając weryfikację wiarygodności przez potwierdzenie, należy uwzględnić dwa elementy występujące w wywiadzie jawnoźródłowym. Pierwszy to „efekt echa", kiedy źródło pierwotne oceniane jest jako wysoce wiarygodne, ponieważ jednocześnie wiele innych źródeł wtórnych powiela te same informacje, korzystając z tego źródła pierwotnego. Drugi element stanowi tendencja do bardzo szybkiego rozprzestrzeniania się dezinformacji, szczególnie w mediach społecznościowych.

Ocena wiarygodności informacji zależy od oceny wiarygodności źródła. Oceny te wpływają na siebie nawzajem i muszą być przeprowadzane w określonej kolejności: najpierw ocenia się źródło informacji, a następnie informację. W ocenie istotne są również interakcje zachodzące pomiędzy informacją jawnoźródłową a otwartym źródłem. Źródło wiarygodne może przekazać informację niewiarygodną, natomiast źródło niewiarygodne może przekazać informację wiarygodną. Ocena wiarygodności informacji stanowi zatem wypadkową oceny wiarygodności źródła oraz oceny informacji, w tym stosunku źródła do informacji. Za przykład może posłużyć model oceny informacji w systemie 4×4 stosowany przez Europol, wykorzystywany w państwach członkowskich w celu ustalenia autentyczności i dokładności dostarczanych informacji[119]. Ocena źródła obejmuje kategorie od A (nie ma wątpliwości co do autentyczności, wiarygodności i rzetelności źródła) do X (rzetelności źródła nie można ocenić). Ocena informacji natomiast klasyfikuje dane od 1 (informacje, których dokładność nie budzi żadnych wątpliwości) do 4 (informacje, których nie można potwierdzić). Model oceny informacji przedstawiono na rysunku 2.4.

[118] H. Gibson, S. Ramwell, T. Day, *Analysis, Interpretation and Validation of Open Source Data*, [w:] B. Akhgar, P.S. Bayerl, F. Sampson (eds.), *Open Source Intelligence: Investigation From Strategy to Implementation*, Springer, 2023, s. 108.

[119] Europol, *Strategia zarządzania informacjami. Wsparcie wdrożenia rozporządzenia Europolu i Strategii Europolu 2020+*, Europol, Haga 2018, s. 9–10.



Rysunek 2.4. Kody oceny stosowane przy wymianie informacji za pośrednictwem Europolu

Źródło: Europol, *Strategia zarządzania informacjami. Wsparcie wdrożenia rozporządzenia Europolu i Strategii Europolu 2020+*, Europol, Haga 2018, s. 10.

Kontekstualizacja to proces umożliwiający analitykowi przekazanie specjalistycznej wiedzy tematycznej odbiorcy. Polega na wzbogacaniu surowych danych dodatkowymi informacjami, które pomagają w ocenie ich wiarygodności i relewantności. Przykłady takich informacji obejmują ocenę źródła, kontekst historyczny lub polityczny oraz potencjalne uprzedzenia. Kontekstualizacja może również polegać na syntezie różnych elementów informacji w spójny produkt analityczny. Dzięki integracji różnorodnych źródeł i perspektyw analitycy mogą stworzyć pełniejszy i wieloaspektowy obraz sytuacji, co zwiększa wartość analityczną dostarczanych danych. Przykładem może być analiza zagrożeń cybernetycznych, w której uwzględnia się zarówno techniczne aspekty incydentu, jak i szeroki kontekst polityczny oraz możliwe motywy działania zaangażowanych podmiotów.

Analiza informacji stanowi czynność poznawczą, która wykorzystuje dane empiryczne oraz rozumowanie w celu uzyskania wieloaspektowej charakterystyki określonych sytuacji, ich zrozumienia, formułowania sądów oraz prognozowania ich rozwoju. Polega na poszukiwaniu odpowiedzi na dwa pytania: „co?" (co się stało, co wiemy, co należałoby jeszcze wiedzieć) i „co z tego?" (jaka jest prognoza dalszego rozwoju sytuacji, jakie działania należałoby podjąć)[120]. Celem analizy informacji jest zapewnienie wsparcia organom decyzyjnym poprzez zmniejszenie stanu niepewności informacyjnej. W obszarze bezpieczeństwa państwa istotną jej częścią jest również formułowanie rekomendacji dotyczących podjęcia pokreślonych działań. W podejmowanych czynnościach istotne są krytyczne myślenie oraz kreatywne rozwiązywanie problemów. Analiza jawnoźródłowa jest dziedziną wielodyscyplinarną, która nabiera znaczenia, gdy wprowadza nowe elementy do już zebranych informacji, co umożliwia decydentom odpowiedzialnym za bezpieczeństwo państwa podejmowanie bardziej optymalnych decyzji.

Pierwszym etapem analizy informacji jest postawienie problemu, czyli sformułowanie pytania, na które analityk ma odpowiedzieć. Trafne, poprawne sformułowanie pytania wymaga wyobraźni i kreatywności. Można wyróżnić kilka typów problemów, tj. problemy oszacowania, eksploatacyjne, predykcyjne, związku przyczynowego oraz optymalizacyjne[121]. Kolejny komponent analizy stanowi formułowanie hipotez. W prowadzonych analizach istotne są również założenia analityczne, które najczęściej występują w formie generalizacji tworzących rodzaj połączenia rozumowań. W toku analizy mogą pojawić się na etapie formułowania hipotez, wnioskowania oraz jako element wspomagający ocenę wiarygodności źródeł informacji. Ostatnim komponentem analizy informacji jest rozumowanie, w zakresie którego wyróżnia się najczęściej trzy typy: dedukcyjne, indukcyjne i abdukcyjne. Rozumowanie dedukcyjne jest rozumowaniem niezawodnym, czyli prawdziwość przesłanek tego rozumowania przesądza o prawdziwości jego wniosku. Ograniczenie dedukcji stanowi brak możliwości wyjścia poza informacje składające się na przesłanki, co oznacza, że wnioski są ściśle uzależnione od założeń początkowych. Rozumowanie dedukcyjne przebiega zgodnie z kierunkiem wynikania logicznego, zapewniając spójność i precyzyjność wniosków. Drugi typ rozumowania to indukcja, w zakresie

[120] J. Konieczny, *Kryminalistyczny leksykon*…, op. cit., s. 28.
[121] J. Konieczny, *Analiza w wywiadzie zagranicznym*, [w:] J. Konieczny (red.), *Analiza informacji w służbach*…, op. cit., s. 350.

której pomiędzy przesłankami a konkluzją nie zachodzi stosunek wynikania logicznego. Jest to rozumowanie zawodne, ogólne wnioski wyprowadzane są z przesłanek będących partykularnymi przypadkami urzeczywistnienia się tych wniosków. Przyjęcie wniosku jest decyzją analityka. Trzeci, najbardziej twórczy, typ rozumowania to abdukcja. Polega na formułowaniu najbardziej prawdopodobnych hipotez na podstawie niekompletnych informacji w celu wyjaśnienia zgromadzonych informacji. Rozumowanie abdukcyjne ma zastosowanie w sytuacjach niepewności lub braku pełnej wiedzy w analizie dostępnych danych.

Zastosowanie krytycznego myślenia w analizie wywiadowczej pozwala analitykom na autorefleksję oraz poszukiwanie błędów w swoim myśleniu. Wymaga to świadomości charakterystycznych błędów poznawczych i logicznych, wykrywania błędów w rozumowaniu innych, opanowania sposobów myślenia przeciwnika i gotowości do krytyki ich rozumowań. Ważnym aspektem krytycznego myślenia jest również stosowanie dialektyki, która wspiera kreatywne myślenie poprzez analizę sprzeczności w założeniach i wnioskach, przedstawienie tezy, znalezienie sprzeczności, rozwinięcie antytezy i dojście do syntezy[122].

Na potrzeby analizy wywiadowczej wykorzystywany jest podział metod analizy zaproponowany przez R.J. Heuera i R.H. Phersona, którzy wyróżniają cztery kategorie: metodę osądu eksperckiego, metody ustrukturyzowane, metody ilościowe wykorzystujące dane wygenerowane przez ekspertów (quasi-ilościowe) oraz metody ilościowe z wykorzystaniem danych empirycznych. Autorzy jednocześnie podkreślają, że metody te różnią się od siebie, jednak granice między nimi są często rozmyte i trudno rozpoznawalne[123].

Metoda osądu eksperckiego polega na wykorzystaniu zarówno wiedzy ogólnej i specjalistycznej analityka, jak i jego doświadczenia zawodowego oraz krytycznego myślenia. Charakterystyczną cechą tej metody są subiektywne szacowania przeprowadzane praktycznie w sferze koncepcyjnej. Techniki stosowane w tej metodzie to m.in. wnioskowanie na podstawie dowodów, metody historyczne, studium przypadku oraz wnioskowanie przez analogię. Krytyczne myślenie jest ważnym elementem pomagającym w organizowaniu danych, walidacji źródeł informacji, a także w przekazywaniu wniosków w sposób klarowny i logiczny, zapewniając większą

[122] W.M. Hall, G. Citrenbaum, *Intelligence Analysis: How to Think in Complex Environments*, Praeger Security International, 2010, s. 116–120.
[123] R.J. Heuer, R.H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, CQ Press, Thousand Oaks, 2021, s. 5–6.

precyzję, jasność i skuteczność w przetwarzaniu i interpretacji danych. Krytyczne myślenie stanowi istotny element pomagający w organizowaniu danych, walidacji źródeł informacji, a także w przekazywaniu wniosków w sposób klarowny i logiczny. Metoda osądu eksperckiego ma zastosowanie w sytuacjach, w których konieczne jest zrozumienie złożonych problemów i ocena wielu możliwych scenariuszy. Staje się szczególnie użyteczna, gdy dostępne dane są ograniczone lub niejednoznaczne.

Ustrukturyzowane metody analityczne są sposobem na systematyczne i przejrzyste ujawnianie procesów myślowych analityków, a w rezultacie łatwiejsze ich udostępnianie, rozwijanie oraz dyskusję nad nimi. Metody te są wykorzystywane w wywiadzie jawnoźródłowym, kiedy konieczne jest precyzyjne zrozumienie i udokumentowanie procesu analitycznego. Mają również zastosowanie w sytuacjach wymagających oceny konkurencyjnych hipotez oraz systematycznego przeglądu założeń i dowodów. Są one wyjątkowo użyteczne w analizach prowadzonych zespołowo, usprawniając komunikację oraz poprawiając gromadzenie i interpretację informacji. Głównym celem technik stosowanych w tej metodzie jest poprawa jakości analizy wywiadowczej poprzez redukcję powszechnie występujących błędów poznawczych oraz uprzedzeń wśród analityków. Częste jest stosowanie kombinacji kilku technik w prowadzonej analizie. Transparentna metodologia pozwala na weryfikację poszczególnych części i całości wnioskowania oraz uwzględnienie różnorodnych punktów widzenia już na wczesnym etapie analizy. Ustrukturyzowane metody umożliwiają redukcję częstotliwości i pojawiania się błędów większej wagi poprzez zapewnienie, że założenia i modele myślowe są wyraźnie sprawdzane i testowane[124]. Jednocześnie strukturalizacja procesu analitycznego może ograniczać elastyczność działań analityków w dynamicznym i zmiennym otoczeniu. Podział technik stosowanych w ustrukturyzowanych metodach analizy przedstawiony został w tabeli 2.8.

[124] Ibidem.

Tabela 2.8 Podział technik stosowanych w ustrukturyzowanych metodach analizy

Kategoria	**Techniki**
Techniki eksploracyjne	• burza mózgów (prosta oraz z grupowaniem) • technika grup nominalnych • circleboarding, starbursting • mapy myśli i mapy konceptualne • analiza Venna • analiza sieciowa
Techniki diagnostyczne	• sprawdzanie kluczowych założeń • chronologie i ramy czasowe • macierz wpływów krzyżowych • generowanie konkurencyjnych hipotez • rozumowanie diagnostyczne • analiza konkurencyjnych hipotez • wyszukiwarka niespójności • wykrywanie oszustw • mapowanie argumentów
Techniki z użyciem wyobraźni (zmian ram analizy)	• myślenie „z zewnątrz do wewnątrz” • analogie strukturalne • analiza czerwonych kapeluszy • crunching kwadrantów • analiza *pre mortem* • strukturalna autokrytyka • metoda „co, jeśli?” • analiza wysokiego wpływu/niskiego prawdopodobieństwa • metoda delficka • współpraca adwersarialna • debata strukturalna
Techniki foresightu	• generowanie kluczowych czynników • wyszukiwarka kluczowych niepewności • odwracanie założeń • proste scenariusze • stożek prawdopodobieństwa • alternatywna analiza przyszłości • tworzenie scenariuszy wielokrotnych • analiza morfologiczna • rozumowanie kontrfaktyczne • analiza przeciwnych narracji • generowanie, walidacja i ocena wskaźników
Techniki wspomagania decyzji	• inkubator możliwości • analiza BowTie • matryca wpływów • analiza SWOT • analiza ścieżek krytycznych • drzewa decyzyjne • matryca decyzyjna • analiza pola sił • technika *Pros-Cons-Faults-and-Fixes* • menedżer złożoności

Źródło: R.J. Heuer, R.H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, CQ Press, Thousand Oaks, 2021.

Metody quasi-ilościowe (inaczej: metody ilościowe wykorzystujące dane wygenerowane przez ekspertów) są stosowane w analizie wywiadowczej w sytuacjach braku danych empirycznych, gdy istnieje potrzeba wypełnienia luk poprzez wykorzystanie danych wygenerowanych przez ekspertów[125]. Są one szczególnie przydatne w ocenie podatności przywódców na zamach stanu, w przewidywaniu wyniku debaty dotyczącej legislacji oraz w przypadku terroryzmu. Ten rodzaj analizy umożliwia wykorzystanie danych eksperckich, zwłaszcza w subiektywnej ocenie prawdopodobieństwa i modelowaniu złożonych zjawisk. Narzędziem pozwalającym na zwiększenie efektywności tych metod są procedury umożliwiające wydobycie takich sądów[126]. Metody quasi-ilościowe stosowane są w modelowaniu dynamicznych procesów i symulacjach zjawisk związanych z bezpieczeństwem oraz stabilnością polityczną. Wadami tych metod mogą być utrudniona weryfikacja i walidacja danych eksperckich oraz sama jakość tych danych. Wyniki analizy, ze względu na subiektywność ocen, mogą być mniej precyzyjne. Metody te obejmują wnioskowanie bayesowskie, które wykorzystuje zarówno dane pochodzące z wyników badań określonych zdarzeń, jak i założone z góry prawdopodobieństwa. Kolejną technikę stanowi modelowanie dynamiczne, pozwalające na analizę systemów zmieniających się w czasie i przewidywanie przyszłych zachowań na podstawie bieżących danych. Inną techniką są symulacje, które pozwalają na stworzenie modeli rzeczywistych zjawisk i eksperymentowanie z nimi w kontrolowanych warunkach. Przygotowanie do stosowania tych metod wymaga wykształcenia w dziedzinach matematyki, informatyki oraz badań operacyjnych i ekonomii.

Metody ilościowe z wykorzystaniem danych empirycznych są stosowane w analizie wywiadowczej w sytuacji dostępności dużych ilości danych, na przykład big data. Umożliwiają one przeprowadzanie precyzyjnych analiz dzięki zastosowaniu zaawansowanych algorytmów i technik modelowania ekonometrycznego. Dane ilościowe są gromadzone m.in. za pomocą różnych czujników i mogą być używane do analizy systemów broni lub reakcji publicznej na nowe produkty. Wraz ze wzrostem ilości danych dostępnych od dostawców mediów społecznościowych i internetu rzeczy możliwa jest również identyfikacja trendów oraz obiektywne testowanie hipotez[127]. Metody te wymagają jednak dużych zasobów obliczeniowych oraz dostępu do

[125] Ibidem.
[126] K. Liedel, *Analiza w przeciwdziałaniu terroryzmowi*, [w:] J. Konieczny (red.), *Analiza informacji w służbach*…, op. cit., s. 335.
[127] R.J. Heuer, R.H. Pherson, *Structured Analytic Techniques*…, op. cit.

kompletnych i konkretnych danych. Analiza dużych zbiorów danych wymaga nie tylko stosowania zaawansowanych technik obliczeniowych, lecz także weryfikacji i filtrowania danych w celu zniwelowania ryzyka błędów poznawczych oraz ich manipulacji. Rozwój systemów analitycznych opartych na algorytmach sztucznej inteligencji i metodach ilościowych prowadzi do częściowej automatyzacji procesów decyzyjnych. Wprowadzenie systemów big data umożliwia dynamiczne monitorowanie i korektę procesów operacyjnych w oparciu o dane historyczne oraz analizę czynników wpływających na podejmowanie decyzji[128]. Jednak jakość danych wejściowych pozostaje czynnikiem krytycznym, wpływającym na wiarygodność i praktyczne zastosowanie wyników analizy ilościowej.

2.6. Podsumowanie

Podsumowując ustalenia badawcze dotyczące charakterystyki wywiadu jawnoźródłowego należy stwierdzić, że jego istotą jest zaplanowane i zorganizowane pozyskiwanie informacji z ogólnodostępnych, legalnych źródeł, ich przetwarzanie, analiza oraz przekazanie powstałego w tym procesie produktu analitycznego decydentom w ustalonej formie, zgodnie z wcześniej określonym zapotrzebowaniem informacyjnym.

Działania te umożliwiają szybką i skuteczną analizę zagrożeń oraz zjawisk istotnych dla bezpieczeństwa państwa. Wywiad jawnoźródłowy uzupełnia informacje pozyskane z innych źródeł, dostarcza ogólnego kontekstu badanego problemu oraz może ukierunkowywać dalsze działania operacyjne. Wykorzystanie wywiadu jawnoźródłowego przed zastosowaniem innych form rozpoznania przyczynia się do optymalizacji kosztów pozyskiwania informacji.

Zważywszy na specyfikę informacji z otwartych źródeł oraz dynamikę zmian w środowisku bezpieczeństwa, cykl wywiadowczy ulega przyspieszeniu, szczególnie w kontekście wywiadu jawnoźródłowego. Wymaga to modyfikacji w zadaniowaniu i finansowaniu służb specjalnych oraz stworzenia warunków sprzyjających efektywnemu wykorzystaniu wyników ich pracy w procesie decyzyjnym na rzecz bezpieczeństwa państwa.

[128] P. Zaskórski, W. Zaskórski, *Big-Data systems in improving modern organizations*, „Nowoczesne Systemy Zarządzania" 2017, z. 12, nr 2, s. 131.

Analiza pojęcia i klasyfikacji informacji jawnoźródłowych wykazała, że ich różnorodność wynika ze specyfiki kanałów przekazu, takich jak obserwacja, dokumenty, media nadawcze oraz treści cyfrowe, z których każdy charakteryzuje się odmiennymi właściwościami determinującymi sposób ich pozyskiwania i analizy. Efektywność wywiadu jawnoźródłowego zależy więc nie tylko od dostępu do odpowiednich źródeł, ale także od właściwego doboru metod ich analizy oraz umiejętności oceny ich rzetelności.

Na podstawie dokonanych ustaleń dotyczącej etapów pozyskiwania informacji z otwartych źródeł oraz metod ich analizy, należy podkreślić, że jednym z głównych wyzwań wywiadu jawnoźródłowego pozostaje ocena wiarygodności zarówno źródeł, jak i pozyskanych informacji. Wyniki badań wskazują, że wartościowanie informacji jawnoźródłowych stanowi jedno z największych wyzwań OSINT ze względu na dynamiczny wzrost liczby dostępnych źródeł oraz ich zróżnicowaną rzetelność.

Jednym z najistotniejszych wyzwań wywiadu jawnoźródłowego pozostaje ocena wiarygodności zarówno samych źródeł, jak i pozyskiwanych informacji. Zastosowane metody analizy mają na celu redukcję niepewności oraz umożliwiają rozwiązywanie konkretnych problemów decyzyjnych. Rosnąca liczba informacji dostępnych w czasie rzeczywistym, przy relatywnie niskich kosztach, powoduje, że w analizach wywiadowczych priorytetem stają się metody ilościowe. Szczególną rolę odgrywają tutaj dane pochodzące z zaawansowanych czujników, komercyjnych satelitów, urządzeń mobilnych, Internetu rzeczy oraz sieci połączonych urządzeń noszonych na ciele, takich jak inteligentne zegarki i inne technologie biometryczne. Nowe otwarte źródła informacji pojawiają się w wyniku postępu technologicznego oraz zmian społecznych, a ich dostępność wzrasta wykładniczo, co prawdopodobnie stanowi trwały kierunek rozwoju. Ze względu na powszechną dostępność, szybkość oraz relatywną łatwość pozyskiwania informacji jawnoźródłowych, ich wykorzystanie skraca czas niezbędny do przeprowadzenia analiz wywiadowczych, co w konsekwencji przyspiesza proces podejmowania decyzji związanych z bezpieczeństwem państwa.

Rozwój otwartych źródeł informacji prowadzi do zacierania się granicy pomiędzy informacjami jawnymi a niejawnymi[129]. Niektóre informacje, które wcześniej były pozyskiwane wyłącznie metodami operacyjnymi, są obecnie dostępne w otwartych

[129] H.J. Williams, I. Blum, *Defining Second Generation*…, op. cit., s. 37.

źródłach. Wymusza to zmianę podejścia do kategoryzacji nowych źródeł informacji oraz metod ich analizy, a także rodzi wyzwania natury prawnej i organizacyjnej.

Reasumując, przeprowadzona analiza dostarcza teoretycznej odpowiedzi na pierwsze szczegółowe pytanie badawcze, wskazując, że wraz ze wzrostem liczby otwartych źródeł informacji oraz powszechnym dostępem do technologii cyfrowych i Internetu rola wywiadu jawnoźródłowego wzrasta w kształtowaniu bezpieczeństwa państwa. Wnioski te stanowią punkt wyjścia do dalszych badań empirycznych, które pozwolą na ich weryfikację oraz kompleksowe ujęcie w końcowej analizie całej dysertacji.

3. ZAAWANSOWANE METODY I ŚRODKI PROWADZENIA WYWIADU JAWNOŹRÓDŁOWEGO

Celem trzeciego rozdziału jest prezentacja wyników badań ukierunkowanych na rozwiązanie szczegółowego problemu badawczego sformułowanego w pytaniu: *W jakim zakresie dostępne metody i środki prowadzenia wywiadu jawnoźródłowego wpływają na bezpieczeństwo państw?*

W niniejszym rozdziale przedstawiony został podział metod pozyskiwania informacji jawnoźródłowych nawiązujący do klasyfikacji otwartych źródeł informacji przedstawionej w rozdziale drugim. Z uwagi na dynamiczne zmiany technologiczne oraz dominację źródeł internetowych zasadne jest również omówienie metod wykorzystywanych w cyfrowym wywiadzie jawnoźródłowym.

W dalszej części rozdziału zaprezentowano klasyfikację narzędzi stosowanych w cyfrowym OSINT, obejmującą rozwiązania językowe i tekstowe, geoprzestrzenne, oparte na teorii sieci oraz wykorzystujące kryminalistykę wizualną. Końcowa część rozdziału poświęcona została analizie przykładowych narzędzi cyfrowego wywiadu jawnoźródłowego, w tym narzędzi open-source, projektowanych na zamówienie oraz komercyjnych. Przeanalizowano ich możliwości techniczne, zastosowanie w wywiadzie jawnoźródłowym, a także ograniczenia wynikające z uwarunkowań technicznych i prawnych. Uwzględniono również zautomatyzowane narzędzia, usprawniające proces pozyskiwania i interpretacji informacji jawnoźródłowych.

Szczególnie istotnym elementem badań w tym rozdziale jest ocena wpływu oraz możliwości rozwoju metod i narzędzi OSINT w kontekście ich wykorzystania na rzecz bezpieczeństwa państwa.

3.1. Ogólny podział metod pozyskiwania informacji jawnoźródłowych

Metody pozyskiwania informacji jawnoźródłowych można klasyfikować według rodzaju otwartego źródła.

Gromadzenie informacji jawnoźródłowych z obserwacji umożliwia poznanie zjawisk w ich niezakłóconym przebiegu poprzez uczestnictwo w publicznych wydarzeniach, konferencjach naukowych, zebraniach, kongresach oraz pozyskanie informacji o otoczeniu (banery, billboardy). Metoda ta może dostarczyć informacji ściśle specjalistycznych i unikatowych.

Pozyskiwanie informacji jawnoźródłowych pochodzących z dokumentów i innych źródeł drukowanych jest tradycyjną metodą pracy wywiadu jawnoźródłowego. Lektura książek, prasy, wydawnictw branżowych, fachowej literatury, broszur, prac naukowych dostarcza informacji o wysokiej i często zweryfikowanej jakości. Ważne jest monitorowanie tytułów prasowych oraz nowości wydawniczych związanych z tematem prowadzonej analizy jawnoźródłowej. Z uwagi na swą charakterystykę szara literatura jest trudna do wyszukania i gromadzenia, w wielu przypadkach jedyną metodą jej pozyskania jest uczestnictwo w wydarzeniu, na których jest udostępniana. Szara literatura gromadzona jest w sposób aktywny na wyraźne żądanie decydentów. W fazie planowania zbierania informacji jawnoźródłowych istotne jest zatem posiadanie wiedzy zarówno o samym wydarzeniu, jak i o fakcie dystrybucji na nim szarej literatury.

Niejednokrotnie brak informacji o autorze, tytule, dacie publikacji czy wydawcy oraz forma papierowa szarej literatury stanowią wyzwanie w etapie digitalizacji i standaryzacji zebranego materiału[130]. Pozyskiwanie informacji jawnoźródłowych z dokumentów i innych źródeł drukowanych może obejmować zamówienie ich drogą elektroniczną w formie papierowej, takich jak książki, czasopisma, gazety, mapy, grafiki, raporty, harmonogramy, kwestionariusze, slajdy, plany, biuletyny, broszury, ulotki i inne oficjalnie opublikowane treści. Dostawa może również dotyczyć materiałów na nośnikach cyfrowych, takich jak płyty CD, DVD, urządzenia pamięci flash, karty pamięci (np. SD, microSD), dyski zewnętrzne (HDD, SSD) czy dyski USB.

Pozyskiwanie informacji z mediów nadawczych znacząco poszerzyło zakres i skalę wykorzystania otwartych źródeł w działalności wywiadowczej. Proces ten polega na gromadzeniu treści audio i wideo ze źródeł transmisji innych niż internetowe, takich jak radio, telewizja, krótkofalówki oraz publiczne głośniki. Zebrane materiały mogą wymagać zastosowania narzędzi do ich przekształcenia do formatu odpowiedniego dla decydentów[131]. Charakter informacji emitowanych przez te otwarte źródła determinuje metody ich gromadzenia, które mogą być realizowane w sposób ciągły lub cykliczny, w zależności od harmonogramu emisji. Mimo przenoszenia mediów nadawczych do sieci, nie wszystkie treści są dostępne w Internecie. Media nadawcze, które decydują się na rozpowszechnianie treści w sieci teleinformatycznej, tworzą metody dystrybucji odmienne od klasycznych. Zakres emitowanych treści może

[130] M.H. Soule, R.P. Ryan, *Grey Literature*…, op. cit., s. 25–26.
[131] OSINT Foundation, *OSINT Collection Methodologies*, Document Number: 20231120-01, 2023, s. 3.

być jednak różny, dlatego ważne jest uwzględnianie analogowych form przekazu informacji w analizie jawnoźródłowej.

Gromadzenie informacji jawnoźródłowych z Internetu, może być realizowane manualnie lub automatycznie, przy użyciu różnych narzędzi i skryptów. Etapy zarządzania tym procesem obejmują: identyfikacja wymagań informacyjnych, planowanie, koordynacja i realizacja. Stopień złożoności każdego z wymienionych etapów zależy od zakresu wyszukiwanych informacji oraz rozmiaru organizacji. Zarządzanie procesem gromadzenia informacji z Inernetu rozpoczyna się od zdefiniowania wymagań wyszukiwania, które są konsekwencją działań podjętych w pierwszej fazie cyklu wywiadowczego. Po określeniu zakresu wyszukiwania, analityk podejmuje decyzję o metodach i środkach pozyskiwania informacji uwzględniając kryteria miejsca, czasu, technologii i języka gromadzenia informacji[132].

W etapie planowania pozyskiwania informacji cyfrowych określane są najskuteczniejsze opcje wyszukiwania poprzez dostosowanie potencjalnych rozwiązań w zakresie gromadzenia danych do wymagań informacyjnych:

Wymóg informacyjny = Co zbierać + Kto zbiera + Gdzie zbierać + Kiedy zbierać

Wymienione etapy mogą być powtarzane do momentu spełnienia określonych potrzeb informacyjnych. Plany zbierania danych są zazwyczaj macierzą lub arkuszem kalkulacyjnym z trzema kluczowymi informacjami ułożonymi w formie graficznej[133].

W procesie gromadzenie danych cyfrowych istotne jest zabezpieczenie podstawowych elementów zarówno w celach dowodowych jak i oceny oraz wiarygodności strony. Są to: ujednolicony lokalizator zasobów (ang. *Uniform Resource Locator*, URL) lub ujednolicony identyfikator zasobów (ang. *Uniform Resource Identifier*, URI), kod źródłowy języka znaczników hipertekstowych (ang. *HyperText Markup Language*, HTML), który przyczynia się do uwierzytelnienia zebranego materiału oraz przechwytywanie całej strony poprzez wykonanie zrzutu z ekranu ze wskazaną data i godziną[134]. Te trzy elementy spełniają minimalne wymagania w zakresie wiarygodności strony. W przypadku pobierania strony zawierające filmy lub obrazy istotne jest ich wyodrębnienie. Kolejnym elementem jest zebranie metadanych, które mogą obejmować identyfikator użytkownika przesyłającego, identyfikator postu,

[132] J. Oleński, *Ekonomika informacji. Metody*, op. cit., s. 73.
[133] NATO, *Intelligence Exploitation of the Internet*, Brussels, October 2002, s. 20.
[134] *Berkeley Protocol*…, op. cit., s. 59.

zdjęcia lub filmu, datę i godzinę przesłania, geotag, hashtag, komentarze i adnotacje. Należy również zebrać dane kontekstowe, jeśli są istotne dla zrozumienia elementu cyfrowego (np. komentarze do filmu, obrazu lub postu) oraz informacje o przesyłaniu i przesyłającym/użytkowniku, takie jak nazwa użytkownika, prawdziwe imię i nazwisko. Elementem, który wymaga pobrania i zabezpieczenia jest również wartość skrótu (ang. *hash value*), która potwierdza, za pomocą kryptografii, że zebrana zawartość jest unikalna i nie została zmodyfikowana od czasu jej zebrania[135]. Wartość skrótu umożliwia identyfikację i weryfikację zebranych treści cyfrowych.

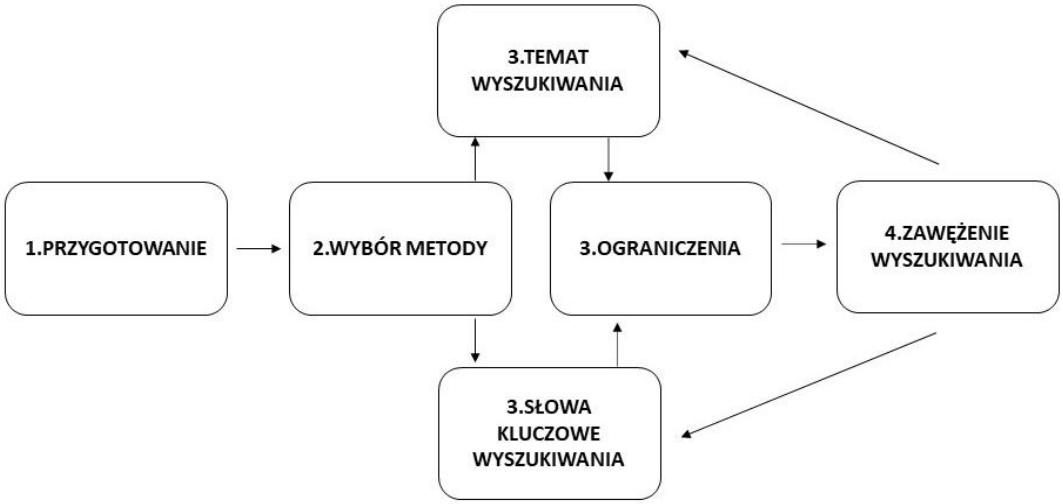
W procesie gromadzenia informacji z Internetu można wyróżnić cztery elementy, tworzące plan wyszukiwania:

1) określenie wymagań dotyczących wyszukiwanych informacji;
2) wybór stron oraz strategii wyszukiwania;
3) zidentyfikowanie szczegółów dostępu lub szczegółów umożliwiających wyszukanie konkretnych informacji;
4) określenie ograniczeń czasowych wyszukiwania[136].

W pierwszym etapie zidentyfikowane wymagania informacyjne przedstawione w ogólnym planie gromadzenia informacji jawnoźródłowych muszą być dostosowane do formy wyszukiwania cyfrowego. Pierwotnie określone wymagania informacyjne mogą być zbyt szerokie, zbyt wąskie, niejasne lub zawierać wyrażenia żargonowe. Istnieje więc potrzeba podzielenia ich na mniejsze, zasadnicze elementy informacyjne (ang. *Essential Elements of Information*)[137]. W kolejnych etapach dokonywany jest wybór stron i określenie strategii wyszukiwania, m.in. poprzez określenie lokalizacji zasobów cyfrowych. Istotne jest również wyznaczenie konkretnych ograniczeń czasowych procesu. Przygotowanie i implementacja planu gromadzenia informacji cyfrowych umożliwia szybkie przeszkolenie wykonawców w zakresie gromadzenia i przygotowania raportów z analizy jawnoźródłowej w ustandaryzowanej formie[138].

Metody wyszukiwania i gromadzenia informacji jawnoźródłowych z otwartych źródeł cyfrowych wymagają systematyzacji według założeń przedstawionych na rysunku 3.1.

[135] Ibidem.
[136] NATO, *Intelligence Exploitation*…, op. cit., s. 22.
[137] Ibidem.
[138] Ibidem, s. 23.



Rysunek 3.1. Schemat wyszukiwania w zasobach Internetu.
Źródło: Opracowanie na podstawie: NATO, *Intelligence Exploitation of the Internet*, Brussels, October 2002, s. 38.

Gromadzenie danych ze wszystkich wyróżnionych kategorii otwartych źródeł informacji może także obejmować ich zakup ze źródeł komercyjnych. Zakupy te mogą dotyczyć zarówno książek w księgarniach stacjonarnych, prenumeraty czasopism online, jak i pozyskiwania specyficznych zestawów danych, usług oraz produktów. Po nabyciu produktów fizycznych lub oprogramowania możliwe jest zastosowanie techniki inżynierii odwrotnej (ang. *reverse engineering*)[139]. Jest to proces mający na celu zrozumienie budowy, działania, zasad funkcjonowania oraz kosztów wytworzenia produktu lub systemu. Może obejmować dekompozycję urządzeń mechanicznych, analizę kodu oprogramowania czy badanie struktury genetycznej, w celu szczegółowego poznania metod konstrukcji i funkcjonowania danego obiektu. W wywiadzie jawnoźródłowym technika inżynierii odwrotnej umożliwia m.in. ocenę potencjału technologicznego oraz przewidywanie przyszłych kierunków badań i rozwoju. Pozwala ona również zyskać wgląd w innowacje konkurencyjnych firm, analizować produkty i usługi dostępne na rynku oraz oceniać potencjalne inwestycje lub przejęcia, wspomagając tym samym podejmowanie strategicznych decyzji biznesowych. W sektorze wojskowym, badanie uzbrojenia oraz technologii przeciwnika umożliwia opracowanie środków obronnych i strategii neutralizacji zagrożeń. Analiza zakupionego sprzętu wojskowego pomaga również w rozwoju własnych systemów

[139] B. Hariharan, *Reverse Engineering*, [w:] M. Augier, D.J. Teece (eds.), *The Palgrave Encyclopedia of Strategic Management*, Palgrave Macmillan, London 2018, https://doi.org/10.1057/978-1-137-00772-8_249.

obronnych i ofensywnych. Dodatkowo, technika ta jest stosowana do badania systemów infrastruktury krytycznej, co jest istotne dla zabezpieczenia przed potencjalnymi zagrożeniami.

Pozyskiwanie informacji jawnoźródłowych może być również realizowane poprzez zlecenie zewnętrzne (outsourcing). W ramach tego procesu często wykorzystuje się programy agentowe i boty, które są zdolne do gromadzenia, przetwarzania i adaptacji do wymagań związanych z pozyskiwaniem informacji. Działają one poprzez skanowanie hipertekstowych łączy w Internecie w celu wyszukiwania informacji, co zwiększa efektywność eksploracji i skraca czas ich pozyskiwania. Outsourcing wymaga jednak zachowania odpowiednich standardów bezpieczeństwa oraz efektywnego doboru i wykorzystania narzędzi jawnoźródłowych.

3.2. Metody stosowane w cyfrowym wywiadzie jawnoźródowym

Informacje pochodzące z otwartych źródeł mogą być pozyskiwane trzema metodami, wyodrębnionymi ze względu na poziom interakcji z obiektem prowadzonego rozpoznania: pasywną, półpasywną i aktywną[140]. Wybór metody będzie zależał od rodzaju podmiotu prowadzącego rozpoznanie, gromadzonych informacji, opracowanego planu ich pozyskiwania, charakteru oraz jawności prowadzonego rozpoznania i powinien zostać określony na etapie planowania. Jest to jeden z istotnych elementów bezpieczeństwa operacyjnego (ang. *operations security*, OPSEC)[141], które projektowane z wyprzedzeniem przyczynia się do poprawnego prowadzenia rozpoznania jawnoźródłowego. Zastosowanie metod semi pasywnych oraz aktywnych wykracza poza standardowe działania wywiadu jawnoźródłowego, może prowadzić do naruszenia norm prawnych, zasad etycznych oraz generować potencjalne zagrożenia dla bezpieczeństwa operacyjnego.

Rekonesans pasywny jest podstawowym sposobem gromadzenia informacji jawnoźródłowych. Polega na ich nieagresywnym zbieraniu bez bezpośredniej interakcji z obiektem. Obejmuje m.in. badanie struktur sieciowych, analizę metadanych, *web scraping* oraz pozyskiwanie informacji z *deep web*. Podczas pasywnego rozpoznania nie są wysyłane dane do systemów docelowych, co minimalizuje ryzyko naruszenia

[140] N. Hassan, R. Hijazi, *Open Source*…, op. cit., s. 14.
[141] Bezpieczeństwo operacyjne to analityczny proces mający na celu identyfikację, kontrolę i ochronę informacji krytycznych, aby zapobiec ich ujawnieniu przez przeciwników. Szerzej: P. Davis, *Analyze This: OPSEC is Key in the War on Terrorism*, „Journal of Counterterrorism & Homeland Security International" 2002, vol. 8, no. 2, s. 22–25.

prywatności oraz innych regulacji prawnych. W wywiadzie jawnoźródłowym powinna to być metoda dominująca, z uwagi na cel gromadzenia informacji wyłącznie z otwartych źródeł oraz konieczność zachowania wysokich standardów etycznych i bezpieczeństwa prowadzonych działań. Do metod rekonesansu pasywnego należą: monitorowanie, wyszukiwanie, techniczny footpriniting oraz analiza mediów społecznościowych.

Monitorowanie polega na śledzeniu w określonym przedziale czasowym zmieniających się treści generowanych przez stałe źródło. Jest to działanie ustrukturyzowane, w którym wykorzystywane są listy znanych i wcześniej ocenionych otwartych źródeł online, np. strony internetowe lub konta w mediach społecznościowych, a także zapytania wyszukiwania, które są uruchamiane na bieżąco w odniesieniu do określonych celów.

Wyszukiwanie polega na użyciu wyspecjalizowanego oprogramowania lub strony internetowej do eksploracji Internetu, celem pozyskania informacji istotnych dla określonych potrzeb informacyjnych. Wykorzystanie zaawansowanych algorytmów wyszukiwania oraz technik analitycznych pozwala na selekcję i ocenę relewantnych informacji. Poza wykorzystaniem wyszukiwarek internetowych do gromadzenia informacji z indeksowanych stron, wyszukiwanie strukturalne może być również stosowane w natywnych wyszukiwarkach na platformach mediów społecznościowych oraz w bazach danych. Proces wyszukiwania powinien być ustrukturyzowany i prowadzony w sposób systematyczny, począwszy od jasnego postawienia pytania badawczego, określenia parametrów, słów kluczowych oraz operatorów. Operator ma za zadanie zwrócić określoną wartość, która jest wynikiem operacji wykonywanej na danych, zwanych argumentami operatora. Podstawowe trzy operatory logiczne to: jednoargumentowy operator negacji, dwuargumentowa koniunkcja oraz alternatywa[142]. W zależności od uprawnień mogą one zawężać lub rozszerzać zakres wyszukiwania. Po raz pierwszy zastosowano je w wyszukiwarce Google, z czego wywodzi się nazwa tej techniki tj. Google Hacking[143]. Zapytania wykorzystujące słowa kluczowe określane są jako Google Dorks, stąd inna nazwa tej techniki: Google Dorking. Zapytania do wyszukiwarki Google skierowane są do specyficznych elementów strony internetowej,

[142] Operatory boolowskie – nazwa pochodzi od brytyjskiego matematyka Georga Boole'a, pioniera logiki symbolicznej. Wyszukiwanie polega na łączeniu słów operatorami logicznymi: AND, OR, NOT („i", „lub", „nie").

[143] Por. szerzej: J. Long, B. Gardner, J. Brown, *Google hacking for penetration testers*, vol. 2, Elsevier 2011, s. 2 i nast.; V.K. Velu, *Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite*, Helion, Gliwice 2023, s. 91-93.

takich jak tytuł strony, adres URL, linki do innych stron czy typy plików. Kluczowym aspektem Google Dorking jest umiejętność formułowania zapytań, które wykorzystuje specjalne operatory będące częścią interfejsu wyszukiwarki Google, ale które nie są powszechnie znane.

Operatory wyszukiwania charakteryzowane są przez ich funkcje, co pozwala wyróżnić m.in. operatory chronometryczne (zawężające wyniki do określonych przedziałów czasowych), lokalizacyjne (filtrujące wyniki według całości lub części adresu internetowego), operatory kanałów komunikacyjnych (ograniczające wyszukiwanie do mediów społecznościowych), wyszukiwania określonych typów treści (umożliwiające odnalezienie zdefiniowanych informacji) oraz eksploracji witryny (pozwalające na wyszukiwanie według tytułu, treści czy metaznaczników)[144]. Tabela 3.1. przedstawia przykłady najpopularniejszych operatorów wyszukiwania.

Tabela 3.1. Zaawansowane operatory wyszukiwania

Operator	**Opis**
site:	Ogranicza wyniki wyszukiwania do witryn z podanej domeny
intitle:	Wyświetla strony, które zawierają podany wyraz w tytule strony
allintitle:	Wyświetla strony, które zawierają wszystkie wyrazy zapytania w tytule strony
inurl:	Wyświetla strony, które zawierają podany wyraz w adresie URL
allinurl:	Wyświetla strony, które zawierają wszystkie podane wyrazy w swoim adresie URL
related:	Wyświetla strony, które są tematycznie powiązane z podaną stroną
link:	Wyświetla strony, które zawierają łącza do wskazanej strony
cache:	Wyświetla wynik ostatniego zapisu zawartości strony przez Google, której adres musi być podany po operatorze, bez spacji
inanchor:	Wyświetla strony, które zawierają w treści łącza zawierające wskazane słowa
numrange	Wyświetla strony, które zawierają liczby z podanego zakresu
deterange	Wyświetla strony, które zostały zindeksowane w podanym tekście
author	Pozwala na wyszukiwanie stron według autora
group	Pozwala na wyszukiwanie stron według grup
ext lub filetype	Ogranicza wyniki wyszukiwania tylko do plików posiadających podane rozszerzenie
before/after	Ogranicza wyniki wyszukiwania do informacji zindeksowanej przed lub po wskazanej dacie lub roku
intex:	Wyświetla strony, które zawierają wyszukiwane słowa kluczowego w treści strony
allintex	Wyświetla strony, które zawierają wszystkie wyszukiwane słowa kluczowe w swej treści

Źródło: Opracowanie własne na podstawie: https://www.google.pl/intl/pl/help/operators.html [dostęp: 4.10.2023]; P. Hrabiec-Hojda, J. Trzeciakowska, *Google Hacking*, Infomedia Group, Kraków 2019, s. 61–72.

[144] D. Mider, *Sztuka wyszukiwania w Internecie – autorski przegląd wybranych technik i narzędzi*, „Studia Politologiczne" 2019, nr 54, s. 195.

Najbardziej rozbudowany, dostępny publicznie zbiór technik Google Hacking znajduje się na serwerze firmy edukacyjnej Offensive Security i jest znany pod nazwą Google Hacking Database[145].

Techniczny Footprinting, inaczej odtwarzanie śladów cyfrowych, jest procesem gromadzenia wszelkich dostępnych informacji na temat systemów komputerowych, infrastruktury sieciowej, technologii, usług oraz podmiotów, do których należą. Obejmuje zarówno techniki pasywne, charakterystyczne dla wywiadu jawnoźródłowego, jak i techniki aktywne. Jednym z elementów odtwarzania śladów jest analiza strony internetowej badanego obiektu. Dane, które można uzyskać w tej analizie, obejmują: adresy IP, nazwy domen i subdomen, technologie webowe, metadane, certyfikaty SSL/TLS (ang. *Secure Socket Layer/Transport Layer Security*), publicznie dostępne pliki i zasoby, archiwalne wersje strony, skrypty i wtyczki, pliki konfiguracyjne, technologie używane do budowy strony, dostawcę VPN, pliki cyfrowe i metadane oraz kod HTML, a także inne dane, takie jak adresy firmy, lokalizacje oddziałów, kluczowi pracownicy, schematy e-mail, numery telefonów, firmy partnerskie, informacje o użytkownikach oraz polityki prywatności i bezpieczeństwa. Kolejną metodą footprintingu jest tworzenie kopii strony internetowej (ang. *mirroring*), które polega na zapisaniu całej zawartości witryny na lokalnym dysku w celu dalszej analizy.

Proces ten umożliwia szczegółowe badanie struktury strony, jej zawartości oraz ukrytych elementów, bez ryzyka zakłócenia funkcjonowania oryginalnej witryny. Narzędzia wykorzystywane do tych zadań to m.in. HTTrack[146], GNU Wget[147], Acunetix[148], SiteSucker[149], Cyotek WebCopy[150] oraz BlackWidow[151]. Kolejną techniką footpriniting jest analiza pliku robots.txt, polegająca na badaniu jego zawartości w celu pozyskania informacji o zasadach dotyczących indeksowania i przeglądania stron internetowych, które zostały ustalone przez właściciela strony. W wywiadzie jawnoźródłowym analiza pliku robots.txt pozwala stwierdzić, jakie informacje są celowo ukryte przez właściciela witryny. Inne metody footprintingu obejmują: ekstrakcję linków, sprawdzanie linków zwrotnych, monitorowanie aktualizacji strony

[145] https://www.exploit-db.com/google-hacking-database [dostęp: 5.03.2024].
[146] https://www.httrack.com [dostęp: 5.03.2024].
[147] https://www.gnu.org/software/wget/ [dostęp: 5.03.2024].
[148] https://www.acunetix.com/ [dostęp: 5.03.2024].
[149] https://ricks-apps.com/osx/sitesucker/ [dostęp: 4.03.2024].
[150] https://www.cyotek.com/cyotek-webcopy [dostęp: 4.03.2024].
[151] https://www.softbytelabs.com [dostęp: 4.03.2024].

oraz identyfikację technologii na niej użytych. Najpopularniejsze narzędzia do zidentyfikowania technologii użytych do zbudowania docelowej strony internetowej to BuiltWith[152], Wappalyzer[153] oraz WhatRuns[154]. W celu uzyskania dodatkowych informacji o witrynie można skorzystać również z bazy WHOIS, w której dostępne są dane właściciela domeny (w niektórych przypadkach), datę rejestracji domeny, datę wygaśnięcia domeny, serwery DNS[155], na których znajduje się domena, dane rejestratora domeny, adresy e-mail kontaktowe, numery telefonów kontaktowych, adresy fizyczne organizacji rejestrującej domenę, status domeny (zablokowana, aktywna), historię zmian rejestracyjnych domeny oraz kontakt do osób odpowiedzialnych za zarządzanie domeną. Główną organizacją odpowiedzialną za usługę WHOIS jest ICANN[156], która wraz z regionalnymi rejestrami internetowymi zarządza alokacją i rejestracją adresów IP oraz nazw domen na całym świecie. Regionalne Rejestry Internetowe obejmują pięć organizacji: Afrykańskie Centrum Informacji Sieciowej (ang. *African Network Information Centre*, AFRINIC)[157] obejmuje Afrykę, Centrum Informacyjne Sieci Azji i Pacyfiku (ang. *Asia-Pacific Network Information Centre*, APNIC)[158] obejmuje Azję, Australię Nową Zelandię i sąsiadujące kraje, Amerykański Rejestr Numerów Internetowych (ang. *American Registry for Internet Numbers*, ARIN)[159] obejmujący Amerykę Północną, Antarktykę i część Karaibów, Centrum Informacyjne Sieci Ameryki Łacińskiej i Karaibów (ang. *Latin American and Caribbean Internet Addresses Registry*, LACNIC)[160] obejmujący Amerykę Łacińską i część Karaibów oraz Centrum Koordynacyjne Europejskiej Sieci IP (fr. *Réseaux IP Européens Network Coordination Centre*, RIPE NCC)[161] obejmujący

[152] https://www.builtwith.com [dostęp: 4.03.2024].
[153] https://www.wappalyzer.com/ [dostęp: 4.03.2024].
[154] https://www.whatruns.com/ [dostęp: 4.03.2024].
[155] DNS (ang. *Domain Name System*) to system umożliwiający przekształcanie nazw domenowych (mnemonicznych) na odpowiadające im adresy IP. Transformacja odbywa się za pośrednictwem hierarchicznego systemu zapytań, począwszy od lokalnych serwerów nazw, aż po serwery główne, które przekierowują zapytania do odpowiednich serwerów nazw domenowych najwyższego poziomu (ang. *top-level domain*, TLD). Dodatkowe funkcje DNS obejmują wsparcie dystrybucji obciążenia poprzez efektywne rozdzielanie ruchu sieciowego między różnymi serwerami oraz zwiększenie niezawodności i redundancji usług sieciowych dzięki replikacji danych na wielu serwerach. Por. N. Hassan, R. Hijazi, *Open Source*…, op. cit., s. 327 i nast.
[156] ICANN (ang. *Internet Corporation for Assigned Names and Numbers*) to organizacja non-profit odpowiedzialna za przydzielanie adresów IP, zarządzanie systemem nazw domen (DNS) oraz zapewnianie stabilności i bezpieczeństwa globalnego Internetu. Strona WWW: https://www.icann.org [dostęp: 10.03.2024].
[157] https://www.afrinic.net [dostęp: 10.03.2024].
[158] https://www.apnic.net [dostęp: 10.03.2024].
[159] https://www.arin.net [dostęp: 10.03.2024].
[160] https://www.lacnic.net [dostęp: 10.03.2024].
[161] https://www.ripe.net [dostęp: 10.03.2024].

Europę, Rosję, Środkowy Wschód i centralną Azję. W rozpoznaniu technicznym istotnym elementem jest również określenie subdomen, czyli adresów utworzonych pod domeną główną. Tego typy witryny mogą dostarczać informacji o nowo testowanych przez organizacje technologiach, kodach strony czy nawet treści dokumentów pozostawionych na serwerze. Narzędzia do wyszukiwania subdomen to m.in.: VirusTotal.com[162] czy DNSdumpsetr[163].

Techniczny footprinting obejmuje, poza wyszukiwaniem w bazie WHOIS, również rekonesans DNS, który polega na identyfikacji serwerów obsługujących zapytania DNS dla danej domeny. W tym procesie stosuje się techniki takie jak mapowanie sieci (ang. *route mapping*), które analizuje trasę pakietów, oraz śledzenie adresu IP (ang. *IP address tracking*), monitorujące adresy IP przypisane do serwerów i urządzeń. Te techniki pozwalają na uzyskanie szczegółowego obrazu infrastruktury DNS. Przykładem polecenia umożliwiającego uzyskanie informacji o adresach IP powiązanych z nazwami domen oraz wyszukiwanie różnych typów rekordów DNS jest *nslookup*.

W rekonesansie technicznym wykorzystuje się również technikę *web scraping*, która polega na pozyskiwaniu informacji z sieci internetowej i zapisywaniu ich do systemu plików lub bazy danych w celu późniejszego odzyskiwania lub analizy[164]. Technika ta umożliwia automatyczne pozyskiwanie dużych ilości informacji z różnych źródeł internetowych, zazwyczaj za pomocą protokołu transferu hipertekstu (HTTP) lub przeglądarki internetowej. Proces ten może być realizowany ręcznie przez użytkownika lub automatycznie za pomocą bota lub robota indeksującego. Celem web scraping jest pozyskanie m.in. danych takich jak: adresy e-mail, numery telefonów, metadane, struktura strony HTML, opinie użytkowników. Najpopularniejszym narzędziem web scrappingu jest theHarvest [165].

Analiza mediów społecznościowych obejmuje identyfikację, pozyskiwanie, weryfikację oraz analizę informacji dostępnych na różnych platformach społecznościowych. W procesie tym wykorzystywane są różnorodne formy mediów społecznościowych, takie jak blogi, mikroblogi (np. Twitter, Tumblr, Plurk), fora dyskusyjne (np. Reddit, Quora, Stack Exchange), platformy do gier (np. Twitch,

[162] https://www.virustotal.com/gui/home/upload [dostęp: 10.03.2024].
[163] https://dnsdumpster.com/ [dostęp: 10.03.2024].
[164] V.K.Velu, *Kali Linux*…, op. cit., s. 83.
[165] Inne narzędzia to m.in.: Web Data Extractor (www.webextractor.com), Scrapy (scrapy.org), jARVEST (sing.ei.uvigo.es/jarvest), Web-Harvest (web-harvest.sourceforge.net/) [dostęp: 15.03.2024].

Discord, Steam), platformy do zamieszczania recenzji (np. Yelp, TripAdvisor, Google Reviews), zakładki społecznościowe (np. Delicious, Diigo, Pocket), wikis (np. Wikipedia, Fandom, Wikisource), serwisy do udostępniania wideo i muzyki (np. YouTube, Vimeo, SoundCloud) oraz portale społecznościowe (np.Facebook, LinkedIn, Instagram). Najpopularniejsze media społecznościowe wraz z ich potencjałem dla wywiadu jawnoźródłowego zostały przedstawione w tabeli nr 3.2.

Tabela 3.2. Media społecznościowe i ich potencjał dla wywiadu jawnoźródłowego (stan na drugi kwartał 2024 r.)

Nazwa	**Liczba aktywnych użytkowników miesięcznie**	**Zasięg geograficzny**	**Potencjalne dane dla OSINT**
Facebook	3.065 miliarda	globalny	informacje o lokalizacji, aktywność użytkowników, zdjęcia, wideo, polubienia, komentarze, udostępnienia, grupy i strony, relacje i statusy, dane demograficzne, wydarzenia
YouTube	2.504 miliarda	globalny	historia oglądania, subskrypcje, komentarze, polubienia, dane demograficzne, informacje o lokalizacji
WhatsApp	2.4 miliarda	globalny	wiadomości tekstowe, głosowe, wideo, grupy, statusy, dane demograficzne, informacje o lokalizacji
Instagram	2 miliarda	globalny	zdjęcia, wideo, polubienia, komentarze, udostępnienia, relacje, historie, dane demograficzne, informacje o lokalizacji
TikTok	1.67 miliarda	globalny	wideo, polubienia, komentarze, udostępnienia, trendy, dane demograficzne, informacje o lokalizacji
WeChat	1.343 miliarda	Chiny	wiadomości tekstowe, grupy, statusy, dane demograficzne, informacje o lokalizacji
Facebook Messenger	1.01 miliarda	globalny	wiadomości tekstowe, wideo, grupy, statusy, dane demograficzne, informacje o lokalizacji
Telegram	900 milionów	globalny	wiadomości tekstowe, wideo, grupy, kanały, dane demograficzne, informacje o lokalizacji
Snapchat	800 milionów	globalny	zdjęcia, wideo, polubienia, komentarze, historie, dane demograficzne, informacje o lokalizacji

Nazwa	Liczba aktywnych użytkowników miesięcznie	Zasięg geograficzny	Potencjalne dane dla OSINT
Douyin	755 milionów	Chiny	wideo, polubienia, komentarze, udostępnienia, dane demograficzne, informacje o lokalizacji
Kuaishou	700 milionów	Chiny	wideo, polubienia, komentarze, udostępnienia, dane demograficzne, informacje o lokalizacji
X (Twitter)	611 milionów	globalny	posty, polubienia, komentarze, udostępnienia, retweety, dane demograficzne, informacje o lokalizacji
Weibo	598 milionów	Chiny	posty, polubienia, komentarze, udostępnienia, dane demograficzne, informacje o lokalizacji
QQ	554 milionów	Chiny	wiadomości tekstowe, grupy, statusy, dane demograficzne, informacje o lokalizacji
Pinterest	498 milionów	globalny	zdjęcia, polubienia, komentarze, udostępnienia, dane demograficzne, informacje o lokalizacji
Reddit	430 milionów	globalny	posty, komentarze, polubienia, udostępnienia, dane demograficzne, informacje o lokalizacji
LinkedIn	310 milionów	globalny	profile zawodowe, umiejętności i języki, wykształcenie, posty, polubienia, komentarze, dane demograficzne, informacje o lokalizacji
Quora	305 milionów	globalny	pytania, odpowiedzi, polubienia, komentarze, dane demograficzne, informacje o lokalizacji
Vimeo	260 milionów	globalny	wideo, komentarze, polubienia, udostępnienia, dane demograficzne, informacje o lokalizacji
Line	230 milionów	globalny	wiadomości tekstowe, grupy, statusy, dane demograficzne, informacje o lokalizacji
Xiaohongshu	200 milionów	Chiny	zdjęcia, wideo, polubienia, komentarze, zakupy, dane demograficzne, informacje o lokalizacji
Discord	200 milionów	globalny	wiadomości tekstowe, wideo, grupy, kanały, dane demograficzne, informacje o lokalizacji
ShareChat	180 milionów	Indie	wiadomości tekstowe, wideo, polubienia, komentarze, udostępnienia, dane demograficzne, informacje o lokalizacji

Nazwa	Liczba aktywnych użytkowników miesięcznie	Zasięg geograficzny	Potencjalne dane dla OSINT
Josh	151 milionów	Indie	wideo, polubienia, komentarze, udostępnienia, dane demograficzne, informacje o lokalizacji
Threads	150 milionów	globalny	zdjęcia, polubienia, komentarze, udostępnienia, trendy, dane demograficzne, informacje o lokalizacji
Twitch	140 milionów	globalny	wideo, komentarze, polubienia, udostępnienia, dane demograficzne, informacje o lokalizacji
Tumblr	135 milionów	globalny	posty, polubienia, komentarze, udostępnienia, dane demograficzne, informacje o lokalizacji
Medium	100 milionów	globalny	posty, polubienia, komentarze, udostępnienia, dane demograficzne, informacje o lokalizacji
VK (Vkontakte)	80 milionów	Rosja	posty, polubienia, komentarze, udostępnienia, dane demograficzne, informacje o lokalizacji
Rumble	50 milionów	globalny	wideo, polubienia, komentarze, udostępnienia, dane

Źródło: Opracowanie własne na podstawie: *Digital 2024: Global Overview Report*, DataReportal, https://www.datareportal.com/reports/digital-2024-global-overview-report; *Top 35 Social Media Platforms (2024)*, Exploding Topics, https://www.explodingtopics.com/blog/top-social-media-platforms; *Most Popular Social Networks Worldwide as of January 2024, Ranked by Number of Active Users*, Statista, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ [dostęp: 20.03.2024]

Analiza mediów społecznościowych może dostarczyć informacji wywiadowczych, które wpierają proces podejmowania decyzji w obszarze bezpieczeństwa państwa. Na pierwszym, podstawowym poziomie, pomaga organom ścigania w uzyskaniu wstępnych materiałów naprowadzających poprzez identyfikację informacji o wydarzeniach, które mają miejsce, gdzie się odbywają i kogo dotyczą. Na drugim, bardziej złożonym poziomie, umożliwia konstruowanie wyjaśnień przyczyn obserwowanych zdarzeń. Trzeci poziom analizy obejmuje najbardziej zaawansowane wykorzystanie informacji wywiadowczych, polegające na prognozowaniu przyszłych wydarzeń i modelowaniu sytuacji. Dzięki dostępowi do danych z mediów społecznościowych w czasie rzeczywistym, możliwa jest szybka reakcja, a tym samym

minimalizowanie ryzyka eskalacji przemocy poprzez dostosowanie odpowiedzi do zmieniających się wydarzeń[166].

Analiza mediów społecznościowych umożliwia uzyskanie informacji dotyczących wzorców zachowań użytkowników, trendów społecznych oraz potencjalnych zagrożeń, co jest szczególnie użyteczne dla służb bezpieczeństwa i organów ścigania[167]. Odgrywa istotną rolę w zarządzaniu sytuacjami kryzysowymi, wspomagając przewidywanie i monitorowanie procesów radykalizacji społecznej oraz aktów przemocy, a także prognozowanie przyszłych trendów i zrozumienie zjawisk wpływających na bezpieczeństwo. Informacje pozyskane z mediów społecznościowych mogą być relewantne dla służb w kontekście zwalczania zarówno przestępczości kryminalnej, jak i terroryzmu[168]. Ich analiza jest wykorzystywana w profilowaniu kryminalnym oraz pośrednim szacowaniu osobowości[169], zarówno jako element przygotowania taktyki przesłuchania jak i do typowania kandydatów do roli agenta. Serwisy społecznościowe dostarczają szerokiego i zróżnicowanego spektrum treści, co stanowi istotne źródło dla analiz jawnoźródłowych (tab.3.3).

Tabela 3.3. Dane, które można pozyskać z mediów społecznościowych

Kategoria danych	Rodzaj danych
Informacje o użytkowniku	Imię i nazwisko, nazwa użytkownika, edukacja, miejsce pobytu, pracodawca, data urodzenia, informacje kontaktowe, rodzina/ związki, wydarzenia z życia, informacje medyczne, zdjęcie profilowe, linki do innych kont
Powiązania użytkownika	Rodzina, przyjaciele, współpracownicy, członkowie grup
Aktywności użytkownika	polubienia, komentarze, udostępnienia, reakcje, wiadomości prywatne
Treść postów	kontekst, lokalizacje, nawyki, zainteresowania, przyjaciele/ rodzina, poglądy
Materiały multimedialne	Zdjęcia, filmy, GIFy, transmisje na żywo, zdjęcia lokalizacji, cechy identyfikacyjne (kolor włosów, tatuaże)
Metadane	Data i godzina publikacji, lokalizacja, urządzenie, z którego pochodzą dane

Źródło: Opracowanie własne.

[166] D. Omand, C. Miller, J. Bartlett, *Towards the Discipline of Social Media Intelligence*, [w:] C. Hobbs, M. Moran, D. Salisbury (eds.), *Open Source Intelligence in the Twenty-First Century. New Security Challenges*, Palgrave Macmillan, London 2014, s. 25-26.
[167] A.L. Ivan, C.A. Iov, R.C. Lutai, M.N. Grad, *Social Media Intelligence: Opportunities and Limitations*, „CES Working Papers" 2013, vol. 7, no. 2A, s. 506.
[168] J. Konieczny, *Kryminalistyczny leksykon*…, op. cit., s. 145.
[169] Pośrednie szacowanie osobowości jest formą czynności operacyjno-rozpoznawczej mającą na celu ustalenie motywacji danej osoby poprzez wykorzystanie pełnego zakresu dostępnych informacji o niej, w tym obserwacji jej zachowań. Zob. szerzej: J. Konieczny, *Kryminalistyczny leksykon*…, op. cit., s. 202-203.

Informacje o powiązaniach interpersonalnych są istotne w działaniach prewencyjnych i wykrywaczach w kontekście szpiegostwa, przestępczości zorganizowanej oraz terroryzmu. Powiązania te mogą mieć charakter techniczny, społeczny, organizacyjny lub światopoglądowy. Pozyskane informacje umożliwiają identyfikację potencjalnych zagrożeń oraz osób i grup, które w swoim profilu działaniu mogą naruszyć normy prawne.

Zbieranie semi-pasywne to proces generowania ruchu internetowego do serwerów docelowych w celu uzyskania ogólnych informacji na ich temat. Ruch ten może być zaprojektowany tak, aby przypominał typowy ruch internetowy, co pozwala uniknąć zwrócenia uwagi na prowadzone działania rozpoznawcze. Mimo, że ten rodzaj pozyskiwania informacji jest uznawany do pewnego stopnia za anonimowy, obiekt może być świadomy prowadzonego rozpoznania, jeśli podjęte zostaną odpowiednie działania np.: sprawdzenie serwera lub urządzenia sieciowego.

Rekonesans aktywny polega na bezpośredniej interakcji z obiektem lub systemem w celu zebrania informacji, co niesie za sobą ryzyko wykrycia prowadzonych działań. Stosowanie metody aktywnej umożliwia uzyskanie szerszego zakresu informacji poprzez zastosowanie zaawansowanych technik, które pozwalają na dostęp do otwartych portów oraz skanowanie serwerów lub aplikacji internetowych w celu wykrycia luk w zabezpieczeniach. Tego rodzaju aktywność może być postrzegana jako podejrzane zachowanie i najprawdopodobniej pozostawi ślady w systemach wykrywania włamań, systemach zapobiegania włamaniom oraz w zaporze ogniowej. Do metod rekonesansu aktywnego należą: skanowanie sieci, portów i hostów[170].

3.3. Podział narzędzi cyfrowego wywiadu jawnoźródłowego

Początek drugiej generacji wywiadu jawnoźródłowego wiąże się z rozwojem nowych form narzędzi wykorzystujących innowacyjne rozwiązania techniczne. Mimo, że codziennie powstają kolejne narzędzia OSINT, dynamika zaimplementowanych w nich metod jest mniej intensywna. Ze względu na metody pozyskiwania i przetwarzania informacji jawnoźródłowych można wyróżnić cztery główne kategorii narzędzi[171]:

1) językowe i tekstowe,

[170] Zob. szerzej: R. Messier, *Kali Linux. Testy bezpieczeństwa. Testy penetracyjne i etyczne hakowanie*, Helion, Gliwice 2019, s. 96-105.
[171] A. Unver, *Digital open-source intelligence and international security: a primer*, EDAM Research Reports, Cyber Governance and Digital Democracy, 2018, s. 8.

2) geoprzestrzenne,
3) oparte na teorii sieci,
4) wykorzystujące kryminalistykę wizualną.

Narzędzia lingwistyczne służą do wyszukiwania i analizy danych tekstowych. Wraz z analizą sentymentu są wykorzystywane w wywiadzie jawnoźródłowym już od jego pierwszej generacji. Dzięki analizie mowy i pisma możliwe było wnioskowanie o motywacji przywódców, kierunkach prowadzonej polityki czy spójności poszczególnych organizacji. W okresie zimnej wojny powszechną praktyką stosowaną przez obie strony konfliktu było gromadzenie wycinków z gazet oraz czasopism naukowych. Od czasów I wojny światowej zarówno lingwistyka, jak i antropologia oraz badania danych przestrzennych zyskały na znaczeniu jako integralna część praktyki wywiadowczej[172]. Przejawiało się to również w tworzeniu dedykowanych wydziałów na najważniejszych uniwersytetach oraz w znaczącym wsparciu finansowym ze strony rządów na rozwój tych dziedzin. Do rozwoju analizy lingwistycznej przyczyniły się digitalizacja prac naukowych, literatury, prasy, narodowych archiwów, wystąpień publicznych, rozwój metod opartych na analizie tekstu jako danych w naukach społecznych oraz standaryzacja danych. Narzędzia lingwistyczne w erze mediów społecznościowych są wykorzystywane do jednoczesnego agregowania dużych ilości tekstu z różnorodnych źródeł, w wielu językach, odzwierciedlających różne kultury i narodowości.

Metody analizy leksykalnej są stosowane w narzędziach lingwistycznych w wywiadzie jawnoźródłowym w dwojaki sposób. Po pierwsze, możliwe jest pozyskiwanie informacji o najczęściej wyszukiwanych w danym przedziale czasowym frazach lub słowach kluczowych. Po drugie, umożliwiają one analizowanie znaczenia języka oraz wnioskowanie o podmiotach korzystających z mediów społecznościowych, w tym o ich cechach demograficznych, takich jak wiek, klasa społeczna, status ekonomiczny czy poziom wykształcenia.

Standaryzacja danych przyczyniła się do rozwój narzędzi leksykalnych, w których wykorzystywane są: kluczowość, profilowanie częstotliwości, klastrowanie, identyfikacja kolokacji, analiza sentymentu, analiza stanowiska, przetwarzanie języka naturalnego (ang. *natural language processing*, NLP) oraz uczenie maszynowe. Kluczowość jest miarą częstotliwości występowania słowa w danym zdaniu lub

[172] L.K. Johnson, *The Oxford Handbook of National Security Intelligence*, Oxford Handbooks, 2010, s. 144.

fragmencie tekstu. Za pomocą tego parametru możliwe jest stworzenie profilu podmiotu, w oparciu o słowa, których używa. Kluczowość jest również wykorzystywana do określania profilowania częstotliwości, które polega na odróżnienia jednego korpusu[173] od drugiego na podstawie występowania słów kluczowych w każdym z nich lub porównania przykładowego korpusu z dużym lub większym korpusem. Jednym z zastosowań profilowania częstotliwości jest możliwość przypisania danych do źródła, biorąc pod uwagę ich wystarczający korpus oraz odróżnienie różnorodnych etapów w piśmie lub mowie danej osoby. Klastrowość odnosi się do sekwencji dwóch lub więcej słów, które same w sobie mogą nie tworzyć poprawnej gramatycznie lub semantycznie jednostki, ale mogą być uwzględnione w analizie słów kluczowych. Kolokacja to prawdopodobieństwo, że dwa słowa wykryte w analizie kluczowości często pojawiają się obok siebie, zazwyczaj w odległości pięciu słów od badanego wyrazu. Kolokacja może być wykorzystywana zarówno do poprawy funkcji wyszukiwania, jak i do identyfikacji głównych tematów w tekście.

W narzędziach tekstowych wywiadu jawnoźródłowego wykorzystywana jest również analiza sentymentu (ang. *sentiment analysis*), czyli wydźwięku emocjonalnego tekstu. Analiza sentymentu umożliwia identyfikację obiektów lub jednostek, wobec których autor tekstu ma określone nastawienie. Jej podstawową funkcją jest klasyfikacja opinii wyrażanych online jako pozytywne, negatywne lub neutralne. Główną metodą stosowaną w analizie sentymentu jest klasyfikacja biegunowa, która pozwala ocenić emocjonalny ton tekstu jako pozytywny, negatywny lub neutralny. Bardziej zaawansowane techniki obejmują analizę aspektową, która identyfikuje konkretne elementy lub cechy podmiotu oraz ocenia nastawienie wobec każdego z tych aspektów. Inną metodą jest analiza emocji, klasyfikująca tekst na podstawie różnych emocji, takich jak radość, smutek, złość czy strach. Analiza stanowiska (ang. *stance analysis*) wykorzystuje preferencje językowe, aby ujawnić głębsze wartości jednostki oraz wyrazić jej postawę wobec określonego tematu czy zjawiska. W przeciwieństwie do analizy sentymentu, koncentruje się na tym, jak język odzwierciedla wartości i przekonania osoby, a nie tylko jej emocjonalne nastawienie. W wywiadzie jawnoźródłowym analiza stanowiska jest wykorzystywana do identyfikacji i zrozumienia postaw wobec kluczowych zagadnień związanych z bezpieczeństwem

[173] Korpus to zbiór materiałów pisanych lub mówionych w formie zrozumiałej przez maszyny, zebranych w celu badań lingwistycznych. Oxford English Dictionary, https://www.oed.com/?tl=true [dostęp: 20.04.2024].

państwa, co pozwala na dokładniejszą interpretację intencji badanych podmiotów oraz mitygację zagrożeń.

W związku z postępującą digitalizacją, coraz większe znaczenie w narzędziach lingwistycznych wykorzystywanych w wywiadzie jawnoźródłowym odgrywa przetwarzanie języka naturalnego. Jest to interdyscyplinarna dziedzina łącząca zagadnienia językoznawstwa i sztucznej inteligencji. Język naturalny jest używany do komunikacji interpersonalnej i cechuje się niejednoznacznością ze względu na bogactwo znaczeń oraz kontekst. W przeciwieństwie do niego, język formalny jest zaprojektowany tak, aby był zrozumiały dla komputerów i charakteryzuje się jednoznacznością, zwięzłością oraz precyzją. Początkowo NLP koncentrowało się na automatycznych tłumaczeniach między językami naturalnymi, obecnie skupia się na odkrywaniu wzorców w tekstach strukturalnych i niestrukturalnych, wielojęzycznych oraz obejmujących duże zbiory danych, poprzez analizę jednostek, słów kluczowych, relacji między słowami i frazami oraz ról semantycznych i syntaktycznych. NLP znajduje zastosowanie w połączeniu z algorytmami wyszukiwania informacji do analizy informacji jawnoźródłowych.

Zastosowanie uczenia maszynowego zwiększa efektywność narzędzi lingwistycznych, jednak wymaga od analityka zaawansowanej wiedzy zarówno z zakresu lingwistyki komputerowej, jak i technik uczenia maszynowego już na etapie projektowania systemu. Ważnym elementem tego procesu jest precyzyjne określenie parametrów modelu oraz odpowiednie przeprowadzenie treningu, co umożliwia rozpoznawanie konkretnych wzorców językowych w analizowanych tekstach. Istotny jest również rodzaj danych źródłowych, gdyż reguły zdefiniowane na podstawie jednej kategorii źródeł informacji mogą się znacząco różnić w odniesieniu do innego typu materiałów.

Narzędzia geoprzestrzenne służą do zbierania i analizowania informacji jawnoźródłowych, bezpośrednio lub pośrednio sytuujących podmiot lub grupę podmiotów w przestrzeni. Kartografia, podobnie jak językoznawstwo, była historycznie stałą częścią analiz wywiadowczych. Zmienne geopolityczne i geograficzne odgrywały kluczową rolę w kształtowaniu strategii bezpieczeństwa państwa oraz przewidywaniu potencjalnych zagrożeń i kierunków rozwoju w stosunkach międzynarodowych. Współcześnie, zaawansowane narzędzia geoprzestrzenne umożliwiają mapowanie indywidualnych i zbiorowych zachowań ludzkich, kryzysów, konfliktów, katastrof naturalnych oraz przemieszczania się ludności w trakcie konfliktów zbrojnych czy

migracji uchodźców. Rozpoznanie obrazowe dostarcza szczegółowych i precyzyjnych informacji na temat terenu, konstrukcji i infrastruktury, wspierając dowódców wojskowych w procesie decyzyjnym oraz w ochronie i efektywnym wykorzystaniu potencjału bojowego poprzez redukcję niepewności co do pozycji sił przeciwnika i warunków środowiskowych. Metody analizy geoprzestrzennej są często łączone z analizą sieciową i leksykalną w celu uzyskania bardziej precyzyjnych informacji o sytuacji politycznej, militarnej czy społecznej. Media społecznościowe zdynamizowały rozwój analiz geoprzestrzennych ze względu na funkcję automatycznego łączenia wypowiedzi z lokalizacją. Zastosowanie narzędzi geoprzestrzenych w wywiadzie jawnoźródłowych obejmuje geotagowanie, geolokację, geownioskowanie oraz georeferencjonowanie[174].

Geotagowanie to proces przypisywania znaczników z informacją o położeniu geograficznym danego obiektu do danych cyfrowych, takich jak zdjęcia, filmy, wpisy w mediach społecznościowych czy strony internetowe. Zazwyczaj obejmuje informacje o szerokości i długości geograficznej, a czasem także wysokości i orientacji urządzenia rejestrującego. Pozwala na dokładne określenie miejsca, w którym dana treść została utworzona lub do którego się odnosi, co jest szczególnie użyteczne w kontekście mapowania, analiz geoprzestrzennych oraz dokumentowania zdarzeń w czasie ich trwania. Obecnie większość urządzeń mobilnych automatycznie tworzy geotagi dla treści cyfrowych, korzystając z wewnętrznych danych lokalizacji globalnego systemu pozycjonowania (ang. *Global Positioning System*, GPS)[175]. Geotagi mogą być dodawane do plików na podstawie znanej pozycji urządzenia lub ręcznie w procesie wtórnym. Wielu użytkowników platform mediów społecznościowych celowo geotaguje posty, aby zaznaczyć swoją obecność na wydarzeniu lub przekazać informacje o rozwijającym się zdarzeniu w czasie rzeczywistym. Ta forma gromadzenia i rozpowszechniania danych lokalizacyjnych, określana jako „ochotnicza geografia”[176],

[174] H.J. Williams, I. Blum, *Defining Second Generation*…, op. cit., s. 33.

[175] Globalny system pozycjonowania (GPS) to satelitarny system nawigacyjny opracowany i zarządzany przez Departament Obrony USA umożliwiający precyzyjne określenie położenia i czasu na całym świecie, przez całą dobę. System ten jest wykorzystywany zarówno do celów wojskowych, jak i cywilnych, zapewniając szeroki zakres funkcji nawigacyjnych, lokalizacyjnych i czasowych. Zob. szerzej: S. Pace, G.P. Frost, I. Lachow, D.R. Frelinger, D. Fossum, D. Wassem, M.M. Pinto, *The Global Positioning System: Assessing National Policies*, RAND Corporation, 1995, https://www.rand.org/pubs/monograph_reports/MR614.html.

[176] „Ochotnicza geografia” to termin wprowadzony przez Michaela F. Goodchilda, który zwrócił uwagę na rosnące zaangażowanie zwykłych ludzi w tworzenie i rozpowszechnianie informacji geograficznych, co jest możliwe dzięki niższym kosztom i szerokiej dostępności nowoczesnych technologii. W zjawisku tym wykorzystywany jest potencjał masowego zaangażowania społeczności do generowania aktualnych

jest wykorzystywana do pozyskiwania informacji o wydarzeniach i ich uczestnikach oraz monitorowania przemieszczenia się dużych grup ludzi[177].

Geolokacja umożliwia precyzyjne określenie położenia geograficznego obiektów i zdarzeń na podstawie dostępnych publicznie danych cyfrowych. Analiza zdjęć i filmów przy użyciu ogólnie dostępnych programów, takich jak Google Earth[178], Google Maps[179], OpenStreetMap[180] i QGIS[181], pozwala na identyfikację charakterystycznych punktów orientacyjnych, a następnie na skojarzenie ich z lokalizacją przy użyciu stron takich jak Flickr[182], Mapillary[183] i Wikimapia[184], które łączą mapy ze zdjęciami oznaczonymi geograficznie.

Geownioskowanie pozwala na ustalenie lokalizacji użytkownika bez potrzeby korzystania z danych oznaczonych geotagami, wykorzystując różnorodne metody. Strony internetowe, takie jak Google, Craigslist, Facebook i Twitter, rejestrują lokalizację użytkownika w celu dostosowania treści i usług do jego indywidualnych potrzeb. Informacje o lokalizacji są przechowywane w pamięci podręcznej przeglądarki i mogą być później dostępne poprzez zastosowanie innych technik oraz technologii do wywnioskowania lokalizacji użytkownika, co pozwala określić jego położenie nawet na poziomie szczegółowej lokalizacji. W wywiadzie jawnoźródłowym geo-wnioskowanie może być wykorzystywane do śledzenia ruchów obserwowanych celów, monitorowania działań grup przestępczych, lokalizowania źródeł zagrożeń oraz wspomagania operacji ratunkowych.

Georeferencjonowanie to proces nadawania obiektom lokalizacji w przestrzeni fizycznej. W systemach informacji geograficznej (ang. *geographic information system*,

---

i szczegółowych danych, które mogą być użyteczne m.in. w kontekście zarządzania kryzysowego czy monitorowania zmian środowiskowych. Zob. szerzej: M.F. Goodchild, *Citizens as Voluntary Sensors*: Spatial *Data Infrastructure in the World of Web 2.0,* „International Journal of Spatial Data Infrastructures Research" 2007*,* vol. 2, no. 1, s. 24–32.

[177] Podczas protestów na placu Tahrir w Kairze w 2011 roku dziesiątki tysięcy demonstrantów zgromadziło się, aby wyrazić sprzeciw wobec reżimu Hosniego Mubaraka. Protestujący korzystali z mediów społecznościowych do geotagowania i przesyłania zdjęć oraz filmów z Tahrir Square, co pozwoliło na szerokie rozprzestrzenianie się tych materiałów przez media międzynarodowe. Ta metoda komunikacji i dokumentacji odegrała kluczową rolę w informowaniu globalnej społeczności o wydarzeniach na miejscu. Zob. szerzej: N. Pratt, *An Historical Overview of the 2011 Egyptian Revolution and its Aftermath*, Politics, Popular Culture and the 2011 Egyptian Revolution, 2020, https://egyptrevolution2011.ac.uk/exhibits/show/overview/overview [dostęp: 5.06.2024].

[178] https://www.google.com/earth [dostęp: 5.06.2024].

[179] https://www.google.com/maps [dostęp: 5.06.2024].

[180] https://www.openstreetmap.org [dostęp: 5.06.2024].

[181] https://www.qgis.org [dostęp: 5.06.2024].

[182] https://www.flickr.com [dostęp: 5.06.2024].

[183] https://www.mapillary.com [dostęp: 5.06.2024].

[184] https://www.wikimapia.org [dostęp: 5.06.2024].

GIS) reprezentacja różnych elementów środowiska geograficznego, takich jak rzeki, lasy, budynki, wysokości terenu i pola temperatury, odbywa się poprzez cyfrowe zakodowanie ich w pamięci komputera. Najczęściej wykorzystuje się do tego dwa rodzaje modeli cyfrowych danych przestrzennych: model wektorowy oraz model rastrowy. Dane wektorowe to cyfrowe reprezentacje obiektów geograficznych za pomocą punktów, linii i wielokątów. Dane rastrowe natomiast to cyfrowe obrazy składające się z pikseli, gdzie każdy piksel reprezentuje określoną wartość, są szczególnie przydatne do przechowywania danych, które zmieniają się w sposób ciągły, takich jak fotografie lotnicze, obrazy satelitarne czy powierzchnie stężeń chemicznych lub elewacji. Georeferencjonowanie jest szeroko stosowane w systemach informacji geograficznej do przypisywania współrzędnych przestrzennych mapom fizycznym lub obrazom rastrowym, które nie mają określonego systemu współrzędnych geograficznych. Umożliwia to nałożenie tych obrazów na nowoczesne dane i tworzenie dokładniejszych map zawierających szczegółowe informacje o infrastrukturze, takiej jak drogi i budynki. Takie informacje mogą być wykorzystywane do celów badawczych, militarnych oraz wywiadowczych[185]. Na poziomie taktycznym informacja geoprzestrzenna i systemy informacji geograficznej są kluczowe dla zwiększenia wiedzy o środowisku fizycznym oraz dostarczania podstaw geoprzestrzennych dla świadomości sytuacyjnej i wspólnego obrazu operacyjnego. GIS jest wykorzystywany do poszerzenia wiedzy o możliwościach i ograniczeniach sił własnych, identyfikacji zagrożeń oraz innych uwarunkowań środowiska operacyjnego[186]. Wraz ze wzrostem popularności GIS, dostępnych jest coraz więcej baz danych geoprzestrzennych. Są one uzupełniane przez dane pozyskiwane z GPS, satelitów oraz dronów, a także przez technologię wykorzystującą światło w postaci pulsującego lasera do pomiaru odległości do Ziemi (LIDAR). Impulsy świetlne, w połączeniu z innymi danymi rejestrowanymi przez system lotniczy, generują precyzyjne, trójwymiarowe informacje o kształcie i cechach Ziemi.

Kontekstualizowanie informacji o danym podmiocie czy obiekcie i jego wpływie na infrastrukturę oraz populację w czasie rzeczywistym ma duże znaczenie w wywiadzie jawnoźródłowym. Analitycy badający trwające konflikty militarne,

[185] Zob. szerzej: NASA Earthdata, „GeoTIFF", 2023, https://www.earthdata.nasa.gov/esdis/esco/standards-and-practices/geotiff [dostęp: 5.06.2024].

[186] *Rozpoznanie geoprzestrzenne*, Vademecum Bezpieczeństwa Informacyjnego, 2020, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/rozpoznanie-geoprzestrzenne/ [dostęp: 5.06.2024].

wszelkie wydarzenia czy sytuacje kryzysowe mogą korzystać z ogólnie dostępnych aplikacji do nawigacji i mapowania[187], publicznie dostępnych wpisów w mediach społecznościowych oraz filmów na YouTube, aby precyzyjnie określić lokalizacje prowadzonych działań. Dzięki możliwości nałożenia na mapy konkretnych czynników, takich jak zasoby wodne oraz dane o składzie etnicznym i religijnym regionu, można ukazać interakcje między fizycznymi cechami geograficznymi a demograficznymi i kulturowymi aspektami lokalnej społeczności na danym obszarze.

Narzędzia sieciowe wykorzystują metody zapożyczone z nauki o sieciach, która bada relacje pomiędzy podmiotami. W klasycznej teorii analizowane są powiązania pomiędzy jednostkami oraz formalnie ukształtowanymi relacjami społecznymi. Zakłada się, że relacje społeczne oraz oddziaływania wewnętrzne i zewnętrzne na te relacje mogą mieć wpływ na przekonania, postawy, wartości i zachowania społeczne. Poprzez badanie tychże relacji możliwe jest odwzorowanie struktur w obrębie badanych grup społecznych. Sieci mogą być jednowymiarowe, gdy zawierają tylko jeden typ jednostki (np. relacje między ludźmi), lub wielowymiarowe, gdy obejmują różne typy jednostek (np. numery telefonów, miejsca, osoby). W wywiadzie jawnoźródłowym pozyskiwanie informacji o osobach związanych z działalnością przestępczą oraz oddziaływaniem na grupy społeczne jest podstawowym elementem dalszego rozpoznania i przygotowania działań blokujących lub opracowania strategii profilaktycznych. Znaczenie teorii sieci rośnie w kontekście rozwijanych narzędzi OSINT, co jest wynikiem ciągłego rozwoju sieci społecznościowych. Teoria sieci umożliwia konceptualizację i ujęcie teoretyczne relacji na poziomach mikro i makro w analizie istniejących procesów bezpieczeństwa, poprzez m.in. dostarczanie struktury dla skomplikowanych interakcji społecznych.

Obliczeniowa analiza sieci rozwija klasyczną teorię sieci, umożliwiając analizę znacznie większych i bardziej skomplikowanych struktur. Dzięki temu możliwe jest nie tylko wyznaczanie relacji między jednostkami, ale także wykorzystanie sztucznej inteligencji, uczenia maszynowego oraz sieci neuronowych do automatycznego modyfikowania tych relacji w czasie rzeczywistym. W wywiadzie jawnoźródłowym narzędzia sieciowe są wykorzystywane w szczególności do analizy mediów społecznościowych poprzez wyszukiwanie, gromadzenie, mapowanie i identyfikację stopnia relacji pomiędzy użytkownikami portali społecznościowych.

[187] Przykładowe aplikacje tego typu to: Google Maps (www.google.com/maps), Apple Maps (www.apple.com/maps), Waze (www.waze.com), Bing Maps (www.bing.com/maps), Here WeGo (www.wego.here.com), OpenStreetMap (www.openstreetmap.org) oraz MapQuest (www.mapquest.com), [dostęp: 5.06.2024].

Istnieje wiele statystyk i miar związanych z analizą sieci dostarczających informacji pomagających zrozumieć, jak pozycje różnych jednostek (węzłów) w sieci wpływają na jej funkcjonowanie. Do najczęściej wykorzystywanych parametrów należą: centralność, pośredniość, bliskość oraz kierunkowość[188].

Centralność (ang. *centrality*), jako podstawowy parametr analizy sieci, opisuje pozycje węzła w strukturze sieci, jednocześnie wskazując jego ważność, znaczenie i wpływ na inne obiekty. Umożliwia analitykom ocenę ważności każdej jednostki w regulowaniu przepływu informacji w grupie. Dzięki temu można lepiej zrozumieć, jak informacje przepływają w sieci i jakie jednostki odgrywają kluczowe role w przekazywaniu informacji. W wywiadzie jawnoźródłowym badanie centralności sieci prowadzone jest w stosunku do najważniejszych członków grupy lub tych, którzy mają największą liczbę połączeń w grupie. W mediach społecznościowych będą to użytkownicy, którzy wywierają wpływ na innych (tzw. *influencerzy*) poprzez duże zasięgi publikowanych treści wśród społeczności, częste ich udostępniania oraz ilości interakcji.

Pośredniość (ang. *betweeness*) wskazuje, w jakim stopniu dany węzeł (jednostka) kontroluje komunikację w sieci. Miara ta jest wykorzystywana do wskazania najbardziej wpływowej jednostki w sieci społecznościowej. W wywiadzie jawnoźródłowym pośredniość pozwala analitykom uzyskać wyraźny obraz tego, o czym dyskutuje mała liczba kluczowych węzłów, nawet jeśli użytkownicy zapewniają wysoki poziom ochrony prywatności w swoich profilach w mediach społecznościowych. Możliwe jest również wywnioskowanie treści przekazu centralnego węzła na podstawie analiz wypowiedzi węzłów sąsiadujących.

Bliskość (ang. *closeness*) jest parametrem określającym, jak blisko dany węzeł znajduje się względem wszystkich pozostałych węzłów w sieci. W wywiadzie jawnoźródłowym, bliskość może być wykorzystywana do identyfikacji kluczowych jednostek w sieciach społecznościowych, które mają najefektywniejszy dostęp do innych jednostek. Przykładowo, w analizie sieci terrorystycznej, węzeł o wysokiej bliskości może być identyfikowany jako potencjalny koordynator działań ze względu na zdolność do szybkiego komunikowania się z wieloma innymi członkami sieci.

Kierunkowość (ang. *directionality*) odnosi się do kierunku, z którego pochodzi informacja oraz kierunku jej przepływu. Mierzona jest jako liczbą informacji

[188] H.J. Williams, I. Blum, *Defining Second Generation*…, op. cit., s. 27-30.

wychodzących lub liczba informacji przychodzących. Jednostki z większą liczbą informacji przychodzących zazwyczaj odgrywają kluczową rolę w strukturze sieci. W kontekście prowadzonego wywiadu jawnoźródłowego, kierunkowość umożliwia analizę dynamiki wpływu i władzy w różnych strukturach społecznych i organizacyjnych poprzez identyfikację najważniejszych podmiotów w badanej grupie społecznej. Analiza kierunkowości może ujawnić, które konta w mediach społecznościowych są centralnymi węzłami w sieci dezinformacji, poprzez identyfikację tych, które otrzymują najwięcej odpowiedzi i są najczęściej udostępniane.

Narzędzia wykorzystujące kryminalistykę wizualną służą do ekstrakcji danych z plików graficznych i wideo, umożliwiają wykrywanie zmanipulowanych obrazów oraz przeprowadzanie analizy fotogrametrycznej. Potrzeba rozwoju tego typu narzędzi zawiązana jest z rozwojem technologii cyfrowych i ewolucją komunikacji w Internecie, z tekstowej na komunikację opartą na mediach. Wynika to z łatwości przesyłania wiadomości głosowych, video czy obrazu, które zastępują konieczność tworzenia tekstów. W sytuacjach kryzysowych, zarówno z powodu stresu, jak i konieczności szybkiego przekazywania informacji, użytkownicy dokumentują wydarzenia wizualnie w czasie rzeczywistym i dzielą się nimi w mediach społecznościowych. Badania obrazów – rozpoznanie obrazowe (ang. *imagery Intelligence*, IMINT) jako dyscyplina wywiadowcza rozwinęło się po II wojnie światowej. Polega na pozyskiwaniu informacji za pomocą środków i systemów obrazujących oraz zdjęć. Do tego celu wykorzystuje się narzędzia optyczne, radary i lasery. Z uwagi na przenikanie się różnych dyscyplin wywiadowczych oraz ogólną dostępność materiałów wizualnych, rozpoznawanie obrazowe jest obecnie integralną częścią wywiadu jawnoźródłowego. Narzędzia wykorzystujące kryminalistykę wizualną służą do pozyskiwania i ustrukturyzowanej analizy umożliwiającej walidację i interpretację informacji jawnoźródłowych. Wykorzystywane są m.in. do działań podejmowanych na obszarach, gdzie dostęp fizyczny jest ograniczony lub stwarza zagrożenie dla zdrowia i życia ludzkiego. Obejmują one sytuacje kryzysowe, takie jak klęski żywiołowe, katastrofy przemysłowe czy konflikty zbrojne. Narzędzia wykorzystujące kryminalistykę wizualną umożliwiają dokładne monitorowanie i dokumentowanie zdarzeń w czasie rzeczywistym, skracając czas podjęcia kluczowych decyzji dotyczących reagowania i koordynacji działań podejmowanych na rzecz bezpieczeństwa. Dodatkowy pozyskany i zweryfikowany materiał stanowi dowód na istnienie zjawiska, faktu czy zdarzenia. Materiały wizualne są jednocześnie podatne na manipulacje, które mogą polegać na fałszerstwie

kopiowania i wklejania, kiedy obiekt jest wstawiany lub usuwany z obrazu lub video albo na fałszerstwie związanym z klatkami, kiedy zestaw klatek jest usuwany z sekwencji wideo lub w których zmieniany jest ich układ[189]. Sabotaż materiałów wizualnych jest szkodliwą operacją, zmieniającą zdarzenia przedstawione na obrazie lub wideo oraz jego znaczenie. Jest celowo wykorzystywany zarówno przez podmioty państwowe jak i niepaństwowe do tworzenia kampanii dezinformacyjnych oraz propagandy.

W tworzonych narzędziach tej kategorii do analizy obrazu i wideo wykorzystywane są m.in. dane pozyskiwane z technologii GIS, dane satelitarne, dane z dronów oraz z mediów społecznościowych. Najczęściej wykorzystywane metody to: analiza artefaktów, analiza fotogrametryczna, analiza metadanych, porównanie fotograficzne oraz analiza cyfrowa. Wraz z rozwojem technologii można spodziewać się jeszcze większej integracji i zaawansowania tych narzędzi, a przez to szybszego i dokładniejszego gromadzenia informacji jawnoźródłowych.

Analiza artefaktów umożliwia identyfikację widocznych zniekształceń i błędów wizualnych w materiałach medialnych, takich jak wideo, audio czy obrazy. Artefakty to wszelkie anomalie, które mogą wynikać z procesów kompresji, transmisji danych lub manipulacji cyfrowej. Homogeniczność artefaktów, czyli równomierność tych zniekształceń w całym materiale, jest wskaźnikiem ich autentyczności. Nierównomierność artefaktów często wskazuje na manipulację i fałszowanie treści. Metody analizy artefaktów obejmują badanie tych zniekształceń w celu wykrycia potencjalnych nieprawidłowości.

Fotogrametria pozwala na dokładne pomiary zdjęć, które mogą obejmować precyzyjne współrzędne lub odległości między elementami na obrazach. W analityce jawnoźródłowej jest wykorzystywana do analizy obrazów 2D i 3D pozyskiwanych z satelitów, dronów lub technologii LIDAR. Algorytmy stosowane w fotogrametrii zazwyczaj dążą do minimalizacji sumy kwadratów błędów w zakresie współrzędnych i względnych przemieszczeń punktów odniesienia. Analiza fotogrametryczna wykorzystywana jest do rekonstrukcji miejsc zbrodni oraz tworzenia trójwymiarowych modeli, które mogą być użyte jako dowody w sądzie. Analiza wideo umożliwia przeglądanie i analizowanie nagrań z monitoringu w celu identyfikacji podejrzanych

[189] W.D. Ferreira, C.B.R. Ferreira, G. da Cruz Júnior, F. Soares, *A review of digital image forensics*, „Computers & Electrical Engineering" 2020, vol. 85, 106685, https://doi.org/10.1016/j.compeleceng.2020.106685 [dostęp: 10.06.2024].

zachowania i rekonstrukcji przebiegu zdarzeń. Wykorzystanie zaawansowanych algorytmów do analizy wideo umożliwia automatyczne wykrywanie i śledzenie ruchu, identyfikację twarzy oraz analizę podejrzanych zachowań.

Analiza metadanych obejmuje badanie właściwości plików multimedialnych, które opisują ich zawartość, takich jak tytuł, autor, gatunek, oraz parametry kodowania, w tym algorytm kodowania, rozmiar klatki wideo, liczba klatek na sekundę, ilość danych zużywanych do przekazywania strumienia dźwięku w jednostce czasu i częstotliwość próbkowania audio. Dostęp do tych informacji poprzez metadane może być szybszy niż poprzez bezpośrednią analizę technicznych parametrów plików multimedialnych.

Porównanie fotograficzne umożliwia sprawdzenie autentyczności lub zmian w różnych wersjach tego samego obrazu oraz jest wykorzystywane do przeszukiwania dużych zasobów podobnych obrazów w celu zidentyfikowania oryginału. W sytuacjach kryzysowych oraz istotnych wydarzeniach politycznych czy społecznych, oprogramowanie do automatycznego porównywania może wykrywać zmiany niedostrzegalne dla ludzkiego oka.

Analiza cyfrowa obejmuje zarówno wyszukiwanie usuniętych lub ukrytych danych, jak i zrozumienie technik implementowanych w tworzonych narzędziach oraz zdolność do prezentowania materiału mającego wartość dowodową. W związku ze wzrostem przestępczości popełnianej przy użyciu nowych technologii, konieczne jest skuteczne wykrywanie i analizowanie dowodów cyfrowych w celu oceny ich autentyczności i integralności[190].

Narzędzia kryminalistyki wizualnej danych satelitarnych i dronów wykorzystywane są do monitorowania i śledzenia ruchów osób oraz pojazdów. Dane te mogą być wykorzystywane do identyfikacji podejrzanych, monitorowania działań przestępczych oraz wsparcia operacji policyjnych. Dzięki wykorzystaniu technologii zdalnego monitoringu, organy ścigania mogą reagować szybciej i skuteczniej na zaistniałe zagrożenia. Wykorzystanie zaawansowanych technologii w narzędziach opartych na kryminalistyce wizualnej przynosi korzyści zarówno w kontekście operacyjnym, jak i strategicznym, przyczyniając się do zwiększenia skuteczności działań na rzecz bezpieczeństwa państwa.

[190] H.B. Wolfe, *Computer forensics*, „Computers & Security" 2003, vol. 22, no. 1, s. 26, https://doi.org/10.1016/S0167-4048(03)00105-6 [dostęp: 10.06.2024].

Narzędzia wykorzystujące kryminalistykę wizualną są również tworzone oraz rozwijane w ramach prywatnych inicjatyw, które korzystają z materiałów jawnoźródłowych do specjalistycznej analizy obrazów i filmów wideo oraz prowadzą dochodzenia dotyczące naruszeń praw człowieka i konfliktów zbrojnych. Te multidyscyplinarne grupy badawcze stosują zaawansowane metody analizy wizualnej i dziennikarstwa śledczego. Najbardziej znane inicjatywy to m.in.: Bellingcat[191], Human Rights Watch Digital Investigations Lab[192], WINTESS [193] oraz Forensic Architecture[194].

Konkludując, narzędzia cyfrowego OSINT ukazują złożoność współczesnych metod analizy informacji jawnoźródłowych. Każda z wyróżnionych kategorii odpowiada na odmienne potrzeby operacyjne – od analizy danych tekstowych i sieci powiązań, przez rozwiązania geoprzestrzenne, po przetwarzanie materiałów wizualnych. Wyzwaniem pozostaje ich integracja w procesie analitycznym, mająca na celu minimalizację ryzyka błędów oraz zwiększenie efektywności pozyskiwania informacji. W tym kontekście szczególnego znaczenia nabiera automatyzacja tych narzędzi oraz ocena ich wpływu na skuteczność działań wywiadowczych i procesy decyzyjne w obszarze bezpieczeństwa państwa.

3.4. Przykładowe narzędzia cyfrowego wywiadu jawnoźródłowego

Dynamiczny rozwój nowych technologii i przeobrażenia w interakcjach cyfrowych determinują zmienność narzędzi służących do pozyskiwania informacji jawnoźródłowych. Narzędzia OSINT to zarówno proste wtyczki do przeglądarek, usługi online, referencyjne bazy danych, zainstalowane aplikacje jak i narzędzia automatyzujące[195]. Wywiad jawnoźródłowy jest stosowany zarówno przez podmioty publiczne jak i prywatne, które mają różne cele i obszary rozpoznania, infrastrukturę techniczną, ramy prawne działania oraz stopień akceptacji ryzyka. Możliwości techniczne tych podmiotów wyznaczane są dodatkowo przez źródła finansowania oraz wiedzę osób projektujących i obsługujących narzędzia służące do jawnoźródłowego rozpoznania. Dodatkowo aspekty techniczne i prawne maja wpływ na sposób

[191] https://www.bellingcat.com/ [dostęp: 10.06.2024].
[192] https://www.hrw.org/topic/technology-and-rights/digital-investigations-lab [dostęp: 10.06.2024].
[193] https://www.witness.org/ [dostęp: 10.06.2024].
[194] https://forensic-architecture.org/ [dostęp: 10.06.2024].
[195] M. Bazzell, *Open Source Intelligence Techniques. Resources for searchning and analyzing online information*, Sixth Edition, CreateSpace Independent Publishing Platform 2018, s. 33 i nast.

organizacji i zmienność otwartych źródeł informacji (np. duża dynamika portali społecznościowych), w odpowiedzi na co zmieniają się również narzędzia służące do eksploracji tych zasobów. Z tych względów uznać należy, iż jakikolwiek przegląd środków pozyskiwania i gromadzenia informacji z publicznie dostępnych źródeł może mieć jedynie charakter poglądowy.

Ze względu na kryterium dostępności i elastyczności można wyróżnić trzy rodzaje narzędzi OSINT: komercyjne, projektowane na zamówienie oraz oparte na oprogramowaniu open source, dostępnym publicznie i modyfikowalnym. Każde z narzędzi charakteryzuje się swoistymi zaletami i ograniczeniami, które zostały przedstawione w tabeli 3.4. Wybór narzędzia uzależniony jest od specyficznych wymagań, dostępności otwartych źródeł, możliwości skalowania, poziomu automatyzacji, wymagań dotyczących przechowywania i aktualizacji informacji, zgodności z obowiązującymi przepisami prawa oraz kompetencji analityka.

Tabela 3.4. Zestawienie różnic w narzędziach OSINT

Parametry oceny	**Narzędzia komercyjne**	**Narzędzia projektowane na zamówienie**	**Narzędzi open-source**
Bezpieczeństwo i wsparcie	Prywatne firmy mogą oferować lepszą infrastrukturę bezpieczeństwa i ciągłe wsparcie techniczne	Organizacja utrzymuje pełną kontrolę i ponosi pełną odpowiedzialność nad całym systemem i danymi	Bezpieczeństwo i prywatność mogą być zagrożone, jeśli narzędzia udostępniają/sprzedają dane
Koszty	Wysokie koszty zakupy i potencjalne, dalsze ukryte koszty	Wysokie koszty. Dłuższy czas wymagany do budowy i wsparcia systemu	Darmowe
Interakcje z podmiotami trzecimi	Możliwe interakcje z podmiotami trzecimi/możliwość potencjalnego ujawnienia rozpoznania	Kontrola nad interakcją z podmiotami trzecimi	Potencjalna możliwość interakcji, weryfikowana poprzez wcześniejsze badania mające na celu uzyskanie informacji o twórcy i budowie narzędzia.

Parametry oceny	Narzędzia komercyjne	Narzędzia projektowane na zamówienie	Narzędzi open-source
Kontrola kodu źródłowego	Zamknięty kod źródłowy ze względu na ochronę własności intelektualnej.	Pełna kontrola na kodem źródłowym.	Otwarty kod źródłowy, które można swobodnie modyfikować.
Kontrola nad danymi/możliwość przenoszenie danych	Istnieje obawa o władztwo nad danymi i możliwość ich przenoszenia.	Pełna kontrola nad danymi	Istnieje obawa o władztwo nad danymi i możliwość ich przenoszenia.
Integracja z innymi systemami	Problemy z interoperacyjnością z innymi systemami	Potencjalnie łatwiejsza integracja z innymi systemami tworzonymi na zamówienie	Wymaga każdorazowego badania
Wymogi prawne	Potencjalne naruszenie prywatności wynikające z działań podejmowanych przez organy władzy publicznej	Zgodnie z zapisami umowy	Potencjalne problemy prawne w razie ewentualnego sporu i zakwestionowania narzędzia przez stronę przeciwną

Źródło: Opracowanie własne na podstawie: *Berkeley Protocol on Digital Open Source Investigations, HR/PUB/20/2,* Nowy York–Genewa 2022, s. 50–51.

Przykładem narzędzia wspomagającego pozyskiwanie informacji jawnoźródłowych jest OSINT Framework[196]. Jest to platforma sieciowa, która organizuje różne obszary tematyczne i integruje je z narzędziami ułatwiającymi gromadzenie informacji. Narzędzia te są pogrupowane według kategorii, a po ich wyborze dostępne są odpowiednie zasoby wspierające proces pozyskiwania danych. Wybór narzędzi wyszukiwania jawnoźródłowego powinien być ściśle związany ze zidentyfikowanym zapytaniem.

Do najpopularniejszych narzędzi wywiadu jawnoźródłowego należą wyszukiwarki internetowe, czyli wyspecjalizowane programy lub strony internetowe przeznaczone do wyszukiwania informacji dostępnych w zasobach Internetu. Wyszukiwanie odbywa się na podstawie zapytania, słowa kluczowego lub innej wartości wyjściowej. Wśród wyszukiwarek można wyróżnić: wyszukiwarki oparte na robotach, katalogi obsługiwane przez ludzi, wyszukiwarki hybrydowe

[196] https://osintframework.com/ [dostęp: 2.07.2024].

i metawyszukiwarki[197]. Do najpopularniejszych wyszukiwarek należą: Google[198], Bing[199], Yandex[200], Baidu [201] oraz DuckDuckGo[202]. Wyszukiwarki wykonują trzy operacje: przeszukiwanie, indeksowanie i wyszukiwanie.

Wyszukiwanie przy pomocy internetowych wyszukiwarek wymaga opracowania i wdrożenia haseł wyszukiwawczych odnoszących się do treści wyszukiwania oraz operatorów, które odnoszą się do zapytania. Istnieją zarówno bezpłatne jak i płatne narzędzia do tworzenia słów kluczowych, które pozwalają dobrać frazy najtrafniej identyfikujące poszukiwane treści. Wiele z nich zostało zaprojektowanych celem optymalizacji wyszukiwarek (ang. *search engine optimization*, SEO), te same narzędzia mogą być przydatne w wyszukiwaniu informacji jawnoźródłowych w Internecie.

Przy tworzeniu haseł wyszukiwawczych istotna jest zarówno ich warstwa semantyczna i syntaktyczna, jak i ograniczenia techniczne wpływające na długość. Ważne jest również opracowanie różnych wariantów tego samego hasła oraz przygotowanie alternatywnych form wyszukiwanych pojęć[203].

Każda wyszukiwarka indeksuje zasoby Internetu przy użyciu innych algorytmów, w różnych dostępach czasowych[204], przez co wyszukiwanie nie jest prowadzone we wszystkich dostępnych zasobach. Narzędziami, które usprawniają procesy wyszukiwania z uwagi na zakres i czas są multiwyszukiwarki. Są to programy umożliwiające jednoczesne wyszukiwanie w wielu elektronicznych bazach danych oraz grupowanie wyników. Podobnym narzędziem wyszukiwania są metawyszukiwarki, których funkcje rozszerzone są o agregowanie i rangowanie wyników wyszukiwania. W jednym zapytaniu można łączyć różne formaty wyszukiwania. Na przykład narzędzie Google Multisearch, wykorzystujące sztuczną inteligencję, pozwala na jednoczesne przeszukiwanie zasobów tekstowych i graficznych.

Wyszukiwarki semantyczne (ang. *semantic search engines*) to technologie wykorzystujące uczenie maszynowe (ang. *machine learning*, ML), które odnajdują

[197] K. Tarakeswar, D. Kavitha, *Search engines: a study*, „Journal of Computer Applications (JCA)" 2011, vol. 4, no. 1, s. 29–33.
[198] https://www.google.com/. „OSINT rozpoczyna się od prostego wyszukiwania w Google" – stwierdza Alexandra Jousset, współautorka (z Ksenią Bolchakovą) nagrodzonego filmu dokumentalnego *Wagnerowcy, tajna armia Putina* (Francja 5, 2022). https://ihedn.fr/en/2023/06/08/aubaines-et-limites-de-losint-le-nouveau-nerf-de-la-guerre/ [dostęp: 2.01.2023].
[199] https://www.bing.com/ [dostęp: 2.01.2023].
[200] https://yandex.com/ [dostęp: 2.01.2023].
[201] https://www.baidu.com/ [dostęp: 2.01.2023].
[202] https://duckduckgo.com/ [dostęp: 2.01.2023].
[203] D. Mider, *Sztuka wyszukiwania*…, op. cit., s. 192–193.
[204] Ibidem, s. 209.

informacje na podstawie wpisanego ciąg znaków, kontekstu wyszukiwania oraz intencji osoby wyszukującej[205]. Ich dokładność jest wynikiem zintegrowania oprogramowania wyszukiwania z przetwarzaniem języka naturalnego. Wyszukiwarki semantyczne, ze względu na źródło szukania odpowiedzi, można podzielić na dwie kategorię: wyszukiwarki analizujące znaczenie indeksowanych dokumentów oraz wyszukiwarki przeszukujące istniejące zasoby sieci[206].

Kolejnym typem są wyszukiwarki urządzeń podłączonych do Internetu, które skanują publicznie dostępne sieci w poszukiwaniu otwartych portów oraz usług zidentyfikowanych jako działające na tych portach. Wyszukiwarki internetu rzeczy (ang. *internet of things*, IoT)[207] umożliwiają rozpoznanie różnorodnych urządzeń, niezależnie od ich technologicznego zaawansowania czy wykonywanych funkcji, takich jak: kamery routery, serwery czy sensory. Najpopularniejszym[208] tego typu narzędziem jest Shodan[209]. Jest to jednocześnie wyszukiwarka i skaner portów służąca do identyfikacji urządzeń połączonych z Internetem, takich jak serwery, routery, kamery, sieci IP. Narzędzie nie ogranicza się tylko do badania tradycyjnej sieci WWW, ale poszerza swoje działanie na obszar internetu rzeczy (IoT). Shodan udostępnia na żądanie historyczne adresy IP oraz adresy wyszukiwane, pobierane z bazy danych hostów z otwartymi portami i dostępnymi usługami. Systematycznie skanuje sieć w celu identyfikacji różnych usług internetowych i urządzeń, a następnie gromadzi i zapisuje informacje o nich. Informacje gromadzone przez Shodan obejmują lokalizację geograficzną urządzeń, używane oprogramowanie, otwarte porty oraz dostępne usługi internetowe. Na ich podstawie podmioty prowadzące rozpoznanie jawnoźródłowe mogą zbudować kompleksowy obraz architektury sieciowej badanych obiektów.

W wywiadzie jawnoźródłowym obok wyszukiwarek internetowych istotną rolę pełnią również web crawlery, zwane inaczej „pająkami internetowymi". Są to

[205] H. Bast, B. Buchhold, E. Haussmann, *Semantic Search on Text and Knowledge Bases*, „Foundations and Trends in Information Retrieval" 2016, vol. 10, no. 2–3, s. 119–271.
[206] B. Gontar, J. Papińska-Kacperek, *Semantyczne wyszukiwarki internetowe, (Semantic Search Engines)*, „Acta Universitatis Lodziensis. Folia Oeconomica" 261, 2011, s. 172.
[207] Internet rzeczy został zdefiniowany w Rekomendacji ITU-T Y.2060 (06/2012) jako globalna infrastruktura dla społeczeństwa informacyjnego, umożliwiająca dostęp do zaawansowanych usług przez połączenie (fizyczne lub wirtualne) przedmiotów (obiektów), bazujące na istniejących i rozwijanych interoperacyjnych technologiach informacyjno-komunikacyjnych. Zob. International Telecommunication Union, *Next Generation Networks – Framework and functional architecture models – Overview of the Internet of things*, ITU-T Y.2060, 06/2012, s. 2–3.
[208] Przykłady innych wyszukiwarek IoT: ZoomEye (https://www.zoomeye.org/), Censys (https://censys.com/), BinaryEdge (https://www.binaryedge.io/), Wigle (https://wigle.net/).
[209] https://www.shodan.io/ [dostęp: 5.07.2024]; por. D.G. Graham, *Etyczny haking. Praktyczne wprowadzenie do hakingu*, Helion, Gliwice 2021, s. 163–164.

zaawansowane narzędzia automatycznie przeszukujące i indeksujące zawartość stron internetowych, umożliwiając tym samym gromadzenie i analizę dużych ilości danych. Ich główną funkcją jest identyfikacja i pobieranie zasobów internetowych, które mogą być następnie wykorzystywane do indeksowania w wyszukiwarkach, analizy dużych zbiorów danych oraz agregacji i kategoryzacji treści na potrzeby konkretnych analiz lub aplikacji. Web crawlery mogą być również tworzone do realizacji wyspecjalizowanych zadań, w ramach których oceniają wartość hiperłączy na podstawie kontekstu, w jakim się pojawiają. Przykładem są "focused crawlers", które są skonfigurowane do wyszukiwania konkretnych informacji. Web crawlery mogą być dostosowane do przeszukiwania Darknetu poprzez konfigurację umożliwiającą dostęp do sieci takich jak Tor, I2P i Freenet. W wywiadzie jawnoźródłowym mogą służyć do monitorowania i analizowania aktywności w sieciach społecznościowych. Dzięki możliwości automatycznego przeszukiwania Darknetu, pozwalają na identyfikację nielegalnych działań, takich jak handel bronią, narkotykami czy ludźmi. Ponadto mogą być wykorzystywane do śledzenia propagandy, dezinformacji oraz procesów rekrutacji prowadzonych przez grupy ekstremistyczne. Przykładowe narzędzia to Common Crawl[210] oraz Octoparse [211].

Dostępnych jest wiele narzędzi wspierających realizację technicznego footprintingu. Popularne narzędzia WHOIS, które są wykorzystywane do zbierania i analizowania danych dotyczących rejestracji domen oraz informacji kontaktowych właścicieli domen, to m.in.: Whois[212], Whoisology[213] oraz Robtex[214].

Istnieje również wiele narzędzi wspomagających śledzenie adresów IP, które są wykorzystywane w procesie technicznego footprintingu. Do pozyskiwania informacji o adresach IP wykorzystywane są narzędzia takie jak: Onyphe[215] oraz Reverse Lookup[216], które umożliwiają gromadzenie szczegółowych danych na temat konkretnych adresów IP oraz ich powiązań w sieci. W przypadku, gdy adresy IP znajdują się na listach blokowanych, do ich identyfikacji służą narzędzia takie jak Spamhaus IP Blocklist[217]. Informacje o zablokowanych adresach IP są istotne dla

[210] https://commoncrawl.org/ [dostęp: 2.07.2024].
[211] https://www.octoparse.com/ [dostęp: 2.07.2024].
[212] https://www.whois.com/ [dostęp: 3.07.2024].
[213] https://whoisology.com/ [dostęp: 3.07.2024].
[214] https://www.robtex.com/ [dostęp: 3.07.2024].
[215] https://www.onyphe.io/ [dostęp: 10.07.2024].
[216] https://mxtoolbox.com/ReverseLookup.aspx [dostęp: 10.07.2024].
[217] https://check.spamhaus.org/ [dostęp: 10.07.2024].

ochrony przed niepożądanym ruchem sieciowym oraz potencjalnymi zagrożeniami cybernetycznymi.

Najpopularniejszym narzędziem do web scrapingu jest The Harvester, który wyszukuje szczegółowe informacje m.in. z wyszukiwarek Google, Bing, biznesowego serwisu społecznościowego LinkedIn, Exalead, serwisów Twitter oraz Pretty Good Privacy (PGP). Nowe funkcje The Harvester obejmują: możliwość ustawienia opóźnień czasowych między zapytaniami, wyszukiwanie domeny we wszystkich dostępnych źródłach oraz funkcję weryfikacji wirtualnych hostów. Jest to narzędzie, które dostarcza informacji o adresach poczty elektronicznej, nazwach użytkowników i nazwach hostów/subdomen, otwartych portach/banerach i nazwiskach pracowników z różnych publicznych źródeł (wyszukiwarki, serwery kluczy PGP).

W procesie inżynierii odwrotnej, stosowanej do analizy zasobów cyfrowych, niezbędnymi narzędziami są deasemblery i dekompilatory[218]. Deasemblery konwertują kod maszynowy na język asemblera, co umożliwia analizę niskopoziomowego działania programu i lepsze zrozumienie jego struktury. Dekompilatory przekształcają język maszynowy lub kod bajtowy do postaci języka wyższego poziomu. Choć proces ten nie zawsze zapewnia pełną dokładność, pozwala na lepsze zrozumienie logiki programu oraz jego funkcji. Debugery są kolejnym narzędziem w inżynierii odwrotnej, pozwalającym na monitorowanie działania programu w czasie rzeczywistym, identyfikację błędów i analizę zachowania oprogramowania. Celem usprawnienia analizy jawnoźródłowej tworzone są zautomatyzowane narzędzia do wyszukiwania i gromadzenia oraz analizy informacji, które umożliwiają również badanie innych zasobów i struktur obiektów w aspekcie informatycznym. Przykładem takich narzędzi są: Oryon Browser, Maltego, FOCA, SpiderFoot oraz Recon-ng. Ich zaletą w wywiadzie jawnoźródłowym jest zdolność do szybkiego wyszukiwania i konsolidacji informacji pozyskanych z różnych zasobów, a także przedstawianie relacji między nimi, ich systematyzacja oraz przejrzysta wizualizacja. Narzędzia automatyzujące usprawniają gromadzenie i przetwarzanie dużych ilości zróżnicowanych informacji, znacząco skracając czas potrzebny na analizę. Może to jednak prowadzić do wyzwań związanych z dokładnością i wiarygodnością, potencjalnymi uprzedzeniami w algorytmach oraz zgodnością z przepisami dotyczącymi prywatności.

[218] Akademia Wywiadu, *Podstawy inżynierii wstecznej w cyberbezpieczeństwie*, 2023, https://akademiawywiadu.pl/podstawy-inzynierii-wstecznej-w-cyberbezpieczenstwie/ [dostęp: 12.07.2024].

Maltego to rozbudowane narzędzie, które umożliwia automatyczne pozyskiwanie informacji jawnoźródłowych, odnajduje relacje między nimi i przedstawia wyniki w formie interaktywnej siatki powiązań. Działa w oparciu o dedykowane skrypty (transformacje), które poprzez określone wyszukiwania na podstawie zadanych danych wejściowych, wprowadzają na tworzony graf zależności. Wyszukiwania wykonywane z Maltego nie powodują pozostawiania śladów w rozpoznawanej infrastrukturze, jednak zasada działania wbudowanych transformacji opiera się na wysyłaniu zapytań do serwera transformacji Maltego[219].

Oryon OSINT Browser to popularne bezpłatne narzędzie do prowadzenia rozpoznania jawnoźródłowego. Jest wyposażone w dziesiątki wstępnie zainstalowanych narzędzi, m.in do analizy domen, wyszukiwarki osób i firm, wyszukiwarki w *deep web* i Darknecie, programy do analizy i wyszukiwania video oraz metadanych.

FOCA (ang. *Fingerprinting Organizations with Collected Archives*)[220] to pakiet oprogramowania typu open source, który umożliwia wyszukiwanie oraz pozyskiwanie metadanych i innych informacji zawartych w publicznie dostępnych dokumentach. Za pośrednictwem wyszukiwarek Google, Bing oraz DuckDuckGo odnajduje materiały udostępnione przez podmioty będące obiektem rozpoznania, pobiera je i automatycznie wydobywa z nich informacje, w tym metadane. FOCA, oprócz zastosowania w wywiadzie jawnoźródłowym, jest również wykorzystywana do przeprowadzania audytów bezpieczeństwa.

SpiderFoot[221] to narzędzie zaprojektowane w celu automatyzacji procesów związanych z wywiadem jawnoźródłowym. Umożliwia gromadzenie m.in. adresów IP, adresów e-mail, numerów telefonów, nazwy domen, adresów Bitcoina, nazw hostów z ponad stu publicznie dostępnych źródeł[222]. Narzędzie to jest dedykowane do prowadzenia analiz cyberbezpieczeństwa oraz do zdalnego rekonesansu, w tym pasywnego. SpiderFoot służy do wykrywania potencjalnych zagrożeń oraz identyfikacji podatności, takich jak otwarte porty, a także umożliwia przeprowadzenie analizy sieciowej i geolokalizacji. Wykorzystanie ponad dwustu modułów w SpiderFoot pozwala na precyzyjną konfigurację narzędzia, dostosowaną do specyficznych potrzeb użytkownika poprzez aktywację lub dezaktywację dedykowanych funkcji. Elastyczność w dostosowywaniu narzędzia do konkretnych zadań w ramach wywiadu

[219] Zob. szerzej: https://www.maltego.com/ [dostęp: 12.07.2024]; V.K. Velu, *Kali Linux*…, op. cit., s. 77–80.
[220] https://foca.softonic.pl/ [dostęp: 12.07.2024].
[221] https://www.spiderfoot.net/attack-surface-monitoring/ [dostęp: 12.07.2024].
[222] https://github.com/smicallef/spiderfoot [dostęp: 12.07.2024].

jawnoźródłowego optymalizuje proces ekstrakcji danych, zwiększając efektywność i precyzję działań.

Recon-ng[223] jest rozwiązaniem modułowym, które umożliwia dostęp do wielu różnych funkcji za pośrednictwem interfejsu wiersza poleceń. Moduły umożliwiają gromadzenie informacji z różnych źródeł, takich jak strony internetowe, bazy danych WHOIS, narzędzia DNS, media społecznościowe. Tworzenie „przestrzeni roboczych" (ang. *workspaces*) ułatwia segregowanie wyników pochodzących z poszczególnych modułów. Zebrane informacje zapisywane są w bazie danych SQLite, co zapewnia ich dostępność oraz możliwość ich eksportowania i wykorzystania w innych narzędziach[224]. Poprzez wykorzystanie modułów (z których każdy korzysta z innego źródła informacji), możliwe jest uzupełnianie pierwotnej bazy danych związanej z prowadzonym rozpoznaniem jawnoźródłowym. Moduły są sklasyfikowane według rodzaju danych wejściowych i wyjściowych, co ułatwia wybór odpowiedniego modułu do danego zadania. Zgromadzone informacje mogą być wykorzystane jako dane wejściowe dla kolejnych modułów, co stopniowo rozszerza zakres poszukiwań. Narzędzie pozwala również na generowanie raportów z przeprowadzonej eksploracji.

Zintegrowanie różnych narzędzi OSINT umożliwia ich synergiczne wykorzystanie w celu pozyskania większej liczby informacji niż w przypadku korzystania z pojedynczego narzędzia. Dane uzyskane za pomocą jednego narzędzia wzbogacają wyniki kolejnych, po czym następna porcja danych jest uzupełniana o nowe informacje. Ten iteracyjny proces może trwać, aż narzędzia OSINT pozyskają wszystkie dostępne informacje. Modułowa konstrukcja umożliwia dodawanie zasobów niezbędnych analitykowi, uwzględniając jego preferencje, doświadczenie, specyfikę organizacji oraz prowadzonego rozpoznania jawnoźródłowego.

Wyzwania wynikające z rosnącej ilości i zróżnicowania informacji jawnoźródłowych wymagają udoskonalenia procesów ich zbierania i analizy. Zaawansowane technologie, takie jak sztuczna inteligencja (ang. *artificial intelligence*, AI), uczenie maszynowe (ang. *machine learning*), Big Data, przetwarzanie języka naturalnego (ang. *natural language processing*, NLP) oraz eksploracja danych (ang. *data mining*), usprawniają narzędzia wykorzystywane w wywiadzie jawnoźródłowym. Coraz większe zastosowanie sztucznej inteligencji i uczenia

[223] https://github.com/lanmaster53/recon-ng [dostęp: 12.07.2024].
[224] M. Hickey, J. Arcuri, *Warsztat Hakera. Testy penetracyjne i inne techniki wykrywania podatności*, Helion, Gliwice 2022, s. 95.

maszynowego w automatyzacji procesów pozyskiwania i analizy informacji jawnoźródłowych pozwala na efektywniejsze wykrywanie wzorców i korelacji, które trudno zidentyfikować manualnie, a także umożliwia szybkie streszczanie ich obszernych zbiorów[225]. Eksploracja danych odgrywa istotną rolę w identyfikacji ukrytych zależności i nieoczywistych wzorców, które nie są możliwe do wykrycia za pomocą tradycyjnych metod analizy. Połączenie tych zaawansowanych technologii przyspiesza procesy decyzyjne w działaniach wywiadowczych.

Efektywność korzystania z automatycznych narzędzi do pozyskiwania i analizy informacji jawnoźródłowych jest uzależniona od poziomu wiedzy teoretycznej oraz praktycznych umiejętności w zakresie obsługi oprogramowania, zastosowania technik eksploracji danych i doboru odpowiedniej taktyki wyszukiwania.

Podsumowując ten fragment analizy, można dostrzec wyraźną tendencję do rozwoju i dywersyfikacji narzędzi OSINT. W prowadzeniu wywiadu jawnoźródłowego istotne znaczenie ma nie tylko znajomość dostępnych rozwiązań i ich funkcjonalności, ale przede wszystkim umiejętność ich adekwatnego wykorzystania w odniesieniu do określonego celu rozpoznania. Ważnym zagadnieniem pozostaje także kwestia integracji różnych narzędzi, w jakim stopniu przyczynia się ona do pogłębienia analizy, a na ile prowadzi do rozproszenia danych i konieczności ich wieloetapowej weryfikacji. W tym kontekście zasadne jest również pytanie o granice automatyzacji w procesie analitycznym – czy zastosowanie algorytmów rzeczywiście zwiększa precyzję oceny, czy też prowadzi do utraty najistotniejszych aspektów kontekstowych, wymagających interpretacji eksperckiej.

3.5. Podsumowanie

Analiza zaawansowanych metod i środków prowadzenia wywiadu jawnoźródłowego wykazała, że rozwój technologii znacząco wpłynął na efektywność oraz precyzję pozyskiwania i analizy informacji jawnoźródłowych. W szczególności nowoczesne narzędzia OSINT umożliwiają nie tylko gromadzenie ogromnych ilości danych, ale także ich automatyczną analizę, co skraca czas dostarczania produktów wywiadowczych i zwiększa ich dokładność. W odniesieniu do postawionego problemu badawczego można stwierdzić, że zastosowanie zaawansowanych metod wywiadu

[225] Zob. J. Pastor-Galindo, P. Nespoli, F. Gómez Mármol, G. Martínez Pérez, *The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends*, „IEEE Access" 2020, vol. 8, s. 10285.

jawnoźródłowego znacząco wpływa na zdolność państwa do identyfikacji zagrożeń oraz skutecznego reagowania na dynamiczne zmiany w środowisku bezpieczeństwa.

Przeprowadzone badania wykazały, że dynamiczny rozwój infrastruktury IT oraz regularne aktualizacje narzędzi i technologii wymuszają wdrażanie rozwiązań automatyzujących procesy pozyskiwania i analizy informacji jawnoźródłowych Coraz większą rolę odgrywają nowoczesne technologie, w tym sztuczna inteligencja, które przyczyniają się do zwiększenia efektywności działań na każdym etapie cyklu wywiadowczego. Wzrost znaczenia mediów społecznościowych sprawił, że ich analiza stała się nieodzownym elementem badań nastrojów społecznych, opinii publicznej oraz monitorowania działań przestępczych i ekstremistycznych grup. W rezultacie wzrosło znaczenie narzędzi sieciowych, językowych oraz tekstowych, w tym przetwarzania języka naturalnego, które pozwala na precyzyjną analizę treści pochodzących z tych źródeł oraz innych otwartych platform. Algorytmy NLP umożliwiają precyzyjne wydobywanie danych, takich jak imiona czy lokalizacje, co usprawnia proces analizy i pozwala na skuteczniejsze wykrywanie manipulacji informacyjnych.

W działaniach ofensywnych i defensywnych podejmowanych na rzecz bezpieczeństwa państwa coraz większe znaczenie zyskały narzędzia do analizy geolokalizacyjnej, które umożliwiają precyzyjne ustalanie lokalizacji osób i zdarzeń, często w czasie rzeczywistym. Ich wykorzystanie pozwala na precyzyjne mapowanie zachowań ludzkich, identyfikację zagrożeń oraz monitorowanie kryzysów i konfliktów. Dzięki zaawansowanym technologiom, takim jak GIS, GPS oraz dane satelitarne, narzędzia te dostarczają szczegółowych informacji, które wspierają procesy decyzyjne oraz pomagają w kształtowaniu polityki bezpieczeństwa państwa. Równocześnie rozwój narzędzi kryminalistyki wizualnej umożliwia skuteczniejszą weryfikację materiałów wizualnych w czasie rzeczywistym. Wykorzystanie technik takich jak fotogrametria, analiza artefaktów i metadanych pozwala na ocenę autentyczności treści, co zwiększa możliwości wykrywania manipulacji audiowizualnej.

Rekapitulując ustalenia badawcze w niniejszym rozdziale, można stwierdzić, że dostępne metody i środki prowadzenia wywiadu jawnoźródłowego znacząco przyczyniają się do zwiększenia skuteczności działań na rzecz bezpieczeństwa państwa. Automatyzacja procesów analitycznych, rozwój technologii opartych na sztucznej inteligencji oraz rosnące znaczenie analiz geolokalizacyjnych i kryminalistyki wizualnej pozwalają na skuteczniejsze rozpoznanie zagrożeń i wspieranie działań decyzyjnych.

Wnioski te stanowią podstawę do dalszych badań nad wykorzystaniem wywiadu jawnoźródłowego w bezpieczeństwie państwa.

4. PRAWNE I POZAPRAWNE ASPEKTY WYWIADU JAWNOŹRÓDŁOWEGO

Celem niniejszego rozdziału jest prezentacja wyników badań poświęconych rozwiązaniu problemu szczegółowego sprowadzającego się do odpowiedzi na pytanie: *Jakie prawne i pozaprawne aspekty wpływają na prowadzenie wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa?*

W niniejszym rozdziale omówione zostały prawne aspekty wywiadu jawnoźródłowego, określające jego wykorzystanie zarówno na poziomie krajowym, jak i międzynarodowym. Następnie przeanalizowano pozaprawne aspekty wywiadu jawnoźródłowego, w tym kwestie etyczne oraz metodologiczne, takie jak błędy poznawcze, błędy językowe, a także naruszenia cyklu wywiadowczego. W dalszej części rozdziału uwzględnione zostały również zagadnienia techniczne i informacyjne związane z pozyskiwaniem oraz analizą informacji z otwartych źródeł, które mają wpływ na wywiad jawnoźródłowy.

Analiza wyników pozwoliła na sformułowanie wniosków dotyczących aspektów prawnych i pozaprawnych, kształtujących wykorzystanie wywiadu jawnoźródłowego w sektorze bezpieczeństwie państwa.

4.1. Aspekty prawne

Zagadnienia prawne związane z wywiadem jawnoźródłowym pozostają niejasne w wielu obszarach. Przede wszystkim, zarówno w polskim, jak i międzynarodowym porządku prawnym, brak ujednoliconych regulacji dotyczących podstawowych pojęć związanych z OSINT, w tym zasad pozyskiwania i przetwarzania informacji jawnoźródłowych. Powoduje to znaczną niepewność prawną, która może ograniczać działania podmiotów publicznych. Dodatkowo, pozyskiwanie i analiza informacji jawnoźródłowych wiążą się z licznymi, złożonymi kwestiami prawnymi, które są uregulowane w różnych aktach prawnych. Wynikają one m.in. z ochrony podstawowych praw człowieka, takich jak prawo do prywatności, ochrona danych osobowych oraz własności intelektualnej. Regulacje te obejmują również międzynarodowe prawo humanitarne i prawa człowieka. Na te przepisy nakładają się regulacje prawa cyfrowego oraz rozwijające się normy dotyczące sztucznej inteligencji.

Istotnym zagadnieniem w kontekście wywiadu jawnoźródłowego wykorzystującego technologie informacyjne i komunikacyjne jest zgodność działań

z przepisami dotyczącymi ochrony prywatności i danych osobowych. Prywatność zapewnia możliwość swobodnego wyrażania tożsamości, chroni godność oraz wartości takie jak wolność zrzeszania się i wypowiedzi. W ujęciu normatywnym oznacza uprawnienie do kształtowania sfery życia prywatnego oraz podejmowania działań bez nadzoru i ingerencji zewnętrznej. Prawo do prywatności, uznane za jedno z fundamentalnych praw człowieka, odgrywa istotną rolę w ochronie autonomii oraz swobody działania w demokratycznym porządku prawnym[226].

Ochrona prywatności jest regulowana przez krajowe i międzynarodowe przepisy prawne, które różnią się zakresem oraz sposobem równoważenia celów bezpieczeństwa państwowego z prawami i wolnościami osobistymi[227]. Państwa przyjmują zróżnicowane podejścia do harmonizowania tych interesów, w zależności od tradycji prawnych i kontekstu kulturowego. Zgodnie z art. 69 ust. 7 Statutu Rzymskiego z 1998 roku[228], naruszenie prawa do prywatności stanowi jedną z nielicznych przesłanek, na podstawie których sędziowie mogą wykluczyć dowody przed Międzynarodowym Trybunałem Karnym. Może to również prowadzić do kwestionowania dowodów uzyskanych w ramach OSINT w postępowaniach karnych oraz skutkować powództwami cywilnymi.

Prawo do prywatności musi być przestrzegane zarówno podczas pozyskiwania i analizy informacji jawnoźródłowych, jak i na etapie projektowania narzędzi OSINT. Przykładem transparentnej realizacji tych zasad był projekt VIRTUOSO, którego celem było opracowanie platformy do zbierania, przetwarzania i analizy informacji jawnoźródłowych oraz dostarczenie narzędzi dla organów ścigania i agencji wywiadowczych, umożliwiających bardziej efektywne pozyskiwanie informacji z otwartych źródeł przy jednoczesnym zachowaniu standardów ochrony prywatności[229]. W ramach VIRTUOSO sformułowano zestaw pytań, mających na celu dostosowanie projektowanych narzędzi do wymogów prawa ochrony prywatności. W szczególności dokonano oceny czy dane narzędzie narusza prywatność obywateli, czy posiada

[226] Por. szerzej: A.F. Westin, *Privacy and Freedom*, „Washington and Lee Law Review" 1968, vol. 25, no. 1, s. 24–25 oraz M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni*, Wolters Kluwer, Warszawa 2019, s. 45–46.

[227] Zob. art. 47 Konstytucji RP, art. 12 Powszechnej Deklaracji Praw Człowieka, art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności, art. 7 Karty Praw Podstawowych Unii Europejskiej oraz art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych.

[228] Rzymski Statut Międzynarodowego Trybunału Karnego sporządzony w Rzymie dnia 17 lipca 1998 r. (Dz.U. z 2003 r. nr 78, poz. 708).

[229] Projekt VIRTUOSO (Versatile Information Toolkit for end-Users Oriented Open-Source Exploitation) był inicjatywą badawczą sponsorowaną przez Komisję Europejską w latach 2010–2013. Szerzej: C. Cuijpers, *Legal aspects of open source intelligence – Results of the VIRTUOSO project,* „Computer Law & Security Review" 2013, vol. 29, no. 6, https://doi.org/10.1016/j.clsr.2013.09.002 [dostęp: 20.11.2023].

odpowiednią podstawę prawną, czy jego stosowanie znajduje uzasadnienie w art. 8 Europejskiej Konwencji Praw Człowieka oraz czy jest ono niezbędne i proporcjonalne w demokratycznym społeczeństwie.

W zależności od lokalizacji otwartego źródła informacji mogą również występować ograniczenia wynikające z konieczności przestrzegania przepisów o ochronie danych osobowych. W Unii Europejskiej podstawowym aktem prawnym w tym obszarze jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)[230], które definiuje dane osobowe jako wszelkie informacje umożliwiające identyfikację osoby fizycznej. Przetwarzanie danych osobowych, nawet publicznie dostępnych, musi odbywać się zgodnie z zasadami RODO, które obejmują zgodność z prawem, rzetelność, ograniczenie celu, minimalizację danych, prawidłowość, ograniczenie przechowywania, integralność, poufność oraz rozliczalność administratora danych. Zgodność z prawem oznacza, że przetwarzanie danych musi opierać się na określonych przesłankach, takich jak uzyskanie zgody osoby, której dane dotyczą. Dla podmiotów pozyskujących informacje jawnoźródłowe może to być czynnik ograniczający. Rozporządzenie wymaga również przeprowadzenia oceny ryzyka oraz wdrożenia odpowiednich środków zabezpieczających. Osoba, której dane są przetwarzane, musi zostać poinformowana o przysługujących jej prawach. W przypadku naruszenia tych przepisów mogą zostać nałożone kary finansowe. Jedną z metod pozyskiwania informacji jawnoźródłowych jest systematyczne monitorowanie dużych części internetu, co zgodnie z art. 35 ust. 3 RODO wymaga oceny skutków dla ochrony danych, jeśli monitorowanie dotyczy publicznie dostępnych obszarów na dużą skalę.

Odpowiednikiem RODO w Wielkiej Brytanii jest Data Protection Act z 2018 roku[231], który reguluje ochronę danych osobowych w brytyjskiej jurysdykcji, wprowadzając modyfikacje dostosowane do kontekstu prawnego po Brexicie. W Stanach Zjednoczonych ochrona danych osobowych ma charakter fragmentaryczny, a regulacje są dostosowane do konkretnych sektorów, takich jak zdrowie (Health

[230] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE z 2016 r., L 119).

[231] *Data Protection Act 2018*, c. 12, Wielka Brytania, uchwalony 23 maja 2018 r., https://www.legislation.gov.uk/ukpga/2018/12/contents [dostęp: 5.12.2024].

Insurance Portability and Accountability Act, HIPAA z 1996 roku)[232] oraz finanse (Gramm-Leach-Bliley Act, GLBA z 1999 roku)[233], różniąc się jednocześnie w poszczególnych stanach.

Izrael dysponuje jednym z najbardziej zaawansowanych systemów ochrony danych osobowych poza Unią Europejską, co wynika zarówno z rozwoju sektora technologii informacyjnych jak i konieczności zapewnienia wysokiego poziomu bezpieczeństwa państwa. Podstawowym aktem prawnym w tym zakresie jest ustawa o ochronie prywatności z 1981[234] wielokrotnie nowelizowana w celu dostosowania do zmian technologicznych oraz międzynarodowych standardów. W 2011 roku Komisja Europejska uznała Izrael za państwo zapewniające odpowiedni poziom ochrony danych, co umożliwia transfer danych osobowych z Unii Europejskiej bez konieczności stosowania dodatkowych mechanizmów zabezpieczających, takich jak standardowe klauzule umowne[235]. Izraelski system ochrony danych w dużej mierze odpowiada wymogom RODO, jednak obejmuje istotne wyjątki motywowane względami bezpieczeństwa państwa. Na podstawie przywołanej ustawy o ochronie prywatności oraz przepisów szczególnych izraelskie służby wywiadowcze i organy ścigania dysponują rozszerzonymi uprawnieniami w zakresie przetwarzania danych osobowych, zwłaszcza w kontekście zagrożeń terrorystycznych i cyberbezpieczeństwa. W efekcie, mimo ogólnej zgodności z europejskimi standardami, zakres ingerencji państwa w prywatność jednostki w Izraelu jest szerszy niż w jurysdykcjach objętych regulacjami RODO.

Jedną z cech państw demokratycznych jest transparentność życia publicznego, której przejawem jest prawo dostępu do informacji publicznej. W Polsce prawo to zagwarantowane jest konstytucyjnie[236], a szczegółowe regulacje zawarte są w ustawie o dostępie do informacji publicznej z 2001 roku[237]. W Wielkiej Brytanii jego odpowiednikiem jest Freedom of Information Act z 2000, który umożliwia obywatelom

[232] *Health Insurance Portability and Accountability Act (HIPAA)*, Public Law 104-191, uchwalona przez Kongres Stanów Zjednoczonych, 21 sierpnia 1996 r.
[233] *Gramm-Leach-Bliley Act (GLBA)*, Public Law 106-102, uchwalona przez Kongres Stanów Zjednoczonych, 12 listopada 1999 r.
[234] Ustawa o ochronie prywatności z 1981 r., Protection of Privacy Law, 5741-1981, Official Gazette of Israel, No. 990, 23.12.1981.
[235] Decyzja Komisji Europejskiej z dnia 31 stycznia 2011 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniego poziomu ochrony danych osobowych w Państwie Izrael w odniesieniu do zautomatyzowanego przetwarzania danych osobowych, C(2011) 332 (Dz.Urz. UE L 27 z 1.2.2011, s. 39–42).
[236] Art. 61 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. nr 78, poz. 483 ze zm.).
[237] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2020 r. poz. 2176).

dostęp do informacji przechowywanych przez organy publiczne, natomiast w Stanach Zjednoczonych rolę tę pełni Freedom of Information Act z 1966 roku. Przepisy te tworzą ramy prawne, które w znaczący sposób ułatwiają działania wywiadu jawnoźródłowego. Dostęp do informacji publicznej może być ograniczony w sytuacjach, gdy jej ujawnienie mogłoby naruszać prywatność osób trzecich, bezpieczeństwo publiczne, tajemnicę przedsiębiorstwa lub interes państwa.

Istotą wywiadu jawnoźródłowego jest wykorzystywanie informacji z publicznie dostępnych źródeł jednak fakt ten nie eliminuje obaw związanych z ochroną prywatności i danymi osobowymi. Nowoczesne narzędzia OSINT agregują dane z różnych źródeł, co w efekcie może prowadzić do identyfikacji osoby fizycznej. Takie zestawienie danych określane jest w środowisku wywiadowczym jako „efekt mozaiki". Znajomość jedynie kilku punktów danych, takich jak data urodzenia, płeć i kod pocztowy, umożliwia ponowną identyfikację osób fizycznych z wysoką dokładnością (87%) w zbiorze danych pozbawionym elementów umożliwiających identyfikację[238]. Łączenie elementów ułatwia odkrywanie wzajemnych powiazań i generuje analityczne synergie, przez co mozaika informacji jest cenniejsza niż suma jej części[239]. Efekt mozaiki stwarza zagrożenie dla prywatności jednostki.

Oprócz ograniczeń związanych z ochroną prywatności i danych osobowych, informacje z otwartych źródeł mogą podlegać ochronie praw autorskich[240] oraz praw dotyczących baz danych. W przypadku treści chronionych, działania takie jak reprodukcja utworów lub ekstrakcja danych mogą być dozwolone wyłącznie za zgodą właściciela praw lub na podstawie wyjątków przewidzianych w obowiązujących przepisach. W kontekście inżynierii odwrotnej, która jest jedną z metod pozyskiwania informacji jawnoźródłowych, szczegółowa analiza oprogramowania lub technologii objętych ochroną patentową wymaga ścisłego przestrzegania regulacji dotyczących własności intelektualnej.

Wykorzystanie wywiadu jawnoźródłowego odgrywa coraz większą rolę w konfliktach zbrojnych XXI wieku. W konflikcie rosyjsko-ukraińskim, prywatne firmy satelitarne dostarczają ukraińskim siłom zbrojnym dane geoprzestrzenne[241],

[238] P. Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (August 13, 2009), „UCLA Law Review" 2010, vol. 57, s. 1705, https://ssrn.com/abstract=1450006 [dostęp: 20.08.2024].
[239] D.E. Pozen, *The Mosaic Theory*, *National Security, and the Freedom of Information Act*, „Yale Law Journal" 2005, vol. 115, s. 630.
[240] Por. szerzej: K. Chałubińska-Jentkiewicz, *Prawna ochrona*…, op. cit., s. 61 i nast.
[241] M. Cerre, D. Sagalyn, *Private companies track the war in Ukraine in real time,* PBS Newshour, 2022,

a organizacje społeczeństwa obywatelskiego wykorzystują geolokalizowane nagrania oraz posty w mediach społecznościowych do precyzyjnego mapowania incydentów związanych z działaniami wobec ludności cywilnej[242]. W konflikcie izraelsko-palestyńskim, narzędzia OSINT są wykorzystywane do analizy materiałów wizualnych i geolokalizacji w celu weryfikacji informacji o atakach i działaniach wojennych. Międzynarodowe organizacje oraz analitycy korzystają z danych satelitarnych i nagrań w mediach społecznościowych, aby potwierdzić doniesienia, takie jak eksplozje w szpitalu Al-Ahli w Gazie[243]. Pozyskiwanie i analiza informacji z otwartych źródeł muszą być zgodne zarówno z międzynarodowym prawem ochrony praw człowieka, jak i międzynarodowym prawem humanitarnym, w szczególności z zasadami dotyczącymi ochrony ludności cywilnej. Niewłaściwe stosowanie tych norm może prowadzić do poważnych konsekwencji, takich jak identyfikacja i skierowanie ataków na osoby cywilne[244]. Ponadto, strony konfliktu są zobowiązane do poszanowania i ochrony usług oraz infrastruktury medycznej, co obejmuje również ochronę poufności, integralności i dostępności danych dotyczących zdrowia. Te obowiązki muszą być odpowiednio uwzględniane w działaniach OSINT.

Wykorzystanie wywiadu jawnoźródłowego przez podmioty prywatne wprowadza istotną zmianę w dotychczasowym modelu, w którym państwa odgrywały rolę głównych arbitrów w zakresie publicznego dostępu do informacji wywiadowczych w czasie konfliktów zbrojnych[245]. Pozyskiwanie, analiza i rozpowszechnianie informacji jawnoźródłowych przez prywatne podmioty może jednak stanowić poważne zagrożenie zarówno dla prywatności jednostek, jak i dla bezpieczeństwa państwa. Jednym z takich zagrożeń jest zjawisko doxxingu, czyli gromadzenie i publikowania danych osobowych pozyskanych z otwartych źródeł w celu zastraszenia, nękania lub dyskredytowania określonych osób. Doxxing jest stosowany jako metoda walki informacyjnej, mająca na celu nie tylko represje wobec wskazanych jednostek, ale także

---

https://www.pbs.org/newshour/show/private-companies-track-the-war-in-ukraine-in-real-time [dostęp: 22.08.2024].

[242] Bellingcat Investigation Team, *Hospitals Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine*, 2022, https://www.bellingcat.com/news/2022/03/17/hospitals-bombed-and-apartments-destroyed-mapping-incidents-of-civilian-harm-in-ukraine/ [dostęp: 22.08.2024].

[243] K. Gretel, *The Israel-Hamas war highlights the power (and the limits) of open-source reporting*, 2023, https://reutersinstitute.politics.ox.ac.uk/news/israel-gaza-war-highlights-power-and-limits-open-source-reporting [dostęp: 22.08.2024].

[244] E. Millet, *Deploying OSINT in armed con ict settings: law, ethics, and the need for a new theory of harm*, 2023, https://blogs.icrc.org/law-and-policy/2023/12/05/deploying-osint-in-armed-conflict-settings-law-ethics-theory-of-harm/ [dostęp: 24.08.2024].

[245] A. Janjeva, A. Harris, J. Byrne, *The Future of Open-Source Intelligence for UK National Security*, Royal United Services Institute for Defence and Security Studies, 2022, s. 11.

osiągnięcie efektu psychologicznego – wywołania strachu, ograniczenia swobody działania oraz osłabienia morale przeciwnika. W konflikcie rosyjsko-ukraińskim doxxing stał się narzędziem wykorzystywanym przez obie strony w celu identyfikacji i ujawniania danych osób zaangażowanych w działania wojenne oraz operacje wywiadowcze[246]. Przykładem może być rosyjski Projekt Nemesis, który regularnie publikuje dane osobowe ukraińskich żołnierzy, funkcjonariuszy służb specjalnych oraz międzynarodowych instruktorów szkolących ukraińskie wojsko. Działania te prowadzą do narażenia tych osób i ich bliskich na różne formy przemocy, obniżając morale i stanowiąc zagrożenie dla bezpieczeństwa operacyjnego podczas trwającego konfliktu. Zjawisko doxxingu w kontekście wywiadu jawnoźródłowego ukazuje rozmycie granic między działalnością służb a aktywnością prywatnych podmiotów oraz użytkowników indywidualnych, którzy coraz częściej angażują się w zbieranie, analizowanie i rozpowszechnianie informacji istotnych dla konfliktu zbrojnego. Prowadzi to do fundamentalnych pytań o zakres dopuszczalności takich działań w świetle prawa międzynarodowego, ochrony prywatności oraz odpowiedzialności za skutki ujawniania danych osobowych w warunkach wojennych.

4.2. Aspekty etyczne

Na styku zagadnień prawnych pojawiają się kwestie etyczne, które akcentują konieczność postępowania zgodnego z zasadą nieszkodzenia innym[247]. Etyka posługuje się różnego rodzaju normami, zwyczajami, poglądami ugruntowanymi kulturowo, co czyni ją zdolną do rozwiązywania problemów zarówno społecznych jak i indywidualnych. We współczesnym społeczeństwie pojawia się dylemat dotyczący równowagi między zakresem prowadzonego rozpoznania jawnoźródłowego w działaniach podejmowanych na rzecz bezpieczeństwa państwa a obawami przed nadmierną inwigilacją obywateli oraz ochroną ich prywatności. Działalność wywiadowcza, w tym OSINT, często jest kojarzona z manipulacją, dezinformacją oraz nielegalnym pozyskiwaniem danych.[248]. Zagadnienia etyczne nabierają szczególnego znaczenia w kontekście automatyzacji procesów gromadzenia i analizy dużych zbiorów

[246] E. Thomas, *Project Nemesis, Doxxing and the New Frontier of Informational Warfare,* 2022, https://www.isdglobal.org/digital_dispatches/project-nemesis-and-the-new-frontiers-of-informational-warfare/ [dostęp: 25.08.2024].
[247] Zob. szerzej: Arystoteles, *Etyka nikomachejska,* Wydawnictwo Naukowe PWN, 2023.
[248] M. Herman*, Ethics in Intelligence after September 2001*, „Intelligence and National Security" 2004, vol. 19, no. 2, s. 342.

danych (Big Data), gdzie wyzwaniem jest zachowanie kompromisu między ochroną prywatności, wolnością jednostki oraz prawami człowieka a koniecznością zapewnienia bezpieczeństwa państwa. W związku z tym zarówno w praktyce jak i dostępnej literaturze przedmiotu dostrzeżona została pilna potrzeba wytyczenia ram etycznych dla prowadzonych wywiadu jawnoźródłowego, zarówno przez podmioty państwowe jak i prywatne[249].

Teoretyczne uzasadnienie bezpieczeństwa państwa niejednokrotnie usprawiedliwia użycie inwazyjnych metod zbierania informacji przez podmioty państwowe. Powstaje jednak pułapka, polegająca na tym, że oficerowie służb specjalnych pod legendą działań propaństwowych będą wykorzystywali pozyskane informacje do działań partykularnych, antydemokratycznych i politycznych. W społeczeństwie demokratycznym istnieje dychotomia między potrzebą prywatności a koniecznością ochrony przed anonimowością innych osób i zapewnieniem bezpieczeństwa państwa. Dotychczasowe modele etycznej pracy wywiadowczej określające stopień potencjalnej ingerencji w prywatność oraz akceptowalny zakres pozyskiwanych danych przedstawione są w tabeli 4.1.

Kolejnym obszarem problemowym jest pozyskiwanie informacji jawnoźródłowych, poza zakresem postawionego zapytania. Takie działanie może nie tylko naruszać przepisy prawa, ale również implikować wątpliwości natury etycznej w zakresie prywatności i godności jednostki. W przypadku służb specjalnych pozyskanie nadmiarowych informacji jawnoźródłowych, a następnie ich wykorzystanie do dalszych działaniach operacyjnych, jest ewidentnym naruszeniem demokratycznych zasad postępowania oraz instrukcji o pracy operacyjnej. Sprzeczne z demokratycznymi zasadami i społecznymi normami jest również typowanie na podstawie nadmiarowo pozyskanych danych osobowych źródeł informacji (werbunek). Ujawnienie informacji dotyczących poglądów politycznych, orientacji seksualnej, przekonań religijnych w środowisku, dla których informacje te nie były dedykowane (informacje nieprzynależne), może prowadzić nie tylko do naruszenia prywatności jednostki, ale również zagrażać jej bezpieczeństwu.

[249] Projekty na temat etycznych aspektów wywiadu jawnoźródłowego: „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).

Tabela 4.1. Modele etyczne w działalności wywiadowczej

Model etyczny	**Charakterystyka**	**Konsekwencje**
Realistyczny	Działanie w interesie narodowym jest najważniejsze; zlekceważenie tego obowiązku narażałoby obywateli na niepożądane zagrożenia zewnętrzne.	Zbieranie informacji wywiadowczych jest podstawowym obowiązkiem państwa i nie powinno być uważane za nieetyczne. W rzeczywistości zaniechanie takich działań mogłoby być postrzegane jako niemoralne, narażając obywateli na potencjalne zagrożenia i niekorzystne wpływy.
Konsekwencjonalistyczny	Etyka działalności wywiadowczej polega na zachowaniu równowagi, która jest determinowana przez konsekwencje podejmowanych działań; rozważenie "etycznego bilansu" jest wynikiem tej aktywności.	Działalność wywiadowcza jest dopuszczalna, gdy służy wyraźnie dobru publicznemu lub ochronie, ale zawsze należy oceniać jej skutki. W pewnych sytuacjach działania te mogą być uznane za nieodpowiednie/niewłaściwe lub niezgodne z etyką.
Deontologiczny	Odrzuca konieczność wszelkich form gromadzenia danych wywiadowczych, uznając je z natury za głęboko nieetyczne.	Dopuszcza pewne działania związane z gromadzeniem informacji wywiadowczych, o ile nie są one szkodliwe, takie jak pasywne monitorowanie komunikacji w obronie państwa, ale odrzuca wszelkie niewłaściwe moralnie działania, takie jak wprowadzanie w błąd.

Źródło: J. Richards, *The Art and Science of Intelligence Analysis*, Oxford University Press, 2010, s. 88.

Innym zagadnieniem jest wykorzystywanie informacji pochodzących z działań przestępczych lub naruszeń cyberbezpieczeństwa, które zostały upublicznione np. przez aktywistów w celu udowodnienia przeprowadzonego ataku. Rodzi to uzasadnione wątpliwości etyczne oraz obawy o generowanie przestępczych działań.

Korzystanie z narzędzi OSINT przez podmioty prywatne może prowadzić do nieetycznych zachowań, np. poprzez udostępnianie w Internecie niepotwierdzonych prywatnych informacji lub błędną identyfikację osób zaangażowanych w nielegalną działalność. Takie praktyki mogą mieć poważne konsekwencje dla bezpieczeństwa osób, których dane osobowe zostały upublicznione.

Kolejnym zagadnieniem, które stanowi zarówno wyzwanie dla bezpieczeństwa państwa, jak i rodzi dylematy etyczne, jest zjawisko raportowania obywatelskiego,

znane również jako internetowy crowdsourcing. Są to dochodzenia przeprowadzane przez grupy użytkowników w sieci, które odpowiadają na rosnące zapotrzebowanie na szybką i wszechstronną analizę publicznie dostępnych danych, takich jak treści zamieszczane w mediach społecznościowych. Ich celem jest rozwiązanie złożonych przestępstw oraz spraw ważnych dla społeczeństwa[250]. Dochodzenia te są realizowane w czasie rzeczywistym przy użyciu platform do współpracy zespołowej oraz forów internetowych, takich jak Discord, Twitter, Slack czy Reddit.

Amerykańska agencja rządowa DARPA (*Defense Advanced Research Projects Agency*) jako pierwsza zastosowała crowdsourcing do analizy danych wywiadowczych w 2009 roku podczas cyfrowych ćwiczeń pod kryptonimem "Network Challenge "[251]. Eksperyment ten miał na celu zbadanie czy sieć użytkowników współpracujących za pośrednictwem narzędzi społecznościowych mogłaby lepiej zarządzać wyzwaniami przed którymi stoją służby specjalne. Z przeprowadzonych badań wynikało, że czas prowadzenia wywiadu jawnoźródłowego opartego na crowdsourcingu był krótszy oraz nie podlegał ograniczeniom administracyjnym ani wpływom politycznym. W każdym z trzech typów dochodzeń crowdsourcingowych wyróżnionych w literaturze przedmiotu: oddolnych, odgórnych oraz hybrydowych[252], pojawiają się dylematy etyczne oraz wyzwania organizacyjne i informacyjne. Przykładowo, w dochodzeniach oddolnych angażujących amatorów mogą pojawić się wyzwania związane z ochroną prywatności i danych osobowych oraz z wiarygodnością zgromadzonych informacji. Z kolei w dochodzeniach odgórnych i hybrydowych mogą wystąpić dodatkowe zagadnienia, takie jak zarządzanie dużymi zespołami oraz zapewnienie spójności metodologicznej.

Zakres, przejrzystość oraz sposób definiowania norm etycznych zależą od podmiotu prowadzącego rozpoznanie jawnoźródłowe. Pozyskiwanie informacji jawnoźródłowych przez podmioty publiczne oraz służby państwowe ma na celu prowadzenie działań zgodnych z interesami państwa. Normy etyki zawodowej tych podmiotów wywodzą się z przepisów prawnych regulujących strukturę organizacyjną oraz metody ich działania. W przypadku wywiadu jawnoźródłowego prowadzonego przez podmioty prywatne cele i zadania wyznaczane są indywidualnie. Różnorodne

[250] A. Mukhopadhyay, S. Venkatagiri, K. Luther, *OSINT Research Studios: A Flexible Crowdsourcing Framework to Scale Up Open Source Intelligence Investigations*, „Proc. ACM Hum.-Comput. Interact." 2024, vol. 8, issue CSCW1, art. 105, https://doi.org/10.1145/3637382 [dostęp: 5.07.2024].
[251] Defense Advanced Research Projects Agency, *Darpa Network Challenge Project Report*, 2010, https://www.eecs.harvard.edu/cs286r/courses/fall10/papers/ProjectReport.pdf [dostęp: 3.07.2024].
[252] A. Mukhopadhyay, S. Venkatagiri, K. Luther, *OSINT Research Studios*…, op. cit.

motywacje decydują o wyborze tematu analizy, obejmują one osobiste zainteresowanie zagadnieniem, dążenie do promowania politycznych lub ideologicznych celów, a także osiągnięcie korzyści finansowych. Brak przeszkolenia oraz zobowiązań do przestrzegania wewnętrznych kodeksów organizacji opartych na przepisach prawa powodują, że podmioty prywatne prowadzące wywiad jawnoźródłowy są często nieświadome konsekwencji prowadzonych działań dla bezpieczeństwa państwa.

Dla organizacji zawodowych o charakterze profesjonalnym prowadzących wywiad jawnoźródłowy tworzone są dedykowane kodeksy etyczne formalizujące pożądane standardy postępowania. Dokumenty te są zorientowane na zapobieganie wystąpieniu możliwych nieprawidłowości i ich minimalizowanie, budowanie świadomości odpowiedzialnej pracy wywiadowczej, a także na określenie norm i wartości, które mają być przestrzegane przez wszystkie osoby zaangażowane w prowadzoną działalność. Wytyczne i zasady zawarte w kodeksach mają na celu kształtowanie postaw umożliwiających podejmowanie etycznie uzasadnionych decyzji, a także budowanie zaufania i akceptacji społecznej dla działań wywiadu jawnoźródłowego. Etyka zawodowa systematyzuje i wdraża oceny i normy moralne w praktyce zawodowej, a także formułuje postulowane normy moralne, które powinny być przyjęte przez przedstawicieli danego zawodu[253]. Kodeksy etyki zawodowej przyjmują m.in. regułę imperatywu kategorycznego Immanuela Kanta: „*postępuj wedle takiej tylko zasady, co do której mógłbyś jednocześnie chcieć, aby stała się prawem powszechnym*”[254].

Funkcją etyki zawodowej jest implementacja ogólnych norm moralnych występujących w danym społeczeństwie do konkretnych sytuacji zawodowych[255]. Zasady moralne mogą jednak różnić się w zależności od czasu, obszaru geograficznego i kontekstu, co wymaga dostosowania kodeksów etycznych do specyfiki zawodu. W tym kontekście Kodeks Etyki Strategicznego Konsorcjum Specjalistów Wywiadu (ang. *Strategic Consortium of Intelligence Professionals*, SCIP) stanowi jeden z najbardziej rozpowszechnionych wzorców[256]. SCIP jako globalna organizacja non-profit, zrzesza ekspertów biznesu, przedstawicieli środowisk akademickich

[253] Z. Ziembiński, *Podstawy nauki o moralności*, Uniwersytet im. Adama Mickiewicza, Poznań 1981, s. 106.
[254] W. Tatarkiewicz, *Historia filozofii*, t. 2, Wydawnictwo Naukowe PWN, Warszawa 1993, s. 178.
[255] Por. M. Michalik, *Społeczne przesłanki, swoistość i funkcje etyki zawodowej*, [w:] A. Sarapata, *Etyka zawodowa*, Warszawa 1971, s. 17.
[256] Kodeks etyczny organizacji „Strategic and Competitive Intelligence Professionals”, https://www.scip.org/page/Ethical-Intelligence [dostęp: 20.07.2023].

i funkcjonariuszy służby publicznej, którzy wspólnie gromadzą i dzielą się doświadczeniami, wiedzą oraz narzędziami na temat procesów i możliwości analitycznych. Podobnie, Kodeks Etyki Infobrokerów Stowarzyszenia Niezależnych Profesjonalistów Informacji (ang The Association of Independent Information Professionals, AIIP), zawiera zbiór norm i wytycznych mających na celu zapewnienie najwyższego poziomu profesjonalizmu w działalności wywiadu jawnoźródłowego[257]. Stosowanie się do jego zasad umożliwia członkom stowarzyszenia dążenie do osiągnięcia standardów doskonałości w swojej pracy, co przekłada się na budowanie zaufania wśród odbiorców usług i współpracujących instytucji. Kodeks AIIP służy również jako model referencyjny dla innych organizacji specjalizujących się w analizie jawnoźródłowej. Branżowe kodeksy etyczne, tworzone przez organizacje zajmujące się wywiadem jawnoźródłowym, często zawierają zbieżne elementy, takie jak uczciwość, rzetelność, przestrzeganie przepisów prawa, poszanowanie poufności, promowanie profesjonalizmu oraz odpowiedzialność za stosowanie się do kodeksu etycznego.

Zagadnienia etyczne związane z analizą z otwartych źródeł są obecnie przedmiotem badań naukowych[258]. Ich celem jest przygotowanie rekomendacji podnoszących poziom bezpieczeństwa prowadzonego rozpoznania jawnoźródłowego oraz ograniczenie decyzji mogących generować potencjalne zagrożenia. Przy współpracy Centrum Praw Człowieka na Uniwersytecie Kalifornijskim w Berkeley oraz Biura Prawa Człowieka ONZ zainicjowany został projekt badawczy dotyczący dochodzeń jawnoźródłowych. W efekcie powstał *„Berkeley protocol on Digital Open Source Investigations*", który określa ramy etyczne oraz proceduralne dla prowadzenia wywiadu jawnoźródłowego.

Zgodnie z treścią tego dokumentu, podmioty prowadzące działania rozpoznawcze powinny kierować się normami etycznymi, począwszy od ochrony godności wszystkich osób zaangażowanych w analizę lub objętych jej zakresem, aż po

[257] Kodeks etyczny Infobrokerów stworzony przez The Association of Independent Information Professionals, https://aiip.org/About/Professional-Standards [dostęp: 20.07.2023].

[258] *Berkeley Protocol on Digital Open Source Investigations*, wydany przez Uniwersytet Kalifornijski w Berkeley we współpracy z Biurem Praw Człowieka ONZ, jest międzynarodowym protokołem określającym standardy i wytyczne dla profesjonalistów w zakresie identyfikacji, gromadzenia, przechowywania, weryfikacji i analizy cyfrowych informacji jawnoźródłowych w celu poprawy ich skutecznego wykorzystania w międzynarodowych dochodzeniach karnych i dochodzeniach dotyczących praw człowieka. Jest podsumowaniem trzyletniego projektu badawczego prowadzonego z udziałem ponad 150 ekspertów z całego świata. Protokół wyznacza wspólne światowe standardy prawne, metodologiczne i etyczne korzystania z publicznych informacji cyfrowych. Szerzej: *Berkeley Protocol*…, op. cit.

promowanie zasad pokory, inkluzywności, niezależności oraz przejrzystości działań[259]. Poszanowanie godności w prowadzonym dochodzeniu jawnoźródłowym wiąże się ze świadomością ochrony podstawowych kwestii związanych z godnością jednostki, zwłaszcza tych interesów, które są chronione przez międzynarodowe normy oraz prawa człowieka. W protokole podkreślono znaczenie przestrzegania zasad niedyskryminacji, które mogą wpływać na przedmiot oraz sposób prowadzonego rozpoznania. Zaakcentowano również konieczność zapewnienia bezpieczeństwa zarówno zgromadzonych materiałów, jak i fizycznego oraz psychicznego bezpieczeństwa osób zaangażowanych biernie i czynnie w analizę jawnoźródłową. Inkluzja oznacza, że przy pozyskiwaniu i wartościowaniu informacji jawnoźródłowych należy uwzględniać różnorodne perspektywy i doświadczenia. Czynniki, które mogą wpływać na inkluzję w trakcie prowadzonych działań rozpoznawczych, obejmują zakres geograficzny, analizę działań grup zajmujących się międzynarodową przestępczością, oraz świadomość zróżnicowanego charakteru informacji jawnoźródłowych pod względem jakości, dostępności, rzetelności, lub zakresu w odniesieniu do różnych grup społecznych. Pokora podmiotów prowadzących działania rozpoznawcze powinna przejawiać się w uznaniu własnych ograniczeń, świadomości braków wiedzy oraz przyjęciu odpowiedzialności za popełnione błędy. Oznacza to również raportowanie błędów, aby zminimalizować potencjalne szkody i usprawnić przyszłe analizy jawnoźródłowe.

W raporcie za istotny aspekt etyczny rozpoznania jawnoźródłowego uznano zapewnienie niezależności analityków, w tym identyfikowanie oraz unikanie wszelkich rzeczywistych lub potencjalnych konfliktów interesów. Realizacja tej zasady powinna być osiągana poprzez transparentność w stosowanych metodach oraz źródłach finansowania. Z niezależnością wiąże się zasada przejrzystości, która w wywiadzie jawnoźródłowymi może być rozpatrywana w dwóch wymiarach: odpowiedzialności analityka za jawność zastosowanych metod i publikowanych wyników oraz etycznego zachowania analityków w działaniach w Internecie i w relacjach z otoczeniem.

W celu realizacji tej zasady istotne jest unikanie dezinformacji oraz uwzględnienie negatywnych konsekwencji wprowadzania w błąd, takich jak utrata reputacji i osłabienie wiarygodności zarówno prowadzonych działań, jak i samych analityków. Celowe wprowadzanie w błąd w procesie pozyskiwania informacji

[259] *Berkeley Protocol*…, op. cit., s. 14–15.

jawnoźródłowych jest nie tylko sprzeczne z zasadami etycznymi, ale również może naruszać prawo do prywatności i zniekształcać wyniki analizy.

4.3. Aspekty metodologiczne

4.3.1. Naruszenia cyklu wywiadowczego

Przedstawiony w rozdziale II cykl wywiadowczy jest konstruktem, który w znacznej mierze systematyzuje prowadzenie wywiadu jawnoźródłowego. Jednocześnie na każdym jego etapie mogą występować zakłócenia, skutkujące błędami w ostatecznym opracowaniu analitycznym. W ujęciu systemowym można wyróżnić cztery podstawowe kategorie zmiennych wpływających na cykl wywiadowczy: ogólne, metodologiczne, specyficzne, komunikacyjne[260] (tabela 4.2).

Tabela 4.2. Taksonomia zmiennych w analizie wywiadowczej według R. Johnstona

Ogólne	Metodologiczne	Specyficzne	Komunikacyjne
• Organizacja • Otoczenie • Polityka	• Zapotrzebowanie odbiorców • Operacje zdobywania informacji • Zasoby informacyjne • Metodologia analityczna • Forma dystrybucji	• Światopogląd • Afiliacje • Psychologia • Wykształcenie • Szkolenia • Gotowość	• Formalne • Nieformalne • Technologie komunikacyjne

Źródło: Opracowanie na podstawie: R. Johnston, *Analytic Culture in the U.S. Intelligence Community. An Ethnographic Study*, DC, Washington 2005, s. 32.

Zmienne ogólne dotyczą organizacji, w ramach której powstaje analiza oraz środowiska analitycznego. Zmienne organizacyjne obejmują strukturę organizacji wywiadowczej: kierownictwo, zarządzanie i praktyki zarządcze, historię i tradycje; kulturę pracy, praktyki społeczne w organizacji i tabu w miejscu pracy, grupy robocze a także zasoby materialne i ludzkie. Na tę grupę zmiennych składają się również:

[260] R. Johnston, *Analytic Culture*…, op. cit., s. 32.

polityka wewnętrzna organizacji, polityka krajową i międzynarodowa a także potrzeby odbiorców oraz struktura, hierarchia i organizacja odbiorcy.

Zmienne metodologiczne wpływają bezpośrednio na proces powstawania analizy. Do zmiennych tych można zaklasyfikować: wymagania decydenta, sposób pozyskania informacji, ich jakość, sposób przechowywania, zastosowane metody analizy i konkretne strategie podejmowania decyzji na temat informacji, dedykowane strategie decyzyjne w odniesieniu do pozyskanych danych, jak również procedury prezentacji wyników analiz odbiorcom. Możliwości generowania informacji w każdym systemie społeczno-gospodarczym podlegają ograniczeniom obiektywnym, niezależnym od dysponenta procesu informacyjnego, oraz subiektywnym, zależnym od jego decyzji[261].

Zmienne specyficzne związane są bezpośrednio z osobami wykonującymi analizę. Zaliczane są do nich afiliacje: rodzinne, kulturowe, etniczne, religijne, językowe i politycznej. Obejmują także czynniki psychologiczne takie jak: uprzedzenia, profile osobowości, procesy poznawcze, obciążenie poznawcze, podejście do rozwiązywania problemów, styl podejmowania decyzji i reakcje na stres. Wyróżnić można również zmienne specyficzne dla danej dziedziny, takie jak poziom wykształcenia, doświadczenie szkoleniowe oraz zdolność do praktycznego zastosowania posiadanej wiedzy, umiejętności i zdolności w kontekście wykonywanego zadania.

Zmienne komunikacyjne wpływają na interakcje zachodzące wewnątrz grup, jak i pomiędzy grupami. Zmienne komunikacyjne zawierają różne formy interakcji, zarówno formalne jak i nieformalne, wewnątrz danej organizacji, między różnymi organizacjami, a także między poszczególnymi jednostkami i stworzonymi przez nie sieciami społecznymi.

W praktyce występuje zazwyczaj kilka błędów równocześnie, co w kontekście procesów analitycznych i decyzyjnych może prowadzić do nieprecyzyjnych lub nieadekwatnych wyników analizy. Zarówno zmienne ogólne, metodologiczne, specyficzne jak i komunikacyjne, mogą wpływać na skomplikowane interakcje, które skutkują błędami na różnych poziomach działania. Błędy te, szczególnie gdy występują jednocześnie, mogą mieć negatywny wpływ na funkcjonowanie organizacji

[261] J. Oleński, *Ekonomika informacji. Metody*, op. cit., s. 56 i nast.

wywiadowczej, zmniejszając jej efektywność oraz obniżając jakość i wiarygodność dostarczanych informacji.

Możliwość pojawienia się błędów występuje zarówno po stronie analityków jak i decydentów[262]. Decydent w pierwszej fazie cyklu wywiadowczego może sformułować zapytanie w sposób niejasny lub z innych powodów niewłaściwy. W fazie gromadzenia informacji może nie rozumieć dostępnych środków i metod pozyskiwania i wartościowania informacji jawnoźródłowych. Taki brak wiedzy może prowadzić do wyników o niskiej wartości, a w konsekwencji błędnych decyzji. Analityk na etapie gromadzenia informacji może nie mieć możliwości zebrania adekwatnych do postawionych zadań informacji. Dodatkowo może sięgnąć do niewłaściwych źródeł, z uwagi na niedostatecznie jasno określone zapytanie i przekazane wstępne informacje przez decydenta. Na etapie analizy i wartościowania informacji jawnoźródłowych błędy, które mogą się pojawić wynikają z niskiego poziomu czynności wiedzotwórczych, ulegania uprzedzeniom, mniejszej sprawności poznawczej czy braku kompetencji profesjonalnych. W praktyce, dla uniknięcia tego typu błędów przy pozyskiwaniu i wartościowaniu informacji jawnoźródłowych, pomocne jest zastosowanie listy kontrolnej zawierającej następujące zagadnienia:

1) Czy przedstawione zapytanie jest faktycznie skierowane na rozwiązanie problemu? Jaka jest logika wiedzy wywiadowczej, która generuje konieczność przedstawienia zapytania? Czy zapytanie dotyczy faktycznie konkretnej informacji, a nie danych wywiadowczych? Jaki jest poziom pewności odbiorcy odnośnie do potrzeby pozyskania żądanej wiedzy?
2) Czy wykorzystywane są najlepsze i właściwe źródła informacji? Czy wraz z postępem prac można uzyskać dostęp do innych źródeł informacji? Czy inne podmioty partnerskie dysponują informacjami na dany temat i mogą się nimi podzielić?
3) Czy sformułowano i przetestowano założenia hipotezy i założenia analityczne? Czy istnieją alternatywne interpretacje informacji, które mogą być równie ważne? Czy proces formułowania wniosków nie został zakłócony przez istniejące uprzedzenia lub selektywną interpretację problemu? Czy wszystkie dostępne informacje zostały dokładnie sprawdzone pod kątem wiarygodności? Czy w analizie została uwzględniona niepewność? [263]

[262] J. Richards, *The Art and Science of Intelligence Analysis*, Oxford University Press 2019, s. 33–34.
[263] Ibidem, s. 39.

W pracy analityka istotne są również czynniki psychologiczne. Wykonywanie czynności pod presją czasu, w warunkach niepewności i przewagi kierownictwa, może prowadzić do tworzenia materiałów zgodnych z ich oczekiwaniami. Każda analiza tworzona jest w ramach jakiegoś paradygmatu, przy czym w danej dziedzinie może istnieć wiele konkurujących ze sobą paradygmatów[264]. Przy pozyskiwaniu informacji jawnoźródłowych przez służby i podmioty państwowe, profesjonalista przechodzi szkolenie i zapoznaje się z paradygmatem swej dyscypliny. Występujące zagrożenie z tym związane określane jest „efektem kaczki", oznacza ono preferowaniu pierwotnie nabytych metod i przyswojonych sposobów działania i niechęć a nawet odrzucenia nowych paradygmatów.

4.3.2. Błędy poznawcze

Analiza wywiadowcza stanowi połączenie sztuki, rzemiosła i nauki. Pomimo zastosowania specjalistycznych narzędzi i technik, które wspomagają prowadzenie wywiadu jawnoźródłowego, ostateczne decyzje są zależne od osądu człowieka, opartego na jego doświadczeniu i wiedzy eksperckiej. Ograniczenia w analizie informacji wynikają zatem z ograniczeń ludzkiego poznania, a te z kolei są uwarunkowane przez złożoność procesów kognitywnych, które obejmują percepcję, pamięć, myślenie i rozumowanie. Najistotniejsze ograniczenia analizy informacji wywiadowczej wynikają z następujących okoliczności:

1) Okazjonalne występowanie sytuacji nieprzewidzianych jest nieuniknione. Decydenci powinni zaakceptować ten fakt i dostosować do tego swoje oczekiwania;
2) Ograniczenia percepcji u osób uczestniczących w procesach informacyjnych, które są równie istotne jak niekompetencja czy błąd myślenia grupowego przy formułowaniu błędnych ocen;
3) Trudności analityków w spojrzeniu na badaną informację z różnych perspektyw;
4) Utrwalone wzorce myślenia, które mogą negatywnie wpływać na przeprowadzane analityczne rozumowania;
5) Problemy analityków z komunikowaniem niepewności własnych sądów;
6) Uprzedzenia analityków wpływające na ich pracę[265].

W analizie wywiadowczej decyzje są podejmowane w warunkach niepewności i niekompletności danych. Dlatego kognitywne techniki krytycznego rozumowania są

[264] J. Konieczny, *Analiza informacji w dziedzinie bezpieczeństwa państwa*, ABW, Warszawa 2014, s. 245.
[265] R.J. Heuer Jr., *Limits of Intelligence Analysis*, „Orbis" 2005, vol. 49, no. 1, s. 76.

niezbędne dla efektywnego procesu zdobywania i interpretacji informacji przez analityka. Analiza wywiadowcza nie jest procesem liniowym[266], stawia przed analitykami specyficzne wyzwania, które różnią się od standardowych problemów rozumowania w innych dziedzinach Można wyróżnić cztery główne problemy związane z rozumowaniem w tym obszarze:

1) Niewystarczalność (ang. *insufficiency*): problem ten wynika z relacji między zebranymi danymi a wiedzą wykorzystywaną w prowadzonej analizie wywiadowczej. Dwa główne aspekty tej niewystarczalności to ograniczony zakres pozyskanych danych oraz ich wiarygodność. Analiza wywiadowcza jest prowadzona na podstawie danych, które są niekompletne i często niedokładne. Mimo tych ograniczeń, dąży się do formułowania jak najbardziej uzasadnionych i prawdziwych wniosków na podstawie dostępnych danych.
2) Brak relewancji (ang. *irrelevancy*): problem ten dotyczy braku związku pozyskanych danych z konkretnym zagadnieniem analizy, co utrudnia proces wnioskowania. Poziom relewancji różni się w zależności od podmiotu przeprowadzającego analizę. Kluczowe jest każdorazowe odróżnienie informacji istotnych od tych, które są nierelewantne.
3) Nieokreśloność (ang. *indeterminacy*): problem ten wynika z relacji między wiedzą a całą siecią analizy oraz otoczeniem. Zdarzenia, które analitycy starają się zrozumieć, zwłaszcza te, które próbują przewidzieć, są jedynie hipotezą. Nawet posiadając pełną wiedzę na temat konkretnego zagrożenia, nie można z pewnością przewidzieć jego wystąpienia. Decyzje i działania ludzi, a także zachodzące procesy naturalne są indeterministyczne. Analitycy muszą uwzględniać wiele potencjalnych, rozbieżnych scenariuszy przyszłości i przewidywać konsekwencje każdego z nich.
4) Instrumentalność (ang. *instrumentality*): problem ten wynika z relacji pomiędzy zrozumieniem a wiedzą. Analitycy zdobywają wiedzę nie tylko dla niej samej, ale aby sprostać wyzwaniom stawianym przez decydentów. To narzuca dodatkowe ograniczenia w zdobywaniu wiedzy, szczególnie w pętli sprzężenia zwrotnego od

[266] W analizie wywiadowczej analitycy stoją przed wyzwaniami poznawczymi związanymi z formułowaniem dobrze uzasadnionych i prawdziwych wniosków. Proces ten polega na przemieszczaniu się w różnych kierunkach w „strukturze analizy", która skupia się wokół czterech kluczowych elementów: danych, informacji, wiedzy i zrozumienia. Szerzej: N. Hendrickson, *Critical Thinking in Intelligence Analysis*, „International Journal of Intelligence and Counterintelligence" 2010, vol. 21, no. 4, s. 681.

zrozumienia do wiedzy. Analitycy nie mają nieograniczonego czasu na analizę i muszą uwzględniać konkretne cele oraz potrzeby decyzyjne odbiorców[267].

Błędy poznawcze to błędy umysłowe spowodowane uproszczonymi strategiami przetwarzania informacji. Nie wynikają z intelektualnych predyspozycji do określonego osądu, ale z podświadomych mechanizmów umysłowych. Te nieświadome wzorce myślowe mogą prowadzić do nieprawidłowych ocen w analizie wywiadowczej na każdym jej etapie poprzez brak obiektywizmu podczas przetwarzania danych. Najczęściej pojawiające się błędy w analizie jawnoźródłowej zostały scharakteryzowane poniżej.

Błąd lustrzanego odbicia (ang. *mirror-imaging effect*) polega na projekcji odczuć, przekonań i aksjologii analityka na przewidywane działania lub motywacje zachowań innych osób. Jest to jeden z najczęściej popełnianych błędów analitycznych, który może prowadzić do znaczących pomyłek w interpretacji, poprzez założenie, że inni działają i myślą w sposób analogiczny do analityka. Efekt dostosowania i zakotwiczenia (ang. *adjustment and anchoring effect*) jest błędem poznawczym, który wynika z przyjęcia jakiejś informacji jako decydującej o dalszym przebiegu rozumowania, używanej jako punkt odniesienia (zakotwiczenie), a następnie dokonywania dostosowań w oparciu o to zakotwiczenie[268]. Błąd potwierdzenia (ang. *confirmation bias*) to tendencja do wyszukiwania informacji wspierających wcześniej przyjęte stanowisko, przy jednoczesnym ignorowaniu lub minimalizowaniu informacji sprzecznych[269]. Podczas próby odkrycia lub weryfikacji reguły często prezentowane są przykłady zgodne z przewidywaną regułą, zamiast tych, które mogłyby ją obalić. Analityk, który ulega błędowi potwierdzenia, unika testowania hipotez w sposób, który mógłby je podważyć. Błąd konfirmacji w analizie wywiadowczej może skutkować pominięciem kluczowych informacji i prowadzić do formułowania nieprawidłowych ocen. Błąd dostępności (ang. *availability bias*), znany również jako heurystyka dostępności, jest rodzajem uproszczonego wnioskowania[270]. Polega on na opieraniu ocen i decyzji na informacjach, które są łatwo dostępne lub silnie nacechowane emocjonalnie, zamiast na pełnym zestawie bardziej reprezentatywnych danych, co prowadzi do nadmiernego szacowania wartości tych

[267] Ibidem, s. 681–682.
[268] A. Tversky, D. Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, „Science. New Series" 1975, vol. 185, no. 4157, s. 1124–1131.
[269] P.C. Wason, *Reasoning about a rule*, „Quarterly Journal of Experimental Psychology" 1968, vol. 20, no. 3, s. 273–281.
[270] A. Tversky, D. Kahneman, *Judgment under Uncertainty*…, op. cit., s. 1124–1131.

informacji. Iluzja grupowania (ang. *clustering illusion*) odnosi się do skłonności człowieka do niedoszacowania zmienności w przypadkowych danych, co w efekcie prowadzi do dostrzegania nieistniejących wzorców. Konsekwencją iluzji grupowania w analizie jawnoźródłowej jest ryzyko błędnej interpretacji dostępnych informacji, co może prowadzić do fałszywych wniosków opartych na pozornych wzorcach, zwłaszcza gdy analizowane dane są ograniczone.

4.3.3. Aspekty językowe

Z uwagi na różnorodność źródeł informacji w wywiadzie jawnoźródłowym, wyzwaniem pozostaje translacja wiadomości z języka, w jakim informacja została wygenerowana, na inne języki. Nieprawidłowa lub niedokładna translacja może ograniczać skuteczność tych działań, wpływając negatywnie na pełne zrozumienie i interpretację zgromadzonych informacji. Na etapie pozyskiwania informacji z otwartych źródeł translacja jest niezbędna, gdy zachodzi potrzeba zmiany nośnika materialnego, gdy informacje są pozyskiwane przez osoby posługujące się innym językiem niż ten, w którym informacja została wygenerowana, oraz gdy używane technologie wymagają zastosowania innego języka niż ten, w którym informacja została stworzona[271]. W procesie tłumaczenia uwzględniane są aspekty kulturowe, stylistyczne i gramatyczne obu języków. Zagrożeniem dla translacji jest ryzyko niezamierzonej modyfikacji treści informacji, ich utraty lub tworzenia informacji różniących się od tych, które zostały pozyskane z pierwotnych źródeł. Błędy w translacji w fazie gromadzenia informacji są trudne do wykrycia, a ich identyfikacja i korekta z reguły kosztowna, stąd w wielu procesach informacyjnych stosowane są mechanizmy poprawności translacji[272].

Historyczna działalność wywiadu jawnoźródłowego polegała głównie na tłumaczeniu i udostępnianiu zagranicznych publikacji informacyjnych analitykom wywiadu. Po przetłumaczeniu większości treści oryginalnego materiału, można było przekazać i zintegrować z końcowym opracowaniem. Współczesne technologie, w tym tłumaczenie maszynowe, znacznie usprawniły ten proces, szczególnie dla języków o wspólnej składni i korpusie. Tłumaczenie maszynowe jest najbardziej efektywne dla treści mediów informacyjnych o standardowym słownictwie i strukturze. W szarej literaturze przestrzegane są standardy pisania, ale specyficzne tematy mogą wymagać

[271] J. Oleński, *Ekonomika informacji. Metody*, op. cit., s. 83.
[272] Ibidem.

konsultacji analityka. W treściach w mediach społecznościowych pojawiają się skróty, błędy językowe i typograficzne oraz wyrażenia potoczne[273].

W przypadku korzystania z języka zapisanego w oryginale znakami jednego pisma fonetycznego (np. język polski) i pozyskania informacji zapisanej w innym systemie pisma fonetycznego (np. język arabski), konieczna jest transliteracja (przy zachowaniu ścisłej odpowiedniości liter), aby można było wykorzystać taki tekst do przetwarzania i analizy. Dokładność tłumaczenia jest szczególnie istotna w odniesieniu do nazw osób i miejsc. W przypadku konieczności dokonania transliteracji, informacja musi zostać zweryfikowana na każdym etapie cyklu wywiadowczego. Nieudane potwierdzenie stopnia poziomu pewności informacji jawnoźródłowych w języku ojczystym może prowadzić do błędnej identyfikacji osoby, nieprawidłowego rozpoznania obszaru i utrudniać ściganie. Konieczność transliteracji zwiększa prawdopodobieństwo odchyleń w dokładności przetłumaczonych informacji[274].

Podczas działań operacyjnych w stosunku do osób z krajów spoza kręgu europejskiego, prowadzący działania muszą wykazać się choć minimalną wiedzą na temat identyfikacji danych osób w ich języku ojczystym, z prawidłowym zapisywaniem imion i nazwisk. Błędy w weryfikacji nazwisk w języku pierwotnym mogą prowadzić do pomyłek w identyfikacji osób, a przez to błędnego podjęcie działań dochodzeniowo-śledczych w stosunku do innej osoby, niż to było zamierzone. Sprawdzenie poprawności danych wejściowych z danymi wyjściowymi znacznie zmniejsza możliwość wystąpienia kaskadowych błędów w całym cyklu wywiadowczym.

Nieporozumienia językowe, wynikające z braku uwzględnienia cech języka narodowego, mogą wpływać na weryfikację otwartych źródeł informacji oraz na wartościowanie informacji. Do najczęstszych błędów występujących w analizie wywiadowczej należą: wieloznaczność wyrażeń, amfibologia, ekwiwokacja oraz błąd hipostazowania.

Wieloznaczność wyrażeń polega na faktycznym użyciu terminu w różnych znaczeniach. Jest to spowodowane użyciem nazw homonimicznych. Każda nazwa może być wieloznaczna, gdyż może być zastosowana w odniesieniu do klasy swoich desygnatów. Przez to wieloznaczność jest często popełnianym błędem. Amfibologia jest błędem syntaktycznym, powodującym wieloznaczność zdania. Może skutkować

[273] H.J. Williams, I. Blum, *Defining Second Generation*…, op. cit., s. 17.
[274] K. Lieberthal, *The U.S. Intelligence Community and Foreign Policy: Getting Analysis Right*, „John L. Thornton China Center Monograph Series" no. 2, „Foreign Policy Paper Series" no. 18, 2009.

przyjęciem innej interpretacji wyrażenia przez odbiorcę niż zamierzona przez autora. Kolejnym błędem jest ekwiwokacja, która polega na użyciu w jednym rozumowaniu tego samego wyrażenia w różnych znaczeniach. W konsekwencji może prowadzić do niejasności lub mylących wniosków, jest używana w dezinformacji, aby doprowadzić odbiorcę do fałszywych konkluzji. Błąd hipostazowania polega na przypisaniu nazwom abstrakcyjnym cech nazw konkretnych. W celu uniknięcia tego błędu w analizie wywiadowczej najlepiej nie stosować nazw abstrakcyjnych[275].

Czynnikiem zaburzającym percepcje informacji może być również logomachia, zwana też sporem słownym. Logomachia jako instrument dezinformacji po pierwsze może prowadzić do błędnego wartościowania informacji, poprzez przyjęcie formuł lingwistycznych zgodnych z tymi, którymi posługuje się analityk. Po drugie poprzez uruchomienie mechanizmu projekcji u analityka może prowadzić do błędnych decyzji. W końcu, na każdym etapie analizy może wystąpić w dyskusji, której uczestnicy stosują nieświadomie jakieś wyrażenie, pojmując je w różnych znaczeniach. Potencjalna możliwość wystąpienia logomachii generuje konieczność uzgadniani znaczeń stosowanych wyrażeń na początku analizy. Element ten jest równie istotny przy wdrażaniu procesów automatyzujących i projektowaniu narzędzi służących do translacji informacji.

4.4. Aspekty techniczne

W erze cyfrowej paradygmat pozyskiwania informacji z otwartych źródeł uległ znaczącej transformacji. Dla prowadzenia wywiadu jawnoźródłowego niezbędna jest specjalistyczna wiedza na temat zmieniających się wzorców generowania, dystrybucji oraz przechowywania informacji w Internecie. Równie istotna jest zaawansowana infrastruktura techniczna, która pozwala sprostać wyzwaniom związanym z gromadzeniem dużych ilości danych oraz ich skutecznym zarządzaniem, zapewniając jednocześnie bezpieczeństwo i dostępność w dynamicznie zmieniającym się środowisku cyfrowym.

Na etapie pozyskiwania informacji jawnoźródłowych szczególne znaczenie ma projektowanie oraz kontrola dedykowanych narzędzi do ich gromadzenia. Niewłaściwa konfiguracja robotów indeksujących może skutkować ich zapętleniem podczas śledzenia linków w obrębie tej samej strony. Wysyłanie nadmiernej liczby zapytań

[275] J. Konieczny, *Analiza informacji w dziedzinie bezpieczeństwa*…, op. cit., s. 243.

obciąża serwer sieciowy, co może doprowadzić do zidentyfikowania adresu IP, z którego prowadzone jest wyszukiwanie, a następnie do jego zablokowania przez administratora witryny. Dla efektywności i bezpieczeństwa prowadzonego rozpoznania jawnoźródłowego istotne jest również przestrzeganie wytycznych zawartych w pliku robots.txt. Jest to plik utworzony przez administratora strony internetowej, który zawiera instrukcje dla robotów internetowych określające, które obszary strony mogą być przez nie skanowane. Nieprzestrzeganie tych wytycznych może skutkować zablokowaniem adresu IP przez administratora strony, co uniemożliwi dalsze działania rozpoznawcze.

Innym wyzwaniem technologicznym jest deszyfrowanie danych pozyskanych w ramach wywiadu jawnoźródłowego. Współczesne systemy komunikacyjne często wykorzystują zaawansowane techniki szyfrowania, aby zapewnić prywatność i bezpieczeństwo przekazu[276]. Podmioty prowadzące rozpoznanie OSINT muszą dysponować odpowiednimi narzędziami i kompetencjami, aby skutecznie odszyfrować te komunikaty, jednocześnie zachowując integralność pierwotnej treści.

Na etapie integracji danych jawnoźródłowych wyzwania technologiczne dotyczą projektowania oraz budowy systemu, który pozwala na harmonizację danych z różnych, niezależnych źródeł, tworząc spójną reprezentację. Ważnym elementem jest ujednolicenie zasad dostępu do tych źródeł. Dynamiczny wzrost ilości danych jawnoźródłowych oraz ich niestabilność, wynikająca z losowych zmian w formatach i strukturze danych, a także autonomii źródeł, może znacząco utrudniać analizę[277].

Na etapie przechowywania pozyskanych danych jawnoźródłowych wyzwaniem jest zapewnienie infrastruktury do zarządzania dużymi zbiorami nieustrukturyzowanych danych, która umożliwia ich integrację, interoperacyjność pomiędzy różnymi systemami oraz zapewnia niezawodność, dostępność i ochronę pozyskanych danych. Stałe wsparcie techniczne, które gwarantuje sprawną eksploatację systemu oraz szybką reakcję na ewentualne problemy, jest przewagą narzędzi płatnych nad darmowymi.

Podczas analizy informacji pochodzących z otwartych źródeł istotnym wyzwaniem jest przetwarzanie dużych ilości często nieustrukturyzowanych danych pochodzących z różnych źródeł, uwzględnieniem różnic kulturowych i społecznych oraz efektywnego tłumaczenia z wielu języków. Automatyzacja znacząco skraca czas analizy, jednak określenie parametrów niezbędnych do zachowania precyzji, zwłaszcza

[276] H.J. Williams, I. Blum, *Defining Second Generation*…, op. cit., s. 41.
[277] B. Szafrański, *Analiza danych*…, op. cit., s. 76–77.

w kontekście tłumaczenia terminów technicznych i slangowych, pozostaje trudnym zadaniem, które może wpływać na dokładność wyników.

Znajomość wykorzystywanych narzędzi oraz świadomość, że stosowane metody mogą prowadzić do wykrycia i śledzenia aktywności w internecie, umożliwiając identyfikację osoby przeprowadzającej rozpoznanie, stanowi istotny aspekt utrzymania bezpieczeństwa operacyjnego (OPSEC). Termin ten został po raz pierwszy wprowadzony przez armię amerykańską w odpowiedzi na wydarzenia związane z wojną w Wietnamie[278]. Opracowano go w celu zwiększenia efektywności operacyjnej poprzez ograniczenie dostępu do jawnych danych, które mogłyby ujawniać poufne działania, zdolności lub intencje.[279] Wraz z rozwojem zagrożeń w XXI wieku, OPSEC zaczął być stosowany w szerszym kontekście bezpieczeństwa. Obecnie przeszkolenia w zakresie bezpieczeństwa prowadzenia działań ma istotne znaczenie w wywiadzie jawnoźródłowym. OPSEC jest definiowany jako proces analityczny mający na celu uniemożliwienie przeciwnikowi uzyskania informacji o naszych zamiarach i zdolnościach poprzez identyfikację, kontrolę i ochronę wskaźników związanych z procesami planowania lub operacjami[280]. Celem OPSEC jest identyfikacja działań własnych, które mogą zostać wykryte przez systemy wywiadu przeciwnika, oraz ustalenie, jakie wskaźniki mogą być zebrane i wykorzystane do uzyskania informacji krytycznych. Proces ten obejmuje również wdrażanie środków minimalizujących wrażliwość tych działań na eksploatację, redukując ryzyko do akceptowalnego poziomu. Proces OPSEC składa się z pięciu etapów (rys. 4.1).

[278] Podczas wojny w Wietnamie armia amerykańska odkryła, że przeciwnik skutecznie wykorzystywał publicznie dostępne, nieodpowiednio zabezpieczone informacje, takie jak ruchy wojsk, harmonogramy operacji i wzorce komunikacyjne, co umożliwiało wietnamskim siłom precyzyjne prowadzenie działań sabotażowych. W odpowiedzi Armia Stanów Zjednoczonych przeprowadziła operację „Fioletowy Smok" (ang. *Purple Dragon*), której celem było zidentyfikowanie nadmiarowo udostępnianych informacji oraz opracowanie środków ochrony mających na celu zapobieżenie ich dalszemu wykorzystaniu przez przeciwnika. Zob. DCMA, *OPSEC history: from ancient origins to modern challenges*, 2023, https://www.dcma.mil/News/Article-View/Article/3258274/opsec-history-from-ancient-origins-to-modern-challenges/ [dostęp: 5.02.2024].

[279] FAS Intelligence Resource Program, *Operations Security Intelligence Threat Handbook*, https://irp.fas.org/nsa/ioss/threat96/part01.htm [dostęp: 5.02.2024].

[280] *Operations Security Guide*, RCC dokument 600-11, kwiecień 2011, Secretariat, Range Commanders Council, U.S. Army White Sands Missile Range, New Mexico, USA. Podobnie OPSEC definiowany jest w dokumentach NATO jako proces zapewniający odpowiedni poziom bezpieczeństwa operacjom lub działaniom wojskowym, realizowany za pomocą środków pasywnych lub aktywnych, w celu ukrycia przed przeciwnikiem możliwości i zamiarów sił własnych. NATO Standardization Office, *AAP-6: Słownik terminów*…, op. cit., s. 336.

Rysunek 4.1. Etapy strategii OPSEC

Źródło: Opracowanie własne na podstawie *Operations Security Guide*, RCC dokument 600-11, kwiecień 2011, Secretariat, Range Commanders Council, U.S. Army White Sands Missile Range, New Mexico, USA

Pierwszy etap polega na zdefiniowaniu informacji krytycznych podlegających ochronie oraz ustaleniu jaki poziom ochrony i kosztów jest akceptowalny dla decydentów. Informacje uznane za krytyczne na jednym etapie rozpoznania mogą nie być już uznawane jako istotne w dalszych fazach procesu. Definiowanie informacji krytycznych powinno być więc dostosowane do każdego przypadku i kontekstu operacyjnego, a proces ten musi być przeprowadzany indywidualnie dla każdej operacji wywiadowczej.

W kolejnym etapie przeprowadzana jest szczegółowa analiza zagrożeń, w tym identyfikacja potencjalnego przeciwnika posiadajacego środki oraz motywację do podjęcia działań zakłócających. Określane są również metody zakłócania, możliwości operacyjne a także ustala są jakie informacje przeciwnik może już posiadać. Aktualne informacje na temat zagrożeń są niezbędne do opracowania skutecznych środków ochrony w ramach OPSEC.

Trzeci etap, czyli analiza podatności, polega na identyfikacji słabych punktów mogących narażać krytyczne informacje na ryzyko ujawnienia. Podatności te mogą wynikać z niewystarczających środków ochrony danych lub z wykorzystania wskaźników, które mogą być łatwo dostrzeżone przez przeciwnika. Po zidentyfikowaniu tych podatności należy opracować wstępne środki OPSEC, mające

na celu wyeliminowanie tych podatności lub zminimalizowanie ryzyka ich wykorzystania przez przeciwnika.

W czwartym etapie przeprowadzana jest analiza ryzyka oraz ocena potencjalnych szkód, które przeciwnik mógłby wyrządzić poprzez ich wykorzystanie. Przeprowadzana jest również szczegółowa ocena wpływu tych podatności na przebieg operacji oraz na szanse jej powodzenia. Na tym etapie decydenci powinni określić akceptowalny poziom ryzyka, co umożliwi dostosowanie odpowiednich środków OPSEC do zidentyfikowanych zagrożeń oraz skuteczne zarządzanie ryzykiem.

Ostatnim etapem jest dobór oraz wdrożenie środków zaradczych mających na celu ochronę informacji krytycznych. Działania te mogą obejmować zarówno zabezpieczenia fizyczne, jak i techniczne oraz operacyjne, które mają na celu minimalizację ryzyka wykorzystania przez przeciwnika zidentyfikowanych podatności.

Strategia OPSEC powinna być każdorazowo dostosowywana do specyfiki planowanego rozpoznania jawnoźródłowego oraz elastycznie reagować na zmieniające się potrzeby i wymagania. Istotną rolę w tworzeniu strategii odgrywają decydenci, którzy są odpowiedzialni za definiowanie krytycznych założeń na każdym etapie, z uwzględnieniem dostępnych zasobów finansowych[281].

W cyfrowym wywiadzie jawnoźródłowym można wyróżnić dwa główne aspekty OPSEC: organizacyjny i techniczny. W ramach aspektów organizacyjnych szczególne znaczenie ma oddzielenie prywatnej aktywności od środowiska wykorzystywanego do prowadzenia dochodzenia, co obejmuje separację systemów, połączeń internetowych oraz kont w mediach społecznościowych. Taki podział pozwala również na uzyskanie bardziej obiektywnych wyników wyszukiwania.

Zasadniczym elementem technicznym OPSEC w operacjach wywiadu jawnoźródłowego jest stosowanie rozwiązań umożliwiających tworzenie maszyn wirtualnych. Wirtualne środowisko pozwala na skonfigurowanie oprogramowania, przeglądarki oraz funkcji systemowych w sposób dostosowany do specyfiki prowadzonego rozpoznania. Wirtualizacja zapewnia również ochronę własnego systemu przed potencjalnym zainfekowaniem, umożliwiając jednocześnie bezpieczną analizę złośliwego oprogramowania. W sytuacjach, gdy pozyskiwanie informacji jawnoźródłowych wymaga dostępu do platform mediów społecznościowych dostępnych jedynie w wersji mobilnej, efektywnym rozwiązaniem jest wykorzystanie emulatorów

[281] R. Baker, *Prawdziwa głębia OSINT*…, op. cit., s. 99.

urządzeń mobilnych. Tego rodzaju narzędzia umożliwiają symulację środowiska mobilnego, co pozwala na uruchamianie aplikacji mobilnych bez potrzeby instalowania ich na fizycznym urządzeniu. Umożliwia to wysyłanie i odbieranie wiadomości SMS, wykonywanie połączeń oraz korzystanie z czatów, a także dokonywanie weryfikacji tożsamości w serwisach społecznościowych, przy zachowaniu pełnej anonimowości.

Kolejnym elementem OPSEC jest używanie połączeń gwarantujących anonimowość poprzez maskowanie rzeczywistego adresu IP. Zastosowanie wirtualnych sieci prywatnych (VPN) nie tylko zapewnia bezpieczny dostęp do zamkniętych zasobów sieci prywatnych, ale również umożliwia omijanie cenzury państwowej i odblokowywanie treści strumieniowych ograniczonych regionalnie. Wadą korzystania z VPN jest fakt, że dostęp do wielu serwisów najczęściej wiąże się z opłatami. Ponadto, VPN przekierowuje cały ruch internetowy w pierwszej kolejności do serwera dostawcy usługi, co może wpłynąć na prędkość połączenia oraz zwiększyć ryzyko przechwycenia danych, jeśli dostawca nie zapewnia odpowiednich zabezpieczeń. Dodatkowo, podmioty, które są przedmiotem analizy, mogą monitorować swoje logi sieciowe w celu identyfikacji publicznych adresów IP łączących się z ich serwerami. Przy użyciu narzędzi do wyszukiwania adresów IP, mogą ustalić, czy analityk, korzystał z sieci VPN, co potencjalnie może ujawnić jego tożsamość. Alternatywnym sposobem na zachowanie anonimowości jest korzystanie z przeglądarek skoncentrowanych na ochronie prywatności, takich jak TOR[282], Freenet[283] czy I2P[284]. Tego rodzaju rozwiązania znacząco utrudniają lub wręcz uniemożliwiają analizę ruchu sieciowego, zapewniając poufność oraz anonimowość użytkownika. Innym rozwiązaniem jest korzystanie ze stron pośredniczących w uzyskiwaniu dostępu do informacji, które przekazują żądania użytkownika do docelowej strony internetowej i zwracają odpowiedź, co umożliwia ukrycie prawdziwego adresu IP i zachowanie anonimowości. Takie podejście jest często stosowane w celu omijania blokad regionalnych, cenzury, a także w sytuacjach, gdy bezpośredni dostęp do informacji może być monitorowany przez docelowy podmiot.

Podczas pozyskiwania informacji jawnoźródłowych istotne jest nie tylko tworzenie odrębnych tożsamości wirtualnych dla różnych dochodzeń, ale również zapewnienie wyraźnego oddzielenia działań osobistych od zawodowych, w tym poprzez

[282] https://www.torproject.org/ [dostęp: 20.08.2024].
[283] https://freenetproject.org/ [dostęp: 20.08.2024].
[284] https://geti2p.net/ [dostęp: 20.08.2024].

unikanie wykorzystywania prywatnych danych do tworzenia loginów i haseł. Nawet drobne szczegóły, takie jak styl wypowiedzi czy preferencje językowe, mogą prowadzić do identyfikacji osoby prowadzącej rozpoznanie. W wywiadzie jawnoźródłowym, zgodnie z zasadami OPSEC, stosuje się konta badawcze (ang. *research accounts*), określane również jako konta skarpetkowe (ang. *sock puppet accounts*). Pozwalają one na prowadzenie rozpoznania bez ujawniania tożsamości ani powiązań z instytucją odpowiedzialną za jego przeprowadzenie. Korzystanie z kont badawczych pozwala na zachowanie anonimowości oraz uzyskanie dostępu do informacji dostępnych jedynie dla zalogowanych użytkowników. Konta badawcze powinny być odpowiednio dostosowane do specyfiki oraz wymagań prowadzonego rozpoznania, poprzez m.in. wybór odpowiedniego pseudonimu, dopasowanie płci, wieku oraz zawodu, użycie nowych adresów e-mail i numerów telefonów, a także budowanie wiarygodnych sieci powiązań z innymi użytkownikami.

4.5. Aspekty informacyjne

Informacje jawnoźródłowe z uwagi na swoje cechy są podatne na manipulacje. Manipulacja informacją to celowe, ukryte modyfikowanie informacji lub procesów informacyjnych (takich jak transmisja, udostępnianie, interpretacja i wykorzystanie), mające na celu wpływanie na odbiorcę bez jego wiedzy, w celu zmiany jego postawy i zachowania[285]. Wyzwaniem dla wywiadu jawnoźródłowego są w szczególności dezinformacja i propaganda, które poprzez celowe zniekształcanie rzeczywistości oraz manipulowanie przekazem, utrudniają rzetelną analizę i ocenę dostępnych informacji.

Propaganda to świadoma i inteligentna manipulacja faktami, której celem jest ukształtowanie określonych poglądów i zachować społeczeństw lub jednostki[286]. Ten rodzaj komunikowania znacząco wpływa na postrzeganie rzeczywistości społecznej przez obywateli, a nowoczesne technologie tworzą sprzyjające warunki do efektywnego połączenia go z kampaniami dezinformacyjnymi. Współczesne media odgrywają istotną rolę w kreowaniu i wzmacnianiu propagandy, nadając jej większą dynamikę i interaktywność. W warunkach rosnącego wpływu opinii publicznej na procesy polityczne propaganda ewoluowała, stając się nie tylko narzędziem perswazji, lecz

[285] P. Motylińska, *Manipulacja informacją*, [w:] Vademecum Bezpieczeństwa informacyjnego, 2020, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/manipulacja-informacja/ [dostęp: 12.04.2024].
[286] E.I. Bernays, *Propaganda*, Wydawnictwo Ig Publishing, New York 2004, s. 9.

także mechanizmem mobilizacyjnym oraz instrumentem kształtowania narracji społeczno-politycznych[287]. Wywiad jawnoźródłowy pozwala na identyfikację i analizę mechanizmów dezinformacyjnych i propagandowych, a także na opracowanie skutecznych metod przeciwdziałania ich wpływowi.

W *Leksykonie tajnych służb świata*[288] dezinformacja została określona jako metodologiczny sposób oddziaływania na przeciwnika, podejmowany z zamiarem wykreowania celowego, ukierunkowanego wpływu na kształtowanie opinii i bieg możliwych do przewidzenia zdarzeń.

Z perspektywy zagrożeń dla systemu bezpieczeństwa państwa, Vladimir Volkoff, ekspert w tej dziedzinie, definiuje dezinformację jako gałąź operacji specjalnych, polegającą na zmyleniu przeciwnika poprzez dostarczanie mu nieprawdziwych informacji, którymi posłuży się on do wyciągania wniosków, jakich życzy sobie inicjator operacji[289].

Oprócz przytoczonych, istnieje wiele innych definicji dezinformacji[290]. Ich analiza prowadzi do wniosku, że istotą dezinformacji są zaplanowane, podstępne i świadome działanie polegające na przekazywaniu zarówno częściowo prawdziwych, jak i fałszywych informacji w celu wprowadzenia odbiorcy w błąd oraz wpływania na opinię publiczną, zniekształcenia obrazu rzeczywistości i nakłaniania do podejmowania określonych decyzji zgodnych z interesami podmiotu dezinformującego.

Volkoff sformułował zestaw metod działań dezinformacyjnych, które obejmują:

- przekazywanie wiadomości całkowicie fałszywej, co do której odbiorca nie dysponuje żadnymi możliwościami jej weryfikacji,
- łączenie informacji prawdziwych z nieprawdziwymi, gdy odbiorca ma pewną wiedzę na dany temat, lecz nie zna wszystkich jej szczegółów,
- dobór informacji, z których każda oddzielnie jest prawdziwa przy jednoczesnej sugestii odbiorcy określonej intencji,

---

[287] I.T. Dziubek, *Media a współczesny terroryzm*, [w:] K. Jałoszyński, T. Aleksandrowicz, K. Wiciak (red.), *Bezpieczeństwo państwa a zagrożenie terroryzmem. Terroryzm na przełomie XX i XXI wieku*, t. 1. WSPol, Szczytno 2016.

[288] J.H. Larecki, *Wielki leksykon*…, op. cit., s. 211.

[289] V. Volkoff, *Psychosocjotechnika, dezinformacja, oręż wojny*, Wydawnictwo Antyk, Komorów 1999, s. 81.

[290] Zob. M. Ogiński, *Dezinformacja w dobie cyfryzacji*, „Zeszyty Naukowe Zbliżenie Cywilizacyjne" 2023, vol. 19, no. 1, s. 136; *Kodeks dobrych praktyk. Wspólnie przeciw dezinformacji*, 2023, s. 6 https://www.nask.pl/pl/wlaczweryfikacje/kodeks-dobrych-praktyk/4991,Kodeks-Dobrych-Praktyk.html [dostęp: 11.07.2024]; *Leksykon wiedzy wojskowej*, Ministerstwo Obrony Narodowej, Warszawa 1979, s. 87; S. Hoc, *Przestępstwo dezinformacji wywiadowczej w kodeksie karnym*, „Przegląd Sądowy" 2000, nr 5, s. 50; M. Wrzosek, *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, NASK Państwowy Instytut Badawczy, Warszawa 2019, s. 7.

- „rozmycie” polegające na zakłóceniu równowagi pod względem jakości i objętości przykazywanych informacji na korzyści tych nieprawdziwych mających wpływać na odbiorcę,
- selekcję faktów poprzez przedstawienie informacji prawdziwych, lecz niekompletnych, tak aby przekaz był jak najbardziej korzystny dla podmiotu dezinformującego,
- tendencyjny komentarz to działanie, w którym podmiot dezinformujący, zamiast zaprzeczać faktom, wybiórczo je omawia, stosując interpretacje mające na celu wywołanie korzystnych dla siebie skojarzeń,
- ilustrację, gdy jednostkowe zdarzenie jest wykorzystywane jako ilustracja szerszego zjawiska,
- uogólnienie polegające na przedstawieniu informacji fałszywej w taki sposób, że jawi się ona jako zjawisko powszechne, a tym samym akceptowalne,
- zakłócenie równowagi pod względem ilości i objętości prezentowanych informacji na korzyść tych dezinformujących,
- równe proporcje, czyli przedstawienie podobnej ilości informacji prawdziwych i fałszywych, przy czym argumenty poparcia jakiejś tezy przedstawione zostają starannie przy pomocy wiarygodnych materiałów natomiast argumenty przeciwstawne przekazywane są w sposób mało wiarygodny[291].

Zagrożenia dla bezpieczeństwa informacji mogą występować w różnych formach, oddziałując zarówno na ich integralność, jak i dostępność, co bezpośrednio wpływa na procesy decyzyjne związane z bezpieczeństwem państwa. Wyróżnia się zagrożenia wewnętrzne, zewnętrzne oraz fizyczne, w zależności od lokalizacji źródeł informacji. Zagrożenia wewnętrzne powstają wewnątrz danego podmiotu i obejmują utratę, uszkodzenie, modyfikację informacji powodowaną zamierzonym lub niezamierzonym działaniem ich użytkowników. Zagrożenia zewnętrzne powstają poza danym podmiotem i obejmują wszystkie powyższe działania dokonywanej jednak ze strony podmiotów trzecich. Zagrożenia fizyczne odnoszą się do utraty, uszkodzenia danych lub informacji bądź braku możliwości ich użycia wynikających z wypadków,

[291] V. Volkoff, *Psychosocjotechnika*…, op. cit., s. 164–166.

awarii, katastrof lub innych nagłych zdarzeń, które zakłócają funkcjonowanie systemów informacyjnych albo urządzeń sieciowych[292].

Media społecznościowe odgrywają istotną rolę w rozprzestrzenianiu dezinformacji, ponieważ umożliwiają szybkie i szerokie udostępnianie treści wśród dużej liczby użytkowników. Ich algorytmy promują angażujące treści, co często sprzyja rozpowszechnianiu sensacyjnych, a nierzadko fałszywych informacji. Ponadto, media społecznościowe są często wykorzystywane jako narzędzie manipulacji przez grupy polityczne lub państwa, które tworzą i amplifikują dezinformację w celu wpływania na opinię publiczną oraz destabilizowania procesów demokratycznych. Możliwość pozornej multiplikacji źródeł informacji wzmacnia wrażenie ich wiarygodności, ponieważ różne kanały medialne potwierdzają te same treści, mimo, że często pochodzą one z jednego, celowo zmanipulowanego źródła[293]. Tego rodzaju strategia intensyfikuje efekt „bańki informacyjnej", w której odbiorcy są narażeni na treści potwierdzające ich istniejące przekonania, co utrudnia krytyczną analizę informacji i sprzyja rozprzestrzenianiu fałszywych narracji. Dezinformacja oddziałuje nie tylko na jednostki, ale również na szeroką opinię publiczną. W celu jej eskalacji wykorzystywane są konta w mediach społecznościowych, boty oraz fałszywe konta automatyczne, zaprogramowane do powielania określonych treści, jak również internetowe trolle, których zadaniem jest prowokowanie emocjonalnych reakcji oraz intensyfikowanie polaryzacji dyskursu publicznego. Zaawansowane narzędzia cyfrowe, w tym boty oraz skoordynowane kampanie dezinformacyjne, są wykorzystywane jako element strategii państw dążących do osiągnięcia przewagi bez konieczności użycia środków militarnych. Analiza współczesnych konfliktów wskazuje, że zatarcie granicy między działaniami wojskowymi a niemilitarnymi stanowi jeden z aspektów operacji wpływu. Integracja dezinformacji z presją polityczną, gospodarczą i cyfrową prowadzi do osłabienia instytucji państwowych, podważenia ich legitymacji oraz kształtowania postaw społecznych zgodnie z interesami podmiotu prowadzącego operację[294].

Zagrożenia generowane przez dezinformację oddziałują na funkcjonowanie systemów politycznych, nastroje społeczne, relacje i preferencje obywateli, gospodarkę,

[292] Szerzej: A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000, s. 65; D. Fleszer, *Wokół problematyki bezpieczeństwa informacji*, „Roczniki Administracji i Prawa" 2018, nr 1, s. 190.
[293] T.R. Aleksandrowicz, *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*, Difin, Warszawa 2021, s. 56.
[294] Zob. szerzej: L. Elak, Z. Śliwa, *Hybridity – a 'new' method to accomplish dominance,* „Security and Defence Quarterly" 2019, vol. 23, no. 1.

podejście do kwestii ekologicznych, a także na sferę militarną i kulturową[295]. Dezinformacja stanowi poważne zagrożenie dla działalności wywiadowczej oraz może znacznie ograniczać jej skuteczność. Chociaż mechanizmy manipulacji informacją nie ulegają zmianie, rozwój nowoczesnych technologii i cyberprzestrzeni stwarza nowe możliwości oraz znacząco zwiększa skuteczność i efektywność działań dezinformacyjnych. Przykładem są *deepfaki* i *fake newsy,* które wykorzystują zaawansowane technologie do tworzenia fałszywych treści wizualnych i informacyjnych.

Fake newsy to celowo rozpowszechniane fałszywe lub wprowadzające w błąd informacje, które mają na celu manipulowanie opinią publiczną. *Deepfake* to technologia oparta na sztucznej inteligencji i uczeniu maszynowym, umożliwiająca tworzenie realistycznych materiałów audiowizualnych, takich jak obrazy i wideo, przedstawiających osoby wykonujące lub wypowiadające rzeczy, których w rzeczywistości nie robiły ani nie mówiły. Sieci neuronowe oraz generatywne sieci współzawodniczące (ang. *generative adversarial networks*, GAN) są podstawą działania tej technologii, pozwalając na precyzyjne modelowanie i manipulowanie obrazami. Siła oddziaływania deepfake wynika z faktu, że obrazy nie tylko silnie zapadają w pamięć i oddziałują na podświadomość człowieka, ale także wzbudzają emocje, co dodatkowo potęguje ich wpływ na odbiorców poprzez realistyczne wizualizacje trudne do odróżnienia od rzeczywistości. Zarówno deepfake, jak i fake newsy są szeroko wykorzystywane w kampaniach dezinformacyjnych, zwłaszcza w mediach społecznościowych, gdzie ich zasięg i tempo rozprzestrzeniania się znacząco rosną. Przykładem zastosowania technologii deepfake w konflikcie zbrojnym były działania Rosji podjęte w 2022 roku[296]. Po przełamaniu zabezpieczeń strony ukraińskiego kanału telewizyjnego Ukraina 24 opublikowano sfałszowane nagranie wideo z wizerunkiem prezydenta Wołodymyra Zełenskiego, w którym sugerowano, że ukraińskie siły zbrojne poniosły klęskę, a władze podjęły decyzję o kapitulacji. Celem deepfake'u było wywołanie chaosu informacyjnego oraz osłabienie morale zarówno ukraińskiego społeczeństwa, jak i armii. Fałszywe nagranie zostało jednak szybko

[295] W. Fehler, *Podstawy bezpieczeństwa informacyjnego*, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, 2021, s. 154.
[296] J. Pearson, N. Zinets, *Deepfake footage purports to show Ukrainian president capitulating*, 2022, https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/ [dostęp: 12.04.2024].

zdemaskowane i zdementowane przez ukraińskie władze, co uniemożliwiło osiągnięcie zamierzonych efektów.

Dezinformacja stanowi element wrogich operacji informacyjnych prowadzonych przez państwa oraz kampanii wpływu realizowanych przez podmioty niepaństwowe, których celem jest destabilizacja zarówno sytuacji wewnętrznej, jak i międzynarodowej oraz osłabienie instytucji państwowych. Skuteczne wykorzystanie dezinformacji w tych obszarach może mieć poważne konsekwencje, zagrażając suwerenności i stabilności państwa[297]. Odwrócenie jej skutków jest wyzwaniem, ze względu na szybkie rozprzestrzenianie fałszywych informacji, brak możliwości dotarcia do wszystkich odbiorców oraz pojawianie się teorii spiskowych, które utrudniają proces sprostowania.

W wywiadzie jawnoźródłowym do badania dezinformacji oraz wykrywania kampanii dezinformacyjnych i sieci, przez które jest ona rozpowszechniana, można wykorzystać różne narzędzia i metody automatyzujące. Przykładem są implementowane na poziomie europejskim rozwiązania, takie jak FIMI Framework[298], DISARM Framework[299] oraz STIX[300]. Ich zastosowanie nie tylko usprawnia analizę, lecz także umożliwia współpracę z innymi podmiotami oraz sojusznikami w celu weryfikacji informacji jawnoźródłowych.

Manipulacje informacją, takie jak dezinformacja, propaganda, fake newsy, Deepfake czy nadmiar informacji, są zagrożeniem ograniczającym skuteczne wykorzystywanie wywiadu jawnoźródłowego. W związku z tym istotnym elementem przeciwdziałania tym zagrożeniom jest edukacja zarówno analityków wywiadu jawnoźródłowego, jak i całego społeczeństwa[301]. Z kolei wykorzystanie metod i środków wywiadu jawnoźródłowego, wspartych nowoczesnymi technologiami, może znacząco zwiększyć odporność na manipulacje informacyjne.

---

[297] B. Jagusiak., P. Żukowski, *Zagrożenia procesów*…, op. cit., s. 101.

[298] FIMI (Foreign Information Manipulation and Interference) Framework, opracowany przez Europejską Służbę Działań Zewnętrznych, jest narzędziem do walki z manipulacją informacyjną i dezinformacją, wspierającym analizę i koordynację reakcji na zagrożenia hybrydowe oraz zewnętrzne ingerencje poprzez współpracę między państwami członkowskimi. Strona: *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en [dostęp: 6.07.2024].

[299] DISARM Framework (ang. *Disinformation Analysis and Risk Management*) to narzędzie open-source stworzone do walki z dezinformacją poprzez udostępnianie danych, analiz oraz koordynację działań. Strona: DISARM Red Framework, https://www.disarm.foundation/framework [dostęp: 10.07.2024].

[300] STIX (ang. *Structured Threat Information eXpression*) jest standardem opisu i wymiany informacji o zagrożeniach, który został opracowany na potrzeby cyberbezpieczeństwa.

[301] *Nowe podejście do walki z dezinformacją,* 2024, https://www.gov.pl/web/cyfryzacja/nowe-podejscie-do-walki-z-dezinformacja [dostęp: 20.05.2024].

4.6. Podsumowanie

Przeprowadzone badania wykazały, że brak jednoznacznych regulacji prawnych w zakresie wywiadu jawnoźródłowego, zarówno na szczeblu krajowym, jak i międzynarodowym, prowadzi do niepewności prawnej oraz fragmentarycznego podejścia użytkowników. Skutkuje to rozbieżnościami interpretacyjnymi oraz zróżnicowanymi praktykami, które mogą ograniczać skuteczność działań OSINT. Taki stan rzeczy jednocześnie zwiększa ryzyko powstawania zagrożeń dla bezpieczeństwa państwa zarówno ze strony innych państw, jak i podmiotów niepaństwowych.

Rozproszenie przepisów prawnych dotyczących wywiadu jawnoźródłowego przenosi regulacje na poziom doktryn etycznych. Etyka wypełnia luki prawne i wspiera odpowiedzialne podejście do pozyskiwania i analizy informacji jawnoźródłowych. Jednak dobrowolny charakter tych zasad okazuje się niewystarczający do pełnego zniwelowania zagrożeń, szczególnie w zakresie ochrony prywatności i bezpieczeństwa.

Zidentyfikowano zakłócenia mogące występować na każdym etapie cyklu wywiadowczego. Wynikają one z czynników ogólnych, metodologicznych, specyficznych oraz komunikacyjnych, które mogą prowadzić do błędów w procesie analitycznym. Złożoność tych zmiennych oraz ich wzajemne oddziaływanie mogą obniżać efektywność działań wywiadowczych i negatywnie wpływać na jakość oraz wiarygodność pozyskiwanych informacji. Zarówno decydenci, jak i analitycy mogą popełniać błędy na różnych etapach, wynikające z nieprecyzyjnego sformułowania zapytań, niewłaściwego doboru źródeł, uprzedzeń czy ograniczeń poznawczych.

Przeanalizowane błędy poznawcze wykazują znaczący wpływ na ocenę sytuacji oraz proces decyzyjny analityków, co bezpośrednio odnosi się do problemu skuteczności wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa. Wynikają one z ograniczeń ludzkiego poznania i mogą prowadzić do zniekształceń w interpretacji pozyskanych informacji. W toku badań scharakteryzowano najczęściej występujące błędy, takie jak błąd lustrzanego odbicia, efekt dostosowania i zakotwiczenia, błąd konfirmacji, błąd dostępności oraz iluzja grupowania. Konsekwencją ich występowania jest pomijanie istotnych aspektów lub wyróżniania tych nieistotnych, co skutkuje formułowaniem nieprawidłowych wniosków, na podstawie których podejmowane są niewłaściwe decyzje. W rezultacie identyfikacja błędów oraz ocena ich wpływu na podejmowanie decyzji stanowią znaczący postęp w dążeniu do ograniczenia ich wpływu na ostateczny rezultat rozpoznania.

Badania objęły również aspekty językowe OSINT, w tym translację i transliterację, które wymagają specjalistycznej wiedzy oraz zaawansowanych narzędzi informatycznych. Nieprecyzyjna translacja materiałów z różnych języków może prowadzić do błędów wpływających na interpretację oraz weryfikację informacji jawnoźródłowych, co stanowi istotne ograniczenie w procesie decyzyjnym. W ramach przeprowadzonej analizy zidentyfikowano podstawowe problemy językowe, takie jak wieloznaczność wyrażeń, amfibologia, ekwiwokacja oraz błąd hipostazowania. Ponadto wykazano, że logomachia, stanowiąca jedno z zagrożeń w analizie OSINT, może być wykorzystywana jako instrument dezinformacji, prowadzić do błędnych decyzji analitycznych oraz nieporozumień w procesie uzgadniania znaczeń terminów na każdym etapie prowadzenia wywiadu jawnoźródłowego. Wymaga ona szczególnej uwagi przy wdrażaniu zautomatyzowanych procesów analitycznych oraz projektowaniu narzędzi służących do tłumaczenia i analizy lingwistycznej w ramach wywiadu jawnoźródłowego.

Analiza aspektów technicznych wykazała, że wywierają one znaczący wpływ na wywiad jawnoźródłowy. Działania OSINT wymagają zaawansowanej infrastruktury oraz systemów umożliwiających integrację i analizę dużych zbiorów danych, ich efektywne zarządzanie, zapewnienie interoperacyjności oraz wdrożenie odpowiednich mechanizmów ochrony. Najważniejsze wyzwania w tym zakresie obejmują konfigurację systemów, deszyfrowanie i integrację danych z różnych źródeł, a także zapewnienie wysokiego poziomu bezpieczeństwa operacyjnego. W związku z tym niezbędne są specjalistyczne szkolenia, które zapewnią odpowiednią wiedzę zarówno w zakresie technologii, jak i bezpieczeństwa operacyjnego.

Informacje jawnoźródłowe są szczególnie podatne na manipulacje, w tym dezinformację, których celem jest świadome zniekształcanie rzeczywistości i wywieranie wpływu na odbiorców. Skala oraz zasięg tego zjawiska, intensyfikowane przez rozwój zaawansowanych technologii, stanowią poważne zagrożenie dla procesów decyzyjnych w obszarze bezpieczeństwa państwa. W związku z tym przeciwdziałanie tym zagrożeniom wymaga zarówno wdrożenia nowoczesnych technologii wspierających analizę OSINT, jak i działań edukacyjnych skierowanych do analityków, podmiotów zaangażowanych w procesy decyzyjne oraz społeczeństwa w zakresie rozpoznawania i neutralizowania manipulacji informacyjnych.

Ze zgromadzonych w niniejszym rozdziale ustaleń naukowych wynika, że uwarunkowania prawne i pozaprawne, obejmujące aspekty metodologiczne, etyczne,

techniczne i informacyjne, kształtują sposób prowadzenia wywiadu jawnoźródłowego oraz wpływają na jego skuteczność w dostarczaniu informacji wspierających procesy decyzyjne na rzecz bezpieczeństwa państwa.

5. WYWIAD JAWNOŹRÓDŁOWY W WYBRANYCH PAŃSTWACH DEMOKRATYCZNYCH

Rozdział ten poświęcony został analizie doświadczeń związanych z wykorzystaniem wywiadu jawnoźródłowego na rzecz bezpieczeństwa w wybranych państwach demokratycznych. Przedmiot badań stanowi zastosowanie wywiadu jawnoźródłowego w Stanach Zjednoczonych, Wielkiej Brytanii oraz Izraelu, państwach charakteryzujących się wysokim poziomem rozwoju instytucji odpowiedzialnych za bezpieczeństwo oraz długoletnim doświadczeniem w wykorzystaniu informacji jawnoźródłowych. Szczegółowy problem badawczy, wyznaczający zakres analizy, sformułowano następująco: *Jakie są dotychczasowe kierunki prowadzenia wywiadu jawnoźródłowego na rzecz bezpieczeństwa w wybranych państwach demokratycznych?*

Omówione zostały ewolucja wywiadu jawnoźródłowego w analizowanych krajach, specyfika rozwiązań instytucjonalnych, a także sposoby definiowania i postrzegania jego roli przez instytucje odpowiedzialne za bezpieczeństwo. Szczególny nacisk położono na identyfikację różnic i podobieństw w podejściu tych państw do wywiadu jawnoźródłowego, uwzględniając obowiązujące regulacje prawne, doświadczenia praktyczne oraz stosowane technologie.

Analiza porównawcza umożliwiła wyodrębnienie najlepszych praktyk oraz określenie czynników warunkujących skuteczność wywiadu jawnoźródłowego w systemach demokratycznych. Wyniki tych badań stanowią podstawę do dalszych rozważań w kolejnych rozdziałach pracy oraz formułowania rekomendacji.

5.1. Wywiad jawnoźródłowy w Stanach Zjednoczonych

Rozwój wywiadu jawnoźródłowego w Stanach Zjednoczonych jest rezultatem ewolucji strategii wywiadowczych, które dostosowywały się do zmieniającego się otoczenia informacyjnego, politycznego i technologicznego. Informacje jawnoźródłowe umożliwiały uzyskanie przewagi na polu walki, rozpoznanie przeciwnika oraz pojawiających się zagrożeń. Zmiany w tej dziedzinie wraz z jej rosnącym znaczeniem jako integralnej części aparatu bezpieczeństwa Stanów Zjednoczonych, doprowadziły do formalizacji oraz profesjonalizacji wywiadu jawnoźródłowego. Pozyskiwanie i analiza informacji jawnoźródłowych przeszły ewolucję od mało uporządkowanych działań do strategicznych operacji wymagających zastosowania precyzyjnych metod i specjalistycznych narzędzi.

Podczas wojny secesyjnej wojska Unii oraz Konfederacji wykorzystywały gazety i inne publiczne dokumenty do zdobywania informacji na temat ruchów wojsk oraz zasobów przeciwnika. Początek drugiej wojny światowej przyniósł bardziej systematyczne podejście do wykorzystywania otwartych źródeł informacji w Stanach Zjednoczonych. Przejawem tego było ustanowienie przez prezydenta Franklina D. Roosevelta Służby Monitoringu Nadawców Zagranicznych (ang. *Foreign Broadcast Monitoring Service*, FBMS), która była częścią Federalnej Komisji Komunikacji. Jej głównym zadaniem było wspieranie działań służb oraz przeciwdziałanie propagandzie poprzez monitorowanie, tłumaczenie, transkrypcję oraz analizę informacji pochodzących z audycji radiowych Państw Osi. Na podkreślenie zasługuje, że pierwszy raport analityczny tej służby, opublikowany dzień przed atakiem na Pearl Harbor, wskazywał na nasilenie antyamerykańskich postaw w audycjach japońskiego radia. Pod koniec lutego 1942 roku, serwis telegraficzny FBMS obsługiwał osiemnaście organizacji Departamentu Wojny i przekazywał średnio 25 000 słów dziennie. Po ataku na Pearl Harbor, FBMS zyskała na znaczeniu i 26 lipca 1942 roku została przemianowana na Federalną Służbę Informacji Radiowej (ang. *Federal Broadcast Information Service*, FBIS). Po II wojnie światowej była bliska likwidacji, ale ostatecznie, po licznych interwencjach Departamentów Wojny i Stanu, została włączona do struktury Departamentu Wojny. Następnie została przeniesiona do swojej stałej siedziby jako część Centralnej Grupy Wywiadowczej (ang. *Central Intelligence Group*, CIG), która po przyjęciu ustawy o bezpieczeństwie narodowym w 1947 roku została przekształcona w Centralną Agencję Wywiadowczą (CIA). W tym samym czasie zmieniono nazwę Federalnej Służby Informacji Radiowej na Służbę Zagraniczną Informacji Radiowej (ang. *Foreign Broadcast Information Service*). Do nowych zadań organizacji należało monitorowanie zagranicznych nadawców o strategicznym znaczeniu, zakładanie stacji terenowych, nawiązywanie współpracy z zagranicznymi rządami, przygotowywanie tłumaczonych dziennych transkrypcji zagranicznych audycji oraz dystrybucja informacji zgodnie z zatwierdzonymi rozdzielnikiem. Dzięki doświadczeniom wyniesionym z okresu wojny organizacja sprawnie funkcjonowała, dysponując wiedzą operacyjną i przeszkolonym personelem.

Do lat dziewięćdziesiątych działalność FBIS skupiała się głównie na monitorowaniu i tłumaczeniu zagranicznych źródeł prasowych. Gromadzenie materiałów, charakterystyczne dla pierwszej generacji wywiadu jawnoźródłowego, było kluczowym elementem pracy FBIS. Stworzono sieć dwudziestu biur na całym świecie,

które zajmowały się zarówno fizycznym zbieraniem, jak i analizowaniem zagranicznych materiałów. FBIS zawierało również umowy o współpracę ze służbami monitorującymi innych krajów. Przykładem było porozumienie pomiędzy Stanami Zjednoczonymi a agencją brytyjską, na mocy którego obie strony zobowiązały się do współpracy i wymiany analiz. Na mocy porozumienia dokonano podziału obszarów geograficznych do monitorowania. FBIS zajmowało się Ameryką Południową oraz Dalekim Wschodem, natomiast British Broadcasting Corporation (BBC) monitorowało Azję Centralną i ZSRR. Materiały były również pozyskiwane od ambasad, które tworzyły platformy do ich zbierania, oraz od attaché obrony. Oprócz gromadzenia informacji, na podkreślenie zasługują również analizy prowadzone przez FBIS, przede wszystkim analiza trendów[302].

Stany Zjednoczone w czasie II wojny również monitorowały i analizowały media drukowane. Odpowiedzialność za prowadzenie wywiadu jawnoźródłowego w tym zakresie powierzono Międzywydziałowemu Komitetowi ds. Pozyskiwania Zagranicznych Czasopism, który zbudował globalną sieć, umożliwiającą skuteczne zdobywanie cennych publikacji, czego przykładem było nabycie 5000 chińskich książek w Chongqing w 1945 roku, przekazanych do Biblioteki Kongresu. Celem usprawnienia dostępu utworzono repozytorium i indeks wszystkich pozyskanych pozycji. W momencie zakończenia wojny zawierało 300 tys. fotografii, 350 tys. numerów czasopism, ponad milion map, 50 tys. książek oraz 300 tys. innych dokumentów.

Po zakończeniu II wojny światowej Stany Zjednoczone zdecydowały się na rozwój struktur zajmujących się wywiadem jawnoźródłowym. Utworzono Wydział Dokumentacji Zagranicznej, który był odpowiedzialny za analizę publicznie dostępnych dokumentów i prasy zagranicznej. W skład Biblioteki Kongresu wszedł również Obronny Wydział Badawczy, utworzony na wniosek Departamentu Lotnictwa. Początkowo jego działalność skupiała się na analizie materiałów drukowanych dotyczących techniki lotniczej, a następnie zakres analiz rozszerzono o aktualne zagadnienia międzynarodowe. W 1970 roku struktura ta została przemianowana na Federalny Wydział Badawczy, odpowiedzialny za analizę i specjalistyczne tłumaczenia materiałów pochodzących z zagranicy, którego analizy do dziś wspierają rząd USA.

[302] J. Niles Riddel, *The Role of the Foreign Broadcast Information Service in Open Source Intelligence*, 1992, https://irp.fas.org/fbis/riddel.html [dostęp: 3.11.2023].

Mimo że w okresie zimnej wojny dostęp do informacji jawnoźródłowych i ich wykorzystanie przez Stany Zjednoczone były ograniczone, FBIS odnosiła pewne sukcesy, dostarczając informacji wywiadowczych głównie poprzez analizę i tłumaczenie zagranicznych źródeł prasowych. Niektórzy autorzy szacują, że od 70 do 90 procent informacji na temat geograficznych, gospodarczych i naukowych trudności bloku sowieckiego pochodziło z analiz otwartych źródeł znajdujących się za żelazną kurtyną[303]. Podczas kryzysu kubańskiego praca FBIS odegrała kluczową rolę, dostarczając informacje niezbędne do podejmowania strategicznych decyzji wojskowych. Monitorowanie audycji Radia Moskwa przez FBIS ujawniło decyzję Nikity Chruszczowa o wycofaniu radzieckich rakiet z Kuby, co miało decydujący wpływ na przebieg wydarzeń. FBIS dostarczyło również istotnych informacji dotyczących wczesnych oznak wycofywania się wojsk radzieckich z Afganistanu oraz informacji, które pomogły w analizie i zrozumieniu tła kryzysów na Węgrzech i w Czechosłowacji.

Po zakończeniu zimnej wojny narastały kontrowersje wokół wywiadu jawnoźródłowego. Z jednej strony dostrzegano zmiany związane z dynamicznym rozwojem technologii, zasobów cyfrowych, wyszukiwarek internetowych i szerokopasmowych sieci komunikacyjnych, prowadzące do wzrostu komercjalizacji informacji[304]. Z drugiej strony, wywiad jawnoźródłowy postrzegano jako dziedzinę rozproszoną i zdecentralizowaną, w której podmioty często nie miały pełnej wiedzy na temat swoich własnych zasobów i możliwości. Większą wagę przywiązywano do informacji zdobywanych innymi metodami operacyjnymi, co wynikało między innymi z faktu, że podejmowane przez podmioty zajmujące się wywiadem jawnoźródłowym przedsięwzięcia były odizolowane od szerszych działań analitycznych wywiadu. FBIS nie dostosowywało swojej działalności do postępu technologicznego, co przejawiało się opóźnionym włączeniem takich źródeł jak szara literatura, komercyjne bazy danych oraz serwisy subskrypcyjne, a także brakiem systematycznego wykorzystania zasobów internetowych. W latach 90. administracja USA powołała specjalną komisję, nazwaną Komisją Aspina-Browna, od nazwisk jej dwóch przewodniczących, w celu zbadania roli i funkcjonowania amerykańskiej wspólnoty wywiadowczej po zakończeniu zimnej

[303] M.M. Lowenthal, R.N. Clark, *The Five Disciplines*…, op. cit., 2015, s. 16.
[304] J. Niles Riddel, *The Role of the Foreign Broadcast*…, op. cit.

wojny. Raport tej komisji[305], opublikowany w 1996 roku, miał na celu ocenę wyzwań, przed którymi stanęły amerykańskie agencje wywiadowcze w nowej rzeczywistości geopolitycznej. Komisja podkreśliła m.in. potrzebę priorytetowego wykorzystania informacji jawnoźródłowych oraz konieczność dostosowania działalności wywiadu do złożonych i wielowymiarowych zagrożeń, które pojawiły się po zakończeniu zimnej wojny. W odpowiedzi na te rekomendacje CIA utworzyła Biuro Programu Źródeł Otwartych Wspólnoty Wywiadowczej (ang. *Community Open Source Program Office*, COSPO) na podstawie zarządzenia wewnętrznego Dyrektora Centralnego Wywiadu. Biuro miało za zadanie rozwijać, koordynować i nadzorować działania służb wywiadu w zakresie źródeł otwartych, skupiając się na trzech kluczowych obszarach: stworzeniu wirtualnej sieci prywatnej Open Source Information System (OSIS), systemu jednokierunkowego transferu, który umożliwiał płynne przenoszenie jawnych informacji do stacji roboczych przeznaczonych do przetwarzania informacji niejawnych, oraz wirtualnej biblioteki World Basic Information Library (WBIL). Konkurujące FBIS doprowadziło do zamknięcia COSPO i groziło likwidacją OSIS. Jednakże protesty użytkowników z całej społeczności wywiadowczej skłoniły Dyrektora Centralnego Wywiadu do przeniesienia OSIS, co ostatecznie doprowadziło do przekształcenia systemu w sieć Intelink-U. Obecnie, pod nazwą DNI-U, stanowi ona główną platformę rozpowszechniania informacji jawnoźródłowych dla członków Wspólnoty Wywiadowczej oraz partnerów na poziomie federalnym, stanowym i lokalnym.

W latach 90 XX wieku COSPO utworzyło Międzynarodową Grupę Roboczą ds. Otwartego Wywiadu (ang. *International Open Source Working Group*, IOSWG) jako platformę współpracy dla wymiany OSINT między dwunastoma państwami: Australią, Kanadą, Danią, Francją, Niemcami, Wielką Brytanią, Izraelem, Włochami, Holandią, Norwegią, Szwecją i Stanami Zjednoczonymi[306]. Członkowie wzajemnie wymieniali się produktami wywiadu jawnoźródłowego oraz spotykali się na corocznych konferencjach i szkoleniach organizowanych przez partnerów. Współpraca w ramach IOSWG została ostatecznie zastąpiona umowami dwustronnymi.

Marynarka Wojenna Stanów Zjednoczonych dostrzegła wartość informacji jawnoźródłowych, szczególnie po tym, jak Departament Obrony Stanów

[305] Commission on the Roles and Capabilities of the U.S. Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, William J. Clinton Presidential Library & Museum, 1996, https://clinton.presidentiallibraries.us/items/show/36064 [dostęp: 12.03.2024].
[306] M.M. Lowenthal, R.N. Clark, *The Five Disciplines*…, op. cit., s. 37–38.

Zjednoczonych wykrył braki w polityce, doktrynie, szkoleniu i zarządzaniu w tej dziedzinie. W odpowiedzi na te wyzwania powołano radę ds. wywiadu jawnoźródłowego w resorcie obrony (ang. *Defense Open Source Council*)[307], która została ustanowiona jako główny organ odpowiedzialny za koordynację wywiadu jawnoźródłowego w Departamencie Obrony Stanów Zjednoczonych.

Po zamachu terrorystycznym na World Trade Center 11 września 2001 roku rozpoczęto dyskusję na temat restrukturyzacji służb wywiadowczych oraz ich metod działania. W raporcie Komisji 9/11, opublikowanym w 2004 roku, zalecano przede wszystkim reformę struktury wywiadowczej USA, w tym utworzenie podmiotu odpowiedzialnego za wywiad jawnoźródłowy[308]. Na mocy ustawy o reformie wywiadu i zapobieganiu terroryzmowi (ang. *Intelligence Reform and Terrorism Prevention Act*)[309], w 2004 r. ustanowiono Biuro Dyrektora Wywiadu Narodowego (Office of the Director of National Intelligence, ODNI). Biuro to zostało powołane jako organ nadzorczy dla całej Wspólnoty Wywiadu (ang. *Intelligence Community*, IC)[310], którego misją jest zapewnienie efektywności i spójności w działaniach wywiadowczych. ODNI ma również za zadanie integrowanie różnych elementów wywiadu, aby skuteczniej reagować na zagrożenia i zapewniać bezpieczeństwo Stanów Zjednoczonych.

W przywołanej ustawie zaakcentowano rolę i znaczenie wywiadu jawnoźródłowego dla bezpieczeństwa państwa, podkreślając konieczność jego integracji w cyklu wywiadowczym. W ustawie tej znalazły się również zapisy obligujące Dyrektora Wywiadu Narodowego do utworzenia centrum koordynującego wywiad jawnoźródłowy oraz do opracowania metod integracji tej formy wywiadu w cyklu wywiadowczym. Dyrektor Wywiadu Narodowego został zobligowany do utworzenia centrum koordynującego wywiad jawnoźródłowy oraz do opracowania metod integracji tej formy wywiadu w cyklu wywiadowczym. Ponadto, Dyrektor

[307] Department of Defense, *Department of Defense Instruction 3115.12, Open Source Intelligence (OSINT)*, August 24, 2010, s. 1.
[308] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, U.S. Government Printing Office, Washington, D.C. 2004, https://www.9-11commission.gov/report/911Report.pdf [dostęp: 12.03.2024].
[309] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3638 (2004).
[310] Wspólnota Wywiadowcza (ang. *Intelligence Community*, IC) to federacja 18 amerykańskich agencji wywiadowczych, w tym agencji cywilnych, wojskowych oraz biur wywiadowczych działających w ramach wybranych departamentów rządu federalnego. Została utworzona na mocy dekretu wykonawczego nr 12333, podpisanego 4 grudnia 1981 roku przez prezydenta Ronalda Reagana. W skład Wspólnoty wchodzi również Biuro Dyrektora Wywiadu Narodowego, które pełni funkcje administracyjne.

Wywiadu Narodowego był odpowiedzialny za zapewnienie, że gromadzenie i analiza informacji z otwartych źródeł były efektywnie i skutecznie wykorzystywane przez wspólnotę wywiadowczą zgodnie z ich misją oraz zakresem działania. Spełnieniem wymogów tej ustawy było utworzenie w 2005 r. Centrum Otwartych Źródeł (ang. *Open Source Center*, OSC), działającego w ramach CIA. Celem działania OSC było nie tylko pozyskiwanie i analiza materiałów jawnoźródłowych, ale również szkolenie w zakresie wykorzystywania i analizy otwartych źródeł, opracowywanie narzędzi oraz testowanie nowych technologii. W celu zapewnienia specjalistycznych szkoleń z zakresu analizy i pozyskiwania informacji z otwartych źródeł, OSC utworzyło Akademię Open Source, która oferowała szeroki wachlarz kursów i programów szkoleniowych. W pierwszym roku działalności OSC efektywność tej organizacji była wyraźnie widoczna, gdy znacząco wzrosła liczba produktów wywiadu jawnoźródłowego włączanych do codziennego briefingu dla Prezydenta USA[311]. To zjawisko świadczyło o rosnącym znaczeniu tej formy wywiadu w procesach decyzyjnych na najwyższym szczeblu. Rozwój Web 2.0, związany z dynamicznym wzrostem popularności internetu, mediów społecznościowych oraz nowymi sposobami korzystania z treści cyfrowych, doprowadził do istotnych zmian w dostępności danych jawnoźródłowych. Przejście od statycznych stron internetowych do treści generowanych przez użytkowników całkowicie zmieniło krajobraz informacyjny. OSC analizowało informacje pochodzące z mediów społecznościowych, w tym wpisy i komentarze zamieszczane przez osoby przebywające w strefach konfliktów i wojen. Przykładem takich analiz były dane zebrane podczas Arabskiej Wiosny oraz irańskiej Zielonej Rewolucji w 2009 roku, znanej również jako "Rewolucja Twittera", co ukazało znaczenie gromadzenia informacji wywiadowczych w czasie rzeczywistym i możliwości ich wykorzystania dla zapewnienia bezpieczeństwa.

W 2006 roku Departament Obrony USA po raz pierwszy sformułował definicję wywiadu jawnoźródłowego w ustawie o upoważnieniu do wydatkowania funduszy na rzecz obrony narodowej (ang. *National Defense Authorization Act*)[312], jako „wywiad oparty na publicznie dostępnych informacjach, które są zbierane, analizowane i rozpowszechniane w odpowiednim czasie właściwym odbiorcom, aby spełnić konkretne potrzeby wywiadowcze”.

[311] M.M. Lowenthal, R.N. Clark, *The Five Disciplines*…, op. cit., 2015, s. 21.
[312] *National Defense Authorization Act for Fiscal Year 2006*, Pub. L. No. 109-163, 119 Stat. 3136 (2006).

Od 2015 roku OSC działa pod nową nazwą Open Source Enterprise (OSE) i jest częścią Dyrektoriatu Innowacji Cyfrowych (ang. *Directorate of Digital Innovation*) w Centralnej Agencji Wywiadowczej. OSE zajmuje się zbieraniem i analizą informacji ze wszystkich otwartych źródeł, takich jak telewizja, radio, prasa internet, w tym media społecznościowe takie jak Twitter i Facebook, a także platformy komunikacyjne. Organizacja ta przetwarza również materiały z konferencji, raporty ośrodków badawczych i opinie ekspertów. Zakres zbieranych informacji obejmuje m.in. monitorowanie bieżących wydarzeń na świecie, analizę nastrojów społecznych oraz kryzysów politycznych i gospodarczych. Analitycy OSE pracują zarówno w głównej siedzibie CIA, jak i w placówkach dyplomatycznych Stanów Zjednoczonych za granicą. Pozyskiwane dane są tłumaczone na język angielski i przesyłane do centrali za pomocą systemu Open Source System (OSS). Głównymi odbiorcami informacji OSE są najważniejsze instytucje rządowe, takie jak np.: Biały Dom, który wykorzystuje te dane do formułowania polityki krajowej i zagranicznej, Wspólnota Wywiadowcza USA, która koordynuje działania wywiadowcze i bezpieczeństwa narodowego, Departament Obrony, odpowiedzialny za strategię obronną i operacje militarne, Departament Stanu, który kształtuje politykę zagraniczną USA, oraz Departament Skarbu, który analizuje informacje finansowe i gospodarcze. Dzięki tej strukturze, OSE wspiera podejmowanie decyzji na najwyższym szczeblu poprzez dostarczanie bieżących analiz i prognoz, co pozwala na szybkie reagowanie na zmieniającą się sytuację międzynarodową i krajową.

W marcu 2024 roku Biuro Dyrektora Wywiadu Narodowego oraz CIA podjęło działania mające na celu sformalizowanie podejścia do wykorzystania otwartych źródeł informacji, które zostały sformułowane w „Strategii OSINT na lata 2024-2026”[313]. Dokument ten przedstawia kompleksową wizję usprawnienia gromadzenia i wykorzystania danych jawnoźródłowych do celów wywiadowczych. Strategia zawiera definicję OSINT, która nieznacznie różni się od przyjętego dotychczas formułowania wywiadu jawnoźródłowego. OSINT został określony w strategii jako dane wywiadowcze pochodzące z publicznie (ang. *publicly available information*, PAI) lub komercyjnie (ang. *commercially available information*, CAI) dostępnych informacji, mające na celu spełnienie określonych wymagań lub uzupełnienie luk wywiadowczych. Ujęcie komercyjnych źródeł informacji poszerza dotychczasowe możliwości gromadzenia informacji jawnoźródłowych biorąc pod uwagę rozwijające się

[313] *IC OSINT Strategy 2024-2026*, dokument jawny, Biuro Dyrektora Wywiadu Narodowego, 2024.

możliwości zakupu materiałów online jak np. czasopisma naukowe, zdjęcia satelitarne, raporty czy bazy danych. W strategii podkreślono znaczenie aktualnych, istotnych i specjalistycznych danych z otwartych źródeł, które usprawniają i wspomagają proces decyzyjny w obszarze bezpieczeństwa państwa, ochrony narodu i jego interesów oraz współpracy z partnerami USA. Dla rozwoju wywiadu jawnoźródłowego jako istotne wskazano zarówno skuteczne zarządzanie w środowisku wywiadowczym, jak i współpracę z sektorem przemysłowym, środowiskiem akademickim oraz zagranicznymi partnerami. Za implementację strategii, jak i też działania OSINT w ramach amerykańskiej wspólnoty wywiadu odpowiedzialny jest Dyrektor CIA. Treść i realizacja strategii mają podlegać corocznym przeglądom oraz uzupełnieniom w zależności od ewolucji uwarunkowań środowiska jawnoźródłowego. Każdego roku będzie również opracowywany iteracyjny plan działania, aby ukierunkowywać wdrożenie strategii. W dokumencie wyróżniono cztery obszary strategiczne.

Pierwszy z nich to koordynacja pozyskiwania danych z otwartych źródeł i rozszerzenie ich udostępniania. W tym obszarze dąży się do usprawnienia gromadzenia danych jawnoźródłowych, aby ograniczyć sytuacje, w których różne podmioty zaangażowane są w te same zagadnienia, oraz umożliwić realizację zadań statutowych i maksymalne wykorzystanie zasobów wywiadu. Zgodnie z wytycznymi Dyrektora Wywiadu Narodowego zostanie wdrożona platforma CAI, która będzie śledzić publicznie oraz komercyjnie dostępne informacje z otwartych źródeł w scentralizowanym, wielodomenowym katalogu danych. Celem tego rozwiązania jest zwiększenie transparentności procesów analitycznych oraz poprawa dostępności danych. W celu usprawnienia zarządzania danymi zostaną opracowane standardy interoperacyjności i tagowania, co ma zapewnić ich przystępne i terminowe dostarczanie. Dodatkowo, powstaną wspólne platformy do wymiany informacji z otwartych źródeł, raportów oraz narzędzi wywiadu jawnoźródłowego. Nacisk położony w strategii na gromadzenie informacji jawnoźródłowych wynika z potrzeby efektywnego wykorzystania zasobów 18 agencji wywiadowczych w Stanach Zjednoczonych. Często agencje te realizują zbieżne cele, co prowadzi do duplikacji działań oraz wielokrotnego zakupu tych samych danych. Jednocześnie różne agencje wywiadowcze mają różne uprawnienia, dlatego nawet dane pochodzące ze źródeł otwartych, zgodnie z zasadą "wiedzy niezbędnej", muszą być przetwarzane z obowiązującymi regulacjami dotyczącymi dostępu do informacji. W tym obszarze zaznaczono również potrzebę zidentyfikowania i wdrożenia metod bezpiecznego

dostarczania produktów wywiadu jawnoźródłowego do szerszego grona odbiorców w administracji rządowej USA. Systemy stosowane do przekazywania informacji niejawnych, które posiadają poświadczenia bezpieczeństwa, są kosztowne, a ich tworzenie jest czasochłonne. Charakter informacji jawnoźródłowych implikuje potrzebę odrębnego systemu dystrybucji tych danych, który usprawni ich przekazywanie do odpowiednich organów państwowych i agencji federalnych. Rozszerzenie udostępniania danych, przy jednoczesnym przestrzeganiu norm etycznych, prawnych oraz zasad bezpieczeństwa, ma na celu maksymalizację zwrotu z nakładów wspólnoty wywiadowczej oraz zwiększenie wartości danych i narzędzi wywiadu jawnoźródłowego.

Drugim obszarem wyróżnionym w Strategii jest ustanowienie zintegrowanego zarządzania zasobami informacji jawnoźródłowych. Strategia wzywa do lepszej koordynacji w zakresie gromadzenia danych jawnoźródłowych, aby zwiększyć szybkość i skuteczność ich pozyskiwania oraz uniknąć redundancji. Podkreślona została konieczność optymalizacji procesu pozyskiwania tych danych w celu spełnienia zróżnicowanych i zmieniających się wymogów bezpieczeństwa narodowego oraz zadań wspólnoty wywiadów. W związku z tym zalecono opracowanie wspólnych standardów i protokołów, aby wspierać współpracę między agencjami. Ponadto zaznaczono, że istotne jest wdrożenie nowoczesnych narzędzi analitycznych umożliwiających efektywne przetwarzanie i analizę danych. Założono również przeprowadzenie regularnych przeglądów i audytów procesów zbierania danych jawnoźródłowych, aby zapewnić zgodność z obowiązującymi przepisami prawa i najlepszymi praktykami.

Trzeci obszar wyróżniony w strategii koncentruje się na promowaniu innowacji technologicznych w celu dostarczania nowych możliwości dla podmiotów korzystających z wywiadu jawnoźródłowego. aby utrzymać zdolność do terminowego dostarczania na dużą skalę wiarygodnych informacji jawnoźródłowych decydentom politycznym i dowódcom sił zbrojnych. Podkreślono konieczność ciągłej adaptacji narzędzi i metodologii, aby zachować zdolność dostarczania wiarygodnych informacji jawnoźródłowych, wspierających decydentów politycznych oraz dowódców sił zbrojnych, terminowo i na dużą skalę. Informacje te muszą być dostępne w zróżnicowanych formatach, odpowiednio dostosowanych do specyficznych potrzeb i wymagań różnych odbiorców.

Przyspieszenie wprowadzania innowacji związane jest z możliwością wykorzystania systemów jawnych do testowania nowych technologii, które

charakteryzują się niższym ryzykiem i mniejszymi barierami niż sieci dedykowane do przesyłania informacji objętych klauzulą tajności. Narzędzia wywiadu jawnoźródłowego, wykorzystujące zaawansowane technologie obliczeniowe i sztuczną inteligencję, mogą nie być jeszcze gotowe do wdrożenia w systemach niejawnych. Na tempo opracowywania, testowania i wdrażania nowoczesnych narzędzi ma zasadniczy wpływ współpraca z sektorem prywatnym i środowiskiem akademickim.

Ostatnim obszarem strategii jest kształcenie specjalistów oraz doskonalenie metodologii wywiadu jawnoźródłowego. W odpowiedzi na dynamiczny rozwój tej dziedziny, zarekomendowano wprowadzenie jednolitych standardów oraz programów szkoleniowych dotyczących identyfikacji, pozyskiwania i analizy informacji z otwartych źródeł. Strategia podkreśla także istotną rolę generatywnej sztucznej inteligencji (ang. *Generative Artificial Intelligence*), zwracając uwagę zarówno na możliwości, jak i potencjalne zagrożenia wynikające z jej zastosowania w wywiadzie jawnoźródłowym. Generatywna sztuczna inteligencja może zoptymalizować oraz przyspieszyć procesy pozyskiwania i analizy informacji jawnoźródłowych, umożliwiając identyfikację wspólnych tematów lub wzorców w danych oraz zautomatyzowane podsumowywanie dużych zbiorów tekstów. W dokumencie wskazano, że amerykańska wspólnota wywiadowcza powinna priorytetowo traktować testowanie i rozwijanie technologii sztucznej inteligencji, aby efektywnie wykorzystać jej potencjał i dostosować metodologie wywiadu jawnoźródłowego do zmieniającego się środowiska technologicznego.

Strategia OSINT na lata 2024-2026 jest pierwszym w historii Stanów Zjednoczonych dokumentem, który jasno określa priorytety oraz kierunki rozwoju wywiadu jawnoźródłowego mając na celu wzmocnienie jego roli w zapewnianiu wsparcia decydentom politycznym oraz działaniom operacyjnym. Stanowi istotny krok w reintegracji wywiadu jawnoźródłowego oraz uznaniu jego wartości przez analityków i decydentów. Chociaż jawna wersja Strategii jest ograniczona pod względem szczegółowości, dostarcza jednak istotnych informacji na temat podstawowych wyzwań, przed którymi stoi amerykańska wspólnota wywiadowcza.

Uzupełnieniem Strategii OSINT 2024-2026 jest dokument przygotowany i opublikowany w maju 2024 roku przez Biuro Departamentu Stanu USA ds. Wywiadu, Analiz i Prognoz Politycznych (ang. *Bureau of Intelligence and Research*, INR), którego celem jest zwiększenie roli wywiadu jawnoźródłowego w wspieraniu dyplomatów oraz decydentów politycznych. We wstępie dokumentu podkreślono, że

zmiana definicji wywiadu jawnoźródłowego zaproponowana w Strategii OSINT na lata 2024-2026 implikuje zmianę funkcjonowania amerykańskiej wspólnoty wywiadowczej. Informacje jawnoźródłowe są uznawane za „nieoceniony zasób", wzbogacający analizy oraz wspierający działania wywiadowcze i dyplomatyczne. Zapewniają one amerykańskim dyplomatom na całym świecie szerszy dostęp do produktów Departamentu Stanu USA ds. Wywiadu, Analiz i Prognoz Politycznych, które nie są objęte klauzulą tajności. Zapotrzebowanie na jawne produkty i usługi oferowane przez ten Departament będzie rosło w miarę zwiększania się ilości dostępnych informacji jawnoźródłowych. Pierwszym celem wskazanym w strategii jest ustanowienie zarządzania i polityki dotyczącej wykorzystania wywiadu jawnoźródłowego poprzez opracowanie i przyjęcie skutecznych ram, standardów i procedur zgodnych z wymogami prawnymi, a także monitorowanie i ocena wszystkich prowadzonych działań. Drugi cel koncentruje się na inwestycjach w zdolności wywiadu, obejmujących rozwój i realizację planowania budżetowego, procesy pozyskiwania, wdrażania i adaptacji narzędzi oraz platform OSINT, a także nabywanie nowoczesnych technologii i rozszerzanie dostępu do danych. Trzeci cel zawarty w Strategii INR obejmuje rozwój szkoleń i doskonalenie umiejętności w zakresie wywiadu jawnoźródłowego poprzez utworzenie dedykowanego programu edukacyjnego. Założenia tego programu koncentrują się na rozwijaniu kluczowych kompetencji technicznych i metodologicznych, które są niezbędne do skutecznego zbierania, przeglądania oraz analizowania informacji jawnoźródłowych. Jako czwarty cel wskazano nawiązanie oraz zacieśnienie współpracy z sojusznikami, a także wymianę najlepszych praktyk z partnerami z sektora przemysłowego, środowisk akademickich oraz innymi podmiotami pozarządowymi, aby stale aktualizować wiedzę i umiejętności w zakresie pozyskiwania i analizy danych jawnoźródłowych.

Wywiad jawnoźródłowy intensywnie rozwija się w amerykańskim sektorze prywatnym, gdzie specjalistyczne firmy opracowują narzędzia i usługi OSINT. Podmioty publiczne dostrzegły ten potencjał, czego dowodem było utworzenie w 1999 roku przez CIA In-Q-Tel. Firma ta działa jako *venture capital*, a jej celem jest wspieranie rozwoju technologii w dziedzinach takich jak bezpieczeństwo, analiza danych, sztuczna inteligencja i cyberbezpieczeństwo, na potrzeby społeczności wywiadowczej Przewaga sektora prywatnego wynika z mniej rygorystycznych obostrzeń prawnych i ograniczeń finansowych, co umożliwia szybsze wdrażanie nowych technologii oraz wykorzystanie konkurencyjności rynku cyfrowego.

Konieczność współpracy instytucji rządowych Stanów Zjednoczonych z sektorem prywatnym w zakresie bezpieczeństwa jest wyraźnie akcentowana w amerykańskich strategiach bezpieczeństwa. Wymaga to jednak wprowadzenia regulacji prawnych dotyczących bezpieczeństwa danych, ochrony prywatności oraz standardów etycznych. Przykładem kooperacji podmiotów rządowych Stanów Zjednoczonych z sektorem prywatnym jest inwestycja CIA poprzez In-Q-Tel w firmę Recorded Future, która rozwija narzędzia do analizy predykcyjnej wspierające działania wywiadowcze[314]. U.S. Cyber Command, w ramach programu „Under Advisement"[315], współpracuje z prywatnymi firmami, co umożliwia wymianę kluczowych informacji w celu przeciwdziałania zagrożeniom cybernetycznym, natomiast Praescient Analytics[316] dostarcza zaawansowane narzędzia OSINT do analizy danych z otwartych źródeł, wspierając efektywne udostępnianie produktów wywiadowczych.

Ewolucja podejścia do wywiadu jawnoźródłowego w Stanach Zjednoczonych zachodziła zarówno w Wspólnocie Wywiadu, jak i w sektorze prywatnym. Do czasów zimnej wojny OSINT stopniowo zyskiwał na znaczeniu, jednak później jego rola zaczęła być deprecjonowana. Ograniczony dostęp do informacji jawnoźródłowych oraz wykształcenie przekonania, że gromadzenie i wykorzystywanie informacji metodami operacyjnymi ma wyższą wartość, wpłynęły na preferencje pracowników służb specjalnych. Takie podejście miało podkreślać wyjątkowość amerykańskiej społeczności wywiadowczej w porównaniu z innymi podmiotami rządowymi i pozarządowymi. Kongres nieregularnie finansował OSINT, co wpływało na dostępność zasobów jawnoźródłowych dla służb wywiadowczych. W szkoleniach nowych analityków często pomijano znaczenie tych informacji, co prowadziło zarówno do ich niedoceniania, jak i braku możliwości analizy i wartościowania. Kultura przestrzegania prawa w instytucjach rządowych ograniczała ich konkurencyjność w stosunku do sektora prywatnego. Wyzwania związane z finansowaniem Wspólnoty Wywiadowczej obejmują pozyskiwanie i zabezpieczanie zbiorów danych oraz tworzenie narzędzi wykorzystujących sztuczną inteligencję. Partnerstwo między sektorem publicznym a prywatnym jest istotne dla wzmacniania działań w zakresie bezpieczeństwa Stanów Zjednoczonych, zwłaszcza wobec zagrożeń wynikających

[314] Blackdot Solutions, *Leveraging OSINT for Public-Private Partnerships*, https://blackdotsolutions.com/blog/leveraging-osint-for-public-private-partnerships/ [dostęp: 20.01.2024].
[315] U.S. Cyber Command, *Private Sector Partnerships*, https://www.cybercom.mil/Partnerships-and-Outreach/Private-Sector-Partnerships/ [dostęp: 23.01.2024].
[316] Praescient Analytics, *Why OSINT Matters to the Intelligence Community*, https://praescientanalytics.com/why-osint-matters-to-the-intelligence-community/ [dostęp: 23.01.2024].

z nowych technologii oraz wyzwań związanych z bezpieczeństwem zdrowotnym, żywnościowym, humanitarnym, energetycznym oraz migracją. Współpraca ta jest również istotna w kontekście konfliktu na Ukrainie oraz strategicznej rywalizacji Stanów Zjednoczonymi z Chinami i Rosją[317].

5.2. Wywiad jawnoźródłowy w Wielkiej Brytanii

Wielka Brytania ma najdłuższą udokumentowaną historię wywiadu jawnoźródłowego, która związana jest z postępem technologicznym oraz zmieniającymi się potrzebami wywiadowczymi kraju. Rząd brytyjski systematycznie włącza szczegółowe badania nad wywiadem jawnoźródłowym do swojego arsenału wywiadowczego. Już w okresie wiktoriańskim departamenty wywiadu alokowały odrębne środki na gromadzenie informacji z ogólnodostępnych źródeł, co może być uznawane za początek wyodrębniania się wywiadu jawnoźródłowego w Wielkiej Brytanii. Na przełomie XIX i XX wieku powstały komercyjne firmy specjalizujące się w pozyskiwaniu, analizowaniu i tworzeniu baz danych z informacji jawnych. Jednym z pionierów w tej dziedzinie było wydawnictwo założone przez Fred T. Jane, które rozpowszechniało rocznik „All the World's Fighting Ships". Publikacja ta była innowacyjna, ponieważ zawierała szczegółowe dane techniczne oraz ilustracje okrętów wojennych z całego świata, co ułatwiało ich identyfikację na morzu. Atlas ten stał się źródłem informacji dla wywiadów marynarek wojennych, umożliwiając rozpoznawanie okrętów na podstawie ich sylwetek oraz cech konstrukcyjnych.

Na początku I wojny światowej rząd brytyjski utworzył „Wellington House", znane również jako „War Propaganda Bureau", którego zadaniem było prowadzenie kampanii propagandowych mających na celu promowanie interesów Wielkiej Brytanii i przeciwdziałanie niemieckiej propagandzie. Biuro wykorzystywało otwarte źródła, w tym prasę i książki, do gromadzenia informacji o nastrojach opinii publicznej oraz tworzenia propagandowych broszur i artykułów.

W 1939 roku w ramach BBC utworzono komercyjny serwis Digest of Foreign Broadcasts (Przegląd Audycji Zagranicznych), następnie przemianowany na Summary of World Broadcasts (Podsumowanie Wiadomości ze Świata), a obecnie emitowany jako BBC Monitoring Service. Była to pierwsza komórka wywiadu jawnoźródłowego

[317] Office of the Director of National Intelligence*, Annual Threat Assessment of the U.S. Intelligence Community*, February 5, 2024, s. 2 i nast.

o zasięgu międzynarodowym dokonująca analiz informacji pochodzących z prasy i radia na potrzeby służb specjalnych oraz rządu. W połowie 1943 roku BBC monitorowało 1,25 miliona słów dziennie, dostarczając informacji na temat prowadzonych operacji wojskowych[318]. BBC Monitoring Service analizowało audycje propagandowe zarówno państw Osi, jak i aliantów, co pozwalało na ocenę treści, tonu oraz przekazu propagandowego. Dzięki temu możliwe było zdobycie informacji na temat planów wroga, jego morale oraz prób wpływania na opinię publiczną. Pozyskany materiał wspierał działania aliantów w zakresie kontrpropagandy poprzez ujawnianie niespójności i fałszywych informacji. BBC Monitoring dostarczał raporty m.in. do Ministerstwa Wojny Ekonomicznej, Ministerstwa Spraw Zagranicznych, Biura Indii, Biura Kolonialnego, Ministerstwa Informacji, Admiralicji, Ministerstwa Lotnictwa oraz służb specjalnych, w tym MI5[319]. Komórki wywiadu jawnoźródłowego Zjednoczonego Królestwa działały również za granicą. Do pozyskiwania informacji z lokalnej prasy angażowano dziennikarzy, którzy analizowali artykuły i przesyłali raporty o rozmieszczeniu wojsk niemieckich.

Po zakończeniu wojny BBC Monitoring znacząco rozszerzyło swój zasięg i zróżnicowało kategorie monitorowanych źródeł. W miarę postępu technologicznego i zmian geopolitycznych, działalność ta objęła transmisje telewizyjne, media internetowe oraz sieci społecznościowe. Obecnie BBC Monitoring dostarcza informacji wywiadowczych w ramach OSINT dla rządów, przedsiębiorstw oraz środowisk naukowych. W brytyjskich dokumentach rządowych wielokrotnie podkreślano znaczenie pracy BBC Monitoring, szczególnie w kontekście dostarczania rzetelnych, wieloźródłowych raportów, które wspierają formułowanie polityki oraz podejmowanie decyzji strategicznych[320].

W okresie II wojny światowej, z inicjatywy Królewskiego Instytutu Spraw Międzynarodowych, utworzono Służbę Badań i Prasy Zagranicznej (ang. *Foreign Research and Press Service*, FRPS), która później została przemianowana na Departament Badań Ministerstwa Spraw Zagranicznych (ang. *Foreign Office Research Department*, FORD).

---

[318] F. Schaurer, J. Strörger, *The Evolution of Open Source Intelligence (OSINT)*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2012, vol. 19, no. 3, s. 53.
[319] L.M. Calkins, *Patrolling the Ether: US–UK Open-Source Intelligence Cooperation and the BBC's Emergence as an Intelligence Agency*, 1939–1948, „Intelligence and National Security" 2011, vol. 26, no. 1, s. 3.
[320] Zob. Her Majesty's Government, *BBC Monitoring: Evidence to the Defence and Foreign Affairs Committees*, 2016, https://committees.parliament.uk/writtenevidence/74950/pdf/ [dostęp: 8.10.2023].

Organizacja ta koncentrowała się na pozyskiwaniu informacji jawnoźródłowych z całego świata, w tym z terenów okupowanych przez Rzeszę Niemiecką w Związku Radzieckim, które stanowiły podstawowe źródło wywiadowcze dostępne dla rządu brytyjskiego. Analiza zagranicznej prasy oraz audycji radiowych dostarczała cennych informacji na temat sytuacji na froncie wschodnim oraz w okupowanych krajach, umożliwiając brytyjskim analitykom lepsze zrozumienie działań wroga i przewidywanie jego kolejnych posunięć. Sir Harry Hinsley, historyk brytyjskiego wywiadu, zauważył, że około trzy piąte wszystkich raportów sporządzonych podczas II wojny światowej przez Wydział ds. Przeciwnika w Ministerstwie Wojny Ekonomicznej (ang. *Enemy Branch of the Ministry of Economic Warfare*) opierało się na prasie, audycjach radiowych i oficjalnych oświadczeniach[321]. Wywiad jawnoźródłowy dostarczał nie tylko informacji wojskowych, ale także danych gospodarczych i społecznych istotnych dla brytyjskiego rządu, szczególnie w kontekście przygotowania strategii powojennej.

W okresie zimnej wojny władze Wielkiej Brytanii, podobnie jak inne kraje, tworzyły obszerne archiwa informacji jawnych, gromadzonych z drukowanych magazynów, książek i gazet. W latach 90. XX wieku, w wyniku postępu technologicznego oraz rosnącej dostępności źródeł otwartych, wzrosło znaczenie wywiadu jawnoźródłowego w brytyjskich siłach zbrojnych. OSINT zaczął odgrywać istotną rolę w operacjach wojskowych, często służąc do weryfikacji informacji uzyskanych z tajnych źródeł wywiadowczych.

Po zakończeniu drugiej wojny światowej Wielka Brytania zawarła ze Stanami Zjednoczonymi porozumienie dotyczące współpracy w zakresie wywiadu elektronicznego. W późniejszym okresie do porozumienia przystąpiły Australia, Kanada oraz Nowa Zelandia, co doprowadziło do powstania Sojuszu Pięciorga Oczu (ang. *Five Eye*). Organizacja ta od początku uwzględniała również wymianę informacji jawnoźródłowych, adaptując wykorzystywane metody i środki do zmieniających się uwarunkowań technologiczno-społecznych. Sojusz monitoruje przestrzeń terytorialną, obszary morskie oraz powietrzno-kosmiczne, dostosowując swoje operacje do współczesnych wyzwań w zakresie bezpieczeństwa, takich jak terroryzm, szpiegostwo, cyberataki oraz działania wrogich państw. Współczesne operacje wywiadowcze „Five Eyes" w coraz większym stopniu opierają się na wywiadzie jawnoźródłowym[322].

[321] F. Hinsley, *British Intelligence in the Second World War: Vol. 2*, HMSO, London 1981, s. 130–131.
[322] F. Schaurer, J. Störger, *The Evolution*…, op. cit., s. 53.

Wymiana informacji jawnoźródłowych stanowi istotny element wsparcia członków sojuszu w działaniach przeciwko konkurencyjnym i wrogim państwom, zgodnie z pierwotnymi założeniami jego działalności. Sojusz podkreśla konieczność zachowania równowagi między wymaganiami operacyjnymi a zasadami demokratycznych społeczeństw. Wielka Brytania jest również stroną międzynarodowego sojuszu wywiadowczego o nazwie Sojusz Czternastu Oczu (ang. *Fourteen Eyes*), który oprócz "Five Eyes" obejmuje dodatkowo Danię, Francję, Holandię, Norwegię, Niemcy, Belgię, Włochy, Hiszpanię i Szwecję. Kraje te angażują się we współpracę w zakresie wymiany analiz jawnoźródłowych. Wielka Brytania brała udział w różnych wielostronnych inicjatywach Unii Europejskiej dotyczących wymiany informacji jawnoźródłowych, które zostały renegocjowane po Brexicie. Współpraca w zakresie wywiadu jawnoźródłowego jest również kontynuowana w ramach NATO.

Rozwój technologii cyfrowych oraz Internetu znacząco zmieniły metody pozyskiwania informacji. W odpowiedzi na te zmiany, nie tylko służby specjalne i wojsko, ale również brytyjska policja oraz organy ścigania zaczęły dostrzegać potrzebę uwzględniania informacji jawnoźródłowych w swojej pracy. W Wielkiej Brytanii służby specjalne nie prowadzą działań śledczych, dlatego końcowa faza operacji jest często realizowana przez policję, która w swojej działalności wykorzystuje OSINT. Takie pragmatyczne podejście wynika z faktu, że koszt pozyskiwania informacji za pomocą wywiadu jawnoźródłowego jest znacząco niższy niż w przypadku tradycyjnych metod operacyjnych. Znalazło to odzwierciedlenie w opracowywanych przepisach prawa oraz aktach normatywnych wykorzystywanych w działalności policji brytyjskiej. Metropolitan Police utworzyła jednostkę ds. otwartych źródeł (ang. *Open Source Unit*), która specjalizowała się w gromadzeniu i analizie informacji dostępnych publicznie. Była to jedna z pierwszych formalnych struktur policyjnych tego typu w Wielkiej Brytanii. Jednostka ta wykorzystywała zalety informacji z otwartych źródeł, takie jak szybkość, efektywność, dostępność i niskie koszty, wspierając tym samym zarówno strategiczne, jak i taktyczne działania policji[323]. W 2019 roku Krajowa Rada Szefów Policji (NPCC) wydała wytyczne dotyczące korzystania z wywiadu jawnoźródłowego przez organy ścigania w Wielkiej Brytanii. Dokument ten podkreśla

[323] S. Ramwell, T. Day, H. Gibson, *Use Case and Best Practise for LEAs*, [w:] B. Akghar, S. Bayerl, F. Sampson (eds.), *Open Source Intelligence Investigation. From Strategy to Implementation*, Springer, 2016, s. 198.

znaczenie etycznego i zgodnego z prawem wykorzystywania OSINT oraz konieczność odpowiednich szkoleń i posiadania specjalistycznej wiedzy.

Rząd Wielkiej Brytanii od wielu lat uwzględnia wywiad jawnoźródłowy jako element swoich działań na rzecz bezpieczeństwa narodowego oraz egzekwowania prawa. W 2011 roku Ministerstwo Obrony Wielkiej Brytanii zdefiniowało wywiad jawnoźródłowy jako wywiad uzyskiwany z publicznie dostępnych informacji o ograniczonym dostępie lub dystrybucji[324]. Stwierdzono, że materiał OSINT jest szczególnie przydatny w analizach mających na celu potwierdzenie, że uzyskane dane wywiadowcze są bezstronne i wolne od uprzedzeń. Ponadto podkreślono, że materiał z otwartych źródeł jest nie mniej ważny niż materiały klauzulowane. W ten sposób podkreślono, że wywiad jawnoźródłowy stanowi jedną z dyscyplin wywiadowczych.

NPCC zdefiniowała wywiad jawnoźródłowy jako gromadzenie, ocenę i analizę materiałów dostępnych ze źródeł publicznych, zarówno odpłatnie, jak i nieodpłatnie, w celu wykorzystania ich jako danych wywiadowczych lub dowodów w dochodzeniu. Za źródła otwarte uznano publicznie dostępne informacje, które każdy może zgodnie z prawem uzyskać na podstawie wniosku lub obserwacji. Należą do nich książki, gazety, czasopisma, transmisje telewizyjne i radiowe, wiadomości, internet (WWW i grupy dyskusyjne), mapy, obrazy, fotografie, komercyjne subskrypcyjne bazy danych oraz szara literatura (materiały konferencyjne i raporty instytutów). Definicja zaproponowana przez policję jest szersza i bardziej szczegółowa niż ta, zaproponowana przez Ministerstwo Obrony Wielkiej Brytanii. Wynika to z wykorzystywania przez brytyjską policję informacji jawnoźródłowych jako potencjalnych dowodów lub materiałów uzupełniających dowody pochodzące z innych źródeł. Pozyskiwanie i analiza informacji jawnoźródłowych przez brytyjską policję są bardziej ustrukturyzowane i ukierunkowane niż w wojsku czy służbach. Jest to częściowo spowodowane większym naciskiem na gromadzenie dowodów oraz wymogiem, aby te dowody były wiarygodne i mogły być skutecznie wykorzystane w sądzie. Co jest również istotne, sposób działania policji w Wielkiej Brytanii opiera się na zaufaniu społeczeństwa do działań policji oraz przekonaniu o potrzebie udzielania pomocy policji przez społeczeństwo w zakresie zapewnienia bezpieczeństwa publicznego. Związane jest to ukształtowanym przez historię oraz czynniki społeczno-ekonomiczne

[324] Ministerstwo Obrony Narodowej Wielkiej Brytanii, *UK Defence Doctrine (JDP 0-01)*, 2011. Doktryna jest regularnie aktualizowana w celu uwzględnienia nowych wyzwań technologicznych, operacyjnych i geopolitycznych. Ostatnia, szósta wersja, została wydana w 2022 roku.

założeniem sformułowanym przez Sir Roberta Peelow, że „policja to społeczeństwo a społeczeństwo to policja". Zarówno w definicji Ministerstwa Obrony, jak i Krajowej Rady Szefów Policji, obszarem, który może budzić wątpliwości prawne i etyczne jest sposób w jaki gromadzone są informacje jawnoźródłowe. Praktyka policyjna wskazuje, że dane, mimo iż pochodzą ze źródeł publicznych są pozyskiwane w sposób, w którym granica pomiędzy jawnym gromadzeniem informacji a kombinacją operacyjną jest rozmyta. Szczególnie dochodzenia prowadzone w mediach społecznościowych mogą polegać na pozyskiwanie informacji bez informowania użytkowników o przeglądaniu pobieraniu czy gromadzeniu ich danych. Jest to forma niejawnej inwigilacji, która wymaga transparentnych rozwiązań zarówno legislacyjnych jak i organizacyjnych. W wytycznych Krajowej Rady Szefów Policji dotyczących dochodzeń prowadzonych ze źródeł otwartych wyróżniono pięć poziomów dochodzenia. Jedynie dochodzenia na poziomie pierwszym są określane jako jawne. Dochodzenia na czterech pozostałych poziomach, tj. dochodzenia podstawowe, zaawansowane, dochodzenia w Darknecie oraz dochodzenia tajne, ze względu na konieczne uprawnienia, metody i środki ich prowadzenia są tajne. Wytyczne mają na celu zapewnienie spójności, skuteczności i legalności działań operacyjnych, a także maksymalizację korzyści płynących z wykorzystania dostępnych informacji w procesie dochodzeniowym. Opisane w tych dokumentach taktyki pozyskiwania informacji jawnoźródłowych, poprzez podszywanie się lub infiltracji stron internetowych, znacznie poszerzają definicję pojęcia publicznego dostępu do danych oraz podważają jawne metody pozyskiwania informacji charakterystyczne dla wywiadu jawnoźródłowego. Pozyskiwanie informacji jawnoźródłowych przy zastosowaniu metod i środków wskazanych na poziomie niejawnym musi być również zgodne z wytycznymi w zakresie prowadzenia tajnych dochodzeń w internecie zawartych w dokumentach opracowanych zarówno przez Krajową Radę Szefów Policji[325], Stowarzyszenie Głównych Oficerów Policji Anglii, Walii i Irlandii Północnej (ACPO)[326], jak i Kolegium Policji[327]. Dokumenty te podkreślają, że tajne działania w internecie mogą być podejmowane jedynie wtedy, gdy są konieczne i proporcjonalne do osiągnięcia celów konkretnej sprawy oraz prowadzone zgodnie z obowiązującymi przepisami o ochronie danych osobowych i prywatności

[325] National Police Chiefs' Council, 2015, *NPCC Guidance On Open Source Investigations*; National Police Chiefs' Council, 2019, *Internet Intelligence & Investigations Strategy*; National Police Chiefs' Council, 2023, *NPCC Internet Intelligence & Investigations Guidance On Covert Profiles*.
[326] ACPO, *Good Practice Guide for Digital Evidence*, 2012; ACPO, *Online Research and Investigation Guidance*, Version 1.2, 2013.
[327] UK College of Policing, *UK College of Policing Intelligence Report Breakdown*, 2015.

oraz ustawą o uprawnieniach śledczych[328]. Każdorazowe dochodzenie musi być poprzedzone analizą, czy planowane działania mogą ingerować w prawa i wolnościami osoby fizycznej, której dotyczy dochodzenie. Jednocześnie, decyzje operacyjne muszą uwzględniać, czy rozpoznanie ma być przypisane do organów ścigania, gdyż determinuje to rodzaj zastosowanych środków pozyskiwania informacji jawnoźródłowych. Wielka Brytania utrzymuje zdecentralizowany model funkcjonowania policji, obejmujący Anglię, Walię, Szkocję i Irlandię Północną. Różnice w zarządzaniu, finansowaniu oraz uwarunkowaniach społecznych powodują brak spójności w publikowanych dokumentach i wytycznych dotyczących działania policji, jak również w alokacji środków na narzędzia wywiadu jawnoźródłowego i specjalistyczne szkolenia.

Brytyjskie agencje rządowe, takie jak Służba Bezpieczeństwa (MI5) i Tajna Służba Wywiadowcza (MI6), systematycznie wykorzystywały wywiad jawnoźródłowy na przestrzeni lat. Na początku 2000 roku Ministerstwo Obrony Wielkiej Brytanii powołało Defence Open-Source Intelligence Service-DOSIS, aby wspierać zastosowanie OSINT w operacjach wojskowych. W 2011 roku brytyjskie Ministerstwo Spraw Wewnętrznych utworzyło Centrum Nauk Stosowanych i Technologii (ang. *Centre for Applied Science and Technology*, CAST), którego zadaniem było wspieranie działań związanych m.in. z nauką i technologii w obszarze bezpieczeństwa publicznego i zwalczania przestępczości. Centrum rekomendowało i zatwierdzało produkty wykorzystywane w wywiadzie jawnoźródłowym, które były udostępniane za pośrednictwem internetowego portalu. CAST wspierało także rozwój narzędzi OSINT oraz ocenę komercyjnych produktów do użytku przez brytyjskie organy ścigania, koncentrując się na tworzeniu i testowaniu narzędzi do wizualizacji danych oraz agregacji informacji. CAST działało do 2018 roku, kiedy to zostało zintegrowane z Defence Science and Technology Laboratory (ang. *Defence Science and Technology Laboratory*).

W Wielkiej Brytanii funkcjonuje wiele podmiotów prywatnych wyspecjalizowanych w wywiadzie jawnoźródłowym. Wspólne cele i zadania organizacji takich jak Association of British Investigators[329], UK OSINT COMMUNITY[330] oraz UK OSINT and Digital Investigations Network (ODIN)[331]

[328] *Regulation of Investigatory Powers Act 2000*, Wielka Brytania.
[329] https://www.theabi.org.uk/ [dostęp: 5.06.2024].
[330] https://www.osint.uk/ [dostęp: 5.06.2024].

obejmują ocenę i rekomendację narzędzi oraz technologii wykorzystywanych do gromadzenia i analizy danych z otwartych źródeł, promowanie etycznego i prawnego wykorzystywania tych informacji oraz wspieranie rozwoju umiejętności i kompetencji w zakresie OSINT. Podmioty te wspierają również współpracę międzysektorową, umożliwiając wymianę doświadczeń i najlepszych praktyk w wykorzystaniu OSINT w różnych dziedzinach, takich jak śledztwa kryminalne, badania oraz analizy rynkowe.

Od 2014 roku brytyjskie organizacje pozarządowe, takie jak Bellingat[332] czy BBC, znacząco przyczyniły się do rozwoju narzędzi i metod wywiadu jawnoźródłowego. Wykorzystując innowacyjne podejścia do pozyskiwania i analizy danych jawnoźródłowych, organizacje te śledziły m.in. rosyjską rozbudowę wojskową w pobliżu Ukrainy oraz dokumentowały łamanie praw człowieka w Mjanmie/Birmie oraz śledziły osoby z Korei Północnej celowo unikające sankcji nałożonych przez Unię Europejską[333]. Efektem tych działań było ujawnienie dezinformacji i pociągnięcie do odpowiedzialności osób w ramach sankcji nałożonych przez społeczność międzynarodową. Zmiana ta ograniczyła dominującą rolę funkcjonariuszy rządowych jako wyłącznych dysponentów dostępu do informacji wywiadowczych. Jednocześnie, implikowało to wzrost ilości informacji, na podstawie których poszczególne państwa mogą być pociągnięte do odpowiedzialności.

Należy uwzględnić, że niektóre dochodzenia prowadzone przez podmioty prywatne mogą błędnie przypisywać konkretne incydenty lub osoby do badanych zdarzeń. W sektorze publicznym metody weryfikacji informacji z otwartych źródeł oraz dbałość o rygor analityczny są bardziej zaawansowane i zgodne z ustalonymi standardami. W sektorze prywatnym natomiast brakuje usystematyzowanych reguł działania, które byłyby zgodne z przepisami prawa oraz zasadami etyki, co może prowadzić do poważnych konsekwencji.

W brytyjskiej strategii zwalczania terroryzmu z 2011 r.[334], podkreślono kluczowe środki mające na celu zwalczanie przestępczości i terroryzmu w przestrzeni

---

[331] https://blackdotsolutions.com/events/odin/ [dostęp: 5.06.2023].

[332] Bellingcat jest niezależną organizacją zajmującą się dziennikarstwem śledczym, specjalizującą się w analizie informacji pochodzących z otwartych źródeł. Organizacja ta, założona w 2014 roku przez Eliota Higginsa, ma na celu badanie i dokumentowanie konfliktów, przestępstw wojennych oraz innych naruszeń praw człowieka. Bellingcat charakteryzuje się społecznym i egalitarnym podejściem, a dochodzenia są prowadzone zarówno przez zawodowych dziennikarzy śledczych, jak i wolontariuszy. Zob. Bellingcat, https://www.bellingcat.com/ [dostęp: 8.10.2023].

[333] A. Janjeva, A. Harris, J. Byrne, *The Future of Open-Source Intelligence*…, op. cit., s. 11.

[334] W strategii podkreślono konieczność zwiększenia zdolności Wspólnego Centrum Analiz Terroryzmu do identyfikowania i monitorowania pojawiających się zagrożeń, w tym poprzez wykorzystanie otwartych źródeł, prognozowania oraz zaawansowanej analizy danych. Uznano to za istotny element

cyfrowej. Dokument ten wyznaczył podstawowe działania w obszarach zapobiegania, ścigania, ochrony i przygotowania do walki z terroryzmem, wspierając jednocześnie rozwój międzynarodowej i międzysektorowej współpracy w celu skuteczniejszego przeciwdziałania tym zagrożeniom. Podejściem, które może zapewnić innowacyjne rozwiązania w walce z terroryzmem jest współpraca między sektorem publicznym a prywatnym, obejmująca organy ścigania, przemysł oraz środowisko akademickie. Przykładem takiej współpracy jest działalność centrum doskonalenia ds. przeciwdziałania terroryzmowi, aktywności obcych wywiadów i przestępczości zorganizowanej (ang. *Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research*, CENTRIC), które od 2012 roku rozwija zdolności w zakresie operacyjnego wykorzystania wywiadu jawnoźródłowego. W 2016 roku CENTRIC uruchomiło Centrum Wywiadu Jawnoźródłowego – OSINT Hub[335], które pełni funkcję centrum operacyjnego oraz wirtualnej przestrzeni do eksploatacji, rozwoju i dystrybucji narzędzi wywiadu jawnoźródłowego. Centrum to jest wykorzystywane do monitorowania zagrożeń związanych m.in. z terroryzmem, cyberprzestępczością, wykorzystywaniem seksualnym dzieci, zarządzaniem kryzysowym, naruszeniami porządku publicznego oraz identyfikacją i modelowaniem przestępczości zorganizowanej. Jego zdolności techniczne i analityczne są rozwijane we współpracy z partnerami krajowymi, europejskimi oraz międzynarodowymi.

W brytyjskich instytucjach publicznych odpowiedzialnych za pozyskiwanie i wykorzystywanie informacji jawnoźródłowych na rzecz bezpieczeństwa państwa, występuje różnorodne podejście do korzystania z narzędzi opracowanych przez firmy trzecie[336]. Brytyjskie organy ścigania tradycyjnie wykorzystują różnorodne rozwiązania komercyjne, opracowane przez podmioty sektora prywatnego, często specjalnie zaprojektowane na potrzeby prowadzenia dochodzeń policyjnych. Brytyjskie Ministerstwo Obrony natomiast traktuje priorytetowo korzystanie z dedykowanych narzędzi, często wymagając przeprowadzenia weryfikacji bezpieczeństwa współpracujących podmiotów. Rząd Wielkiej Brytanii inicjuje działania mające na celu wsparcie analityków wywiadu i organów odpowiedzialnych za bezpieczeństwo państwa

skutecznego zarządzania zasobami oraz zapewnienia efektywnej reakcji na dynamicznie rozwijające się zagrożenia terrorystyczne. Szerzej: Ministerstwo Spraw Wewnętrznych Wielkiej Brytanii, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, 2011, CP 8134.

[335] CENTRIC, *OSINT Hub*, https://centric-research.co.uk/projects/osint-hub [dostęp: 28.12.2023].

[336] D. Wells, H. Gibson, *OSINT from a UK Perspective: Considerations from the Law Enforcement and Military Domains*, [w:] Proceedings Estonian Academy of Security Sciences, 16: *From Research to Security Union*, Estonian Academy of Security Sciences, 2017, s. 107.

w zarządzaniu szybko rosnącymi ilościami informacji, zarówno z publicznie dostępnych źródeł, jak i wewnętrznych ogólnodostępnych raportów. W ramach tych działań Kancelaria Premiera Wielkiej Brytanii rozwija platformę wymiany informacji o nazwie Information and Data Exchange (INDEX)[337]. Platforma ta jest zaprojektowana jako wspólna przestrzeń dla użytkowników do wyszukiwania, łączenia i wymiany materiałów jawnoźródłowych. Platforma będzie wykorzystywać nowoczesne technologie, takie jak uczenie maszynowe i zaawansowane metody analityczne, aby wzbogacić dostępne zasoby i ułatwić współpracę między różnymi departamentami rządowymi. Docelowo INDEX ma być elementem, który przyczyni się do zrewidowania statusu wywiadu jawnoźródłowego w Wielkiej Brytanii oraz zapewnienia jego pełnej integracji z produktami analitycznymi przeznaczonymi dla odbiorców najwyższego szczebla.

W raporcie „The Future of Open Source Intelligence for UK National Security"[338] eksperci instytutu badawczego Royal United Services Institute (RUSI) oraz centrum badań politycznych Centre for Emerging Technology and Security (CETaS) podkreślają wzrastającą rolę wywiadu jawnoźródłowego w zapewnianiu bezpieczeństwa Wielkiej Brytanii. W dokumencie tym podkreślono wzajemnie uzupełniającą się relację między informacjami publicznie dostępnymi, a informacjami ze źródeł niejawnych. Na wstępnych etapach dochodzenia informacje z otwartych źródeł umożliwiają identyfikację podejrzanych oraz uzyskanie informacji o motywach ich działań, podczas gdy tajne źródła wywiadowcze mogą uzupełniać te informacje, dostarczając specyficznych danych, które dostarczają odpowiedzi na główne pytania analityczne. Przykład inwazji Rosji na Ukrainę pokazuje, że informacje z otwartych źródeł mogą dostarczać szczegółowych danych dotyczących ruchów wojsk, jednak dopiero w połączeniu z informacjami uzyskanych drogą agenturalną można w pełni zrozumieć intencje przeciwnika. Komplementarne wykorzystanie informacji ze źródeł otwartych i niejawnych zwiększa transparentność działań oraz może prowadzić do podniesienia standardów zarządzania informacjami wywiadowczymi. Wzmacnia

[337] J. Hugill, *Introducing INDEX – A Cross-Government Digital Information and Data Exchange*, PUBLIC, 2021, https://www.public.io/introducing-index-a-cross-government-digital-information-and-data-exchange/ [dostęp: 22.11.2023].

[338] Royal United Services Institute (RUSI) to najstarszy brytyjski think tank zajmujący się obronnością i bezpieczeństwem, którego celem jest wspieranie publicznej debaty oraz przekazywanie wiedzy o globalnych zagrożeniach bezpieczeństwa. Centre for Emerging Technology and Security (CETaS) funkcjonuje w ramach Alan Turing Institute i zajmuje się badaniami nad wpływem nowych technologii, takich jak sztuczna inteligencja, na politykę bezpieczeństwa. Zob. A. Janjeva, A. Harris, J. Byrne, *The Future of Open-Source Intelligence*…, op. cit.

również zasadność decyzji rządowych, jednocześnie zmniejszając potrzebę utrzymania wysokiego poziomu tajności.

Jednym z czynników ograniczających rozwój infrastruktury wywiadu jawnoźródłowego w Wielkiej Brytanii jest nierównomierny podział zdolności i zasobów pomiędzy różnymi odbiorcami informacji upoważnionymi do podejmowania określonych decyzji dotyczących bezpieczeństwa państwa, takimi jak społeczność wywiadowcza i organy ścigania. Inne ograniczenia obejmują niewystarczające uwzględnienie środków na rozwój narzędzi OSINT w strategiach inwestycyjnych, które wciąż preferują alokację zasobów na operacje tajne. Taka sytuacja stwarza ryzyko dla utrzymania konkurencyjności technologicznej kraju. Dodatkowym ograniczeniem jest trudność w tworzeniu efektywnych partnerstw z zewnętrznymi interesariuszami, wynikająca z konieczności rzetelnej weryfikacji zarówno produktów wykorzystywanych w wywiadzie jawnoźródłowym, jak i podmiotów je wytwarzających. Inwestowanie przez podmioty rządowe w specjalistyczne szkolenia z zakresu bezpieczeństwa danych i zarządzania dla pracowników służb umożliwia skuteczną ocenę technologii dostarczanych przez zewnętrznych dostawców.

5.3. Wywiad jawnoźródłowy w Izraelu

Od powstania w 1948 roku, Izrael systematycznie rozwijał swoje struktury wywiadowcze. Działają one nie tylko na terenie kraju, ale również w państwach sąsiadujących oraz na całym świecie, zwłaszcza tam, gdzie prowadzone są lub tolerowane działania antysemickie. Liczne konflikty oraz ataki terrorystyczne i militarne skierowane przeciwko Izraelowi spowodowały konieczność ciągłej adaptacji i modyfikacji struktury oraz profilu działań operacyjnych. W rezultacie izraelski wywiad stał się nowoczesną i mobilną organizacją wywiadowczą, uznawaną za jedną z najlepszych na świecie. Przy rozbudowanym dopływie informacji agenturalnych równolegle rozbudowano dopływ informacji z wywiadu jawnoźródłowego, który już w fazie początkowej pozwala na identyfikację przygotowania działań wrogich Izraelowi państw.

Analiza zagadnień związanych z działalnością wywiadowczą Izraela, w tym również dotyczących rozpoznania ze źródeł otwartych prowadzonych na rzecz bezpieczeństwa, stanowi poważne wyzwanie badawcze. Przede wszystkim, wszelkie działania podejmowane zarówno przez służby wywiadowcze, wojsko, jak i podmioty

sektora prywatnego współpracujące w zakresie bezpieczeństwa są z założenia tajne. Wynika to zarówno z uwarunkowań geopolitycznych jak i z konieczności zapewnienia strategicznej przewagi w regionie, który charakteryzuje się wysokim poziomem niestabilności oraz licznymi zagrożeniami zewnętrznymi. Na uwzględnienie zasługuje również fakt, iż część dostępnych informacji, choć jawnych, mogła zostać celowo zniekształcona w ramach działań dezinformacyjnych.

Izraelska społeczność wywiadowcza składa się z trzech organizacji: Służby Wywiadu Wojskowego (hebr. *Aman*), Instytut ds. Wywiadu i Operacji Specjalnych (hebr. *Mossad*) oraz Służby Bezpieczeństwa Ogólnego (hebr. *Szin Bet*, *Szabak*). Każda ze służb ma własne obszary odpowiedzialności oraz specyficzne cechy operacyjne. Służby te pozostają we wzajemnej korelacji służącej do podejmowania najbardziej efektywnych działań w zapewnieniu bezpieczeństwa państwa.

Mossad odpowiada za działalność wywiadowczą i operacje specjalne poza granicami Izraela, mające na celu neutralizację zagrożeń oraz wzmacnianie bezpieczeństwa państwa. Organizacja realizuje swoje cele poprzez gromadzenie informacji z różnych źródeł, prowadzenie operacji na całym świecie oraz współpracę z innymi służbami wywiadowczymi. Mossad odpowiada również za przeciwdziałanie zagrożeniom terrorystycznym, rozwijanie tajnych relacji dyplomatycznych oraz ratowanie społeczności żydowskich z niebezpiecznych miejsc[339]. W 2021 roku Mossad uruchomił specjalny program szkoleniowy dla europejskich funkcjonariuszy wywiadu, dotyczący wykorzystania potencjału wywiadu jawnoźródłowego[340]. Program ten jest podzielony na dwie części: pierwsza jest realizowana i koordynowana bezpośrednio przez izraelski wywiad, natomiast druga przez sektor prywatny ściśle współpracujący z Mossadem. Głównym celem programu jest poprawa efektywności w pozyskiwaniu informacji jawnoźródłowych oraz ich wykorzystywanie do przeprowadzania werbunków osobowych źródeł informacji. Program został opracowany w latach 2016-2021 przez Yossiego Cohena, dyrektora Mossadu, a następnie kontynuowany przez jego następcę. W pierwszym roku z programu skorzystały służby wywiadowcze Belgii, Włoch i Hiszpanii. W szkoleniach organizowanych przez Mossad przekazywana jest wiedza na temat narzędzi i metod pozyskiwania informacji jawnoźródłowych, przy czym szczególna uwagę poświęca się na łączenie tych informacji z danymi

[339] Mossad, https://www.mossad.gov.il/ [dostęp: 8.07.2024].
[340] *Mossad Trains European Intel Agents in Open-Source Spy Tools & Analysis*, Intelligence Online, 2022, https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra [dostęp: 30.03.2024].

pochodzącymi z innych źródeł wywiadowczych. Taka integracja ma na celu wzmocnienie zdolności analitycznych służb wywiadowczych. Dodatkowo, istotnym elementem szkoleń jest krytyczna ocena źródeł informacji. Na podstawie analizy programu szkoleń organizowanych przez Mossad oraz sposobu ich przeprowadzania można stwierdzić, że izraelski wywiad intensywnie wykorzystuje wywiad jawnoźródłowy w swojej działalności operacyjnej. Integracja informacji jawnoźródłowych z danymi pochodzącymi z innych źródeł wywiadowczych, podkreślana w tych szkoleniach, wskazuje na strategiczne znaczenie danych z otwartych źródeł w procesie analitycznym Mossadu. Podejście oparte na nowoczesnych metodach zbierania i analizy danych, świadczy również o zaawansowanej adaptacji technologii informacyjnych przez izraelskie służby wywiadowcze.

Shin Bet odpowiada za utrzymanie bezpieczeństwa państwa, porządku ustroju demokratycznego i jego instytucji przed zagrożeniami terrorystycznymi, sabotażem, szpiegostwem, dywersją i ujawnianiem tajemnic państwowych[341]. Organizacja działa na terytorium Państwa Izrael i na obszarach znajdujących się pod jego kontrolą. Rolą kontrwywiadu jest również ochrona bezpieczeństwa osobistego obywateli Izraela i jego mieszkańców. Charakterystyka działania Shin Bet powoduje, że dostęp do informacji na temat zakresu i metod wykorzystania źródeł jawnych jest ograniczony. Analiza wybranych operacji wskazuje jednak na skuteczne wykorzystanie wywiadu jawnoźródłowego przez tę służbę. Przykładem jest udaremnienie planowanych ataków terrorystycznych Al-Kaidy na ambasadę USA w Tel Awiwie oraz Międzynarodowe Centrum Konferencyjne w Jerozolimie. Dzięki monitorowaniu i analizie komunikacji internetowej, m.in. za pośrednictwem Skype'a i Facebooka, Shin Bet zidentyfikował i zatrzymał grupę palestyńskich terrorystów odpowiedzialnych za te plany[342].

Aman działa w ramach Sił Obronnych Izraela, a jego zadaniem jest dostarczanie informacji wywiadowczych oraz analiz wojskowych i politycznych ministrowi obrony oraz rządowi w zakresie strategicznego bezpieczeństwa państwa[343]. Organizacja gromadzi dane z różnych źródeł, w tym także z otwartych źródeł informacji, w celu przygotowywania analiz będących podstawą do podejmowania decyzji politycznych,

[341] SHABAK, https://www.shabak.gov.il/en/about/values/ [dostęp: 8.07.2024].
[342] *Al-Qaeda Targeting US Embassy, Jerusalem Convention Center*, The Times of Israel, 2014, https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/, [dostęp: 25.04.2024].
[343] *Military Intelligence Directorate*, Israel Defense Forces, https://www.idf.il/en/mini-sites/directorates/military-intelligence-directorate/military-intelligence-directorate/ [dostęp: 22.04.2024].

oceny sytuacji związanych z zagrożeniami bezpieczeństwa państwa a także podejmowania decyzji dotyczących użycia siły.

Ważnym aspektem jest stałe doskonalenie systemów i narzędzi służących do zbierania, przetwarzania oraz analizy informacji wywiadowczych. Żołnierze odpowiedzialni za te zadania są zobowiązani do przekazywania informacji i ich bieżącej aktualizacji w czasie rzeczywistym, co wspiera podejmowanie decyzji na najwyższym poziomie. Jednostki pionu badawczego podporządkowane są szefowi Amanu, który określa priorytety i najważniejsze kategorie informacji wywiadowczych.

W ramach izraelskiego wywiadu wojskowego funkcjonuje jednostka 8200, specjalizująca się w wywiadzie elektronicznym (SIGINT). W jej strukturach utworzono jednostkę Hatzav, odpowiedzialną za wywiad jawnoźródłowy. Materiały opracowane przez Hatzav były przekazywane innym służbom wywiadowczym oraz do Biura Rzecznika Prasowego Sił Obronnych Izraela. Biuro to decydowało o ich ewentualnym przekazaniu mediom, mając na celu utrzymanie wizerunku Izraela zgodnie z przyjętą linią polityczną[344]. Początkowo Hatzav koncentrowała się na monitorowaniu tradycyjnych mediów arabskich, takich jak prasa, radio i telewizja. Ewolucja form komunikacji oraz rozwój mediów społecznościowych znacząco zwiększyły rolę jednostki Hatzav. Informacje pozyskiwane z platform takich jak Facebook, Twitter, TikTok oraz Instagram, w tym nieocenzurowane dane publikowane przez reporterów i obywateli w czasie rzeczywistym, stanowiły cenne źródło danych wywiadowczych. Dane te miały zarówno znaczenie taktyczne, na przykład w kontekście tweetów dotyczących konkretnych operacji, jak i strategiczne, umożliwiając analizę nastrojów społecznych. Kierownictwo Hatzav podkreślało, że o skuteczności podejmowanych działań decyduje szybkość przekazywania informacji niezbędnych do podejmowania decyzji. Jednostka wykorzystywała dedykowane oprogramowanie, które umożliwiało katalogowanie i przechowywanie tweetów oraz postów a także ich wizualizację. Hatzav dostosował zarówno profil szkoleń, jak i proces rekrutacji, tak aby sprostać wymaganiom wynikającym ze zmieniających się źródeł informacji. Szczególny nacisk położono na pozyskiwanie osób ze znajomością języków obcych, zwłaszcza arabskiego oraz żołnierzy z wiedzą na temat mediów społecznościowych i umiejętnościami informatycznymi. W wyniku tego zatrudniano bardzo młode osoby, często bez wcześniejszego doświadczenia operacyjnego. Oceniano, że Hatzav pozyskiwał

[344] Y. Hadarem, *The IDF's Not-So-Secret Unit*, 2015, https://www.israelhayom.co.il/article/306247, [dostęp: 20.04.2024].

50% wszystkich danych wywiadowczych Sił Obronnych Izraela[345]. Jednostka Hatzav systematycznie doskonaliła metody analizy jawnoźródłowej, wyciągając wnioski również z popełnionych błędów. Przykładem tego była m.in. niezdolność do przewidzenia obalenia prezydenta Egiptu Hosniego Mubaraka, co doprowadziło do większego nacisku na rozwój metod analizy informacji z mediów społecznościowych, w efekcie czego rozbudowano techniki analizy nastrojów społecznych[346].

W 2021 roku, w ramach reorganizacji izraelskiego wywiadu wojskowego, jednostka Hatzav została rozwiązana, a jej funkcje przeniesiono do innych wydziałów jednostki 8200 oraz regionalnych departamentów analitycznych. Decyzja ta miała dwa główne aspekty. Po pierwsze, niedoszacowano znaczenia wywiadu jawnoźródłowego na rzecz technicznych metod pozyskiwania i analizy informacji, takich jak wykorzystanie sztucznej inteligencji i elektronicznego nasłuchu. Drugim aspektem tej decyzji było prawdopodobne zawarcie umów z podmiotami prywatnymi w celu monitorowania ruchu internetowego oraz prowadzenia wywiadu jawnoźródłowego, w tym głównie zbierania informacji na temat nastrojów antyizraelskich[347]. Rozwiązanie jednostki Hatzav i rozproszenie jej funkcji w innych strukturach wywiadu spotkało się z krytyką, ponieważ uznano, że nadmierne poleganie na technologii nie może w pełni zastąpić ludzkiej analizy, szczególnie w kontekście niuansów kulturowych i językowych[348].

W Izraelu wywiad jawnoźródłowy został zdefiniowany przez społeczność wywiadowczą jako zbieranie informacji i danych z otwartych źródeł, takich jak media pisane i elektroniczne, publikacje rządowe, akademickie oraz ogólnodostępne bazy danych, w odróżnieniu od pozyskiwania informacji w sposób tajny. W ramach tej definicji uwzględniono również półjawne pozyskiwanie informacji, które obejmuje gromadzenie danych przez korpus dyplomatyczny w tym działalność ambasadorów, attachés wojskowych oraz innych pracowników placówek[349]. Jest to bardzo ogólne ujęcie wywiadu jawnoźródłowego, które pozostawia wiele niejasności zarówno co do samego określenia otwartych źródeł informacji, jak i metod ich pozyskiwania oraz analizy. W Izraelu faktyczne działania podejmowane zarówno przez podmioty

[345] M.M. Lowenthal, R.M. Clark, *The Five Disciplines*…, op. cit., 2016, s. 35.
[346] Y. Hadarem, *The IDF's*…, op. cit.
[347] *Israel Downgrades Its Open-source Military Intelligence Unit*, Haaretz, 2016, https://www.haaretz.com/israel-news/2016-10-30/ty-article/israel-downgrades-its-open-source-military-intelligence-unit/0000017f-e351-d75c-a7ff-ffddb17b0000 [dostęp: 12.03.2024].
[348] S. Bar, *7 October – The Unlearning of the Lessons of 1973*, National Institute for Public Policy, Information Series, no. 589, June 11, 2024, s. 5.
[349] https://www.iicc.org.il/?module=articles&item_id=4&article_id=188&art_category_id=3&q=%D7%90%D7%95%D7%A1%D7%99%D7%A0%D7%98 [dostęp: 12.08.2024].

publiczne, jak i prywatne w zakresie pozyskiwania informacji jawnoźródłowych wskazują na odmienne podejście od klasycznego rozumienia tego pojęcia. W izraelskim ujęciu wywiad jawnoźródłowy obejmuje wszelkie dostępne metody gromadzenia danych z otwartych źródeł, w tym zarówno działania półpasywne, jak i aktywne. De facto może to oznaczać przełamywanie systemów informatycznych w celu pozyskania informacji, często w sposób niezgodny z prawem.

Działania służb odpowiedzialnych na bezpieczeństwo państwa na całym świecie uległy znaczącej transformacji, koncentrując się obecnie na wrogach niepaństwowych, organizacjach terrorystycznych oraz indywidualnych terrorystach. Zjawisko to jest określane jako: „masy mają głos" a w izraelskim żargonie wywiadowczym jest znane jako „masowa percepcja"[350]. Skutkuje to wzrostem znaczenia otwartych cyfrowych źródeł informacji, w tym szczególnie mediów społecznościowych. Podmioty odpowiedzialne za bezpieczeństwo państwa stają przed wyzwaniami technologicznymi, metodologicznymi oraz organizacyjnymi wynikającymi z przekształceń środowiska informacyjnego. Obok dużego wzrostu ilości informacji, rośnie również znaczenie ich wizualizacji. W efekcie w Izraelu otwarte źródła, oprócz swojej wartości wywiadowczej, są wykorzystywane w krajowych działaniach propagandowych, określanych jako "dyplomacja publiczna"[351].

Dla izraelskich służb specjalnych ważnym obszarem prowadzenia rozpoznania jawnoźródłowego jest Darknet. Poprzez monitorowanie Darknetu prowadzone jest rozpoznanie osób powiązanych przede wszystkim z organizacjami terrorystycznymi oraz wrogo nastawionymi do państwa Izrael. Szczególną uwagę służby izraelskie zwracają na nakłanianie do podejmowania działań niezgodnych z prawem i tworzenie oraz działalność ugrupowań o charakterze terrorystycznym. Informacje o działalności izraelskich służb specjalnych w zakresie rozpoznania w Darknecie można również uzyskać podczas szkoleń prowadzonych przez byłych funkcjonariuszy tych służb.

W warunkach izraelskich do służb specjalnych zalicza się również Matam, czyli oddział Specjalnego Rozpoznania i zadań zarządu Śledczego Komendy Głównej Policji, który został już utworzony w latach 50' XX wieku[352]. W swoich działaniach pozyskuje on informacje jawnoźródłowe do wykrywania i zwalczania sprawców przestępstw

[350] E. Lapid, *OSINT: A Major Source of Up-to-Date Information*, „National Security and the Future" 2016, vol. 17, nr 1–2, s. 40.
[351] Ibidem.
[352] J.H. Larecki, *Wielki leksykon*…, op. cit., s. 373.

o charakterze politycznym, w tym szczególnie penetracji ekstremistycznych ugrupować palestyńskich jak również terrorystycznych i środowisk imigracyjnych.

Izrael skutecznie dostosowuje swoje działania na rzecz bezpieczeństwa do dynamicznie zmieniających się warunków technologicznych i geopolitycznych. Już około 2000 roku zidentyfikowano cyberprzestrzeń jako istotne zagrożenie dla bezpieczeństwa państwa. W odpowiedzi na te wyzwania przeprowadzono szereg reform organizacyjnych w systemie bezpieczeństwa Izraela, które miały na celu zwiększenie efektywności w reagowaniu na zagrożenia w cyberprzestrzeni. W 2011 roku utworzono Krajowe Biuro ds. Cyberbezpieczeństwa (ang. *Israeli National Cyber Bureau*, INCB) jako organ doradczy premiera, rządu oraz jego komisji, odpowiedzialny za tworzenie krajowej polityki cybernetycznej. Do jego zadań należało opracowanie krajowej strategii cyberbezpieczeństwa oraz nawiązywanie współpracy międzynarodowej w tym obszarze. W 2016 roku powołano Narodowy Urząd ds. Cyberbezpieczeństwa (ang. *National Cyber Security Authority*, NCSA), który pełni rolę centralnego organu operacyjnego odpowiedzialnego za prowadzenie działań w zakresie ochrony cyberprzestrzeni Państwa Izrael.

W 2017 roku rząd Izraela przedstawił pierwszą strategię cyberbezpieczeństwa[353], w której uznał cyberprzestrzeń za globalną sferę działań, a cyberbezpieczeństwo za wyzwanie o charakterze międzynarodowym. W ramach tej strategii podjęto decyzję o połączeniu Krajowego Biura ds. Cyberbezpieczeństwa i Narodowego Urząd ds. Cyberbezpieczeństwa, w jedną jednostkę organizacyjną – Izraelską Krajową Dyrekcję ds. Cyberbezpieczeństwa (ang. *Israel National Cyber Directorate*, INCD), funkcjonującą w ramach biura premiera. Instytucja ta odpowiada za kompleksowe działania w zakresie cyberobrony w sferze cywilnej, obejmujące zarówno formułowanie polityki i rozwój zdolności technologicznych, jak i operacyjną obronę w cyberprzestrzeni. Druga strategia cyberbezpieczeństwa została opublikowana w 2021 roku i kontynuuje ten kierunek, podkreślając rolę Izraela jako lidera w dziedzinie cyberbezpieczeństwa oraz aktywnego uczestnika międzynarodowych inicjatyw i porozumień dotyczących cyberobrony[354]. W obu dokumentach brak jest bezpośrednich odniesień do wywiadu jawnoźródłowego. Wspólnym elementem tych dwóch strategii jest jednak silne podkreślenie roli międzynarodowej współpracy

[353] *Israel National Cyber Security Strategy in Brief*, National Cyber Directorate, Prime Minister's Office, 2017.
[354] *Israel International Cyber Strategy: International Engagement for Global Resilience*, National Cyber Directorate, Prime Minister's Office, 2021.

w dziedzinie cyberbezpieczeństwa, co ma na celu budowanie bezpiecznej i stabilnej przestrzeni cybernetycznej. W obu strategiach podkreślono również potrzebę wymiany informacji, technologii oraz najlepszych praktyk, aby wzmocnić cyberbezpieczeństwo zarówno na poziomie krajowym, jak i globalnym.

Izrael zbudował złożony system współpracy w dziedzinie cybernetyki między rządem, środowiskiem akademickim oraz sektorem przemysłowym. Jego podstawą jest założenie, że inwestowanie w rozwój kapitału ludzkiego oraz innowacje przemysłowe są niezbędne dla zapewnienia skutecznej obrony w cyberprzestrzeni i utrzymania przewagi technologicznej nad potencjalnymi przeciwnikami. Izrael uczestniczył w międzynarodowej grupie roboczej ds. wywiadu jawnoźródłowego (ang. *International Open Source Working Group*, IOSWG), której głównym celem była wymiana produktów wywiadowczych opartych na otwartych źródłach[355]. W 2014 roku utworzono CyberSpark Innovation Arena jako rezultat wspólnego przedsięwzięcia Krajowego Biura ds. Cyberbezpieczeństwa, władz miejskich Be'er Sheva, Uniwersytetu Ben Guriona oraz kluczowych partnerów przemysłowych, takich jak EMC-RSA, Lockheed Martin, IBM i Deutsche Telekom. CyberSpark stworzył wielostronny „ekosystem", w którym rząd, środowiska akademickie, przemysł, władze lokalne oraz inicjatywy społeczne mogą wspólnie opracowywać i testować innowacyjne pomysły oraz koncepcje dotyczące cyberbezpieczeństwa, w tym wywiadu jawnoźródłowego[356].

Służby wywiadu izraelskiego, zarówno w formie tradycyjnej, jak i elektronicznej, współpracują z podmiotami komercyjnymi, które przygotowują naprowadzenia i analizy dotyczące poszczególnych osób i podmiotów gospodarczych. Struktury wywiadu regularnie dokonują penetracji organizacji i aparatów rządowych wrogo nastawionych wobec państwa Izrael. Podmioty komercyjne współdziałające ze służbami specjalnymi Izraela odgrywają szczególnie istotną rolę nie tylko w państwach Bliskiego Wschodu, ale przede wszystkim w odniesieniu do Iranu, który jest uznawany przez Izrael za państwo wspierające wszelkie organizacje terrorystyczne podejmujące działania przeciwko Izraelowi.

Wraz z pojawieniem się II generacji wywiadu jawnoźródłowego wzrosło zainteresowanie jego wykorzystaniem w działaniach na rzecz bezpieczeństwa Izraela. Jednak kolejne zmiany technologiczne, w tym rozwój sztucznej inteligencji

[355] Szerzej: Działalność IOSWG jest opisana w podrozdziale dotyczącym Stanów Zjednoczonych.
[356] *Prime Minister Benjamin Netanyahu Announces Creation of CyberSpark in Beer-Sheva*, Americans for Ben-Gurion University, 2014, https://americansforbgu.org/prime-minister-benjamin-netanyahu-announces-creation-of-cyberspark-in-beer-sheva/ [dostęp: 8.10.2023].

i automatycznego przetwarzania danych, doprowadziły do wzrostu znaczenia wywiadu cybernetycznego, kosztem wywiadu jawnoźródłowego. W izraelskich służbach ugruntowało się przekonanie, że wywiad jawnoźródłowy jest jedynie elementem naprowadzającym, wspierającym podejmowanie złożonych działań operacyjnych. Dla wszystkich podmiotów działających na rzecz bezpieczeństwa Izraela, które korzystają z cyberwywiadu, integralnym elementem pozostaje rozpoznanie oparte na metodach wywiadu jawnoźródłowego.

5.4. Podsumowanie

Analiza rozwoju i wykorzystania wywiadu jawnoźródłowego w Stanach Zjednoczonych, Wielkiej Brytanii i Izraelu prowadzi do wniosku, że wszystkie te państwa dostrzegają rosnącą rolę otwartych źródeł informacji oraz ich istotny wpływ na bezpieczeństwo. Wzrost liczby dostępnych informacji jawnoźródłowych oraz postęp w zakresie ich analizy pozwalają na skuteczniejsze monitorowanie zagrożeń i działań przeciwników. Jednocześnie państwa demokratyczne stoją przed wyzwaniem związanym z koniecznością dalszego inwestowania w infrastrukturę technologiczną oraz rozwój metod analitycznych. Różnice w definicjach otwartych źródeł oraz wywiadu jawnoźródłowego skutkują implementacją odmiennych rozwiązań przez poszczególne państwa, zgodnie z przyjętą przez nie terminologią.

Sposób postrzegania wywiadu jawnoźródłowego w trzech analizowanych krajach demokratycznych jest również zróżnicowany. Stany Zjednoczone i Wielka Brytania intensywnie rozwijają zarówno organizacyjne, jak i legislacyjne aspekty wywiadu jawnoźródłowego. W Izraelu natomiast wywiad jawnoźródłowy pełni jedynie funkcję wspomagającą, stanowiąc element naprowadzający do podejmowania złożonych działań operacyjnych.

Wspólną cechą wszystkich analizowanych państw jest rozproszenie działań i odpowiedzialności w zakresie rozpoznania jawnoźródłowego w ramach podmiotów publicznych. Konsekwencję tego stanowią brak współpracy, niedostateczne finansowanie potrzeb operacyjnych oraz zróżnicowanie w poziomach dostępu i metodach gromadzenia danych, co w wielu przypadkach znacząco ogranicza efektywność działań w obszarze wywiadu jawnoźródłowego.

Kolejnym zagadnieniem jest rozwój kompetencji w zakresie wywiadu jawnoźródłowego. Zarówno w Stanach Zjednoczonych, jak i w Wielkiej Brytanii

kompetencje służb wywiadowczych są rozwijane głównie w obszarze pozyskiwania i przetwarzania informacji ze źródeł operacyjnych. Jednak nadal widoczne są braki w zakresie umiejętności zawodowych niezbędnych do analizy, selekcji, dystrybucji oraz integracji informacji jawnoźródłowych w całym cyklu wywiadowczym. W Izraelu umiejętności w zakresie wywiadu jawnoźródłowego są systematycznie rozwijane przez służby specjalne we współpracy z sektorem prywatnym, co obejmuje wymianę wiedzy oraz technologii. Służby te organizują również szkolenia dla przedstawicieli służb wywiadowczych innych państw oraz oferują programy szkoleniowe dla podmiotów komercyjnych.

Nowoczesne technologie, takie jak sztuczna inteligencja i big data, odgrywają zasadniczą rolę w przetwarzaniu informacji z otwartych źródeł w badanych państwach. W Stanach Zjednoczonych rozwój nowoczesnych narzędzi wywiadu jawnoźródłowego został wskazany jako priorytetowy obszar w strategii rozwoju OSINT na lata 2024–2026. W Wielkiej Brytanii zaawansowane technologie są stosowane w działaniach policyjnych oraz monitorowaniu zagrożeń wewnętrznych. Izrael natomiast integruje OSINT z operacjami cyberbezpieczeństwa, poszerzając jego zastosowanie poza tradycyjne ramy wywiadu jawnoźródłowego.

Ważnym elementem strategii wywiadowczych w analizowanych państwach pozostaje współpraca międzynarodowa, która obejmuje wymianę informacji wywiadowczych i koordynację działań w zakresie bezpieczeństwa państw. Sojusze te, takie jak „Five Eyes” czy współpraca bilateralna, umożliwiają bardziej efektywne wykorzystanie zasobów wywiadowczych oraz wzmacniają wspólne zdolności w obliczu globalnych zagrożeń. Równolegle wszystkie trzy państwa rozwijają współpracę z sektorem prywatnym, jednak w różnym zakresie: Stany Zjednoczone koncentrują się na wdrażaniu nowoczesnych technologii, Wielka Brytania rozwija narzędzia OSINT na potrzeby policyjne. Z kolei w Izraelu współpraca z sektorem prywatnym skupiona jest na integracji wywiadu jawnoźródłowego z operacjami wywiadowczymi oraz cyberbezpieczeństwem.

Podsumowując ustalenia dotyczące ewolucji i wykorzystania wywiadu jawnoźródłowego w Stanach Zjednoczonych, Wielkiej Brytanii oraz Izraelu, należy podkreślić, że OSINT odgrywa istotną rolę w działaniach podejmowanych na rzecz bezpieczeństwa. Każde z tych państw wypracowało unikatowe podejście, dostosowane do specyficznych potrzeb oraz uwarunkowań geopolitycznych. Różnice w rozwoju wywiadu jawnoźródłowego dotyczą zarówno kwestii terminologicznych, jak

i organizacyjnych. Zróżnicowane podejścia odzwierciedlają różne priorytety i wyzwania stojące przed tymi państwami. Wyniki badań wskazują, że wszystkie analizowane państwa zwiększają wykorzystanie wywiadu jawnoźródłowego, co znacząco przekłada się na wzrost ich zdolności zarówno w zakresie działań defensywnych, jak i ofensywnych.

6. WPŁYW WYWIADU JAWNOŹRÓDŁOWEGO NA BEZPIECZEŃSTWO PAŃSTWA W ŚWIETLE BADAŃ WŁASNYCH

Celem niniejszego rozdziału jest przedstawienie wyników badań własnych dotyczących wpływu wywiadu jawnoźródłowego na bezpieczeństwo państwa. Przeprowadzona analiza empiryczna umożliwiła identyfikację zależności między wykorzystaniem wywiadu jawnoźródłowego a możliwościami państwa w zakresie przeciwdziałania zagrożeniom o charakterze wewnętrznym i zewnętrznym. Uzyskane wyniki stanowią podstawę do sformułowania wniosków oraz opracowania propozycji rozwiązań ukierunkowanych na zwiększenie efektywności wykorzystania potencjału wywiadu jawnoźródłowego w sektorze bezpieczeństwa państwa. Przedstawione rekomendacje mają charakter zarówno praktyczny, jak i prognostyczny, wskazując możliwe kierunki dalszych działań instytucjonalnych, legislacyjnych oraz badawczych. Rozdział ten pełni zatem funkcję koncepcyjno-prognostyczną, integrując ustalenia teoretyczno-empiryczne z perspektywą rozwojową badanego obszaru.

6.1. Analiza wyników badań empirycznych

6.1.1. Charakterystyka

Przeprowadzone badania dotyczyły znaczenia wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa. Do realizacji badań zastosowano metodę indywidualnych wywiadów pogłębionych (ang. *in-depth interviews*, IDI). Metoda ta, oparta na bezpośredniej interakcji, pozwala na dogłębną rekonstrukcję opinii uczestników oraz zapewnia kontekstualne zrozumienie analizowanej problematyki. Dodatkowo umożliwia badaczowi obserwację zachowań respondenta, co dodatkowo wzbogaca uzyskane wypowiedzi i umożliwia głębszą analizę badanej kwestii[357].

Badania przeprowadzono od grudnia 2023 roku do kwietnia 2024 roku. Relatywnie krótki czas trwania badań pozwolił na zachowanie stałości warunków bezpieczeństwa w odniesieniu do metod i środków technicznych stosowanych w rozpoznaniu z wykorzystaniem otwartych źródeł, uwarunkowań geopolitycznych oraz prawnych i pozaprawnych czynników determinujących wykorzystanie wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa.

[357] J. Sztumski, *Wstęp do metod i technik badań społecznych*, „Śląsk" Sp. z o.o. Wydawnictwo Naukowe, Katowice 2010, s. 176–180.

Celem wywiadów było uzyskanie jakościowych informacji na temat roli i znaczenia wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa. W ramach badania przeprowadzono 12 indywidualnych wywiadów pogłębionych. Respondentami byli eksperci posiadający specjalistyczną wiedzę oraz bogate doświadczenie w dziedzinie wywiadu jawnoźródłowego i bezpieczeństwa państwa. Dobór uczestników oparto na ich dorobku zawodowym, unikalnych kompetencjach oraz wkładzie w rozwój zagadnień związanych z wywiadem jawnoźródłowym. Respondenci reprezentowali różnorodne środowiska zawodowe, co umożliwiło analizę w szerokiej perspektywie. Należą do nich:

1. **Gen. bryg. Paweł Pruszyński** – były z-ca Szefa Urzędu Ochrony Państwa i Agencji Bezpieczeństwa Wewnętrznego odpowiedzialny m.in. za zagadnienia związane z pracą operacyjną oraz rozpoznaniem środkami technicznymi.
2. **Płk Sylwester Sawicki** – Dyrektor Departamentu Zezwoleń i Koncesji Ministerstwa Spraw Wewnętrznych i Administracji, były Inspektor Policji, Komendant w Komendzie Stołecznej Policji Warszawa Mokotów.
3. **Płk Dariusz Trojszczak** – były Naczelnik Biura Spraw Wewnętrznych Straży Granicznej.
4. **Mjr Artur Szachno** – były Szef Grupy Informatyki w Wydziale Łączności i Informatyki Jednostki Wojskowej GROM, ekspert z obszaru cyberbezpieczeństwa w Urzędzie Komunikacji Elektronicznej, oficer Łącznikowy NATO
5. **Ppłk Stanisław Ignaciuk** – były oficer wywiadu, doświadczenie w pracy w kraju i za granicą,
6. **Ppłk dr.inż. Przemysław Kornacki** – dowódca batalionu lekkiej piechoty w Łasku w ramach 9 Łódzkiej Brygady Obrony Terytorialnej, wieloletnie doświadczenie zawodowe zdobyte podczas służby w jednostkach organizacyjnych resortu obrony narodowej oraz Ministerstwa Spraw Wewnętrznych i Administracji, wieloletni Szef Sekcji Rozpoznawczej odpowiedzialny za pozyskiwanie, gromadzenie, przetwarzanie i dystrybucję informacji mających wpływ na bezpieczeństwo państwa
7. **Insp. Piotr Caliński** – były Komendant Centrum Szkolenia w Legionowie
8. **Dr hab. Mirosław Kwieciński** – twórca i popularyzator polskiej teorii wywiadu i kontrwywiadu gospodarczego jako fundamentalnego narzędzia ekspansji i ochrony zasobów w działalności przedsiębiorstw, autor pierwszej polskiej monografii z tego zakresu, Profesor Państwowej Akademii Nauk Stosowanych w Krośnie.

9. **Kpt. Piotr Niemczyk** – były Dyrektor Biura Analiz Informacji Urzędu Ochrony Państwa, w latach 1993–1994 zastępca dyrektora Zarządu Wywiadu Urzędu Ochrony Państwa, wieloletni ekspert Komisji do Spraw Służb Specjalnych, ekspert Komisji do spraw przestrzegania praw obywatelskich w działaniach służb specjalnych.
10. **Bartosz Pastuszka** – Prezes Zarządu NaviRisk, specjalizuje się w zarządzaniu ryzykiem i bezpieczeństwem, wywiadu gospodarczym, audytach śledczych i sprawdzaniu przeszłości (wywiadownia gospodarcza). Pierwszy dyrektor Pinkerton, najstarszej na świecie agencji detektywistycznej w Polsce i Europie Środkowo-Wschodniej.
11. **Gen. bryg. dr Mariusz Chmielewski** – Zastępca Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni, architekt IT i naukowiec, zajmujący się budową systemów i badaniami z zakresu sztucznej inteligencji, cyberbezpieczeństwa i wspomagania decyzyjnego.
12. **Płk Łukasz Wojewoda** – Dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji**.** Oficer z wieloletnim doświadczeniem w obszarze cyberbezpieczeństwa, łączności i informatyki, a w szczególności w organizowaniu i prowadzeniu procesów obsługi incydentów bezpieczeństwa teleinformatycznego oraz testów bezpieczeństwa systemów teleinformatycznych. Służbie Kontrwywiadu Wojskowego.

Wywiady zostały przeprowadzone na podstawie scenariusza obejmującego 11 pytań, opracowanych zgodnie z przyjętą metodologią badawczą. Transkrypcje wszystkich wywiadów zawarte w załączniku. Respondenci autoryzowali wywiady, a zgody na ich publikację wraz z oświadczeniami potwierdzającymi weryfikację wypowiedzi zostały dołączone do pracy. Zebrany materiał badawczy umożliwił udzielenie odpowiedzi na postawione pytania badawcze.

6.1.2. Wyniki badań

W odniesieniu do odpowiedzi ekspertów na 12 szczegółowych pytań zadanych podczas wywiadów IDI, prezentacja wyników badań obejmuje analizę zagadnień dotyczących wywiadu jawnoźródłowego oraz jego wpływu na bezpieczeństwo państwa.

Pytanie 1: Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?

Analiza odpowiedzi ekspertów ujawnia jednolity pogląd co do pozytywnego wpływu wywiadu jawnoźródłowego na bezpieczeństwo państwa. Respondenci określili obecne wykorzystanie OSINT jako: "istotne", "kluczowe", "cenne", "ważne", "podstawowe", "znaczące", "sprawcze", a wręcz "fundamentalne". Wszyscy eksperci zgodzili się, że wywiad jawnoźródłowy przyczynia się do poprawy bezpieczeństwa państwa. Ich opinie są jednak podzielone w ocenie jego roli i potencjalnych ograniczeń: część uznaje OSINT za kluczowy element szybkiego reagowania na zagrożenia, podczas gdy inni postrzegają go jako uzupełnienie tradycyjnych metod wywiadowczych, takich jak HUMINT.

Eksperci podkreślili rolę wywiadu jawnoźródłowego w dostarczaniu szybkich i aktualnych informacji, co umożliwia służbom sprawniejsze reagowanie na zagrożenia oraz lepsze przewidywanie i neutralizowanie kryzysów. Zwrócili również uwagę na rosnące znaczenie OSINT w kontekście rozwoju technologii i zwiększonej dostępności danych, co przyspiesza procesy analityczne oraz poprawia reakcje na potencjalne zagrożenia. OSINT jest kluczowym narzędziem w planowaniu działań strategicznych i bieżących, uzupełnia dane z innych źródeł, co zwiększa skuteczność operacyjną. Wywiad jawnoźródłowy pozwala także na lepsze zrozumienie sytuacji zarówno w kraju, jak i na arenie międzynarodowej, co stanowi podstawę do projektowania bardziej efektywnych działań prewencyjnych w obszarze bezpieczeństwa państwa. Wykorzystanie wywiadu jawnoźródłowego w Polsce jest wspierane przez wyspecjalizowane ośrodki, m.in. takie jak Ośrodek Studiów Wschodnich oraz Polski Instytut Analiz Międzynarodowych, które monitorują sytuację międzynarodową i dostarczają analizy na potrzeby organów władzy państwowej.

Wśród ekspertów pojawiła się także opinia, że potencjał OSINT nie jest obecnie w pełni wykorzystywany do identyfikacji szans (ang. *opportunities*) dla państwa i jego gospodarki. Informacje jawnoźródłowe odgrywają istotną rolę nie tylko w kontekście bezpieczeństwa militarnego, ale także w identyfikacji szans biznesowych, umożliwiających ekspansję produkcji, zdobycie nowych rynków oraz budowanie przewagi konkurencyjnej. Ich analiza pod kątem optymalnego wykorzystania możliwości rozwoju państwa ma zasadnicze znaczenie. Ponadto, aspekt ekonomiczny odgrywa fundamentalną rolę w bezpieczeństwie państwa, gdyż przewaga gospodarcza

umożliwia akumulację zasobów, generowanie środków finansowych oraz efektywną produkcję, co w długoterminowej perspektywie wzmacnia zdolność państw do rywalizacji na arenie międzynarodowej.

Pytanie 2: Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?

Eksperci zgodnie uznali wysoką przydatność informacji jawnoźródłowych w weryfikacji danych operacyjnych. Zwrócono uwagę, że OSINT często stanowi punkt wyjścia do bardziej zaawansowanych analiz, umożliwiając pogłębienie wiedzy i zwiększenie wiarygodności danych pozyskiwanych z innych źródeł, takich jak HUMINT czy SIGINT. Szczególnie w kontekście działań defensywnych związanych z dezinformacją oraz zagrożeniami cybernetycznymi, wywiad jawnoźródłowy pełni podstawową rolę zarówno na etapie wstępnej weryfikacji, jak i późniejszego potwierdzania hipotez operacyjnych. OSINT zwiększa zdolności wywiadowcze a także odgrywa istotną rolę w monitorowaniu i neutralizowaniu zagrożeń związanych z dezinformacją i cyberbezpieczeństwem, umożliwiając wczesne ostrzeganie przed potencjalnymi zagrożeniami. Wywiad jawnoźródłowy wspiera także działania dyplomatyczne, dostarczając aktualnych informacji wykorzystywanych w kontekście międzynarodowych relacji i polityki zagranicznej. Wśród ekspertów pojawiła się opinia, że polskie służby nie wykorzystują w pełni potencjału wywiadu jawnoźródłowego z powodu niedoboru wykwalifikowanych specjalistów.

W odniesieniu do działań ofensywnych opinie ekspertów były bardziej zróżnicowane. Część z nich uważa, że wywiad jawnoźródłowy jest przydatny w identyfikacji słabości przeciwnika i planowaniu operacji zaczepnych, natomiast inni wskazali na ograniczenia wynikające z ogólnej dostępności tych danych, co może obniżać ich skuteczność w zaawansowanych operacjach ofensywnych. Podkreślono również, że weryfikacja informacji jawnoźródłowych staje się kluczowym elementem krzyżowej weryfikacji danych, co jest istotne zarówno dla działań wywiadowczych, jak i kontrwywiadowczych. Zauważono także, że synergia między informacjami jawnoźródłowymi a niejawnymi pozwala na bardziej kompleksowe zrozumienie przeciwników. Kilku ekspertów wyraziło obawy związane z manipulacją danymi jawnoźródłowymi, co wymaga szczególnej ostrożności w działaniach ofensywnych.

Pytanie 3: Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?

Wszyscy eksperci uznali analizę jawnoźródłową za integralny element procesu decyzyjnego dotyczącego bezpieczeństwa państwa. Podkreślano jej „istotne" i „kluczowe" znaczenie w dostarczaniu informacji niezbędnych do podejmowania decyzji. Analizy jawnoźródłowe poszerzają lub weryfikują informacje pozyskane z innych źródeł, znacząco uzupełniając informacje wywiadowcze. Dzięki temu możliwe jest zrozumienie kontekstu społecznego, politycznego oraz relacji międzynarodowych. Przyczyniają się do identyfikacji zagrożeń i podejmowania trafniejszych decyzji strategicznych, a także są wykorzystywane przy planowaniu działań informacyjnych. Dobrze przygotowane analizy materiału jawnoźródłowego mają wpływ na planowanie, przebieg oraz realizację działań operacyjnych, a także na weryfikację, czy nie doszło do dekonspiracji lub wycieku informacji.

W kontekście bezpieczeństwa ekonomicznego państwa, respondenci podkreślili znaczenie analiz jawnoźródłowych w budowaniu przewagi konkurencyjnej, trafności podejmowanych decyzji oraz optymalizacji ryzyka. Podkreślono, że analizy te wspierają działalność podmiotów gospodarczych, pozwalając lepiej oceniać zagrożenia oraz podejmować bardziej przemyślane decyzje. Wskazano na ich rolę w zapewnianiu stabilności i bezpieczeństwa państwa, szczególnie w obszarach związanych z gospodarką i relacjami międzynarodowymi.

Jeden z ekspertów zwrócił uwagę na tworzenie specjalnych komórek analiz cyberbezpieczeństwa, które integrują informacje jawnoźródłowe z innymi źródłami, w tym niejawnymi. Podkreślił, że nie zawsze wymagane są dodatkowe źródła danych, ponieważ odpowiednio zweryfikowane informacje jawnoźródłowe często wystarczają do potwierdzenia lub zaprzeczenia hipotez operacyjnych. Ponadto wskazał na konieczność posiadania odpowiednich kompetencji przez analityków oraz ich stałego rozwoju, mimo ograniczeń budżetowych. W jego opinii, inwestowanie w rozwój umiejętności pracowników bezpośrednio przekłada się na efektywność i jakość analiz, co jest kluczowe dla bezpieczeństwa cyfrowego państwa.

Z wypowiedzi ekspertów wynika, że analizy jawnoźródłowe są nie tylko niezbędne do weryfikacji informacji, ale również gwarantują, że podejmowane decyzje opierają się na rzetelnych danych. Eksperci wskazali na konieczność korzystania z szerokiego spektrum źródeł i podkreślili znaczenie szybkości dostarczania informacji.

Pytanie 4: Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

Z analizy wypowiedzi ekspertów wynika, że dostępne metody i środki stosowane w wywiadzie jawnoźródłowym są zróżnicowane i stale ewoluują w odpowiedzi na postępującą cyfryzację oraz rozwój technologii.

Eksperci wskazali szereg metod wykorzystywanych w wywiadzie jawnoźródłowym, w tym przeglądanie prasy i literatury specjalistycznej, wywiad środowiskowy, analizę mediów tradycyjnych i cyfrowych, a także monitorowanie mediów społecznościowych. Zwrócili również uwagę na istotność analizy dokumentów publicznych, takich jak raporty rządowe, ustawy oraz strategie państwowe, jak również na śledzenie działań rządu i instytucji publicznych. Ważną rolę odgrywa także uczestnictwo w konferencjach naukowych i branżowych, które dostarczają aktualnych informacji i prognoz.

W zakresie narzędzi eksperci wymienili zarówno darmowe, jak i komercyjne rozwiązania. Wśród darmowych narzędzi wskazano popularne wyszukiwarki internetowe, takie jak Google, Bing i DuckDuckGo, a także narzędzia wykorzystujące sztuczną inteligencję, takie jak Bing Chat i OpenAI. Zidentyfikowano również wyspecjalizowane narzędzia analityczne, takie jak Maltego, Shodan czy Gephi oraz tzw. crawlery, które automatycznie przeszukują różne kanały informacyjne, zapisując dane w bazach, co umożliwia ich skalowalną analizę. Eksperci zwrócili uwagę na narzędzia do analizy danych geoprzestrzennych i sieciowych oraz monitorowania mediów społecznościowych. Podkreślili również, że technologie Big Data, umożliwiające analizę obszernych zbiorów danych, stanowią przyszłość, gdyż znacznie ułatwiają identyfikację wzorców i zależności, które mogą być wykorzystywane w prewencji zagrożeń, takich jak terroryzm czy ataki cybernetyczne.

Jeden z ekspertów podkreślił znaczenie OPSEC dla efektywności działań oraz ochrony wrażliwych informacji przed ich nieautoryzowanym ujawnieniem. Proces identyfikacji i eliminacji potencjalnych zagrożeń poprzez analizę podatności i zarządzanie ryzykiem odgrywa istotną rolę zarówno przy wyborze narzędzi, jak i metod prowadzenia wywiadu jawnoźródłowego.

Eksperci zgodnie uznali, że w wywiadzie jawnoźródłowym istotna jest integracja różnych metod i narzędzi, umożliwiająca uzyskanie pełnego obrazu sytuacji. Zwrócili również uwagę na konieczność dostosowywania metod do bieżących potrzeb

operacyjnych, aby zapewnić skuteczną reakcję na zmieniające się warunki bezpieczeństwa. Podkreślili, że skuteczność wywiadu jawnoźródłowego zależy nie tylko od dostępu do zaawansowanych narzędzi, ale także od kompetencji analityków, zwłaszcza w zakresie selekcji i weryfikacji pozyskanych informacji.

Pytanie 5: Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

Eksperci jednogłośnie uznali weryfikację informacji pozyskiwanych drogą wywiadu jawnoźródłowego za niezbędną. Proces ten został określony jako: "obligatoryjny", "kluczowy", "bardzo istotny" i "celowy", ze względu na konieczność zapewnienia rzetelności i wiarygodności tych informacji. Eksperci podkreślili, że informacje jawnoźródłowe muszą być weryfikowane, ponieważ otwarte źródła są podatne na dezinformację stosowaną przez przeciwników. Podobnie jak w odpowiedzi na pytanie nr 4, niektórzy respondenci ponownie podkreślili zasadniczą rolę analityków, ich specjalistycznej wiedzy, umiejętności krytycznego myślenia i analizy oraz uwzględniania kontekstów kulturowych.

Weryfikacja informacji pozyskanych drogą wywiadu jawnoźródłowego odbywa się na wielu poziomach i za pomocą różnych metod. Informacje te są sprawdzane poprzez porównanie ich ze źródłami operacyjno-technicznymi oraz danymi pochodzącymi z wewnętrznych systemów informacyjnych. Zgodnie podkreślono znaczenie weryfikacji krzyżowej z kilkoma różnymi źródłami. Jeden z ekspertów zauważył, że proces ten opiera się na zaawansowanych technologiach, natomiast inny zwrócił uwagę, że do weryfikacji używa się tych samych narzędzi, które służą do pozyskiwania informacji jawnoźródłowych.

Eksperci wskazali na dwa zasadnicze aspekty weryfikacji informacji jawnoźródłowych tj.: ocenę źródeł oraz weryfikację samych informacji. Weryfikacja otwartych źródeł informacji obejmuje analizę ich reputacji, kontekstu funkcjonowania, historii publikacji oraz źródeł finansowania, co pozwala na ocenę niezależności danego źródła. Istotnym elementem procesu weryfikacji akcentowanym przez respondentów jest sprawdzanie krzyżowe, polegające na porównaniu informacji z innymi niezależnymi źródłami. W weryfikacji informacji jawnoźródłowych dużą rolę odgrywają analiza kontekstu, w jakim informacja została opublikowana, możliwe powiązania między faktami oraz analiza tonu i języka, który został użyty.

Jeden z ekspertów wskazał, że weryfikacja informacji jawnoźródłowych opiera się na trzech podstawowych metodach: fuzji danych, różnicowaniu oraz kooperacji. Fuzja danych polega na integracji informacji z różnych źródeł, co umożliwia stworzenie spójnego obrazu sytuacji oraz identyfikację braków. Różnicowanie pozwala na porównanie informacji w celu wykrycia sprzeczności, natomiast kooperacja umożliwia łączenie uzupełniających się informacji z różnych źródeł, tworząc spójną całość.

Pytanie 6: Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

Wśród opinii ekspertów można wyodrębnić główne kierunki rozwoju metod i środków technicznych wywiadu jawnoźródłowego, takie jak sztuczna inteligencja (SI) oraz zaawansowane narzędzia Big Data, które mają na celu automatyzację procesów pozyskiwania i analizy informacji. Uczenie maszynowe, będące kluczowym elementem SI, może wspierać zarówno automatyzację analizy danych, jak i identyfikację wzorców w czasie rzeczywistym.

Eksperci jednoznacznie wskazali, że głównym kierunkiem rozwoju wywiadu jawnoźródłowego będzie integracja sztucznej inteligencji w narzędziach i metodach wykorzystywanych do pozyskiwania oraz analizy informacji jawnoźródłowych. SI umożliwi automatyzację tych procesów, co przyspieszy przetwarzanie dużych zbiorów danych. Narzędzia oparte na SI pozwolą na bardziej efektywną analizę tekstu, obrazu, dźwięku oraz innych treści multimedialnych, a także na identyfikację wzorców i zależności. Zastosowanie sztucznej inteligencji w połączeniu z sieciami sensorów przyspieszy procesy przetwarzania i porównywania danych, co może znacząco poprawić ocenę sytuacji w czasie rzeczywistym.

Kolejnym istotnym kierunkiem rozwoju będzie doskonalenie narzędzi do analizy mediów społecznościowych i cyfrowych śladów, które umożliwiają identyfikację trendów i monitorowaniu aktywności w cyberprzestrzeni. Innym elementem rozwoju jest doskonalenie narzędzi analitycznych służących do weryfikacji zarówno otwartych źródeł jak i informacji jawnoźródłowych. Jeden z ekspertów podkreślił potencjał zastosowania technologii blockchain jako środka do usprawnienia procesu weryfikacji informacji jawnoźródłowych.

W zakresie metod eksperci wskazali na rozwój analizy predykcyjnej, analizy semantycznej oraz analizy sieci społecznościowych, a także na zwiększenie integracji danych pochodzących z różnych źródeł.

Mimo rozwoju technologii, eksperci ponownie podkreślili zasadniczą rolę analityków, wskazując na konieczność ludzkiej weryfikacji i kontroli nad wszystkimi etapami wywiadu jawnoźródłowego. Analitycy, wyposażeni w odpowiednią wiedzę, umiejętności oraz zdolność krytycznego myślenia, pozostają nieodzowni w ocenie i interpretacji informacji.

Eksperci zwrócili uwagę, że rozwój metod i narzędzi prowadzenia wywiadu jawnoźródłowego stwarza potrzebę specjalistycznych szkoleń dla podmiotów odpowiedzialnych za bezpieczeństwo państwa.

Kolejnym kierunkiem rozwoju będzie integracja OSINT z innymi dyscyplinami wywiadowczymi, co umożliwi tworzenie bardziej wielowymiarowych analiz, zwiększając tym samym efektywność działań na rzecz bezpieczeństwa państwa.

Pytanie 7: Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? Czy wpływają one na zapewnienie bezpieczeństwa państwa?

Z analizy wypowiedzi ekspertów wynika, że jednym z najważniejszych ograniczeń w wywiadzie jawnoźródłowym jest podatność informacji pochodzących z otwartych źródeł na manipulację, w tym wymienione dezinformacja, propaganda, fake newsy oraz smog informacyjny. Wrogie podmioty mogą celowo rozpowszechniać fałszywe informacje, wprowadzając chaos i destabilizację. O ile wykrycie takich działań może dostarczyć cennych wskazówek co do strategii przeciwnika, to ich identyfikacja nie zawsze jest możliwa, co może prowadzić do błędnych decyzji operacyjnych.

Pewne ograniczenia wynikają także z samego charakteru otwartych źródeł informacji. Cechy jawnoźródłowych danych, takie jak ich ogromna ilość, powszechna dostępność oraz określone przez jednego z ekspertów zjawisko „INFOdemii", mogą utrudniać ich efektywne przetwarzanie. Ponadto, zakres tematyczny dostępnych informacji z otwartych źródeł bywa ograniczony, co sprawia, że istotne z perspektywy bezpieczeństwa państwa obszary pozostają poza zasięgiem analizy jawnoźródłowej. Zbyt szerokie gromadzenie informacji jawnoźródłowych dodatkowo komplikuje ich analizę i weryfikację, stanowiąc tym samym przeszkodę w pracy operacyjnej.

Kolejnym wskazanym ograniczeniem są kwestie etyczne oraz prawne, zwłaszcza te związane z prywatnością i ochroną danych osobowych. Chociaż

pozyskiwanie pojedynczych informacji jawnoźródłowych nie narusza prawa, ich agregacja i przetwarzanie mogą prowadzić do identyfikacji osób fizycznych, a w rezultacie do naruszenia norm prawnych i etycznych.

Eksperci zwrócili również uwagę na aspekty techniczne związane z zarządzaniem dużymi ilościami danych, w tym trudności w ich normalizacji oraz interoperacyjności między różnymi systemami. Rozbieżności w architekturze systemów informacyjnych oraz brak jednolitych standardów mogą prowadzić do opóźnień w przekazywaniu i analizowaniu informacji, co negatywnie wpływa na skuteczność działań prewencyjnych i operacyjnych. Ponadto, mimo że na rynku dostępnych jest wiele narzędzi OSINT, ich różnorodność oraz ograniczenia sprawiają, że nie zawsze możliwe jest pełne i efektywne wykorzystanie zgromadzonych informacji jawnoźródłowych.

Eksperci wskazali również na ograniczenia finansowe. Dostęp do specjalistycznych baz danych, narzędzi analitycznych oraz koszty mocy obliczeniowej niezbędnej do pozyskiwania, przetwarzania i przechowywania informacji jawnoźródłowych są często wysokie, a subskrypcje mogą stanowić znaczne obciążenie dla budżetu instytucji publicznych. Wymusza to konieczność podejmowania decyzji o priorytetach finansowych, co w konsekwencji może ograniczać zakres monitorowanych źródeł i analizowanych danych.

Dodatkowo, kilku respondentów zwróciło również uwagę na ograniczenia wynikające z braku efektywnej współpracy między służbami. Kultura „tajności", głęboko zakorzeniona w ich działaniach, stanowi poważną przeszkodę w swobodnej wymianie materiałów jawnoźródłowych. Pozostałe ograniczenia wskazane przez ekspertów dotyczyły kompetencji osób zaangażowanych w analizę informacji jawnoźródłowych, w tym ich doświadczenia, umiejętności, wiedzy specjalistycznej oraz predyspozycji psychologicznych.

Z wypowiedzi ekspertów wynika, że wszystkie te ograniczenia mają bezpośredni wpływ na efektywność oraz czas przekazywania informacji, a w konsekwencji także na czas potrzebny do podjęcia decyzji związanych z bezpieczeństwem państwa.

Pytanie 8: Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Na podstawie analizowanych odpowiedzi można stwierdzić, że brak profesjonalnej weryfikacji i analizy informacji jawnoźródłowych może stanowić zagrożenie dla bezpieczeństwa państwa. Eksperci określili konsekwencje w sposób zróżnicowany – „od banalnych po tragiczne", w tym „poważne", „bardzo poważne", „bardzo duże", a nawet „dramatyczne". Jeden z ekspertów wyraził stanowcze przekonanie, że wykorzystywanie informacji jawnoźródłowych bez odpowiedniej weryfikacji nie powinno mieć miejsca w obszarze bezpieczeństwa państwa.

Przede wszystkim, informacje jawnoźródłowe są podatne na dezinformację, a brak ich weryfikacji może prowadzić do podejmowania błędnych decyzji o charakterze politycznym, militarnym czy gospodarczym, zwłaszcza w strategicznych obszarach, takich jak produkcja żywności, leków czy sprzętu wojskowego. Eksperci zwrócili uwagę na fakt, że dezinformacja może stanowić narzędzie wroga, który prowadzi działania mające na celu destabilizację i dezintegrację państwa. W kontekście cyberprzestrzeni, brak profesjonalnej analizy informacji może dodatkowo potęgować zagrożenia związane z działaniami hybrydowymi, w tym atakami cybernetycznymi.

Niewłaściwie zweryfikowane informacje mogą prowadzić do błędnych interpretacji sytuacji, skutkując nieefektywnym alokowaniem zasobów lub eskalacją konfliktów. Respondenci wskazali, że przykłady błędów wywiadowczych wynikających z braku odpowiedniej analizy miały poważne konsekwencje, zarówno wewnętrzne, jak i międzynarodowe. Brak rzetelnej analizy danych stwarza ryzyko podejmowania nieodpowiednich działań, co destabilizuje sytuację wewnętrzną i relacje międzynarodowe. Rozpowszechnianie niezweryfikowanych informacji gospodarczych i politycznych może być narzędziem dla obcych wywiadów, prowadząc do szpiegostwa, manipulacji i działań przeciwko interesom państwa, szczególnie w odniesieniu do danych o problemach finansowych firm lub osób publicznych.

Wykorzystanie informacji jawnoźródłowych bez profesjonalnej analizy i weryfikacji może prowadzić również do utraty zaufania społecznego oraz podważenia wiarygodności decydentów i instytucji państwowych. Publikowanie niezweryfikowanych materiałów dotyczących konfliktów zbrojnych, zawierających treści drastyczne lub agresywne, prowadzi do zjawiska, które jeden z respondentów

określił jako „oswajanie z agresją". Brak weryfikacji informacji jawnoźródłowych, w połączeniu z nieautoryzowanym ujawnieniem danych prywatnych, może negatywnie wpłynąć na prywatność obywateli oraz funkcjonowanie systemu państwowego.

Eksperci podkreślili, że profesjonalna weryfikacja informacji jawnoźródłowych jest niezbędna dla zapewnienia, że decyzje podejmowane przez władze państwowe opierają się na rzetelnych i wiarygodnych danych. Brak takiej analizy może skutkować utratą zaufania społecznego do instytucji państwowych oraz obniżeniem efektywności działań w sytuacjach kryzysowych. Zwrócono również uwagę, że konieczne jest zastosowanie rygorystycznych metod weryfikacji informacji dla zapewnienia skuteczności działań w obszarze bezpieczeństwa. Ponadto analitycy muszą być świadomi swojej odpowiedzialności za rozpowszechnianie danych oraz ich wpływu na percepcję bezpieczeństwa w społeczeństwie.

Pytanie 9: Czy według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Analiza odpowiedzi ekspertów wskazuje na istotny wpływ omawianych zjawisk na wywiad jawnoźródłowy, podkreślając jego rosnącą rolę w zapewnieniu bezpieczeństwa państwa. Procesy te generują zarówno szanse, zagrożenia, jak i wyzwania, które zostały wyodrębnione i przedstawione w tabeli 5.1.

Tabela 6.1. Szanse, zagrożenia i wyzwania dla wywiadu jawnoźródłowego wynikające z globalizacji, integracji oraz rozwoju cyberprzestrzeni

	SZANSE
GLOBALIZACJA	• Zwiększenie ilości i dostępności informacji jawnoźródłowych w skali globalnej • Niskie koszty pozyskiwania informacji jawnoźródłowych • Lepsza identyfikacja i analiza globalnych trendów oraz zagrożeń w zakresie bezpieczeństwa • Zwiększenie świadomości sytuacyjnej • Ułatwienie analizy jawnoźródłowej poprzez ujednolicenie standardów działania oraz pogłębione zrozumienie różnic kulturowych

	ZAGROŻENIA
	• Nadmiar informacji może prowadzić do przeciążenia służb bezpieczeństwa • Zwiększona niepewność utrudnia weryfikację informacji jawnoźródłowych • Wzrost liczby środowisk, które należy analizować w celu wnioskowania na temat bezpieczeństwa państwa • Rosnąca ilość informacji utrudnia weryfikację ich wiarygodności • Ryzyko wykorzystania publikowanych danych przez obce służby lub instytucje • Ryzyko dezinformacji i kształtowania nastrojów • Zwiększona ekspozycja na ataki ze strony obcych służb oraz instytucji
	WYZWANIA
	• Zarządzanie i analiza ogromnych ilości danych • Zapewnienie skutecznej weryfikacji rosnącej ilości danych • Uwzględnienie aspektów kulturowych i różnic językowych w analizie informacji jawnoźródłowych • Odpowiedzialność za publikowane treści i cyberhigiena w sferze bezpieczeństwa • Konieczne zwiększenie umiejętności analitycznych • Edukacja społeczeństwa w bezpiecznym wykorzystaniu informacji cyfrowych
INTEGRACJA	**SZANSE**
	• Możliwość szybszej i bardziej efektywnej wymiany informacji jawnoźródłowych między państwami w ramach struktur międzynarodowych.
	ZAGROŻENIA
	• Brak skutecznej analizy i działań zarządczych państwa w ramach reagowania na procesy globalizacji, integracji i rozwoju cyberprzestrzeni
	WYZWANIA
	• Współpraca międzynarodowa i koordynacja działań OSINT

ROZWÓJ CYBERPRZESTRZENI	
	SZANSE
	• Rozwój zaawansowanych narzędzi analitycznych wspomagających wywiad jawnoźródłowy • Efektywne śledzenie cyberzagrożeń i działań dezinformacyjnych • Wykorzystanie wywiadu jawnoźródłowego w zwalczaniu dezinformacji • Skuteczniejsze zarządzanie ryzykiem
	ZAGROŻENIA
	• Złożoność i połączenie systemów informacyjnych zwiększają ryzyko manipulacji i błędów. • Wzrost liczby cyberataków i działań wrogich podmiotów w cyberprzestrzeni. • Zależność od technologii, która może zostać wykorzystana przez obce służby do działań destabilizujących.
	WYZWANIA
	• Świadomość i umiejętność korzystania z narzędzi cyfrowych. • Skuteczna analiza i weryfikacja danych w coraz bardziej złożonych i zintegrowanych systemach informacyjnych. • Wyzwania związane z ochroną danych osobowych, ochroną prywatności i cyberbezpieczeństwem. • Zachowanie zdolności do ciągłego dostosowywania się do dynamicznego postępu technologicznego.

Pytanie 10: Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?

Z przeprowadzonych wywiadów wynika, że materiał jawnoźródłowy odgrywa znaczącą rolę w identyfikacji zagrożeń i kształtowaniu polityki bezpieczeństwa w państwach demokratycznych. Stanowi on istotne wsparcie dla procesów decyzyjnych, umożliwiając bieżącą ocenę ryzyk oraz bardziej świadome i efektywne reagowanie na zmieniające się warunki. Właściwe zarządzanie i integracja tych informacji z innymi źródłami informacji są kluczowe dla zachowania bezpieczeństwa i stabilności państwa.

Materiał pozyskiwany z otwartych źródeł, po przeprowadzeniu odpowiedniej weryfikacji i analizy, dostarcza decydentom informacji, umożliwiając stworzenie

szczegółowego obrazu osób, zdarzeń oraz podmiotów. Stanowi fundament dla szybszej identyfikacji wyzwań i zagrożeń oraz formułowania skutecznych strategii ich przeciwdziałania, monitorowania trendów, sytuacji międzynarodowej oraz analizy opinii publicznej. Dodatkowo, materiał jawnoźródłowy wspiera wyznaczanie kierunków zastosowania specjalistycznych rozwiązań w wywiadzie cyfrowym oraz zadaniowanie osobowych źródeł informacji. Odpowiednio zinterpretowane dane jawnoźródłowe wspomagają proces podejmowania decyzji zarówno w sytuacjach kryzysowych, jak i w działaniach prewencyjnych, a także odgrywają istotną rolę w weryfikacji dezinformacji.

Jeden z respondentów zwrócił uwagę, że w obliczu kryzysu elit politycznych materiał jawnoźródłowy powinien stanowić narzędzie wspierające proces decyzyjny, dostarczając raporty i rekomendacje umożliwiające podejmowanie racjonalnych, a nie emocjonalnych decyzji. Koncentracja na priorytetach, takich jak bezpieczeństwo i dobrostan społeczeństwa, pozwoli uniknąć analiz nieistotnych zagadnień.

Eksperci ponownie podkreślili, że skuteczne wykorzystanie materiału jawnoźródłowego wymaga profesjonalnej analizy, opartej na dogłębnym zrozumieniu procesów gospodarczych, politycznych i społecznych. Niewłaściwa interpretacja materiałów jawnoźródłowych, wynikająca z powierzchownej analizy, może prowadzić do błędnych decyzji. Dlatego kluczowe jest, aby opinie i rekomendacje były formułowane przez doświadczonych specjalistów w sposób rzetelny i obiektywny.

Pytanie 11: Czy według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Respondenci jednoznacznie potwierdzają, że kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe jest nie tylko zasadna, ale i niezbędna dla zapewnienia bezpieczeństwa państwa.

Współpraca z partnerami umożliwia dostęp do szerszego zakresu danych, co pozwala na lepsze rozpoznanie zagrożeń, zarówno lokalnych, jak i globalnych. Dzięki wymianie informacji, państwa mogą zwiększać efektywność działań na rzecz bezpieczeństwa, w tym swoje zdolności obronne, operacyjne oraz potencjał rozpoznawczy. Kooperacja międzynarodowa w zakresie wywiadu jawnoźródłowego przyczynia się do skuteczniejszego przeciwdziałania współczesnym zagrożeniom, takim jak terroryzm, cyberataki czy dezinformacja. Wspólne działania umożliwiają wymianę

wiedzy o zjawiskach społecznych oraz nowo powstających grupach przestępczych, a także doświadczeń i najlepszych praktyk. Mogą stanowić uzupełnienie informacji niejawnych oraz inicjować pracę nad zidentyfikowanymi ryzykami transgranicznymi. Jeden z ekspertów stwierdził, że w niektórych aspektach zasadny jest dialog nawet z krajami o odmiennych interesach, takimi jak Korea Północna czy Rosja, zwłaszcza w kontekście zagrożeń terrorystycznych, zwalczania przestępczości zorganizowanej czy proliferacji broni atomowej, biologicznej i chemicznej.

Eksperci podkreślili, że współpraca między sojusznikami powinna opierać się na wzajemnym zaufaniu oraz poszanowaniu suwerenności państw, zgodnie z obowiązującym prawem międzynarodowym. Wymiana danych jawnoźródłowych musi być prowadzona na zasadach równości i wspólnych interesów, z uwzględnieniem potrzeb i priorytetów każdego partnera. Ważne jest również wprowadzenie odpowiednich mechanizmów bezpieczeństwa, które obejmują ochronę przesyłania informacji jawnoźródłowych, a także przestrzeganie standardów etycznych i prawnych. Współpraca tego typu przynosi korzyści w postaci oszczędności zasobów i czasu, dzięki wykorzystaniu już zweryfikowanych danych. Jeden z ekspertów zwrócił uwagę na konieczność weryfikacji materiałów przekazanych przez sojuszników w kontekście ich zgodności ze specyficznymi wymaganiami i oczekiwaniami.

Według opinii jednego z respondentów, obecne sojusze są często „iluzoryczne" i cechuje je brak zaufania pomiędzy państwami członkowskimi, co obniża jakość wymiany informacyjnej. Stwierdził również, że Europa nie osiągnęła znaczącego postępu w porównaniu do dynamicznie rozwijających się potęg, takich jak Chiny czy Indie, podkreślając konieczność budowania silnych relacji opartych na zaufaniu oraz tworzenia centrów analitycznych i grup roboczych, które mogłyby efektywnie wykorzystywać wywiad jawnoźródłowy i wspierać decyzje strategiczne na różnych poziomach.

Eksperci podkreślili jednocześnie, że współpraca międzynarodowa wymaga ostrożności oraz starannego doboru materiału, aby uniknąć ujawnienia sojusznikom słabych punktów, zwłaszcza w kontekście zmiennych relacji międzynarodowych. Istotne jest rozważenie, czy wszystkie elementy wiedzy kluczowe dla bezpieczeństwa są priorytetem dla głównego sojusznika, czy też mogą być traktowane inaczej w zależności od jego priorytetów.

6.1.3. Wnioski

Analiza zebranego materiału badawczego z przeprowadzonych wywiadów IDI umożliwia sformułowanie wniosków, które bezpośrednio odnoszą się do postawionych problemów badawczych. Szczegółowa interpretacja wypowiedzi respondentów pozwala na dogłębną ocenę badanej problematyki oraz wskazuje na zależności i zjawiska istotne dla dalszych rozważań nad tematyką wywiadu jawnoźródłowego i jego roli w zapewnieniu bezpieczeństwa państwa.

W odniesieniu do pierwszego problemu badawczego: ***Jaka jest istota i znaczenie wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa?*** odpowiedzi respondentów wykazały, że:

- Wywiad jawnoźródłowy odgrywa istotną rolę w zapewnianiu bezpieczeństwa państwa na różnych poziomach zarządzania, od lokalnego po międzynarodowy, umożliwiając szybką reakcję na zagrożenia oraz wspierając decyzje strategiczne dzięki dostępności i szybkości przekazu informacji.
- Wywiad jawnoźródłowy uzupełnienia informacje uzyskane z innych źródeł, tworząc kompleksowy obraz zagrożeń i szans dla bezpieczeństwa państwa. Integracja informacji jawnoźródłowych z informacjami operacyjnymi na wczesnym etapie analizy zwiększa zrozumienie sytuacji i efektywność planowania działań na rzecz bezpieczeństwa państwa.
- Dynamicznie zmieniające się zależności międzynarodowe i rozwój technologii informacyjnych zwiększają znaczenie wywiadu jawnoźródłowego dla efektywnego reagowania na zagrożenia oraz identyfikacji i przeciwdziałania dezinformacji.
- Potencjał wywiadu jawnoźródłowego nie jest w pełni wykorzystany, szczególnie w aspektach identyfikacji możliwości dla rozwoju gospodarczego i strategicznego państwa**.**

Analizując drugi szczegółowy problem badawczy: ***W jakim zakresie dostępne metody i środki prowadzenia wywiadu jawnoźródłowego wpływają na bezpieczeństwo państwa?*** Uzyskane dane pozwalają stwierdzić, że:

- Zastosowanie nowoczesnych technologii (w tym sztucznej inteligencji), służących do pozyskiwania i analizy informacji zwiększają efektywność wywiadu jawnoźródłowego.

- Automatyzacja procesów pozyskiwania i analizy danych jawnoźródłowych skraca czas niezbędny do przetwarzania informacji, co przyczynia się do szybszego reagowania na zagrożenia.
- Nowoczesne narzędzia OSINT pozwalają na szersze i ciągłe monitorowanie otwartych źródeł, co zwiększa możliwości identyfikacji i oceny zagrożeń dla bezpieczeństwa państwa.
- Integracja różnorodnych metod i narzędzi wywiadu jawnoźródłowego umożliwia pozyskiwanie bardziej szczegółowych i dokładnych informacji z otwartych źródeł, co zwiększa efektywność wywiadowczą i dokładność w ocenie zagrożeń dla bezpieczeństwa państwa.

W zakresie trzeciego problemu badawczego: ***Jakie prawne i pozaprawne aspekty wpływają na prowadzenie wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa?*** Można wnioskować, że:

- Manipulacja informacją jest największym wyzwaniem wywiadu jawnoźródłowego prowadzonego dla zapewnienia bezpieczeństwa państwa. Stosowanie dezinformacji w celu osiągania korzyści politycznych, militarnych i gospodarczych utrudnia wykorzystanie materiału jawnoźródłowego przy podejmowaniu decyzji na rzecz bezpieczeństwa państwa.
- Aspekty prawne i etyczne wpływając na zakres i sposób pozyskiwania oraz analizowania informacji jawnoźródłowych.
- Aspekty technologiczne (dostęp do nowoczesnych narzędzi OSINT, agregowanie dużych zbiorów danych i ich magazynowanie), ekonomiczne (koszty narzędzi, zakupu baz danych, szkoleń) i organizacyjne (brak współpracy między instytucjami wynikający z niskiego poziomu zrozumienia danej problematyki) ograniczają zdolność do szybkiego reagowania na zagrożenia dla bezpieczeństwa państwa.
- Brak specjalistycznej wiedzy i umiejętności analitycznych oraz tematycznych szkoleń funkcjonariuszy, wpływają negatywnie na efektywność wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa.

W odniesieniu do czwartego szczegółowego problemu badawczego: ***Jakie są dotychczasowe kierunki prowadzenia wywiadu jawnoźródłowego na rzecz bezpieczeństwa w wybranych państwach demokratycznych?*** Przeprowadzone badania ujawniły:

- Państwa demokratyczne coraz częściej angażują się w międzynarodowe sieci współpracy, aby wymieniać się informacjami jawnoźródłowymi, co zwiększa ich zdolności rozpoznawcze i obronne.
- Wymiana informacji jawnoźródłowych z sojusznikami umożliwia lepsze zrozumienie i reagowanie na globalne wyzwania bezpieczeństwa, takie jak terroryzm, cyberataki czy dezinformacja, co wspiera decyzje strategiczne w poszczególnych państwach.
- Zachowanie odpowiednich mechanizmów bezpieczeństwa oraz przestrzeganie standardów etycznych i przepisów prawnych jest kluczowe dla efektywnej współpracy w zakresie wymiany informacji jawnoźródłowych między państwami sojuszniczymi.
- Wywiad jawnoźródłowy w państwach demokratycznych wspiera procesy decyzyjne, dostarczając niezbędnych informacji do identyfikacji zagrożeń, szans i wyzwań, co umożliwia formułowanie skutecznych strategii bezpieczeństwa.

6.2. Wnioski wynikające z pracy

Rewolucja technologiczna XXI wieku, obejmująca rozwój sztucznej inteligencji, uczenia maszynowego, Internetu rzeczy, automatyzacji i robotyki oraz usług cyfrowych doprowadziła do znaczących zmian w komunikacji społecznej, strukturze gospodarczej, a także w porządku społecznym i politycznym.

Widoczna jest wyraźna zmiana w postrzeganiu znaczenia wywiadu jawnoźródłowego przez służby wywiadowcze na świecie. Ze względu na tradycyjną kulturę tajności, kultywowaną w tych służbach, oraz brak ograniczeń w dostępie do otwartych źródeł przez długi czas był on postrzegany jako marginalny. Jednak wraz z postępem technologicznym, zmianami w komunikacji społecznej oraz dynamicznym rozwojem otwartych źródeł informacji wywiad jawnoźródłowy zyskał na znaczeniu. Trend ten znajduje odzwierciedlenie zarówno w dokumentach prawnych, jak i w działaniach państw, które dążą do maksymalnego wykorzystania pełnego potencjału tej formy wywiadu.

Znaczący wpływ na postrzeganie roli wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa wywarł konflikt w Ukrainie, gdzie od samego początku odnotowano bezprecedensowe wykorzystanie OSINT, dotychczas charakterystyczne głównie dla działań wywiadu wojskowego. Wywiad jawnoźródłowy jest używany m.in.

do identyfikacji zmian w rozmieszczeniu sił przeciwnika, ujawniania zbrodni wojennych oraz monitorowania sytuacji operacyjnej na froncie.

Na podstawie wyników badań empirycznych oraz analizy teoretycznej można stwierdzić, że znaczenie wywiadu jawnoźródłowego dla bezpieczeństwa państwa wykazuje tendencję wzrostową. Po pierwsze, jego rosnąca jakość i trafność mają obecnie kluczowe znaczenie dla analizy wszystkich źródeł informacji, tj. HUMINT, SIGINT, IMINT i MASINT, co czyni go integralnym elementem procesów wywiadowczych. Po drugie, wzrost wartości informacyjnej wywiadu jawnoźródłowego wskazuje na konieczność jego rekonceptualizacji oraz uznania za pełnoprawną dyscyplinę w systemie wywiadowczym. Jednocześnie można antycypować, że ten kierunek rozwoju zostanie utrzymany, zważywszy na dynamiczny rozwój otwartych źródeł informacji oraz postęp technologiczny związany z ich pozyskiwaniem i przetwarzaniem.

Historycznie najnowsze rozwiązania technologiczne były opracowywane głównie przez wojsko, a następnie trafiały do sektora cywilnego. Przemiany społeczno-technologiczne oraz globalizacja przyczyniły się do wzrostu przewagi prywatnych podmiotów nad instytucjami publicznymi w zakresie kapitału finansowego i ludzkiego, co sprawiło, że obecnie to one odgrywają kluczową rolę w rozwoju technologii. Przejście do gospodarki opartej na danych radykalnie zmieniło układ sił między sferą cywilną a wojskową. Ma to fundamentalne znaczenie dla wszystkich aspektów technologii informacyjnej wykorzystywanej przez podmioty odpowiedzialne za bezpieczeństwo państwa.

Nowoczesne technologie, takie jak sztuczna inteligencja, uczenie maszynowe oraz eksploracja danych, znacząco zwiększają efektywność i precyzję procesów wywiadu jawnoźródłowego. Zarówno jakość, jak i szybkość dostarczania informacji odgrywają istotną rolę w kontekście zapewnienia bezpieczeństwa państwa. Automatyzacja procesów pozyskiwania i analizy informacji jawnoźródłowych skraca czas potrzebny na przetwarzanie dużych zbiorów danych, co pozwala na szybsze reagowanie na zagrożenia w dynamicznie zmieniającym się środowisku bezpieczeństwa. W obliczu coraz bardziej złożonego krajobrazu informacyjnego integracja zaawansowanych technologii i narzędzi analitycznych w wywiadzie jawnoźródłowym umożliwia optymalizację procesu pozyskiwania i analizy informacji. Rezultatem tej fuzji jest znaczące skrócenie czasu analizy, co przekłada się na sprawniejsze podejmowanie decyzji w obszarze bezpieczeństwa państwa.

Stworzenie scentralizowanego systemu, integrującego nowoczesne technologie i rozwiązania, jest kluczowe dla zapewnienia efektywnego pozyskiwania, przetwarzania oraz wymiany informacji jawnoźródłowych. Takie rozwiązanie na poziomie rządowym pozwoliłoby wyeliminować powielanie działań przez poszczególne służby i instytucje publiczne, które obecnie niezależnie od siebie gromadzą lub nabywają te same informacje w celu realizacji własnych zadań. Sprostanie wyzwaniom związanym z olbrzymią ilością informacji w różnych formatach i przekazywanych w wielu językach, w tym także z warstw *deep web*, jest niezbędne w obliczu rosnącej złożoności zagrożeń. Wdrożenie rządowego systemu znacząco zwiększyłoby wydajność i skuteczność działań wywiadu jawnoźródłowego, usprawniając jednocześnie wymianę informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo państwa.

Rozproszenie przepisów prawnych oraz niejednoznaczność pojęć związanych z wywiadem jawnoźródłowym, a także wybiórcze podejście do etyki skutkują niewystarczającą ochroną prywatności i bezpieczeństwa państwa. Podmioty prywatne są na pozycji uprzywilejowanej w stosunku do podmiotów państwowych, gdyż korzystając z luk prawnych, mogą pozyskiwać i przetwarzać większą ilość informacji jawnoźródłowych, co prowadzi do uzyskania przewagi konkurencyjnej, która wpływa na tworzenie innowacyjnych technologii umożliwiających szersze wykorzystanie OSINT. Tak zbudowany system legislacyjny zaburza zasadę równości dostępu do prawa w rozwoju gospodarczym. W związku z tym konieczne jest zweryfikowanie i ujednolicenie definicji, interpretacji oraz postrzegania informacji z otwartych źródeł i wywiadu jawnoźródłowego. Działania te przyczynią się do profesjonalizacji OSINT, wprowadzenia spójnych standardów operacyjnych oraz dostosowania procedur do zmieniającego się środowiska technologicznego i informacyjnego. Dodatkowo, dla utrzymania przewagi technologicznej sektora publicznego w działaniach na rzecz bezpieczeństwa państwa, konieczna jest ścisła współpraca z sektorem prywatnym, co umożliwi dostosowanie się do dynamicznych zmian w obszarze nowoczesnych technologii.

Wykorzystanie wywiadu jawnoźródłowego przez podmioty naruszające normy prawne i etyczne może osłabiać zaufanie do rzetelności działań OSINT podejmowanych przez instytucje publiczne, co zwiększa podatność społeczeństwa na dezinformację i manipulację. Na podstawie wyników badań stwierdzono, że dezinformacja jest jednym z największych wyzwań dla wywiadu jawnoźródłowego. Przeciwdziałanie tej formie manipulacji wymaga zintegrowanego podejścia, obejmującego wdrożenie

nowoczesnych technologii, wzmocnienie regulacji prawnych oraz rozwój programów edukacyjnych. Koordynacja tych trzech obszarów jest niezbędna dla ochrony procesów decyzyjnych państwa przed skutkami dezinformacji. W tym kontekście wykorzystanie nowoczesnych technologii i systemów informatycznych do monitorowania i analizy otwartych źródeł informacji staje się nieodzownym elementem strategii bezpieczeństwa, umożliwiającym wczesne wykrywanie i reagowanie na potencjalne zagrożenia.

Konieczna jest ścisła współpraca pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo w celu zapewnienia efektywnej wymiany wiedzy i doświadczeń w takich obszarach jak technologia, etyka, metodologia, weryfikacja informacji jawnoźródłowych oraz bezpieczeństwo operacyjne. Kolejnym wnioskiem jest wdrożenie kompleksowych programów szkoleniowych, obejmujących wszystkie wyżej wskazane elementy. Edukacja ta powinna być skierowana zarówno do funkcjonariuszy służb, jak i pracowników administracji publicznej, a w zakresie weryfikacji informacji – również do społeczeństwa. Programy te muszą uwzględniać nie tylko techniki pozyskiwania informacji jawnoźródłowych, ale również metody oceny ich wiarygodności i potencjalnego wpływu na bezpieczeństwo państwa. W szczególności szkolenia przeznaczone dla podmiotów publicznych powinny koncentrować się na efektywnym korzystaniu z narzędzi OSINT, rozwijaniu umiejętności analitycznych oraz krytycznym myśleniu, niezbędnym do identyfikacji potencjalnie szkodliwych dezinformacji.

Znaczenie wywiadu jawnoźródłowego w państwach demokratycznych wzrasta, co przejawia się w inwestycjach w infrastrukturę technologiczną, wprowadzaniu specjalnych strategii, rozwoju zaawansowanych narzędzi analitycznych oraz intensyfikacji współpracy z sektorem prywatnym. OSINT odgrywa coraz większą rolę w procesach decyzyjnych, umożliwiając szybszą identyfikację zagrożeń oraz podejmowanie skutecznych działań ofensywnych i defensywnych w odpowiedzi na wyzwania związane z bezpieczeństwem państwa.

Międzynarodowa współpraca w zakresie wymiany informacji jawnoźródłowych umożliwia bardziej efektywne wykorzystanie zasobów wywiadowczych i zwiększa zdolności monitorowania globalnych zagrożeń, takich jak terroryzm i cyberataki, wzmacniając tym samym zdolności obronne państw demokratycznych. Integracja wysiłków na poziomie międzynarodowym przyczynia się do lepszego zrozumienia mechanizmów rozprzestrzeniania dezinformacji oraz opracowania skutecznych strategii jej przeciwdziałania. Dla zachowania przewagi technologicznej państwa nawiązują

również współpracę z sektorem prywatnym, co pozwala na wdrażanie nowoczesnych rozwiązań i szybsze dostosowanie się do dynamicznych zmian w obszarze bezpieczeństwa.

Współpraca pomiędzy państwami demokratycznymi mogłaby zostać wzmocniona poprzez harmonizację i doprecyzowanie regulacji prawnych, zasad etycznych oraz standardów postępowania w obszarze wywiadu jawnoźródłowego. Zintegrowane podejście, uwzględniające te czynniki, jest niezbędne dla skutecznego przeciwdziałania współczesnym zagrożeniom oraz wsparcia procesów decyzyjnych.

6.3. Rekomendacje

Przedstawione poniżej rekomendacje stanowią rezultat przeprowadzonych badań oraz analiz i mają na celu wskazanie działań, które mogą przyczynić się do dalszego rozwoju oraz zwiększenia efektywności wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa. Proponowane rozwiązania odpowiadają na zidentyfikowane wyzwania oraz odzwierciedlają dynamikę współczesnego środowiska technologicznego i operacyjnego. Rekomendacje uwzględniają także doświadczenia krajów demokratycznych, które najdłużej i najskuteczniej wykorzystują wywiad jawnoźródłowy w celu zapewnienia bezpieczeństwa państwa. Wdrożenie kompleksowych rozwiązań systemowych w Polsce umożliwi efektywną integrację i analizę informacji z otwartych źródeł, co znacząco przyczyni się do wzmocnienia działań na rzecz bezpieczeństwa państwa oraz poprawy jakości procesów decyzyjnych.

W związku z powyższym autorka rozprawy proponuje następujące rekomendacje:

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

Zdefiniowanie podstawowych pojęć związanych z wywiadem jawnoźródłowym umożliwi precyzyjne określenie możliwości pozyskiwania i analizy informacji jawnoźródłowych przy użyciu środków i metod zgodnych z obowiązującymi ramami prawnymi. Wprowadzenie odpowiednich przepisów do polskiego systemu prawnego jest niezbędne dla zagwarantowania przejrzystości regulacji w zakresie wywiadu jawnoźródłowego oraz przyczyni się do jego standaryzacji i profesjonalizacji. Dostosowanie regulacji do międzynarodowych norm prawnych i standardów usprawni współpracę międzynarodową w zakresie wywiadu jawnoźródłowego.

2) Stworzenie Zespołu Koordynacyjnego ds. Wywiadu Jawnoźródłowego.

Powołanie Zespołu Koordynacyjnego ds. Wywiadu Jawnoźródłowego przyczyni się do przyspieszenia procesów pozyskiwania oraz analizy informacji jawnoźródłowych, a także wyeliminuje nieefektywność wynikającą z dublowania działań. W rezultacie poprawi to ekonomikę operacji oraz zoptymalizuje wykorzystanie zasobów. Zespół, podlegający bezpośrednio Premierowi RP, złożony z przedstawicieli poszczególnych służb i agencji rządowych, zapewni koordynację działań administracji rządowej w obszarze wywiadu jawnoźródłowego. Opracowywanie spójnych i jednolitych materiałów, opartych na informacjach zgromadzonych przez różne podmioty, zwiększy kompleksowość analiz, a także znacząco ograniczy, a nawet uniemożliwi stosowanie dezinformacji przez podmioty wrogie wobec państwa polskiego.

Do zadań Zespołu należeć będzie:

- inicjowanie, koordynowanie i monitorowanie działań podejmowanych przez właściwe organy administracji rządowej w zakresie wywiadu jawnoźródłowego;
- dostarczanie danych wyjściowych:
  - ✓ służbom specjalnym,
  - ✓ podmiotom publicznym odpowiedzialnym za bezpieczeństwo państwa, m.in. Prezydentowi, Premierowi, Marszałkom Sejmu i Senatu, Radzie Ministrów według rozdzielnika, Koordynatorowi ds. Służb Specjalnych, Szefom poszczególnych służb,
  - ✓ społeczeństwu;
- tworzenie analiz jawnoźródłowych dla:
  - ✓ służb specjalnych,
  - ✓ podmiotów publicznych,
  - ✓ społeczeństwa;
- organizowanie współpracy z innymi państwami w zakresie wywiadu jawnoźródłowego;
- udzielanie kompendium wiedzy sojuszniczym służbom zagranicznym poprzez opracowywanie zbiorczych informacji dotyczących zagrożeń nie tylko dla Polski, lecz także dla krajów będących członkami paktów i sojuszy, których Polska jest stroną;
- opracowywanie projektów:
  - ✓ standardów etycznych wywiadu jawnoźródłowego,

- ✓ procedur przeprowadzania wywiadu jawnoźródłowego,
- ✓ wytycznych za zakresie wymagań dotyczących narzędzi służących do pozyskiwania i analizy jawnoźródłowej;

– opracowywanie propozycji zmierzających do usprawnienia metod i narzędzi wykorzystywanych w wywiadzie jawnoźródłowym przez podmioty publiczne;
– monitorowanie kierunków działań dezinformacyjnych oraz otwartych źródeł, które je generują i przekazują.

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

Celem jest utworzenie wspólnej, zintegrowanej przestrzeni, która umożliwi efektywne wyszukiwanie, łączenie oraz promowanie materiałów jawnoźródłowych. Rządowa platforma OSINT przyspieszy oraz zwiększy transparentność przepływu informacji jawnoźródłowych, a także usprawni wymianę dobrych praktyk pomiędzy instytucjami. Tak skonstruowana platforma umożliwi wszystkim podmiotom odpowiedzialnym za bezpieczeństwo państwa dostęp do większej ilości informacji, które w istotny sposób przyczynią się do poprawy szybkości i jakości prowadzonych działań operacyjnych, postępowań procesowych oraz formułowania prognoz dotyczących bezpieczeństwa. Dzięki scentralizowanemu dostępowi do zasobów oraz zoptymalizowanej komunikacji zwiększy się efektywność działań związanych z wywiadem jawnoźródłowym.

4) Utworzenie Inkubatora Innowacji Wywiadu Jawnoźródłowego.

Celem inicjatywy jest rozwój współpracy pomiędzy podmiotami państwowymi a komercyjnymi w zakresie pozyskiwania i analizy informacji z otwartych źródeł. Współpraca między instytucjami publicznymi, społeczeństwem obywatelskim, podmiotami gospodarczymi oraz ośrodkami akademickim, sprzyjająca wzajemnej wymianie informacji i budowaniu trwałych więzi, zapewni kompleksowe oraz efektywne wykorzystanie zasobów i wiedzy w obszarze wywiadu jawnoźródłowego. Kadra Inkubatora będzie rekrutowana spośród byłych funkcjonariuszy służb posiadających doświadczenie w działaniach operacyjnych oraz ekspertów zaznajomionych z nowoczesnymi technologiami i współczesnym środowiskiem cyfrowym. Taka struktura zapewni optymalne połączenie wiedzy operacyjnej z innowacyjnymi rozwiązaniami technologicznymi. Współpraca z sektorem prywatnym nie tylko przyczyni się do pozyskiwania nowoczesnych rozwiązań technologicznych,

ale także umożliwi bezpieczny outsourcing procesów związanych z gromadzeniem, przetwarzaniem i analizą informacji, co pozwoli podmiotom odpowiedzialnym za bezpieczeństwo państwa skoncentrować się na bardziej złożonych zadaniach operacyjnych.

Zakres zadań Inkubatora Innowacji Wywiadu Jawnoźródłowego:

- tworzenie nowych technologii i narzędzi wywiadu jawnoźródłowego;
- rozwijanie metod, w tym algorytmów do analizy jawnoźródłowej;
- pozyskiwanie kadr do Inkubatora przy zachowaniu różnorodności zawodowej i zainteresowań osobistych;
- organizacja szkoleń dotyczących wywiadu jawnoźródłowego dla:
  - ✓ służb specjalnych,
  - ✓ pracowników jednostek sektora finansów publicznych,
  - ✓ społeczeństwa;
- organizacja konferencji, sympozjów na szczeblu rządowym i samorządowym;
- współpraca z podmiotami prywatnymi, ośrodkami akademickimi, instytucjami badawczymi.

Implementacja powyższych rekomendacji umożliwi unowocześnienie struktur bezpieczeństwa państwa polskiego, co pozwoli na skuteczniejsze przeciwdziałanie zagrożeniom wynikającym z działalności państw wrogich RP. Dostosowanie oraz przewidywanie działań przeciwników w zakresie nowych technologii i narzędzi stanowi istotny czynnik zwiększający zdolność do skutecznego reagowania na dynamiczne wyzwania w sferze bezpieczeństwa.

ZAKOŃCZENIE

Przedmiotem badań, których wyniki zaprezentowano w niniejszej rozprawie, był wywiad jawnoźródłowego realizowany w obszarze bezpieczeństwa państwa.

Identyfikacja luki badawczej pozwoliła na sformułowanie głównego problemu badawczego, który zawierał się w pytaniu: *Jakie znaczenie ma wywiad jawnoźródłowy w bezpieczeństwa państwa?*

Głównym celem badań w aspekcie poznawczym było określenie znaczenia wywiadu jawnoźródłowego dla bezpieczeństwa państwa. Natomiast w aspekcie praktycznym badania miały na celu zidentyfikowanie możliwości wykorzystania wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa. Zastosowana metodologia umożliwiła osiągnięcie tych celów, czego rezultatem było opracowanie następujących rekomendacji:

– uporządkowanie w polskim systemie prawnym niezbędnych pojęć związanych z wywiadem jawnoźródłowym;
– stworzenie Zespołu Koordynacyjnego ds. Wywiadu Jawnoźródłowego;
– stworzenie platformy wymiany informacji jawnoźródłowych jako wspólnej przestrzeni do wyszukiwania, łączenia i promowania materiałów jawnoźródłowych;
– utworzenia Inkubatora Innowacji Wywiadu Jawnoźródłowego.

W pracy wyróżniono cztery szczegółowe problemy badawcze oraz cztery hipotezy szczegółowe. Pierwszy problemem zawierał się w pytaniu: *Jaka jest istota i znaczenie wywiadu jawnoźródłowego dla bezpieczeństwa państwa?* Do problemu badawczego przyjęto hipotezę*: Dynamiczny rozwój otwartych źródeł informacji oraz technologii związanych z pozyskiwaniem i przetwarzaniem informacji jawnoźródłowych zwiększa potencjał wykorzystania wywiadu jawnoźródłowego w bezpieczeństwie państwa.* W wyniku przeprowadzonych badań stwierdzono, że rozwój otwartych źródeł informacji zwiększa możliwości wywiadu jawnoźródłowego w działaniach podejmowanych na rzecz bezpieczeństwa państwa. Tendencja ta jest szczególnie widoczna w związku z rosnącą liczbą informacji pozyskiwanych z zaawansowanych czujników, komercyjnych satelitów, smartfonów oraz sieci połączonych urządzeń noszonych, takich jak inteligentne zegarki i inne technologie biometryczne. Wywiad jawnoźródłowy wspiera podejmowanie decyzji strategicznych oraz umożliwia szybką reakcję na zagrożenia o charakterze lokalnym i międzynarodowym, uzupełniając informacje z innych źródeł i tworząc kompleksowy obraz zagrożeń oraz szans dla

bezpieczeństwa państwa. Te wyniki jednoznacznie potwierdzają hipotezę, że rozwój otwartych źródeł informacji i powiązanych technologii zwiększa potencjał OSINT w zapewnieniu bezpieczeństwa państwa.

Drugi problem badawczy to pytanie: *W jakim zakresie dostępne metody i środki prowadzenia wywiadu jawnoźródłowego wpływają na bezpieczeństwo państw?* W odpowiedzi na tak sformułowany problem badawczy przyjęto hipotezę: *Założyć można, że nowe technologie umożliwiają efektywne pozyskiwanie informacji jawnoźródłowych, przez co zwiększają precyzję i skracają czas analizy informacji jawnoźródłowych.* Nowoczesne technologie, takie jak sztuczna inteligencja, uczenie maszynowe, eksploracja danych, przetwarzanie języka naturalnego oraz big data, znacząco zwiększają efektywność pozyskiwania i przetwarzania informacji jawnoźródłowych. Automatyzacja procesów analitycznych skraca czas ich realizacji oraz poprawia precyzję wyników. W rezultacie wdrożenie tych technologii umożliwia bardziej skuteczne zarządzanie informacjami, co wzmacnia zdolność państwa do reagowania na zagrożenia i podejmowania trafniejszych decyzji strategicznych.

Kolejny problem badawczy to pytanie: *Jakie prawne i pozaprawne aspekty wpływają na prowadzenie wywiadu jawnoźródłowy na rzecz bezpieczeństwa państwa?* Do tak ujętego problemu badawczego sformułowano hipotezę: *Uwarunkowania prawne oraz pozaprawne, jak etyczne, metodologiczne, techniczne oraz informacyjne, mają wpływ na wywiad jawnoźródłowy.* Uwarunkowania prawne, w tym brak spójnych regulacji, stanowią istotne wyzwanie dla prowadzenia wywiadu jawnoźródłowego. Czynniki etyczne, metodologiczne, techniczne, informacyjne oraz zidentyfikowane dodatkowo ekonomiczne i organizacyjne kształtują proces pozyskiwania i analizy informacji, bezpośrednio wpływając na jego efektywność. W szczególności dezinformacja, niedobór zaawansowanych narzędzi technologicznych oraz brak odpowiednich szkoleń negatywnie wpływają na skuteczność wywiadu jawnoźródłowego. Zidentyfikowane uwarunkowania mają istotny wpływ na wywiad jawnoźródłowy, co potwierdza postawioną hipotezę.

Ostatnim szczegółowym problemem badawczym było pytanie: *Jakie są dotychczasowe kierunki prowadzenia wywiadu jawnoźródłowego na rzecz bezpieczeństwa w wybranych państwach demokratycznych?* Do tak sformułowanego problemu przyjęto hipotezę: *Wywiad jawnoźródłowy prowadzony jest w celu zwiększenia zdolności defensywnych i ofensywnych w wybranych państwach demokratycznych.* W wyniku przeprowadzonych badań stwierdzono, że wywiad

jawnoźródłowy odgrywa coraz większą rolę w systemach bezpieczeństwa wybranych państw demokratycznych, wspierając zarówno procesy operacyjne, jak i decyzyjne. Państwa te, dostrzegając rosnącą wartość informacji z otwartych źródeł, intensyfikują współpracę międzynarodową, co pozwala na skuteczniejsze rozpoznanie i reagowanie na globalne zagrożenia, takie jak terroryzm, cyberataki czy dezinformacja. Potwierdzono więc postawioną hipotezę, że wywiad jawnoźródłowy stanowi istotny element wzmacniający zdolności defensywne i ofensywne w zakresie bezpieczeństwa wybranych państw demokratycznych.

W wyniku przeprowadzonych w ramach procesu badawczego czynności weryfikacyjnych w odniesieniu do hipotezy głównej potwierdzono, że dynamiczny rozwój otwartych źródeł informacji oraz technologii związanych z możliwością pozyskiwania i masowej dystrybucji informacji, a także coraz szersze wykorzystanie nowych technologii do pozyskiwania i analizy informacji jawnoźródłowych powodują wzrost możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa. Informacje dostarczone w wyniku działań wywiadu jawnoźródłowego: a) uzupełniają informacje pozyskane drogą operacyjną, b) skracają czas konieczny do podjęcia decyzji, przez co c) poprawiają jakość i skuteczność działań ofensywnych i defensywnych państwa. Ostateczna weryfikacja hipotezy głównej możliwa była poprzez zastosowanie przyjętych dwóch metod badawczych: teoretycznej i empirycznej. Pierwsza grupa metod wiązała się z analizą zgromadzonej w literaturze przedmiotu wiedzy teoretycznej, druga natomiast grupa to wywiady eksperckie zrealizowane z ekspertami, posiadającymi duże doświadczenie zawodowe oraz specjalistyczną wiedzę w zakresie wywiadu jawnoźródłowego i jego zastosowania w sektorze bezpieczeństwa państwa.

W wyniku przeprowadzonych badań oraz analiz autorki pracy sformułowano zasadnicze wnioski dotyczące znaczenia wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa:

– Wzrost liczby informacji jawnoźródłowych oraz rozwój zaawansowanych narzędzi analitycznych sprawiają, że wywiad jawnoźródłowy zyskuje na znaczeniu i staje się integralnym elementem procesów wywiadowczych, przyczyniając się do bardziej efektywnego monitorowania zagrożeń oraz usprawnienia działań operacyjnych związanych z bezpieczeństwem państwa.
– Nowe technologie, takie jak sztuczna inteligencja, uczenie maszynowe, eksploracja danych oraz automatyzacja, zwiększają efektywność, poprawiają precyzję oraz

skracają czas pozyskiwania i przetwarzania informacji jawnoźródłowych, co umożliwia szybsze reagowanie na zagrożenia w dynamicznie zmieniającym się środowisku bezpieczeństwa.

- Integracja nowoczesnych narzędzi wywiadu jawnoźródłowego umożliwia precyzyjniejsze monitorowanie otwartych źródeł informacji poprzez optymalizację procesów pozyskiwania i analizy informacji.
- Uwarunkowania prawne i pozaprawne wpływają na skuteczność wywiadu jawnoźródłowego, w tym zakres i sposób pozyskiwania oraz analizowania informacji jawnoźródłowych.
- Brak jednolitych regulacji prawnych, niejednoznaczność pojęć oraz zróżnicowane podejście do etyki prowadzą do niepewności prawnej i rozbieżności interpretacyjnych, co może ograniczać efektywność wywiadu jawnoźródłowego.
- Dezinformacja stanowi jedno z największych wyzwań dla wywiadu jawnoźródłowego, a jej przeciwdziałanie wymaga zintegrowanych działań technologicznych, prawnych oraz edukacyjnych w celu ochrony procesów decyzyjnych w obszarze bezpieczeństwa państwa.
- Efektywność i skuteczność wykorzystania wywiadu jawnoźródłowego wymaga wdrożenia rozwiązań prawnych, organizacyjnych oraz technicznych, które zapewnią spójność działań instytucji odpowiedzialnych za bezpieczeństwo państwa.
- Współpraca i wymiana informacji jawnoźródłowych z partnerami zewnętrznymi, w tym z państwami sojuszniczymi, sektorem prywatnym oraz ośrodkami akademickimi, może prowadzić do standaryzacji metod pozyskiwania i analizy, osiągania bardziej powtarzalnych i wiarygodnych wyników, a także zwiększać zdolności monitorowania globalnych zagrożeń oraz wspierać rozwój skutecznych strategii przeciwdziałania dezinformacji.
- Wywiad jawnoźródłowy odgrywa istotną rolę w zwiększaniu zdolności defensywnych i ofensywnych państw demokratycznych, jest wykorzystywany do monitorowania globalnych zagrożeń, takich jak terroryzm i cyberataki, a także wspiera podejmowanie decyzji strategicznych w obszarze bezpieczeństwa państwa.

Na podstawie wyników badań zawartych w poszczególnych rozdziałach, a także wniosków końcowych i rekomendacji, uwypuklających istotne obszary wymagające dalszej eksploracji, wyłaniają się następujące kierunki dalszych badań.

Pierwszym obszarem dalszych badań jest opracowanie oraz precyzyjne uściślenie istniejących pojęć prawnych, a także wprowadzenie terminów adekwatnych

do opisania nowych zjawisk. Działania te wpisują się w rozwój teorii bezpieczeństwa, a w praktyce pozwolą na bardziej efektywne wykorzystanie wywiadu jawnoźródłowego.

Drugi obszar obejmuje intensyfikację badań interdyscyplinarnych ukierunkowanych na doskonalenie rozwiązań instytucjonalnych oraz organizacyjnych związanych z wykorzystaniem wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa.

Trzeci obszar badań dotyczy rozwoju modelu współpracy podmiotów publicznych z sektorem prywatnym i akademickim, w szczególności w kontekście tworzenia nowych narzędzi oraz rozwiązań analitycznych związanych z wywiadem jawnoźródłowym.

Czwarty obszar obejmuje badania nad doskonaleniem metod i środków wykorzystywanych w wywiadzie jawnoźródłowym, co umożliwi bardziej efektywną alokację zasobów w zależności od charakteru otwartych źródeł informacji, ich skuteczniejszą weryfikację oraz precyzyjniejszą analizę.

Procesy wywiadowcze są ściśle związane z informacją i technologią oraz z dynamicznie zmieniającym się środowiskiem, w którym funkcjonują. Wzrost liczby otwartych źródeł informacji sprawia, że podmioty odpowiedzialne za bezpieczeństwo państwa muszą zwrócić większą uwagę na ich wykorzystanie. Zdolność do wyciągania użytecznych wniosków z ogromnych ilości informacji jawnoźródłowych będzie zyskiwać na znaczeniu w kontekście zapewnienia bezpieczeństwa państwa. Podsumowując, wraz z postępem technologicznym, globalizacją i rozwojem narzędzi komunikacyjnych wywiad jawnoźródłowy odgrywa coraz większą rolę w redefiniowaniu działalności wywiadowczej, dostosowując się do nowych wyzwań i możliwości. Niniejsza rozprawa przyczynia się do rozwoju nauki o bezpieczeństwie, podkreślając potrzebę dalszych badań nad rolą wywiadu jawnoźródłowego w bezpieczeństwie państwa.

ZAŁĄCZNIKI

Załącznik 1 – Scenariusz wywiadu eksperckiego

mgr Anna Nastuła miejscowość, __-__2023/2024r.

SCENARIUSZ BADAŃ IDI

W grupie ekspertów wykorzystujących wywiad jawnoźródłowy w swojej pracy zawodowej.

Badania realizowane na potrzeby rozprawy doktorskiej na temat:

„ZNACZENIE WYWIADU JAWNOŹRÓDŁOWEGO W BEZPIECZEŃSTWIE PAŃSTWA”

METODA:

Indywidualne wywiady pogłębione (IDI) w grupie ekspertów posiadających specjalistyczną wiedzę oraz doświadczenie zawodowe w dziedzinie wywiadu jawnoźródłowego i bezpieczeństwa państwa, czas trwania ok. 120 min. każdy.

GŁÓWNE CELE BADANIA:

Poznanie opinii ekspertów dotyczących:

1. Roli i znaczenia wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa.
2. Metod i środków wykorzystywanych w wywiadzie jawnoźródłowych oraz ich wpływu na bezpieczeństwo państwa.
3. Określenie prawnych i pozaprawnych aspektów prowadzenia wywiadu jawnoźródłowego i ich wpływu na bezpieczeństwo państwa.
4. Kierunków prowadzenia wywiadu jawnoźródłowego na rzecz bezpieczeństwa państwa w krajach demokratycznych.

PRÓBA:

Eksperci wykorzystujący wywiad jawnoźródłowy w swojej pracy:

1. Gen. bryg. Paweł Pruszyński
2. Płk Sylwester Sawicki
3. Płk Dariusz Trojszczak
4. Mjr Artur Szachno
5. Ppłk Stanisław Ignaciuk
6. Ppłk dr inż. Przemysław Kornacki
7. Insp. Piotr Caliński
8. Dr hab. Mirosław Kwieciński
9. Kpt. Piotr Niemczyk
10. Bartosz Pastuszka
11. Gen. bryg. Mariusz Chmielewski
12. Płk Łukasz Wojewoda

WPROWADZENIE:

🕒 5 min

- przedstawienie głównych założeń rozprawy doktorskiej oraz przebiegu badań;
- prośba o zgodę na nagrywanie wywiadu na dyktafon.

I. WSTĘP – INFORMACJE O PODMIOCIE, W KTÓRYM EKSPERT PRACUJE

🕒 5 min

Cele:

- zebranie podstawowych informacji na temat ekspertów i podmiotów przez nich reprezentowanych

Pytania:

1) Gdzie i na jakim stanowisku Pan pracuje?
2) Jakiego rodzaju zadania realizuje prezentowany przez Pana podmiot?
3) W jakim zakresie wykorzystuje Pan wywiad jawnoźródłowy w swojej pracy?

II. ROLA I ZNACZENIE WYWIADU JAWNOŹRÓDŁOWEGO W OBSZARZE BEZPIECZEŃSTWA PAŃSTWA

🕒 20 min / 25 min

Cele:

- Zebranie opinii respondentów o roli i znaczeniu wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa
- Ustalenie przydatności wykorzystania wywiadu jawnoźródłowego w weryfikacji innych źródeł informacji w działaniach na rzecz bezpieczeństwa państwa
- Zebranie opinii ekspertów o znaczeniu analizy wywiadu jawnoźródłowego w podejmowanych przez nich decyzjach dotyczących bezpieczeństwa państwa

Pytania:

1) Czy obecne wykorzystanie wywiadu jawnoźródłowy przyczynia się do zapewnienia bezpieczeństwa państwa?
2) Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?
3) Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?

III. METODY I ŚRODKI WYKORZYSTYWANE W WYWIADZIE JAWNOŹRÓDŁOWYM ORAZ ICH WPŁYW NA BEZPIECZEŃSTWO PAŃSTWA

🕒 20 min / 25 min

Cele:

- Zebranie opinii ekspertów o metodach i środkach służących do pozyskiwania informacji jawnoźródłowych
- Analiza sposobów weryfikacji informacji pozyskanych w wywiadzie jawnoźródłowym
- Zebranie opinii respondentów o możliwych kierunkach rozwoju w zakresie metod i środków wykorzystywanych w wywiadzie jawnoźródłowym

Pytania:

1) Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

2) Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?
3) Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

IV. PRAWNE I POZAPRAWNE ASPEKTY PROWADZENIA WYWIADU JAWNOŹRÓDŁOWEGO I ICH WPŁYW NA BEZPIECZEŃSTWO PAŃSTWA

🕒 20 min / 25 min

Cele:

- Identyfikacja aspektów prawnych i pozaprawnych związanych z wywiadem jawnoźródłowym
- Analiza wpływu zidentyfikowanych uwarunkować na bezpieczeństwo państwa
- Poznanie opinii ekspertów na temat konsekwencji dla bezpieczeństwa państwa wynikających z wykorzystania niezweryfikowanego produktu wywiadowczego dostarczonego przez wywiad jawnoźródłowy

Pytania:

1) Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? Czy wpływają one na zapewnienie bezpieczeństwa państwa?
2) Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

V. KIERUNKI PROWADZENIA WYWIADU JAWNOŹRÓDŁOWEGO NA RZECZ BEZPIECZEŃSTWO PAŃSTWA W WYBRANYCH KRAJACH DEMOKRATYCZNYCH

🕒 20 min / 25 min

Cele:

- Zebranie opinie respondentów o wpływie elementów zewnętrznych na prowadzenia wywiadu jawnoźródłowego na rzecz bezpieczeństwa państwa
- Analiza możliwości podejmowania decyzji oraz określenia kierunków szans i zagrożeń dla bezpieczeństwa państwa w oparciu o materiał jawnoźródłowy

- Zebranie opinii respondentów o możliwościach, zasadności i efektywności współpracy ze strukturami wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa.

Pytania:

1) Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?
2) Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?
3) Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

METRYCZKA:

1. Wykształcenie:…….
2. Stanowisko:…….
3. Stopień naukowy:……
4. Tytuł: ……..
5. Staż pracy zawodowej:_

Załącznik 2 – Protokół I wywiadu eksperckiego

przeprowadzonego 7 grudnia 2023 r. w Warszawie

Paweł Pruszyński – były zastępca Szefa Urzędu Ochrony Państwa i Agencji Bezpieczeństwa Wewnętrznego w Warszawie odpowiedzialny m.in. za zagadnienia związane z pracą operacyjną i techniką operacyjną. Wiceprezes Stowarzyszenia Wspierania Bezpieczeństwa Narodowego. Ekspert Krajowego Stowarzyszenia Ochrony Informacji Niejawnych oraz Komitetu Bezpieczeństwa Biznesu Krajowej Izby Gospodarczej, specjalizujący się w zakresie bezpieczeństwa w cyberprzestrzeni, wykładowca akademicki.

1. **Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Wywiad jawnoźródłowy jest podstawowym narzędziem w zakresie planowania i koordynacji działań strategicznych oraz czynności bieżących. W związku z powyższym jest to czynnik wpływający na podejmowanie decyzji w zakresie bezpieczeństwa, tak na szczeblu międzynarodowym, krajowym jak i lokalnym.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

Wykorzystanie wywiadu jawnoźródłowego w swoim założeniu winno być podstawą do zadaniowania i wykorzystania informacji pochodzących z innych źródeł, myślę tu o działaniach operacyjnych tj. informacji od osobowych źródeł (HUMINT) oraz technicznych środków operacyjnych. Służby specjalne powinny traktować informacje pochodzące z wywiadu jawnoźródłowego we wstępnej fazie jako źródło ukierunkowujące, natomiast w fazie rozwiniętej jako źródło potwierdzające.

3. **Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?**

Dobrze przygotowane analizy materiału jawnoźródłowego powinny wpływać i wpływały w mojej pracy na planowanie, przebieg oraz realizację końcową działań operacyjnych. Jednocześnie służyły do weryfikacji, czy w toku pracy operacyjnej, nie nastąpiły elementy dekonspiracji lub wycieku informacji.

4. **Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?**

Do podstawowych metod i środków wykorzystywanych w wywiadzie jawnoźródłowym można zaliczyć: wyszukiwarki (w tym tematyczne), narzędzia do analizy mediów społecznościowych, uczestnictwo w konferencjach, spotkaniach naukowych oraz targach branżowych. Tego rodzaju wydarzenia dostarczają najnowszych informacji i trendów z różnych dziedzin nauki, co umożliwia przewidywanie zmian społecznych, politycznych czy technologicznych.

Pomimo tego, że technologie oferują wiele rozwiązań w zakresie wywiadu jawnoźródłowego, to jednak szczególną rolę odgrywa człowiek z jego wiedzą i doświadczeniem. Dlatego tak istotne są specjalistyczne szkolenia dla analityków OSINT, które zwiększają ich kompetencje oraz efektywność w wykorzystaniu dostępnych metod i narzędzi.

5. **Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?**

Informacje uzyskane drogą wywiadu jawnoźródłowego obligatoryjnie musza być poddawane głębokiej analizie, gdyż informacje zawarte w otwartych źródłach mogą stanowić elementy gry dezinformacyjnej stosowanej przez przeciwnika. Wtedy też jakiekolwiek podejrzane informacje należy zweryfikować poprzez źródła operacyjno-techniczne, a w momencie jednoznacznego stwierdzenia, że jest to próba dezinformacji, należy podjąć grę operacyjną.

6. **Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?**

Środki techniki operacyjnej, a szczególnie wykorzystanie Sztucznej Inteligencji, znacznie pomogą i udoskonalą pozyskiwanie oraz analizowanie informacji jawnoźródłowych. Sztuczna Inteligencja jest najwyższym stopniem, w którym zawarte jest automatyczne pozyskiwanie danych oraz uczenie maszynowe, wykorzystywane w analizie OSINT.

Niekiedy nawet drobne elementy pozyskane w ramach OSINT-u mogą stanowić podstawę do budowania obrazu podejmowanych działań przez przeciwnika. Posłużę się przykładem. Mozaikę tworzy się z drobnych elementów, które porozrzucane nie

stanowią żadnego ciekawego obrazu. Nie mają więc wartości artystycznej. Natomiast po ich odpowiednim ułożeniu stają się pięknym obrazem pokazującym dynamikę, głębię oraz kierunki przekazu artysty. To samo dotyczy działań wywiadowczych, które nawet znalazły określenie jako „wywiad mozaikowy".

7. Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? Czy wpływają one na zapewnienie bezpieczeństwa państwa?

Istnieje możliwość wprowadzania przez przeciwnika działań dezinformacyjnych. Chociaż jak wspomniałem już wcześniej, nawet dezinformacja, jeżeli zostanie przez nas wykryta jako podjęcie działań destabilizujących lub inspirujących do określonego zachowania, może mieć ogromne znaczenie, gdyż pokazuje nam kierunki zainteresowań oraz planowane przedsięwzięcia prowadzone przez przeciwnika. Drugim ograniczeniem jest zapewne aspekt prawny, gdyż forma rozrzuconej informacji nie narusza norm prawnych ani moralnych natomiast jej scalenie może być asumptem do poważnych konsekwencji, w tym wypadku tak moralnych jak i prawnych. Musimy mieć w pełni świadomość, że zbyt szerokie pozyskiwanie informacji bez ich analizy i weryfikacji jest przeszkodą a nie pomocą w pracy operacyjnej. Jest nawet na to polskie powiedzenie: „*Jak zbyt szeroko obejmujesz, to słabo ściskasz*". Niestety potwierdziło to się podczas ataku na World Trade Center, kiedy to służby specjalne Stanów Zjednoczonych posiadały bardzo dużo informacji pochodzących z otwartych źródeł, lecz poprzez ich rozproszenie i brak skoncentrowanej analizy nie stanowiły one elementu uprzedzającego i przeciwdziałającego atakowi terrorystów z użyciem samolotów pasażerskich.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Jak już powyżej stwierdziłem brak profesjonalnej analizy i weryfikacji informacji jawnoźródłowych może być nie tylko pomocą, ale i wręcz stanowić zagrożenie dla bezpieczeństwa państwa. Dziś już powinno się dokonywać analizy czy informacji przekazane, tak drogą klasyczną jak i cybernetyczną, nie stanowią podstawy do prowadzenia przez przeciwnika gry operacyjnej, która w zamiarze ma doprowadzić do destabilizacji oraz dezintegracji społeczeństwa na terenie naszego kraju. Myślę tu o wykorzystywaniu trolli oraz tzw.: „przydatnych idiotów". Musimy pamiętać, że

podejmowanie działań militarnych, czy też złożonych działań gospodarczo-politycznych, poprzedzone będzie wojną w cyberprzestrzeni. Jestem zwolennikiem twierdzenia, że wojna w cyberprzestrzeni już trwa i ukierunkowana jest przeciwko naszemu krajowi. Jeśli dzisiaj nie podejmiemy zdecydowanych działań przeciwko tej formie działalności wroga to najpóźniej za pięć lat poczujemy tego tragiczne skutki. Przyglądajmy się więc wszelkim formą dezinformacji prowadzonej przez przeciwnika, a w tym nie do przecenienia są działania wywiadu jawnoźródłowego.

9. Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Obecnie nie możemy zapomnieć o toczących się procesach geopolitycznych i traktowaniu Polski jako oderwanej cząstki od przemian i rozwoju związanego z geopolityką. Niezauważanie światowych zmian w polityce, gospodarce czy rozwoju technicznym i technologicznym nie tylko zahamowałoby postęp, ale wręcz spowodowałoby regres w rozwoju naszego kraju. Nie możemy też wyczekiwać i przyglądać na biernie rozwojowi cyberprzestrzeni i Cyber technologii, ale musimy być w tej dziedzinie aktywni i prowadzić intensywne przygotowania oraz szkolenia całego społeczeństwa w zakresie korzyści i strat z pozyskiwania informacji jawnoźródłowych na drodze elektronicznej. Jestem zwolennikiem, aby takie szkolenia rozpoczynać już w przedszkolach, oczywiście z uwzględnieniem rozwoju psychiczno-emocjonalnego w tak wczesnym wieku. Pamiętajmy, że informacje jawnoźródłowe są ogromnym dobrodziejstwem, lecz ich wykorzystanie przez przeciwnika stanowi duże zagrożenie dla społeczeństwa, a co za tym idzie zagrożeniem dla bezpieczeństwa państwa.

10. Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?

Oczywiście, że tak. Pozyskiwany materiał jawnoźródłowy, jeżeli w toku jego opracowania nie popełniono błędu, jest ogromnie pomocny w podejmowaniu prawidłowych decyzji przez decydentów politycznych, gospodarczych jak i strategicznych. Musimy jednak pamiętać, że materiał, który nie był poddany głębokiej

weryfikacji może zawierać elementy dezinformacyjne i stanowi wtedy zagrożenie w postaci błędnych decyzji.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Podpisując Sojusze i porozumienia mamy pełną świadomość konieczności współdziałania z partnerami. To informacje pozyskiwane przez naszych sojuszników mogą stanowić istotny element w budowaniu bezpieczeństwa naszego państwa. Ponadto zwiększamy potencjał rozpoznawczy, a co za tym idzie i strukturę obronną. Uzyskujemy więc więcej informacji nie ponosząc aż takich znaczących kosztów. Znów posłużę się powiedzeniem: „*Jedną gałązkę jest łatwo złamać, ale jeżeli tworzy ona pęczek jest nie do zniszczenia*". Dlatego też powinniśmy dążyć się jak najszerszej wymiany informacji z partnerami sojuszniczymi, a szczególnie dbajmy o rozwój wymiany informacji bilateralnej.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: wykładowca akademicki
3. Stopień naukowy: magister
4. Tytuł: generał brygady
5. Staż pracy zawodowej: 49 lat

Załącznik 3 – Protokół II wywiadu eksperckiego

przeprowadzonego 18 grudnia 2023 r. w Warszawie

Sawicki Sylwester – Dyrektor Departamentu Zezwoleń i Koncesji Ministerstwa Spraw Wewnętrznych i Administracji, Inspektor Policji w stanie spoczynku.

1. **Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Wywiad jawnoźródłowy przyczynia się do zapewnienia bezpieczeństwa, choć jego bezpośredni wpływ może być bardziej zauważalny w kontekście bezpieczeństwa publicznego, co jednak wpływa na bezpieczeństwo państwa. Dzięki wykorzystaniu dostępnych informacji jawnoźródłowych, policja może nie tylko szybciej reagować na potencjalne zagrożenia, ale również weryfikować i uzupełniać dane z innych źródeł, co wzmacnia działania prewencyjne oraz operacyjne służb.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

W dzisiejszych czasach, ogólna dostępność informacji jawnoźródłowych w Internecie, odgrywa kluczową rolę w procesie weryfikacji i uzupełniania danych przez służby takie jak policja. Korzystając z różnorodnych wyszukiwarek tematycznych, informacje te są wykorzystywane zarówno na etapie rozpoznawania zagrożeń, jak i w toku postępowań przygotowawczych. Pierwotne dane z systemów policyjnych, takich jak Krajowy System Informacji Policyjnej, są uzupełniane o dane z sieci Internet. Proces ten może również przebiegać w odwrotnej kolejności, tzn. w toku prowadzonego rozpoznania dotyczącego zagrożeń lub osób, informacje jawnoźródłowe pozyskane z Internetu mogą stanowić punkt wyjścia do dalszego poszerzania wiedzy przy wykorzystaniu systemów policyjnych. Dzięki temu możliwe jest kompleksowe gromadzenie danych poprzez łączenie tradycyjnych metody rozpoznania z nowoczesnymi technologiami dostępu do informacji.

3. **Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?**

W podejmowanych działaniach policja opiera się na wykorzystaniu mnogości dostępnych źródeł informacji, dlatego tak istotne są informacje jawnoźródłowe oraz ich

duża różnorodność. Nie opieramy się wyłącznie na jednym źródle; informacje pozyskane w toku działań statutowych są uzupełniane danymi z dedykowanych systemów policyjnych. Jednak kluczowe jest to, że analiza obejmuje wszystkie dostępne elementy, zarówno z systemów policyjnych, jak i otwartych źródeł informacji, w tym prasy, mediów i informacji pozyskanych z Internetu m.in.: z różnorodnych forów społecznościowych, które mogą być skarbnicą wiedzy. Takie podejście pozwala na pełniejsze rozpoznanie i zwiększa efektywność podejmowanych działań.

4. Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

Tradycyjnie, jedną z podstawowych metod wywiadu jawnoźródłowego jest wywiad środowiskowy, polegający na bezpośrednim kontakcie z osobami znajdującymi się na danym terenie, często z osobami starszymi, które spędzają czas na zewnątrz i posiadają szeroką wiedzę na temat lokalnej społeczności. Taka metoda opiera się na zyskaniu zaufania i sympatii tych osób, aby uzyskać od nich szczegółowe informacje.

Współcześnie, obok wywiadu środowiskowego, kluczową rolę odgrywa korzystanie z Internetu, w tym z prasy online, forów internetowych i portali społecznościowych, które są bogatym źródłem informacji. Narzędzia OSINT, w tym głównie darmowe wyszukiwarki internetowe są ważne w początkowym etapie pozyskiwania informacji. Ponadto, rozmowy z pracownikami instytucji takich jak Miejskie Ośrodki Pomocy Społecznej czy prokuratorami działającymi na danym obszarze również są cenną metodą gromadzenia danych.

Wykorzystanie nowoczesnych technologii i oprogramowania umożliwiającego legalne i pełniejsze zbieranie, analizę oraz zarządzanie informacjami ze źródeł otwartych w czasie rzeczywistym, pokazuje nowe możliwości w zakresie wywiadu jawnoźródłowego. Te narzędzia potencjalnie mogą znacząco zwiększyć efektywność działań policyjnych w zakresie identyfikacji i reakcji na zagrożenia, w tym terrorystyczne, poprzez proaktywne identyfikowanie nowych zagrożeń, osób podejrzanych oraz innych anomalii, które mogłyby zostać przeoczone przy użyciu tradycyjnych metod rozpoznania.

W praktyce, kombinacja tych metod i środków pozwala na efektywne pozyskiwanie i analizowanie informacji jawnoźródłowych, co ma kluczowe znaczenie dla zapewnienia bezpieczeństwa państwa.

5. **Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?**

Weryfikacja informacji pozyskanych drogą wywiadu jawnoźródłowego odbywa się na kilka sposobów, zależnie od kontekstu i dostępnych źródeł. Może rozpocząć się od analizy informacji zgromadzonych w toku zawiadomień lub zgłoszonych zdarzeń, które następnie są pogłębiane za pomocą danych z systemów informacyjnych. Informacje te są uzupełniane i zweryfikowane przy użyciu otwartych źródeł danych. Alternatywnie, proces może zacząć się od informacji pozyskanych z otwartych źródeł, które później są uzupełniane i weryfikowane za pomocą bardziej specjalistycznych systemów oraz danych dostępnych tylko dla określonych organów.

Niezbędne jest stosowanie różnorodnych metod weryfikacji, aby zapewnić wiarygodność i dokładność pozyskanych informacji. Krzyżowe sprawdzanie danych z wielu źródeł pozwala na eliminację dezinformacji i zwiększenie precyzji analiz. Dodatkowo, analiza kontekstowa i ocena wiarygodności źródeł są kluczowe, aby zrozumieć, jakie informacje są rzetelne i mogą być użyte w dalszym procesie analitycznym.

6. **Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?**

Rozwój metod i środków technicznych w wywiadzie jawnoźródłowym będzie prawdopodobnie obejmował częstsze wykorzystanie sztucznej inteligencji, w tym czatów AI, które automatyzują proces pozyskiwania i analizy danych. Zmiany te będą również wpływać na system szkolenia policjantów, adaptując go do nowych technologii. Rozwój technologiczny zwiększy dostępność zaawansowanych narzędzi analitycznych, co z kolei może zwiększyć efektywność działań podejmowanych na rzecz bezpieczeństwa państwa. W miarę ewolucji zagrożeń, metody pracy policji, w tym podejście do wywiadu jawnoźródłowego, będą musiały być ciągle dostosowywane, aby zapewnić optymalne wykorzystanie dostępnych zasobów informacyjnych i technologicznych na rzecz ochrony bezpieczeństwa państwa i jego obywateli.

7. **Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?**

W prowadzeniu rozpoznania z otwartych źródeł dostrzegam ograniczenia o charakterze etycznym oraz technicznym, które wpływają na efektywność tego rodzaju działań w zakresie zapewnienia bezpieczeństwa państwa. Dostęp do Internetu i narzędzi analitycznych nie jest już problemem, jednak istotną kwestią pozostają odpowiednie szkolenia funkcjonariuszy i pracowników służb, by mogli oni efektywnie wykorzystywać dostępne zasoby. Na rynku dostępne są liczne aplikacje i wyszukiwarki umożliwiające analizę metadanych ze zdjęć czy pozyskiwanie danych z kamer publicznych, co otwiera szerokie możliwości w zakresie pozyskiwania informacji. Edukacja i przekonanie funkcjonariuszy do korzystania z nowoczesnych technologii jest kluczowa.

Ograniczeniem mogą być również koszty dostępu do niektórych płatnych serwisów, zwłaszcza przy konieczności zakupu licencji na większą skalę dla całej formacji. Przykładowo, koszt rejestracji w niektórych bazach danych czy dostęp do specjalistycznych narzędzi analitycznych może stanowić znaczące obciążenie finansowe, zwłaszcza dla większych organizacji, takich jak policja licząca ponad 360 komend powiatowych w Polsce.

8. **Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?**

Wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy może prowadzić do rozprzestrzeniania dezinformacji i tzw. "fake newsów", co stanowi poważne zagrożenie dla bezpieczeństwa państwa. Niezweryfikowane informacje mogą prowadzać do błędnych decyzji w obszarze bezpieczeństwa. Dlatego tak ważne jest odpowiednie przygotowanie i przeszkolenie funkcjonariuszy policji zarówno do analizowania wiarygodności otwartych źródeł jak i do zbierania oraz analizowania informacji jawnoźródłowych, aby mogli oni skutecznie odróżniać informacje prawdziwe od dezinformacji.

9. **Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?**

Wymienione zjawiska znacząco wpływają na wywiad jawnoźródłowy, podnosząc jego efektywność i podkreślając potrzebę wykorzystania w celu zapewnienia bezpieczeństwa w państwach demokratycznych. Globalizacja umożliwia dostęp do obszernych baz danych i informacji, co jest kluczowe dla identyfikacji i analizy zagrożeń, ale jednocześnie wymaga od organów ścigania i służb bezpieczeństwa profesjonalnej analizy i weryfikacji tych danych, aby unikać dezinformacji. Integracja z sojuszniczymi strukturami międzynarodowymi ułatwia wymianę danych, co jest nieocenione w walce z przestępczością transgraniczną. Rozwój cyberprzestrzeni rozszerza możliwości wywiadu jawnoźródłowego, ale również stawia przed nim nowe wyzwania związane z cyberbezpieczeństwem i ochroną danych.

Problemy związane z migracją i identyfikacją osób, które mogą stanowić zagrożenie, podkreślają znaczenie wywiadu jawnoźródłowego w kontekście bezpieczeństwa państwa. Skala migracji, w tym migracji nielegalnej, utrudnia skuteczną weryfikację tożsamości i intencji osób przekraczających granice. Często zdarza się, że migranci tracą swoje dokumenty, co utrudnia ich identyfikację. Ośrodki przejściowe, mimo że nie są zamkniętymi instytucjami, pełnią ważną rolę w procesie weryfikacji tożsamości, jednak brak współpracy i wymiany informacji z krajami pochodzenia migracji komplikuje tę procedurę. Historyczne doświadczenia, takie jak trudności z identyfikacją obywateli narodowości wietnamskiej przybywającej do Polski bez dokumentów, pokazują, jak ważna jest zdolność do skutecznej weryfikacji tożsamości przy wykorzystaniu informacji jawnoźródłowych w procesie zapewniania bezpieczeństwa.

10. **Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?**

Materiał jawnoźródłowy odgrywa kluczową rolę w określaniu kierunków szans i zagrożeń oraz w podejmowaniu działań na rzecz bezpieczeństwa w państwach demokratycznych. Informacje uzyskane z jawnych źródeł, uzupełnione o dane dostępne

tylko dla organów ścigania, umożliwiają stworzenie szczegółowego obrazu osób, zdarzeń oraz podmiotów, z którymi mamy do czynienia. Taka analiza i przegląd informacji są niezbędne do oceny stanu bezpieczeństwa publicznego, w tym porządku prawnego i poziomu przestępczości.

Ponadto, materiał jawnoźródłowy pomaga zrozumieć, jak różne czynniki wpływają na bezpieczeństwo państwa, w tym na stabilność finansową oraz ryzyko zwiększonej przestępczości lub ponownego pojawienia się przestępczości zorganizowanej. Takie zagrożenia mogą destabilizować funkcjonowanie podstawowych organów państwa, co bezpośrednio wpływa na bezpieczeństwo i dobrostan obywateli. Dzięki temu, zgromadzenie i analiza materiału jawnoźródłowego stają się fundamentem do identyfikacji wyzwań i zagrożeń oraz formułowanie skutecznych strategii ich przeciwdziałania.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Kooperacja ze strukturami sojuszniczymi w zakresie pozyskiwania i wykorzystywania informacji jawnoźródłowych na rzecz bezpieczeństwa państwa jest zasadna i przynosi korzyści na różnych szczeblach, w tym lokalnym. Chociaż w strukturach takich jak policja nie zawsze występuje bezpośrednia współpraca w tym zakresie, instytucje międzynarodowe takie jak Interpol czy Europol umożliwiają wymianę zgromadzonych informacji. Ta współpraca nie ogranicza się jedynie do przekazywania informacji dostępnych w systemach lub przesyłania danych, lecz także dotyczy wymiany wiedzy o zjawiskach społecznych i nowych ugrupowaniach, takich jak np. alterglobaliści**,** którzy mogą organizować wydarzenia zwracające uwagę na różne problemy społeczne.

Rozwój technologii i dostępność Internetu ułatwiają pozyskiwanie informacji z otwartych źródeł w wielu językach, co jest szczególnie ważne w kontekście międzynarodowym. Możliwość tłumaczenia stron internetowych na żywo eliminuje bariery językowe, które dawniej mogły utrudniać dostęp do ważnych informacji. W kontekście globalnych kryzysów, jak wojna na Ukrainie, dostęp do stron w języku kraju zainteresowanego pozwala na szybsze pozyskanie informacji w porównaniu z oczekiwaniem na oficjalne komunikaty.

Współpraca międzynarodowa w zakresie wykorzystania otwartych źródeł informacji jest więc nie tylko zasadna, ale również niezbędna dla skutecznego zapewnienia bezpieczeństwa państwa. Umożliwia ona lepsze rozpoznanie zagrożeń, zjawisk społecznych oraz działań podejmowanych przez różne ugrupowania na całym świecie.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: w dniu przeprowadzania wywiadu – Inspektor Policji
3. Stopień naukowy: magister
4. Tytuł: pułkownik
5. Staż pracy zawodowej: 23 lata

Załącznik 4 – Protokół III wywiadu eksperckiego

przeprowadzonego 15 grudnia 2023 r. w Bielsku-Białej

Dariusz Trojszczak – wykładowca akademicki, były Naczelnik Biura Spraw Wewnętrznych Straży Granicznej. Przez wiele lat prowadził szkolenia z zakresu inwigilacji zorganizowanych grup przestępczych dla funkcjonariuszy Straży Granicznej oraz prokuratorów okręgowych.

1. **Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Oczywiście, że tak. Tym bardziej, że w dzisiejszych czasach wywiad jawnoźródłowy ma zupełnie inne znaczenie i wymiar niż dwadzieścia lat temu. Rozwój nowych technologii i dostępność do źródeł informacji a przede wszystkim „czas" tj. szybkość jej przekazu jest niezwykle istotna w analizie tego zagadnienia. Wywiad jawnoźródłowy, wykorzystując te nowe możliwości, przyczynia się do szybszego reagowania na zagrożenia oraz lepszego przewidywania i neutralizowania potencjalnych kryzysów.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

Niezależnie od tego, czy informacja pochodzi z jawnych, ogólnie dostępnych źródeł, czy jest to informacja niejawna, jej wartość określa się poprzez jej przydatność do analizy konkretnego przypadku. Proces ten obejmuje nie tylko identyfikację potencjalnych zagrożeń, ale również ocenę wiarygodności i realności ich wystąpienia. Dzięki temu jesteśmy w stanie efektywniej przeciwdziałać potencjalnym kryzysom.

3. **Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?**

Jak wspomniałem, każda informacja wymaga weryfikacji, przede wszystkim pod kątem jej wiarygodności. W kontekście podejmowania decyzji, kluczowe jest opieranie się na danych, które są wiarygodne. W tym wypadku, wywiad jawnoźródłowy może służyć jako uzupełnienie już posiadanych informacji, na przykład poprzez potwierdzanie kontaktów czy wizerunku osób. Portale społecznościowe, które mogę

określić jako niekontrolowaną i nieostrożną formę wymiany informacji, stanowią bez wątpienia źródło takich danych.

4. **Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?**

Możemy mówić tutaj wyłącznie o metodach jawnych. Jak wspomniałem, jedną z takich metod jest korzystanie z różnego rodzaju portali internetowych, które są ogólnie dostępne. Bezpieczeństwo państwa wymaga zaangażowania wyspecjalizowanych komórek analitycznych. Ich głównym zadaniem jest wyszukiwanie informacji w obszarach, które są kluczowe dla służb odpowiedzialnych za identyfikację zagrożeń czy potencjalnych przestępstw. Te komórki używają zaawansowanych narzędzi do gromadzenia i analizy danych, zarówno płatnych jak i bezpłatnych.

5. **Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?**

Wywiad jawnoźródłowy to niestety mozolna praca. Jej efekt końcowy ukierunkowany jest na analizę porównawczą. Wbrew pozorom, poszukiwania w dostępnych, jawnych źródłach mogą często przynosić zaskakujące efekty. To właśnie swoboda dostępu oraz brak ostrożności ze strony użytkowników często wpływają na osiąganie oczekiwanych wyników końcowych. W rezultacie, te publicznie dostępne informacje mogą zawierać kluczowe dane, które po odpowiedniej analizie przynoszą wartość dodaną dla decyzji podejmowanych na rzecz bezpieczeństwa państwa. Należy jednak pamiętać, że każda z tych informacji wymaga gruntownej weryfikacji, aby uniknąć błędów interpretacyjnych lub manipulacji.

6. **Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?**

Uważam, że podstawowy kierunek rozwoju metod i środków w wywiadzie jawnoźródłowym to dogłębna analiza. Tworzenie wyspecjalizowanych komórek, które wyłącznie zajmują się wywiadem jawnoźródłowym. To nie jest pionierskie założenie, bo takie komórki funkcjonują od dawna, ale bardziej mi tutaj chodzi o narzędzia do analizy wykorzystywane przez te komórki. Takie, które mają przede wszystkim skrócić

czas. Czas analizy, weryfikacji informacji jawnoźródłowych ma kluczowe znaczenie, jeżeli mówimy o bezpieczeństwie państwa. To przekłada się na podejmowane decyzje, a w zależności od "jakości" informacji, te mają kluczowe znaczenie dla bezpieczeństwa państwa.

7. **Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?**

Dostrzegam kilka istotnych ograniczeń w prowadzeniu rozpoznania z otwartych źródeł, które mogą wpływać na zapewnienie bezpieczeństwa państwa. Przede wszystkim, ograniczenia te wynikają z braku efektywnej współpracy między służbami – nie chodzi o wymianę informacji „na papierze", ale o praktyczną, rzetelną współpracę. Doświadczenie analityczne, intuicja oraz ograniczona, jak to określam, „tajność zainteresowań" również stanowią barierę. Jedna rozmowa robocza może zmienić coś co leży w szufladzie od lat w sukces. I to chyba właśnie rządza sukcesu i chwały powoduje te blokady w weryfikacji różnych informacji.

8. **Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?**

Jak wspomniałem wcześniej, kluczowe znaczenie dla efektywnego wykorzystania informacji jawnoźródłowych leży w ich profesjonalnej analizie i weryfikacji. Aby informacja mogła być wzięta pod uwagę w kontekście decyzji dotyczących bezpieczeństwa państwa, musi być dokładnie oceniona pod kątem wiarygodności i relewancji. Brak profesjonalnej analizy i odpowiedniej oceny może prowadzić do błędnych interpretacji, które z kolei mogą mieć tragiczne konsekwencje dla bezpieczeństwa państwa. Dlatego tak istotne jest, aby proces weryfikacji był równie rygorystyczny jak proces zbierania danych, co zapewnia, że każda wykorzystywana informacja przyczynia się do umacniania, a nie osłabiania, bezpieczeństwa państwa.

9. **Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?**

Rozwój nowych technologii a także powszechność dostępu do nich wykazuje od lat, że znaczna część społeczeństwa właśnie z nich korzysta. Można byłoby się pokusić o stwierdzenie, że w znacznym stopniu jest od nich uzależniona. Dzisiaj nie potrzeba bombardowań, aby osłabić funkcjonowanie państwa, wystarczy skutecznie podjąć działania w cyberprzestrzeni, które sparaliżują jego funkcjonowanie. Można zapytać, dlaczego zatem Rosja działa militarnie w Ukrainie mając na swoich usługach najlepszych hakerów świata. Nie tylko, Rosja prowadzi szeroką wojnę hybrydową mając na uwadze sytuację geopolityczną współczesnego świata. To proces zamierzony, przygotowany i długotrwały. Putin okazał się sprawnym i nieprzewidywalnym graczem sceny politycznej, a Ci którzy lekceważyli jego aspiracje dyktatorskie mają niestety problem. Ten problem to dzisiaj największe wyzwanie dla bezpieczeństwa świata.

10. **Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?**

Każda informacja, która stanowi o hipotetycznym zagrożeń ma wartość dodaną. Musi być ona jak wspomniałem poddana analizie i weryfikacji pod kątem wiarygodności. Wywiad jawnoźródłowy, korzystając z różnorodnych danych dostępnych publicznie, pozwala na szybsze identyfikowanie potencjalnych zagrożeń oraz szans. Dzięki analizie tych danych, decydenci mogą podejmować bardziej świadome i efektywne decyzje, które są niezbędne w dynamicznie zmieniającym się świecie. Ponadto, odpowiednio zweryfikowane i zanalizowane informacje jawnoźródłowe mogą wspierać strategie prewencyjne i reagowanie na kryzysy w realnym czasie, zwiększając tym samym bezpieczeństwo państwa.

11. **Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?**

Wydarzenia z września 2001 roku pokazały, że zagrożenia, które do tej pory były identyfikowane z niektórymi krajami, dzisiaj mają charakter zagrożeń globalnych.

Nie jest przecież tajemnicą, że ugrupowania terrorystyczne czy przestępcze korzystają z nowych technologii. Z raportów FBI wynika, że kilka tysięcy stron zarządzanych przez organizacje terrorystyczne poświęconych i kierowanych jest do nowych, potencjalnych bojowników z Europy. W szczególności o wyglądzie europejskim. To nie tylko swoistego rodzaju propaganda, ale rekrutacja. Biorąc pod uwagę ten tylko przykład, jasne jest, że współpraca międzynarodowa w zakresie rozpoznawania, przeciwdziałania i zwalczania przestępstw oraz zagrożeń o charakterze globalnym nie powinna napotykać żadnych ograniczeń.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: wykładowca akademicki, były Naczelnik Biura Spraw Wewnętrznych Straży Granicznej
3. Stopień naukowy: doktor nauk humanistycznych w dyscyplinie nauki o bezpieczeństwie
4. Tytuł: pułkownik w stanie spoczynku
5. Staż pracy zawodowej: 30 lat

Załącznik 5 – Protokół IV wywiadu eksperckiego

przeprowadzonego w dniu 10 stycznia 2024 r. w Warszawie

Artur Szachno – członek Zarządu VAIOT Ltd, VERIORI SA, audytor systemów informatycznych – CISA (Certified Information Systems Auditor), poprzednio: ekspert z obszaru cyberbezpieczeństwa w Urzędzie Komunikacji Elektronicznej, oficer Łącznikowy NATO Special Operation Component Command – Afghanistan (NSOCC-A), odznaczony: Medalem Departamentu Obrony USA "Defense Meritorious Service Medal", „Non-Article 5 NATO Medal", i „Gwiazdą Afganistanu", Szef Grupy Informatyki w Wydziale Łączności i Informatyki Jednostki Wojskowej GROM.

1. **Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Żyjemy w świecie, którego podstawą jest informacja, dlatego każda informacja, która pojawia się w przestrzeni publicznej wymaga uwagi i wartościowania, ze względu na jej ewentualny wpływ na bezpieczeństwo państwa. Obecnie szybkość propagacji informacji jest dużo większa niż jeszcze kilka lat temu. Często nie jesteśmy w stanie zareagować na każdą informację, tak by zminimalizować jej negatywny skutek. Jeżeli więc w przestrzeni publicznej pojawia się informacja, które może generować negatywny wpływ na bezpieczeństwo państwa czy stabilność systemu finansowego należy dokonać jej analizy. Istotne jest również śledzenie trendów oraz sposobów propagowania informacji w otwartych źródłach. Ma to szczególne znaczenie w identyfikowaniu kampanii dezinformacyjnych, celu jej prowadzenia i ich źródeł.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

Przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji jest znacząca. Mamy możliwość wykorzystania informacji jawnoźródłowych w różny sposób. Po pierwsze mogą być wykorzystywane do prowadzenia zaplanowanych kampanii, których celem jest sprawdzenie bezpieczeństwa osobowego lub bezpieczeństwa kanałów dystrybucji informacji. Np. Celowe wypuszczenie spreparowanej informacji, by ocenić, czy została ujawniona, a w kolejnym kroku kto był źródłem przecieku.

Po drugie, informacje jawnoźródłowe służą do wykrywania trendów, badanie środowiska oraz typowania szans i zagrożeń w obszarze bezpieczeństwa. Przykładowo działania obcych służb, których celem jest destabilizacja aparatu państwa, by uzyskać przewagę nad przeciwnikiem. Tu możemy przedstawić działania informujące o trasie migracji do Europy lub organizacja lotów czarterowych do ostatniego dogodnego lotniska.

Po trzecie, informacje jawnoźródłowe służą do weryfikacji przyjętych założeń jako baza do tworzenia planu działań operacyjnych. Umożliwiają identyfikację słabych i mocnych stron. Należy zwrócić uwagę na szerokie możliwości wprowadzania w błąd m.in. przy wykorzystaniu *honeypotów (specjalnie przygotowane, izolowane środowisko pozwalające na monitorowania działania intruza i rozpoznanie)*.

Po czwarte informacje jawnoźródłowe związane z geolokalizacji i zobrazowaniem terenu mogą przyśpieszyć opracowanie informacyjne pakietu celu, lub przygotowanie rozpoznania przeciwnika przez przygotowanie wstępne przed rekonesansem w terenie.

3. Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?

Tego typu analizy są bardzo istotne. Dokonywanie analiz jawnoźródłowych jest najtańszym, szybkim, stosunkowo bezpiecznym, skutecznym sposobem wspomagającym przygotowanie pakietu informacyjnego na potrzeby realizowanego przedsięwzięcia. Może być obarczone błędem wynikającym z otwartego charakteru źródeł informacji. Osobiście podczas pracy zawodowe Jednostce Wojskowej GROM wykorzystywałem otwarte źródła jako element uzupełniający operacyjne informacje naprowadzające.

4. Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

W zakresie metod można wyróżnić:

1) Przegląd kanałów informacyjnych – portale w sieci web, telewizje informacyjne, stacje radiowe.
2) Przegląd: mediów społecznościowych (obecnie głównie X lub jego konkurent Tumblr), Facebook (Meta), Instagram portali prezentujących materiały audio i video jak Tiktok, Youtube, Spotify, forów dyskusyjnych otwartych i dedykowanych tylko

dla członków, publicznych baz danych (w Polsce Krajowy Rejestr Sądowy (KRS), Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG), listy osób zajmujących eksponowane stanowiska polityczne (PEP), listy sankcyjne, listy beneficjentów rzeczywistych, portale społecznościowe i branżowe, Biuletyn Informacji Publicznej (BIP), Główny Urząd Statystyczny (GUS), Księgi wieczyste, informacje o zmarłych pochowanych na cmentarzach, zdigitalizowane rejestry kościelne, statystyczne – Główny Urząd Statystyczny, mapy wspierające wyszukiwanie podmiotów po adresie lub profilu działalności)

3) Monitorowanie: widma radiowego, ruchu lotniczego i wodnego, transportu publicznego, ruchu drogowego z wykorzystaniem systemów mapowych (zawierają informacje o natężeniu ruch w przypadku ruchu pojazdów samochodowych).

Narzędzia OSINT to, m.in.:

1) Wyszukiwarki internetowe jak: Google, Youtube, Yandex, Bing, DuckDuckGo oraz narzędzia wykorzystujące AI jak Bing Chat, Open AI;
2) Dedykowane narzędzia jak: Maltego, Shoodan, Gephi;
3) Crawlery – są to narzędzia, które przeglądają wszystkie kanały informacyjne, łącznie z: radiowymi, telewizyjnymi, społecznościowymi czy portalami, dlatego, że używają uniwersalnych konektorów, które włączają się do tych źródeł informacji, a zebrane informacje zapisują w bazach danych. Dlatego nie ma dzisiaj konieczności obserwowania wyżej wymienionych źródeł przez osoby, można uruchomić wtyczki (oprogramowanie), które będą automatycznie gromadziły dane, które następnie mogą być masowo analizowane. W przypadku transmisji radiowych, czy video dane są zapisywane w postaci dźwięku, następnie dokonywana jest transkrypcja, by przygotować materiał do automatycznego wnioskowania i analizy. Analiza obrazy wykonywana jest przez wytrenowane do tego algorytmy.

Pozyskiwanie danych jest obecnie często zautomatyzowane, następnie zbiory danych są indeksowane i mogą służą do wyszukiwania trendów, nawet bez wskazania kontekstu.

5. Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

Tego typu informacje powinny zdecydowanie być weryfikowanie. Każde źródło informacji może mieć pewną gradację, oceniającą jej przydatność i wiarygodność. Pierwsza ocena wiarygodności źródła dokonywana jest automatycznie na etapie

pozyskiwania informacji. Prowadzony jest ranking reputacji źródeł (np. portali, redaktorów treści). Informacje jawnoźródłowe muszą być ocenione pod katem ich przydatności oraz wiarygodności. Taka ocena jest możliwa m.in. poprzez osobowe źródła informacji oraz ekspertów.

6. Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

Jako pierwsze wskazałbym rozwój Big Data, który umożliwi wykorzystanie wszelkich zgromadzonych do tej pory informacji na zadane zapytanie. Po drugie, rozwój sztucznej inteligencji, automatyzacja zarówno pozyskiwania jak i analizy informacji jawnoźródłowych. Po trzecie rozwój Sztucznej Inteligencji a przez to usprawnienie narzędzi OSINT – analiza tekstu, obrazu statycznego i dynamicznego, analiza głosu w tym treści i sentymentu, analiza behawioralna na podstawie np. próbki głosu nagrane w rozmowie telefonicznej.

Nie możemy zapominać też o sieciach sensorów związanych z IoT (Internet rzeczy) oraz rozwoju Smart City, rozwoju sieci 5G oraz nowych funkcjonalnościach smartfonów.

7. Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?

Po pierwsze informacje jawnoźródłowe podatne są na różnego rodzaju manipulacje (dezinformację).

Po drugie, konieczność gromadzenia i analizy dużych wolumenów danych, może wiązać się z kosztami magazynowania oraz mocy obliczeniowej wykorzystanej do analizy. Mogą wystąpić również ograniczenia między systemami, wynikające z ich architektury. Budowane są w różny sposób, w zależności od założeń i czasu (roku) ich realizacji. Same dane mogą być przygotowywane według różnych standardów. Brak ich normalizacji może powodować opóźnienia w ich przekazywaniu.

Po trzecie, pewnym ograniczeniem jest również poziom zaufania między instytucjami generującymi i przekazującymi dane. Można zwrócić również uwagę na konsekwencje związane z ujawnieniem i dyfuzji wniosków wynikających z agregacji

jawnych informacji. Kolejny element to wiarygodność źródła oraz wiarygodność informacji jawnoźródłowych.

Wszystkie te ograniczenia w kontekście bezpieczeństwa państwa wpływają na czas, zarówno przekazania informacji oraz co ważniejsze – podjęcia decyzji.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Konsekwencje mogą być bardzo duże, wymienić można: dezinformację, chaos, panię, spadek zaufania do Państwa, destabilizację łańcucha dostaw. Widzieliśmy w pandemii oraz po wybuchu wojny w Ukrainie masowe kupowanie produktów żywnościowych, higieny, leków, paliwa czy wypłaty gotówki z bankomatów.

9. Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Obecnie właśnie przez globalizację, rozwój cyberprzestrzeni oraz wzrost uzależnienia od usług cyfrowych w przestrzeni prywatnej i biznesowej rola wywiadu jawnoźródłowy znacznie wzrosła. Czynnikiem wpierającym jest również gospodarka oparta nie sieci, praca zdalna i powszechna digitalizacja usług, w tym publicznych. Powyższe zjawiska mają wpływ na dostępność i czas propagacji informacji w sieci. Czynnikiem ograniczającym może być alfabet (tu mam na myśli bliski i daleki wschód Chiny, Korea, Japonia jak, kraje arabskie, oraz używających cyrylicę) związane z tym aspekty kulturowe.

10. Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?

Wykorzystując emergencje różnego rodzaju informacji publicznie dostępnych, jesteśmy w stanie zidentyfikować możliwe trendy, które w konsekwencji mogą być świadomie wzmacniane lub osłabiane. Dodatkowo materiał jawnoźródłowy stanowi wskaźnik do obrania kierunku w zastosowaniu specjalistycznych rozwiązań

wykorzystywanych w wywiadzie cyfrowym, jak i zadaniowania osobowych źródeł informacji.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Tego typu kooperacja jest konieczna w ramach współpracy służb wewnątrz kraju jak i wymiany doświadczeń i obserwacji zwłaszcza działań transgranicznych połączonych z aktywnością fizyczną na obszarze wielu krajów (jak np. działania w ramach wojny hybrydowej z wykorzystaniem nielegalnych migrantów). Może stanowić uzupełnienie informacji niejawnych, jak również sygnał do uruchomiania prac nad zidentyfikowanym ryzykiem o charakterze transgranicznym.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: członek Zarządu VAIOT Ltd, VERIORI SA, poprzednio: Szef Grupy Informatyki w Wydziale Łączności i Informatyki Jednostki Wojskowej GROM, uczestnik trzech misji wojskowych: dwóch w ramach Międzynarodowych Sił Wsparcia Bezpieczeństwa (ang. *International Security Assistance Force*, ISAF) oraz Misji Stanowcze Wsparcie (ang. *Resolute Support Mission*, RSM)
3. Stopień naukowy: magister, inżynier
4. Tytuł: major rez. Wojska Polskiego
5. Staż pracy zawodowej: 29 lat.

Załącznik 6 – Protokół V wywiadu eksperckiego

przeprowadzonego 16 stycznia 2024 r. w Warszawie

Stanisław Ignaciuk – były oficer wywiadu, doświadczenie w pracy w kraju i za granicą, były z-ca Dyrektora Gabinetu trzech ministrów spraw wewnętrznych, Dyrektor Gabinetu dwóch szefów Urzędu Ochrony Państwa, wykładowca akademicki**.**

1. **Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Mówiąc o wywiadzie jawnoźrodłowym możemy mówić o jego wykorzystaniu nie tylko przez służby specjalne wymienione w art. 11 ustawy o Agencji Bezpieczeństwa Wewnętrznego, tj. Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego i Centralne Biuro Antykorupcyjne, ale też o innych formacjach odpowiadających szeroko za bezpieczeństwo państwa. tj. Straży Granicznej, Policji. Chciałbym się przede wszystkim skupić na pięciu służbach wymienionych w ustawie, a szczególnie na służbie wywiadu.

Wykorzystanie wywiadu jawnoźródłowego zdecydowanie przyczynia się do zapewnienia bezpieczeństwa państwa. W Polsce są ośrodki zajmujące się wywiadem jawnoźródłowym, np. Ośrodek Studiów Wschodnich. Ośrodek ten zajmuje się monitorowaniem oraz analizą sytuacji politycznej, gospodarczej i społecznej w szeroko rozumianym sąsiedztwie Polski. Jego podstawowym zadaniem jest przygotowywanie analiz, ekspertyz, studiów prognostycznych na potrzeby organów władzy publicznej w Polsce. Drugim takim ośrodkiem jest Polski Instytut Analiz Międzynarodowych, który prowadzi działalność badawczą, analityczną oraz szkoleniową w zakresie spraw międzynarodowych. Instytut ściśle współdziała z Agencją Wywiadu, Agencją Bezpieczeństwa Wewnętrznego, Służbą Wywiadu Wojskowego i Służbą Kontrwywiadu Wojskowego. Oczywiście wywiad jawnoźródłowy nie zastąpi informacji pozyskanych ze źródeł osobowych (HUMINT), które według mej oceny są kluczowe. Według literatury amerykańskiej, w informacji kierowanej ze służb dla odbiorcy 80% informacji pochodzi właśnie z otwartych źródeł.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

Uważam, że przez wiele lat w polskich służbach najistotniejszym elementem było wykorzystanie informacji pozyskanych od osobowych źródeł informacji. Jednakże zawsze w kontekście bezpieczeństwa państwa pojawiały się również informacje jawnoźródłowe. OSINT ma znaczącą wartość w weryfikacji i uzupełnianiu danych z innych źródeł. Jest to szczególnie istotne w działaniach ofensywnych i defensywnych państw, gdzie precyzyjne informacje są podstawą do podejmowania decyzji. Pomimo wyzwań związanych z wiarygodnością i ilością danych, OSINT zwiększa zdolności wywiadowcze, umożliwiając bardziej kompleksowe rozumienie sytuacji i potencjalnych zagrożeń. W służbach istnieje praktyka polegająca na integracji informacji jawnoźródłowych z informacjami pozyskanymi droga operacyjną. Łączenie danych z różnych źródeł (jawnych i niejawnych) odbywa się już na wstępnym etapie analizy. Umożliwia to bardziej kompleksowe i szersze rozumienie sytuacji oraz jej analizę. Pozwala to również chronić poufność kluczowych informacji przez klasyfikowanie całego dokumentu jako niejawny po integracji danych. Taka praktyka jest wyrazem potrzeby zachowania równowagi między transparentnością a bezpieczeństwem państwa. Zweryfikowany wywiad jawnoźródłowy (V-OSINT) ukazuje powiązania między danymi i informacjami pochodzącymi ze źródeł otwartych i operacyjnych. Prowadzona jest ich wspólna analiza, a wynikające z niej wnioski są następnie syntezowane.

3. **Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?**

Analizy jawnoźródłowe poszerzają i weryfikują informacje uzyskane operacyjnie, znacząco uzupełniając analizy wywiadowcze. Jest wiele ośrodków badawczych, które zajmują się szeroko rozumianą problematyką bezpieczeństwa państwa. Ośrodki te wydają szereg publikacji, tworzą analizy i opnie, wykorzystywane przez służby. Przykładowo wspomniane wyżej: Ośrodek Studiów Wschodnich i Polski Instytut Spraw Międzynarodowych opracowują analizy związane z bezpieczeństwem państwa, które są jawne, ale nie są zawsze ogólnie dostępne. Polski Instytut Spraw Międzynarodowych sporządza analizy na potrzeby Ministerstwa Spraw Zagranicznych (MSZ). Analizy jawnoźródłowe mają kluczowe znaczenie dla służb wywiadowczych,

umożliwia im rozpoznanie i prognozowanie zagrożeń na podstawie szeroko dostępnych danych. Ułatwiają identyfikację wzajemnych relacji między zdarzeniami i osobami, co jest nieocenione w planowaniu działań strategicznych. Dzięki nim służby mogą także znacząco obniżyć koszty i ryzyko związane z pozyskiwaniem wiedzy, co przekłada się na wyższą efektywność operacyjną.

4. Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

W wywiadzie jawnoźródłowym wykorzystuje się różne metody i narzędzia, takie jak np.: przeglądanie prasy i literatury specjalistycznej, wyszukiwanie informacji w Internecie, analiza mediów tradycyjnych i cyfrowych oraz korzystanie z otwartych baz danych. Istotnym elementem jest również udział w konferencjach naukowych i branżowych spotkaniach oraz współpraca z ośrodkami badawczymi i akademickimi. Istnieje szeroki wybór narzędzi w wywiadzie jawnoźródłowym, które umożliwiają analizę danych geoprzestrzennych, sieciowych, monitorowanie mediów społecznościowych oraz przetwarzanie zbiorów danych. Te narzędzia pozwalają służbom na gromadzenie, analizę i interpretację informacji, co powoduje lepsze zrozumienie zagrożeń oraz może być wykorzystywane w prowadzonych operacjach.

5. Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

Kluczowa jest weryfikacja i krzyżowe sprawdzanie informacji z różnych źródeł, aby zapewnić wiarygodność i dokładność pozyskanych danych. W procesie analizy wywiadowczej, OSINT często łączy się z innymi formami wywiadu, takimi jak HUMINT (Human Intelligence), SIGINT (Signals Intelligence) czy IMINT (Imagery Intelligence), co pozwala na kompleksową ocenę sytuacji i lepsze rozumienie kontekstu.

6. Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

Oceniam, że rozwój metod i środków technicznych w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa będzie prawdopodobnie koncentrować się na kilku kluczowych obszarach. Po pierwsze, wzrost zastosowania

Sztucznej Inteligencji w celu przetwarzania i analizy dużych zbiorów danych z otwartych źródeł. Po drugie, będzie postępować rozwój narzędzi do analizy mediów społecznościowych i cyfrowych śladów, co zwiększy możliwości identyfikacji trendów i zagrożeń w czasie rzeczywistym. Trzeci kierunek to poprawa metod weryfikacji otwartych źródeł i oceny wiarygodności informacji jawnoźródłowych, aby zmaksymalizować dokładność i użyteczność analiz jawnoźródłowych. Ostatni bardzo istotny obszar rozwoju to zintegrowanie OSINT z innymi dyscyplinami wywiadowczymi, co pozwoli na tworzenie bardziej kompleksowych i wielowymiarowych analiz bezpieczeństwa.

7. Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?

Ograniczeniem jest dostępność informacji jawnoźródłowych, ze względu na ograniczony zasięg odbiorców. Kolejne ograniczenie, to koszt uzyskania informacji, obejmujący zarówno wydatki bezpośrednie związane z subskrypcjami płatnych baz danych, jak i koszty operacyjne dotyczące gromadzenia, przetwarzania oraz analizy zgromadzonych danych. Wymaga to zasobów finansowych, które mogą być znaczne, zwłaszcza przy potrzebie monitorowania szerokiego zakresu źródeł i przetwarzania dużych zbiorów informacji. Kluczowe wyzwania technologiczne obejmują zarządzanie ogromnymi ilościami pozyskiwanych danych, zapewnienie ich aktualności oraz wydajność narzędzi analitycznych. Jest to niezbędne w obliczu dynamicznie zmieniających się cyberzagrożeń. Skuteczność wywiadu jawnoźródłowego zależy od wiedzy, doświadczenia, umiejętności analitycznych oraz predyspozycji psychologicznych osób prowadzących rozpoznanie. Błędy w zadaniowaniu oraz błędy poznawcze, takie jak: błąd dostępności, potwierdzenia, efekt zakotwiczenia czy błąd lustrzanego odbicia, mogą prowadzić do nieprawidłowych wniosków. Te ograniczenia wymagają od służb specjalnych ciągłego doskonalenia metod, właściwych narzędzi analitycznych oraz poszerzania wiedzy i podnoszenia kompetencji pracowników.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Sądzę, że wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy może prowadzić do poważnych konsekwencji dla bezpieczeństwa państwa. Takie przypadki znane są w historii funkcjonowania służb na całym świecie. Decydenci, opierając się na niezweryfikowanych danych, mogą podejmować błędne decyzje o charakterze politycznym, militarnym czy gospodarczym, co z kolei może prowadzić do nieprzewidzianych skutków wewnętrznych i międzynarodowych. Przykładem są ostatnie wydarzenia w Izraelu, gdzie służby nie w pełni rozpoznały informacje jawnoźródłowe. Niewłaściwie zinterpretowane lub fałszywe informacje mogą skutkować błędnym alokowaniem zasobów, nieadekwatnym reagowaniem na zagrożenia, a nawet eskalacją konfliktów. Dlatego niezbędne jest stosowanie rygorystycznych metod weryfikacji pozyskanych informacji jawnoźródłowych, w celu zapewnienia dokładność i wiarygodność informacji wykorzystywanych w procesie decyzyjnym. Informacje z HUMINT-u pogłębione o dane uzyskane z wywiadu jawnoźródłowego stanowią podstawę analiz, które to analizy służby mogą przekazać odbiorcy celem podjęcia określonej decyzji politycznej, gospodarczej lub militarnej.

9. Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Globalizacja i integracja zwiększają wzajemne powiązania i zależności między państwami, co skutkuje większą dostępnością informacji, ale również powstawaniem nowych zagrożeń. Rozwój cyberprzestrzeni poprzez ekspansję mediów społecznościowych, portali informacyjnych i platform komunikacyjnych, otwiera nowe obszary dla pozyskiwania informacji, ale również stwarza wyzwania związane z cyberbezpieczeństwem i dezinformacją. Aktualnie wywiad jawnoźródłowy staje się kluczowym narzędziem w identyfikacji, monitorowaniu i przeciwdziałaniu tym zagrożeniom. Zwiększa on również świadomość sytuacyjną państw, co jest niezbędne w szybko zmieniającym się środowisku międzynarodowym. Należy podkreślić, że w kontekście rosnącej roli cyberprzestrzeni, wywiad jawnoźródłowy umożliwia również

efektywne śledzenie cyberzagrożeń i działań dezinformacyjnych. W państwach, gdzie transparentność i jawność życia publicznego są kluczowymi wartościami, wywiad jawnoźródłowy nabiera coraz większego znaczenia w kontekście bezpieczeństwa. Umożliwia on również skuteczniejsze zarządzanie ryzykiem i reagowanie na nowe wyzwania. Po raz kolejny, chciałbym zwrócić uwagę na zagrożenia wynikające z podejmowania działań dezinformacyjnych.

10. Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?

Nie jest tajemnicą, że istnieje wymiana informacji wywiadowczych pomiędzy państwami – członkami NATO. Materiał jawnoźródłowy odgrywa istotną rolę w określaniu kierunków szans i zagrożeń a także w podejmowaniu działań na rzecz bezpieczeństwa państwa. Dostarcza on również szerokiego spektrum informacji, które mogą być wykorzystane do analizy bieżącej sytuacji geopolitycznej, społeczno-ekonomicznej, technologicznej oraz militarnej. Profesjonalna analiza OSINT umożliwia identyfikację potencjalnych zagrożeń oraz monitorowanie trendów, które mogą wpłynąć na stabilność i bezpieczeństwo państwa. należy podkreślić, że wykorzystanie materiału jawnoźródłowego wymaga jednak od decydentów świadomego zarządzania wyzwaniami związanymi z jego analizą i integracją z tradycyjnymi metodami wywiadowczymi.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Uważam, że kooperacja ze strukturami sojuszniczymi w zakresie pozyskiwania i wykorzystywania informacji jawnoźródłowych jest nie tylko zasadna, ale również niezbędna dla zwiększenia efektywności działań na rzecz bezpieczeństwa państwa. Współpraca ta pozwala na wymianę wiedzy, doświadczeń i najlepszych praktyk. Wzmacnia to zdolności analityczne i operacyjne poszczególnych państw. Niemniej jednak zakres i tematyka przekazywanych materiałów jawnoźródłowych zależy od partykularnych interesów państwa. Kooperacja umożliwia również lepsze zrozumienie globalnego kontekstu zagrożeń, co jest kluczowe w obliczu międzynarodowych wyzwań, takich jak terroryzm, cyberataki czy dezinformacja. Wspólne działania

w ramach sojuszy i organizacji międzynarodowych, takich jak NATO czy Unia Europejska, zwiększają spójność i skuteczność reakcji.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: były oficer wywiadu
3. Stopień naukowy: magister
4. Tytuł: podpułkownik
5. Staż pracy zawodowej: 40 lat

Załącznik 7 – Protokół VI wywiadu eksperckiego

przeprowadzonego 26 stycznia 2024 r. w Warszawie

Piotr Caliński – w latach 1991-2006 Komendant Centrum Szkolenia Policji w Legionowie, w okresie 2001-2004 odpowiedzialny za nadzór nad wybranymi jednostkami terenowymi Policji, współpracę z Parlamentem i Komitetem Doradczym Komendy Głównej Policji, analizę zarządzania i strategię rozwoju Policji oraz audyt Departamentu Porządku i Bezpieczeństwa Wewnętrznego Ministerstwa Spraw Wewnętrznych i Administracji (MSWiA). W latach 2001–2006 przedstawiciel polskiej Policji w międzynarodowych instytucjach, akademiach i organizacjach kadrowo-szkoleniowych: AEPC (Stowarzyszenie Europejskich Kolegiów Policyjnych), MEPA (Środkowoeuropejska Akademia Policyjna), CEPOL (Europejska Akademia Policyjna). Autor Rządowego programu zapobiegania przestępczości samochodowej i ubezpieczeniowej. Wyróżniany polskimi odznaczeniami; Kawaler Narodowego Orderu Zasługi Republiki Francuskiej. Wykładowca akademicki, szkoleniowiec, audytor. Właściciel firmy „Doradztwo gospodarcze, Bezpieczeństwo biznesu".

1. **Czy zdaniem Pana obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Pozyskiwanie informacji w ramach wywiadu jawnoźródłowego jest jednym z narzędzi, z jakich korzysta się w procesie zapewnienia bezpieczeństwa Państwa. OSINT może dostarczać informacje we wszystkich płaszczyznach działań analitycznych, w zakresie każdej sfery bezpieczeństwa naszego kraju, ale domeny wspólne z bezpieczeństwem biznesowym i społecznym, przenikają się przede wszystkim w płaszczyznach ryzyk ekonomicznych oraz cybernetycznego.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

Informacje pozyskane w procesie otwartych źródeł informacji stanowią zazwyczaj pierwszy etap, jak i pewien odnośnik do tego co należy weryfikować w oparciu o inne działania, a tym – operacyjne, chociażby poprzez pracę z osobowymi źródłami informacji.

Trzeba pamiętać, że współczesne narzędzia uzyskiwania informacji stanowią pewne continuum doświadczeń wywiadów i kontrwywiadów państw oraz sfer

biznesowych. Początki promowania wagi informacji i wynikających z nich danych, to przecież Sztuka wojny Sun Tsu (Sun Zi), w której to Autor już w VI w. pne przekonywał, iż „kto zna wroga i siebie, temu nic nie grozi, choćby w stu bitwach; kto nie zna wroga, ale zna siebie, czasami odnosi zwycięstwo, a czasami klęskę; kto nie zna wroga i nie zna siebie, nieuchronnie ponosi klęskę!". Przez stulecia poszukiwano możliwości poszerzenia innych niż osobowe źródeł informacji, co przez ostatnie dziesięciolecia, dzięki rozwojowi technologicznemu, a tym informatyki sensu largo, zaowocowało powstaniem terminu technical collecting, który ilustruje całą gamę technicznych metod zbierania informacji i danych. Przypomnijmy nazwy kilku z nich: SIGINT, MASINT, GEOINT/IMINT, SIGINT, a także – omawiany OSINT.

3. Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?

Analiza informacji pochodzących z otwartych źródeł umożliwia ustalanie niezbędnych danych do oceny sytuacji zarówno ekonomicznej jak i dotyczącej bezpieczeństwa podmiotów gospodarczych. Szczególną uwagę zwracam na dane finansowe, siatkę powiązań osobowo-kapitałowych, zobowiązania, a także – bezpieczeństwo zasobów informacji. Przez identyfikację potencjalnych ryzyk wizerunkowych i innych zagrożeń mogę lepiej przewidywać i minimalizować możliwe zagrożenia, co jest istotne dla stabilności i bezpieczeństwa kraju.

4. Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

Jedną z metod/środków stosowanych w wywiadzie jawnoźródłowy, jest OPSEC, który jest procesem zarządzania bezpieczeństwem zasobów i związanymi z nim ryzykami, który zapobiega przedostaniu się wrażliwych informacji w niepowołane ręce. Kluczowym elementem OPSEC jest wykorzystanie zarządzania ryzykiem do identyfikowania potencjalnych zagrożeń i podatności w procesach organizacji, sposobie jej działania oraz oprogramowaniu i sprzęcie, z którego korzystają pracownicy. Spojrzenie na systemy i operacje z punktu widzenia strony trzeciej, umożliwia zespołom OPSEC odkrycie problemów, które mogły zostać przeoczone i mogą mieć kluczowe znaczenie dla wdrożenia odpowiednich środków zaradczych, zapewniających bezpieczeństwo najbardziej wrażliwych danych. W nowoczesnych technikach

zarządzania projektami analogiczną metodyką jest reguła analizy *pre mortem,* stojąca w opozycji do refleksji *post mortem,* kiedy to kryzys w projekcie już nastąpił.

5. Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

Informacje pozyskane w oparciu o wywiad jawnoźródłowy zawsze podlegają weryfikacji. Dane pozyskane w ten sposób są weryfikowane przez co najmniej trzy inne i niezależne źródła oraz wsparte dodatkowo pracą „w terenie" z osobowymi źródłami informacji. Współczesna skala możliwości jest bardzo rozległa, o czym wspominałem wcześniej.

6. Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

W mojej ocenie kluczowym kierunkiem rozwoju na pewno będą narzędzia badające, analizujące i eliminujące dezinformację, która niestety niesie za sobą szereg zagrożeń w obszarach kluczowych dla bezpieczeństwa kraju. Wpływ treści dezinformacyjnych na obszary produkcyjne i badawcze (w tym – dotyczące sfery zbrojeniowej), finansowy, energetykę czy logistykę, można traktować jako jeden z niebezpieczniejszych elementów choćby konfliktu hybrydowego, gdzie celem jest infrastruktura krytyczna. Szkody w takich przypadkach są niepoliczalne.

Pamiętajmy, że współczesna, nieprzerwana wojna hybrydowa, nie jest pojęciem publicystycznym, lecz dzieje się w naszej globalnej codzienności pod postaciami wojny pomiędzy gospodarkami, kognitywnej, informacyjnej i cybernetycznej, którym towarzyszą operacje wpływu, próby sterowania mediami, ataki typu rozproszona odmowa usługi (DDoS) i inne.

7. Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?

Kluczowym ograniczeniem prowadzenia rozpoznania jawnoźródłowym jest brak możliwości zweryfikowania każdej pozyskanej informacji. Sieć sama w sobie zapewnia niepoliczalne dane przydatne w procesie kwerendy, ale nie dostarcza już tak wielu rozwiązań w walce z fake newsami, dezinformacją czy smogiem informacyjnym.

Po naszych doświadczeniach z pandemią COVIDową, możemy uznać, że współcześnie żyjemy w czasach INFOdemii. Główną przyczyną jest „korek informacyjny" Internetu. Mnogość i ogólnodostępność informacji tworzą problem już przy samym procesie kolekcji danych, kiedy to należy oddzielić informacje definitywnie nieprawdziwe i nastawione na dezinformowanie analityków pozyskujących informacje.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Państwo, które realizując swoją strategię rozwoju (jeśli ją posiada), podejmując decyzje, wdrażając procesy czy przeprowadzając reformy w oparciu o niezweryfikowane i niepotwierdzone informacje pozyskane w oparciu o OSINT, jest nieustannie narażone na ryzyko dezinformacji i inne celowe działania obcych aktorów, mających na celu osłabienie danego państwa i jego organów.

9. Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Idee globalizacji niosą ze sobą jednocześnie szanse i zagrożenia. Tak zwana Globalna Wioska daje nam szansę na dostęp do całej gamy informacji w przeróżnych językach, z różnych kultur, systemów politycznych czy krajów. Paleta informacji, znikomy koszt ich pozyskania i coraz lepiej działające translatory, tworzą czasem sytuacje, w których możemy poczuć wrażenie przewagi, ale jak mawiał F. Nietsche „*Kiedy spoglądasz w otchłań, ona również patrzy na ciebie*." Warto o tym pamiętać, że Internet działa „w dwie strony".

Pełna ekspozycja w mediach społecznościowych, ogólnodostępność państwowych rejestrów dotyczących podmiotów gospodarczych, czy możliwość potwierdzenia danych teleadresowych z najdalszych zakątków świata, daje tyle samo szans, co zagrożeń. To od profesjonalnego operatora/analityka zależy, która z tych sfer ryzyka będzie dominująca.

10. **Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?**

Należy zawsze pamiętać, że materiały pozyskane w procesie badania otwartych źródeł informacji są składową pewnej całości, która dopiero zweryfikowana i skrojona na potrzeby odbiorcy, stanowi istotny element w budowaniu polityki bezpieczeństwa. Pozyskane dane i wybrana metoda analizy, niezależnie od tego, czy jest to typowy SWOT czy PESTEL (ang. *Political, Economic, Social, Technological, Environmental, Legal* – narzędzie analizy otoczenia zewnętrznego organizacji, uwzględniające czynniki polityczne, ekonomiczne, społeczne, technologiczne, środowiskowe i prawne), dają nam odpowiedź na pytanie, co może być szansą, a co zagrożeniem.

11. **Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?**

Kooperacja w pozyskiwaniu i analizowaniu danych w obrębie instytucji natowskich i unijnych działa od lat. Z własnych doświadczeń mogę wskazać, że wymiana danych rejestrowych, fiskalnych czy ogólnych danych osobowych, przybrała na sile w związku z coraz częstszym transgranicznym charakterem takich przestępstw jak przemyt i handel broni, narkotyków, ludzi czy pranie pieniędzy, połączone ze sponsorowaniem terroryzmu. Trzeba mocno podkreślić, że fundamentalnym warunkiem *sine qua non* takiej współpracy jest wzajemne zaufanie pomiędzy państwami – partnerami i ich służbami.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: właściciel firmy „Doradztwo gospodarcze, Bezpieczeństwo biznesu”; były Komendant Centrum Szkolenia Policji w Legionowie.
3. Stopień naukowy: magister
4. Tytuł: Inspektor w stanie spoczynku
5. Staż pracy zawodowej: 48 lat.

Załącznik 8 – Protokół VII wywiadu eksperckiego

przeprowadzonego w dniu 26 stycznia 2024 r. w Łodzi

Ppłk dr inż. Przemysław Kornacki – dowódca 93. batalionu lekkiej piechoty w Łasku w ramach 9 Łódzkiej Brygady Obrony Terytorialnej, posiada wieloletnie doświadczenie zawodowe zdobyte podczas służby w jednostkach organizacyjnych resortu obrony narodowej oraz Ministerstwa Spraw Wewnętrznych i Administracji, wieloletni Szef Sekcji Rozpoznawczej odpowiedzialny za pozyskiwanie, gromadzenie, przetwarzanie i dystrybucję informacji mających wpływ na bezpieczeństwo państwa, wykładowca akademicki.

1. **Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Wywiad jawny, czyli zdobywanie informacji publicznie dostępnych, może odgrywać pewną rolę w zapewnieniu bezpieczeństwa państwa. Dostęp do jawnych źródeł informacji może umożliwić lepsze zrozumienie sytuacji w kraju i na świecie, co może być istotne dla podejmowania decyzji politycznych i dotyczących bezpieczeństwa państwa. Jednakże w kontekście działań wywiadowczych większość informacji istotnych dla bezpieczeństwa państwa jest zazwyczaj trzymana w tajemnicy, aby nie ujawnić strategii, planów lub źródeł informacji. Wywiad jawnoźródłowy może dostarczyć tylko ogólnych informacji, a kluczowe aspekty bezpieczeństwa często wymagają środków dyskrecji. Ostatecznie, bezpieczeństwo państwa zależy od kompleksowego podejścia, które obejmuje zarówno wywiad jawny, jak i tajny, a także skuteczne zarządzanie informacjami i współpracę na szczeblu krajowym i międzynarodowym.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

Informacje jawnoźródłowe mogą być przydatne w różnych aspektach działań ofensywnych i defensywnych państwa. Oto kilka kwestii, które warto rozważyć:

1) Weryfikacja informacji: informacje pochodzące ze źródeł publicznych mogą stanowić bazę danych, która pozwala na weryfikację innych potencjalnie mniej dostępnych źródeł. Porównywanie informacji jawnych z tajnymi może pomóc w ocenie ich wiarygodności i prawdziwości.

2) Analiza sytuacji politycznej i społecznej: dostęp do informacji jawnych może ułatwić analizę sytuacji politycznej, społecznej i gospodarczej w kraju i na świecie. To z kolei może pomóc w prognozowaniu możliwych zagrożeń i szans, co jest istotne zarówno w działaniach ofensywnych, jak i defensywnych.
3) Kształtowanie strategii informacyjnych: informacje jawnoźródłowe mogą być wykorzystywane do kształtowania strategii informacyjnych państwa. Zrozumienie narracji publicznej, opinii społecznych i relacji międzynarodowych może wpływać na skuteczność działań informacyjnych.
4) Wsparcie działań dyplomatycznych: dobre zrozumienie sytuacji na arenie międzynarodowej, uzyskane dzięki informacjom jawnoźródłowym, może pomóc w prowadzeniu skutecznej polityki zagranicznej i dyplomacji.

Jednakże, warto pamiętać, że informacje jawnoźródłowe mają swoje ograniczenia. Często są ogólne i dostępne publicznie, co oznacza, że mogą nie zawierać kluczowych elementów, które są istotne w kontekście działań wywiadowczych. W związku z tym, aby w pełni zrozumieć sytuację i podjąć skuteczne działania ofensywne lub defensywne, państwo musi korzystać także z informacji zdobywanych w sposób tajny. Oba rodzaje informacji powinny współgrać, tworząc kompleksowe podejście do bezpieczeństwa państwa.

3. Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?

W kontekście podejmowania decyzji dotyczących bezpieczeństwa państwa, analiza jawnoźródłowa może odgrywać istotną rolę. Oto kilka aspektów, które ilustrują znaczenie takiej analizy:

1) Zrozumienie kontekstu społecznego i politycznego: analiza informacji jawnoźródłowych pozwala na lepsze zrozumienie sytuacji społecznej, politycznej i gospodarczej w kraju oraz na świecie. To z kolei umożliwia lepsze przewidywanie potencjalnych zagrożeń i szans, co jest istotne dla skutecznego zarządzania bezpieczeństwem państwa
2) Ocena opinii publicznej: informacje jawne dostarczają wglądu w opinie społeczne, postawy obywateli oraz ogólny klimat społeczny. Zrozumienie tych elementów może być kluczowe w procesie podejmowania decyzji, zwłaszcza w kontekście działań, które mogą wpływać na społeczeństwo.

3) Analiza relacji międzynarodowych: informacje jawnoźródłowe pozwalają na monitorowanie relacji międzynarodowych, co jest kluczowe dla opracowania skutecznych strategii bezpieczeństwa państwa. Zrozumienie działań i intencji innych krajów może wpłynąć na podejmowane decyzje.
4) Planowanie działań informacyjnych: analiza informacji jawnoźródłowych jest niezbędna do planowania skutecznych działań informacyjnych. Skoro informacje te są dostępne publicznie, państwo może aktywnie kształtować swoją narrację i zdobywać poparcie społeczne.

4. Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

Wywiad jawnoźródłowy obejmuje gromadzenie informacji z publicznie dostępnych źródeł w celu analizy i wykorzystania ich do celów bezpieczeństwa państwa. Oto kilka metod stosowanych w wywiadzie jawnoźródłowym:

1) Monitorowanie mediów społecznościowych: analiza treści i aktywności na platformach społecznościowych może dostarczyć istotnych informacji na temat opinii publicznej, reakcji społecznych, trendów i wydarzeń.
2) Śledzenie informacji prasowych: analiza artykułów prasowych, raportów medialnych i wiadomości może dostarczyć wglądu w bieżące wydarzenia i kwestie społeczne oraz polityczne.
3) Badania naukowe: analiza wyników badań naukowych, artykułów naukowych i publikacji akademickich może dostarczyć dogłębnej wiedzy na temat różnych dziedzin, co może być przydatne w planowaniu działań i podejmowaniu decyzji na rzecz bezpieczeństwa.
4) Obserwacja publicznych wystąpień: śledzenie publicznych wystąpień, konferencji prasowych, debat publicznych czy przemówień, może dostarczyć informacji na temat stanowiska rządzących, ich strategii oraz planów działania.
5) Analiza dokumentów publicznych: badanie oficjalnych dokumentów, takich jak raporty rządowe, ustawy, strategie państwowe czy protokoły z posiedzeń publicznych, pozwala uzyskać dogłębną wiedzę na temat polityki państwa.
6) Śledzenie działań rządu: obserwacja działań podejmowanych przez rząd, agencje rządowe i instytucje publiczne może dostarczyć informacji na temat ich priorytetów, działań i planów na przyszłość.

7) Kontakty z organizacjami społecznymi: nawiązywanie relacji z przedstawicielami organizacji społecznych, ekspertami branżowymi czy przedstawicielami różnych grup interesu może umożliwić pozyskanie informacji z pierwszej ręki.

Dostępne narzędzia wywiadu jawnoźródłowego dzielą się na bezpłatne i płatne: od prostych wyszukiwarek internetowych, przez specjalistyczne oprogramowanie do analizy mediów społecznościowych, po zaawansowane systemy do analizy big data. Bezpłatne narzędzia mogą służyć do podstawowego monitoringu i zbierania danych, podczas gdy płatne platformy oferują głębszą analizę, personalizację wyszukiwań i bardziej szczegółowe raporty, dostosowane do specyficznych potrzeb użytkowników. Wszystkie te metody wymagają umiejętności analizy, selekcji informacji oraz rozróżniania między wiadomościami rzetelnymi a dezinformacją. Ważne jest także zachowanie zgodności z zasadami etycznymi, aby uniknąć naruszania prywatności i praw obywatelskich. W przeciwnym razie wywiad jawnoźródłowy może spotkać się z krytyką i problemami prawno-etycznymi.

5. Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

Weryfikacja informacji pozyskanych drogą wywiadu jawnoźródłowego jest kluczowym etapem, aby zapewnić ich rzetelność i wiarygodność. Istnieje kilka metod i technik, które mogą być stosowane w procesie weryfikacji informacji jawnoźródłowych:

1) Sprawdzenie krzyżowe: porównywanie informacji z wielu różnych źródeł może pomóc w potwierdzaniu jej poprawności. Jeśli różne, niezależne źródła potwierdzają daną informację, zwiększa to jej wiarygodność.
2) Sprawdzanie reputacji źródła: ocena reputacji i wiarygodności źródła jest kluczowym krokiem weryfikacji informacji. Sprawdzenie, czy dane źródło jest znane z rzetelności i obiektywizmu, może dostarczyć wskazówek co do wiarygodności informacji.
3) Analiza kontekstu: zrozumienie kontekstu, w jakim pojawiła się informacja, może pomóc w ocenie jej wiarygodności. Czas, miejsce i okoliczności mogą mieć istotny wpływ na interpretację informacji.
4) Potwierdzanie faktów: weryfikacja konkretnych faktów zawartych w informacji jest kluczowa. Sprawdzanie dat, miejsc, imion czy innych szczegółów może pomóc ustalić, czy informacja jest precyzyjna i zgodna z rzeczywistością.

5) Konsultacje z ekspertami: weryfikacja informacji może obejmować skonsultowanie się z ekspertami w danej dziedzinie. Specjaliści mogą dostarczyć dodatkowego kontekstu i oceny, które pomogą w ocenie wiarygodności informacji.
6) Analiza źródła finansowania: sprawdzenie, kto finansuje konkretne źródło informacji, może dostarczyć informacji na temat potencjalnych ukierunkowanym czy uprzedzeń. Finansowanie może wpływać na obiektywność danego źródła.
7) Analiza języka i tonu: uważne analizowanie języka użytego w informacji oraz tonu, w jakim została ona przedstawiona, może dostarczyć wskazówek co do ewentualnej stronniczości czy manipulacyjność.

Weryfikacja informacji jest procesem skomplikowanym, który wymaga umiejętności krytycznego myślenia i analizy. W dzisiejszym świecie, w którym dezinformacja jest powszechna, umiejętność prawidłowej weryfikacji informacji jest kluczowa dla podejmowania decyzji na rzecz bezpieczeństwa państwa.

6. Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

Przewidywanie dokładnych kierunków rozwoju metod i środków technicznych w obszarze jawnoźródłowego pozyskiwania i analizy informacji może być trudne, ale istnieją pewne trendy, które można uwzględnić. O to kilka obszarów, które mogą się rozwijać w przyszłości:

1) Automatyzacja analizy danych: postęp w dziedzinie sztucznej inteligencji i analizy danych może prowadzić do większej automatyzacji procesu analizy informacji jawnoźródłowych. Algorytmy uczenia maszynowego mogą pomóc w identyfikowaniu wzorców, analizowaniu tonacji treści czy ekstrakcji kluczowych informacji.
2) Rozwój narzędzi do analizy treści multimedialnych: z uwagi na rosnącą ilość treści multimedialnych w Internecie, narzędzia do analizy treści wideo dźwięku i obrazu będą z pewnością rozwijane. To obejmuje technologię analizy wideo rozpoznawanie mowy czy analizę obrazów.
3) Integracja źródeł danych: w najbliższych latach możemy oczekiwać większej integracji danych pochodzących z różnych źródeł. To może obejmować połączenie informacji z mediów społecznościowych, tradycyjnych mediów, danych rządowych i innych, co umożliwi kompleksową analizę sytuacji.

4) Cyberbezpieczeństwo i ochrona przed dezinformacją: w miarę wzrostu zagrożeń związanych z cyberprzestrzenią rozwijane będą technologie zabezpieczające przed cyberatakami i manipulacją informacją. Narzędzia do identyfikacji dezinformacji oraz analizy fałszywych informacji również będą się rozwijać.
5) Rozwój analizy semantycznej: technologie analizy semantycznej pozwalają na bardziej zaawansowane zrozumienie treści tekstowej, uwzględniając kontekst i znaczenie słów. To może poprawić skuteczność analizy informacji jawnoźródłowych.
6) Zastosowanie blockchain w weryfikacji informacji: technologia blockchain może być używana do potwierdzenia autentyczności informacji. Dzięki zastosowaniu rozproszonych i niezmienialnych baz danych, można utworzyć system weryfikacji informacji, który minimalizuje ryzyko manipulacji.
7) Rozwój analizy predykcyjnej: wykorzystanie analizy predykcyjnej może pomóc w przewidywaniu wydarzeń na podstawie analizy danych jawnoźródłowych. To może być szczególnie ważne dla antycypacji zagrożeń i planowania działań w zakresie bezpieczeństwa państwa.

Oczywiście, rozwój tych technologii będzie również stawiał przed społeczeństwa wyzwania związane z etyką, prywatnością i odpowiedzialnością. Jednak postęp w tych obszarach może znacząco wpłynąć na skuteczność wywiadu jawnoźródłowego i działań podejmowanych na rzecz bezpieczeństwa państwa.

7. Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?

Prowadzenie rozpoznania z otwartych źródeł ma swoje ograniczenia, które mogą wpływać na skuteczność i kompletność gromadzonych informacji oraz ich użyteczność dla zapewnienia bezpieczeństwa państwa. Oto kilka głównych ograniczeń:

1) Brak dostępu do informacji poufnych: wywiad jawnoźródłowy opiera się na informacjach publicznie dostępnych. To oznacza, że wiele kluczowych informacji, zwłaszcza tych dotyczących działań tajnych czy planów przeciwdziałania, nie będzie dostępnych.
2) Ryzyko manipulacji informacją: informacje publiczne mogą być manipulowane w różny sposób, np. poprzez dezinformację, fałszywe informacje czy propagandę.

Bez odpowiednich narzędzi do weryfikacji, istnieje ryzyko opierania decyzji na nieprawdziwych lub zmanipulowanych danych.

3) Brak kontroli nad źródłami informacji: w przeciwieństwie do wywiadu tajnego, gdzie można kontrolować dostęp do źródeł, w przypadku wywiadu jawnoźródłowego trudniej jest kontrolować, kto dostarcza informacji i jak są one gromadzone.
4) Ograniczenia związane z prawem i etyką: prowadzenie rozpoznania z otwartych źródeł podlega ograniczeniom prawno-etycznym. Naruszenie prywatności, szerzenie dezinformacji czy stosowanie nieetycznych praktyk może narazić na odpowiedzialność prawną i szkodzić reputacji.
5) Brak dostępu do informacji tajnych: w przypadku, gdy kluczowe informacje są objęte klauzulą tajności, wywiad jawnoźródłowy może nie dostarczyć pełnego obrazu sytuacji. Dla pełniejszego zrozumienia bezpieczeństwa państwa, konieczne jest korzystanie również z informacji pozyskanych przez wywiad tajny.
6) Ograniczone źródła informacji: nie wszystkie informacje są publicznie dostępne, zwłaszcza te związane z dziedzinami technicznymi czy technologią wojskową. To ogranicza zdolność uzyskania kompleksowej wiedzy na temat pewnych aspektów bezpieczeństwa państwa.
7) Krótkotrwałość informacji: w Internecie wiele informacji zmienia się dynamicznie, a dane mogą szybko utracić aktualność. To utrudnia bieżące analizy sytuacji.

Wpływ tych ograniczeń na zapewnienie bezpieczeństwa państwa polega głównie na tym, że wywiad jawnoźródłowy stanowi tylko jedną część pełnego obrazu sytuacji. Aby skutecznie zarządzać bezpieczeństwem państwa, konieczne jest uzupełnienie go o informacje pozyskane w sposób tajny, dostępne tylko dla uprawnionych agencji i instytucji. Integracja różnych źródeł informacji jest kluczowa dla kompleksowego podejścia do bezpieczeństwa państwa.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy może prowadzić do szeregu potencjalnych konsekwencji dla bezpieczeństwa państwa. Oto kilka aspektów, które mogą być istotne:

1) Ryzyko dezinformacji: niezweryfikowane informacje mogą być podatne na dezinformację jeśli decydenci opierają się na niepotwierdzone danych lub informacjach zmanipulowanych przedsionek może to prowadzić do błędnych ocen sytuacji i podejmowania nieefektywnych decyzji.
2) Słabe przygotowanie do zagrożeń: brak rzetelnej analizy informacji jawnoźródłowych może prowadzić do niedoszacowania lub przesunięcia uwagi w kwestiach bezpieczeństwa państwa. To z kolei może skutkować słabym przygotowaniem do reagowania na potencjalne zagrożenia zarówno w wymiarze wewnętrznym, jak i międzynarodowym.
3) Utrata zaufania społecznego: jeśli informacje publiczne są nieprawdziwe lub źle zinterpretowane, może to prowadzić do utraty zaufania społecznego do decydentów i instytucji państwowych. To może wpływać na stabilność polityczną i społeczną kraju.
4) Konsekwencje w sferze międzynarodowej**:** błędne interpretacje i decyzje oparte na niezweryfikowanych informacjach jawnoźródłowych mogą mieć poważne skutki w relacjach między podmiotami międzynarodowymi. To może prowadzić do nieporozumień, konfliktów czy innych trudności dyplomatycznych.
5) Straty operacyjne: w kontekście działań podejmowanych w obszarze bezpieczeństwa opieranie się na nieprawdziwych danych może prowadzić do strat operacyjnych. Decyzje oparte na błędnych informacjach mogą być nieefektywne i prowadzić do nieoczekiwanych rezultatów.
6) Podważenie wiarygodności: jeśli informacje publiczne są wykorzystywane bez należytej weryfikacji, może to podważyć wiarygodność decydentów i instytucji państwowych. To z kolei może wpływać na zdolność kraju do skutecznego zarządzania sytuacjami kryzysowymi.

W związku z tym, profesjonalna weryfikacja i analiza informacji jawnoźródłowych są kluczowe dla skuteczności działań państwa w zakresie bezpieczeństwa. Dostarczają one solidnej podstawy do podejmowania informowanym decyzji, minimalizując ryzyko błędów i nieprawidłowych ocen sytuacji.

9. Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Procesy globalizacji, integracji oraz rozwój cyberprzestrzeni mają istotny wpływ na efektywność wywiadu jawne źródłowego oraz kreują nowe wyzwania i potrzeby dla państw demokratycznych w zakresie zapewnienia bezpieczeństwa. Poniżej przedstawiam kilka kwestii związanych z tym zagadnieniem:

1) Zwiększona ilość dostępnych informacji: globalizacja i rozwój cyberprzestrzeni skutkują zwiększeniem ilości dostępnych informacji w skali globalnej. Wywiad jawnoźródłowy może być skutecznym narzędziem w analizie tej ogromnej ilości danych, pomagając zrozumieć trendy, wydarzenia i sytuacje w różnych częściach świata
2) Wzrost zagrożeń w cyberprzestrzeni: w miarę rozwoju technologii, cyberprzestrzeń staje się areną dla różnorodnych zagrożeń, takich jak ataki cybernetyczne, dezinformacja czy cyberprzestępczość. Wywiad jawnoźródłowy może być wykorzystywany do monitorowania działań w cyberprzestrzeni i identyfikacji potencjalnych zagrożeń.
3) Potrzeba monitorowania wydarzeń międzynarodowych: w warunkach globalizacji państwa są wzajemnie powiązane, a wydarzenia w jednym regionie mogą mieć wpływ na sytuację w innym. Wywiad jawnoźródłowy jest istotne dla monitorowania wydarzeń międzynarodowych, analizy trendów globalnych i antycypacji potencjalnych zagrożeń.
4) Rozwój narzędzi analitycznych: wraz z postępem technologii informatycznych i analizy danych, wywiad jawnoźródłowy może wykorzystywać zaawansowane narzędzia analityczne, takie jak Sztuczna Inteligencja i analiza *big data*, do lepszej oceny i zrozumienia informacji pochodzących z otwartych źródeł.
5) Wymiar informacyjny konfliktów hybrydowych: współczesne konflikty często obejmują wymiar informacyjny, dezinformację i propagandę. Wywiad jawnoźródłowy jest ważnym narzędziem w zwalczaniu dezinformacji i zrozumienia narracji pochodzących z różnych źródeł.
6) Wymiar społeczny globalizacji**:** procesy globalizacji wpływają również na wymiar społeczny i kulturowy Wywiad jawnoźródłowy może dostarczać informacji na temat

nastrojów społecznych, zmian kulturowych czy tendencji politycznych, co jest istotne dla planowania działań w obszarze bezpieczeństwa państwa.

7) Znaczenie współpracy międzynarodowej: w środowisku globalnym współpraca międzynarodowa jest kluczowa dla skutecznego przeciwdziałania współczesnym zagrożeniom. Wywiad jawnoźródłowy umożliwia wymianę informacji między państwami w sposób legalny i transparentny.

Jednakże, wraz z korzyściami wynikającymi z wywiadu jawnoźródłowego w erze globalizacji, pojawiają się również wyzwania, taki jak skomplikowane kwestie związane z prywatnością, etyką a także konieczność radzenia sobie z dezinformacją w otwartych źródłach. W związku z tym, państwa demokratyczne muszą rozwijać swoje zdolności wywiadowcze w sposób odpowiedzialny i zgodny z zasadami praworządności oraz demokratycznymi wartościami.

10. Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?

Tak, materiał pozyskany z otwartych źródeł może istotnie przyczynić się do określenia kierunków szans i zagrożeń oraz planowanych działań w zakresie bezpieczeństwa w państwach demokratycznych. Oto kilka sposobów, w jaki ten rodzaj informacji może być użyteczny:

1) Analiza trendów społecznych i politycznych: informacje pochodzące w otwartych źródeł mogą pomóc identyfikacji trendów społecznych, politycznych czy gospodarczych. Zrozumienie tych trendów jest kluczowe dla odpowiedniego reagowania na zmieniające się warunki i wyzwania stojące przed bezpieczeństwem państwa.
2) Monitorowanie sytuacji międzynarodowej: wywiad jawnoźródłowy jest skutecznym narzędziem do monitorowania sytuacji międzynarodowej. Analiza informacji pochodzących z różnych części świata pozwala na zrozumienie zmian geopolitycznych, konfliktów czy zagrożeń międzynarodowych.
3) Identyfikacja zagrożeń bezpieczeństwa w cyberprzestrzeni: wywiad jawnoźródłowy może pomóc w identyfikacji zagrożeń związanych z cyberprzestrzenią, takich jak ataki hakerskie, kampanii dezinformacyjne czy inne formy cyberprzestępczości. To istotne dla ochrony infrastruktury krytycznej i danych państwowych.

4) Analiza opinii publicznej: informacje pochodzące z mediów społecznościowych, artykułów prasowych czy innych źródeł publicznych mogą dostarczać wglądu w opinie społeczeństwa na temat różnych kwestii, w tym bezpieczeństwa. Analiza nastrojów społecznych może być przydatna w planowaniu działań informacyjnych czy edukacyjnych.
5) Weryfikacja informacji i dezinformacji: wywiad jawnoźródłowy może pomóc w weryfikacji informacji oraz zwalczaniu dezinformacji. To ważne w kontekście walki z fałszywymi informacjami i utrzymania rzetelności w przekazie publicznym.
6) Planowanie działań prewencyjnych: na podstawie analizy informacji jawnoźródłowych państwa mogą planować działania prewencyjne, zwłaszcza w kontekście zagrożeń terrorystycznych czy innych form przestępczości zorganizowanej.
7) Wspieranie procesów decyzyjnych: informacje pozyskane z otwartych źródeł mogą służyć jako ważny element procesów decyzyjnych. Na poziomie państwowym dostarczają one kontekstu i wiedzy, które pomagają w podejmowaniu informowanych decyzji.

Jednakże, ważne jest aby wywiad jawnoźródłowy był uzupełniany przez inne formy pozyskiwanych informacji zwłaszcza tam, gdzie wymagane są dane o charakterze tajnym czy poufnym. Integracja różnych źródeł informacji pozwala na budowanie pełniejszego obrazu sytuacji i podejmowanie bardziej precyzyjnych działań na rzecz bezpieczeństwa państwa.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Kooperacja ze strukturami sojuszniczymi w zakresie pozyskiwania i wykorzystywania informacji jawność źródłowych jest zazwyczaj bardzo zasadna i może przynosić szereg korzyści dla bezpieczeństwa państwa. Oto kilka powodów, dla których tego rodzaju współpraca jest ważna:

1) Wspólne zrozumienie sytuacji międzynarodowej: współpraca z sojusznikami pozwala na wymianę informacji na temat wydarzeń międzynarodowych, trendów geopolitycznych czy innych zagrożeń. Wspólne zrozumienie sytuacji jest kluczowe dla skutecznego podejmowania decyzji w dziedzinie bezpieczeństwa.

2) Ułatwienie wymiany informacji: sojusznicy często mają dostęp do różnych źródeł informacji i unikalnych perspektyw. Współpraca ułatwia wymianę tych informacji, co może poszerzyć zakres wiedzy na temat potencjalnych zagrożeń.
3) Lepsze zrozumienie lokalnych kontekstów: sojusznicy, posiadający dostęp do informacji jawnoźródłowych z własnych obszarów geograficznych, mogą dostarczyć bardziej szczegółowego i lokalnego kontekstu. To może być istotne przy analizie sytuacji związanych z bezpieczeństwem.
4) Wspólne działania w dziedzinie cyberbezpieczeństwa: w obliczu rosnącego zagrożenia cyberprzestępczością, współpraca w dziedzinie cyberbezpieczeństwa jest kluczowa. Wspólna analiza danych dotyczących ataków cybernetycznych może prowadzić do skuteczniejszej obrony przed zagrożeniami.
5) Zwiększenie skuteczności środków przeciwdziałania: sojusznicy mogą wspólnie opracowywać i wdrażać środki przeciwdziałania wobec wspólnych zagrożeń. Działa to jak wzmacnianie sił poprzez dzielenie się zasobami i kompetencjami.
6) Wzmocnienie relacji międzynarodowych: współpraca w zakresie wywiadu jawnoźródłowego może przyczynić się do wzmocnienia relacji międzynarodowych między państwami sojuszniczymi. To również ma znaczenie dla budowania zaufania i wspólnego podejścia do spraw bezpieczeństwa.
7) Zwiększenie efektywności działań antyterrorystycznych: współpraca sojusznicza może być kluczowa w zwalczaniu terroryzmu i przeciwdziałaniu zorganizowanej przestępczości transgranicznej. Wspólne środki i wymiana informacji mogą zwiększyć skuteczność działań antyterrorystycznych.

Warto jednak podkreślić, że współpraca wymaga odpowiednich mechanizmów bezpieczeństwa i zaufania między sojusznikami. Konieczne jest zachowanie odpowiednich standardów etycznych i prawnych, a także respektowanie przepisów dotyczących ochrony prywatności i praw obywatelskich. Kooperacja w obszarze wywiadu jawnoźródłowego powinna być realizowana z poszanowaniem suwerenności państw oraz zgodnie z obowiązującym prawem międzynarodowym.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: dowódca 93 Batalionu Lekkiej Piechoty w Łasku, w ramach 9 Łódzkiej Brygady Obrony Terytorialnej
3. Stopień naukowy: doktor inżynier
4. Tytuł: podpułkownik
5. Staż pracy zawodowej: 24 lata

Załącznik 9 – Protokół VIII wywiadu eksperckiego

przeprowadzonego 7 lutego 2024 r. w Krakowie

dr hab. Mirosław Kwieciński – twórca i popularyzator polskiej teorii wywiadu i kontrwywiadu gospodarczego jako fundamentalnego narzędzia ekspansji i ochrony zasobów w działalności przedsiębiorstw, autor pierwszej polskiej monografii z tego zakresu, Profesor Państwowej Akademii Nauk Stosowanych w Krośnie

1. **Czy według Pana obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Obecne wykorzystanie wywiadu jawnoźródłowego, czyli analizy informacji dostępnych publicznie, ma kluczowe znaczenie dla zapewnienia bezpieczeństwa państwa. Badanie otwartych źródeł informacji daje podstawy do uzyskania jak najbardziej aktualnej wiedzy w obszarze bezpieczeństwa, jest cenne i bez wątpienia powinno być wykorzystywane w działaniach podejmowanych na rzecz bezpieczeństwa państwa. Wywiad jawnoźródłowy pozwala na szybkie pozyskiwanie i zagospodarowanie wiedzy, co jest niezwykle ważne w dynamicznie zmieniającym się środowisku bezpieczeństwa. Analizy jawnoźródłowe umożliwiają daleko idącą sprawczość, czyli zdolność do podejmowania skutecznych działań. Pojawiają się natomiast dylematy związane z jakością i wiarygodnością informacji jawnoźródłowych.

Podsumowując, wywiad jawnoźródłowy jest fundamentem dla zapewnienia bezpieczeństwa państwa. Jednak jego skuteczność zależy od umiejętności analizy, weryfikacji i odpowiedniego reagowania na uzyskane informacje, co pozwala na wyważenie między szybkim zagospodarowaniem wiedzy a zachowaniem niezbędnej sprawczości w działaniu.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

Informacje jawnoźródłowe pełnią kluczową rolę w kontekście działań ofensywnych i defensywnych państwa, stanowiąc fundament dla weryfikacji innych źródeł informacji. Są podstawowym źródłem wiedzy, na którym opierają się zarówno działania służące bezpieczeństwu, jak i operacje specjalne. Te informacje, wynikające na przykład z dostępu do źródeł prawa, sprawozdań finansowych czy jawnych

dokumentów, pozwalają na pozyskanie danych niezbędnych do planowania i realizacji działań zarówno o charakterze obronnym, jak i ofensywnym.

Wykorzystanie informacji jawnoźródłowych ma kluczowe znaczenie dla zrozumienia środowiska, w którym działają służby specjalne oraz inne instytucje państwowe. Umożliwiają one identyfikację potencjalnych zagrożeń i szans, a także konieczności badania innych dostępnych źródeł informacji, co pozwala na zweryfikowanie i uzupełnienie posiadanej wiedzy.

Jednakże, jak pokazuje przykład analizy funduszy operacyjnych polskich służb specjalnych z lat 2006-2015, dostęp do informacji jawnoźródłowych może być ograniczany przez decyzje polityczne lub decyzje dotyczące bezpieczeństwa państwa. Zakazanie dostępu do pewnych danych przez ówczesnego wicepremiera i ministra finansów Mateusza Morawieckiego, po ujawnieniu informacji o wielkości środków funduszy operacyjnych, stanowi przykład takiego ograniczenia. Ta sytuacja pokazuje, że, dostęp do niektórych informacji może być ograniczany z różnych powodów, co rodzi pytania o przejrzystość, odpowiedzialność i równowagę między jawnością a potrzebą ochrony informacji kluczowych dla bezpieczeństwa państwa.

3. Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?

Dokonywanie analiz jawnoźródłowych ma kluczowe znaczenie w decyzjach dotyczących bezpieczeństwa państwa, co zostało już częściowo omówione w odpowiedzi na poprzednie pytanie. Takie analizy są podstawowym narzędziem w rękach badaczy, analityków i decydentów, umożliwiającym uzyskanie wiedzy o otoczeniu, w którym funkcjonuje państwo oraz o potencjalnych zagrożeniach i możliwościach.

W kontekście badań naukowych dotyczących bezpieczeństwa, jak na przykład analiza funduszy operacyjnych służb specjalnych, informacje jawnoźródłowe służą jako punkt wyjścia do głębszych rozważań. Choć te informacje mogą nie być dostępne dla każdego i mogą nie tłumaczyć całokształtu zjawiska, są one pomocne w określeniu podstawowych trendów i zmian w obszarze bezpieczeństwa.

Jak wynika przeprowadzonych przeze mnie badań, około 70% informacji pozyskiwanych przez przedsiębiorstwa w ramach tzw. białego wywiadu pochodzi ze źródeł jawnych. To pokazuje, że analizy jawnoźródłowe mają fundamentalne znaczenie

nie tylko dla sektora publicznego, ale również dla biznesu, ukierunkowując działania w zakresie bezpieczeństwa i strategii działania.

Jednakże, mimo że analizy te są niezbędne, nie są one wystarczające do pełnego zrozumienia i przewidywania wszystkich aspektów związanych z bezpieczeństwem. Wymagane jest uzupełnienie ich o informacje pochodzące z innych, mniej dostępnych źródeł, często określanych jako "szare" lub operacyjne, które mogą dostarczyć bardziej szczegółowych i specyficznych danych. Pozyskiwanie takich informacji wymaga jednak dostępu do odpowiednich sieci informacyjnych i kontaktów, a także przestrzegania ram prawnych.

4. Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

Metody stosowane w wywiadzie jawnoźródłowym obejmują szeroki zakres działań, począwszy od monitorowania otwartych źródeł informacji, takich jak prasa (zarówno ogólna jak i profesjonalna), źródła prawa, dokumenty pisemne, wydawnictwa książkowe oraz wszelkiego rodzaju treści dostępne w Internecie. Umożliwiają pozyskiwanie informacji o działalności różnych podmiotów, w tym instytucji i przedsiębiorstw. Warto podkreślić, że dostęp do otwartych źródeł jest zazwyczaj nieograniczony, co ułatwia gromadzenie danych.

Inną, mniej konwencjonalną metodą wywiadu jawnoźródłowego jest badanie śmieci. Mimo, że może wydawać się nietypowa, pozwala na pozyskanie cennych informacji o działaniach, zainteresowaniach lub planach z materiałów porzuconych przez badane podmioty. Choć może spotkać się z pewnym sceptycyzmem, w praktyce okazuje się być skuteczną metodą wywiadowczą i jest przykładem kreatywnego podejścia do pozyskiwania danych.

Współczesne technologie, w tym Internet i zaawansowane narzędzia wyszukiwania, są kluczowymi środkami wywiadu jawnoźródłowego. Pozwalają one na efektywne przeszukiwanie dużej ilości danych i identyfikowanie potrzebnych informacji. Konstruowanie skomplikowanych zapytań wyszukiwania jest tu niezbędne do odkrywania ukrytych lub zakamuflowanych danych.

5. Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

Analizy jawnoźródłowe obejmują weryfikację oraz konfrontację uzyskanych informacji z innymi źródłami. Takie podejście pozwala na uzyskanie bardziej wiarygodnej i sprawdzonej wiedzy. Ważne jest, aby nie polegać wyłącznie na jednym źródle informacji, ale zawsze dążyć do potwierdzenia uzyskanych danych przez porównanie ich z innymi dostępnymi informacjami. W tym kontekście wartościowe okazuje się wykorzystywanie nowoczesnych narzędzi technologicznych, w tym szczególnie przydatne mogą być wyszukiwarki internetowe. Gdy pogłębiamy poszukiwania, nawet wydawałoby się oczywistych haseł, okazuje się, że można odkrywać różne ścieżki, które prowadzą do nowych kontekstów i sposobów na weryfikację informacji. Stopień wiarygodności informacji zależy więc od naszej aktywności i sposobu wykorzystania dostępnych środków technicznych. Jak widać, w procesie weryfikacji niezastąpioną rolę odgrywa człowiek, którego umiejętności i krytyczne myślenie są kluczowe w ocenie pozyskanych danych.

6. Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

W przyszłości możemy spodziewać się, że rozwój metod i środków technicznych w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa będzie się koncentrować wokół sztucznej inteligencji. Sztuczna inteligencja, mimo że oferuje wiele korzyści, niesie ze sobą również zagrożenia. Jeżeli w dostępnych źródłach pojawiają się informacje niezweryfikowane lub błędne, a sztuczna inteligencja te dane przyjmuje i powiela, może to prowadzić do rozprzestrzeniania nieścisłości i błędów. Niezbędna jest więc ludzka weryfikacja, aby zapewnić wiarygodność informacji. W wywiadzie jawnoźródłowym kluczowa pozostaje umiejętność zadawania właściwych pytań typu "jak?" oraz "kto?" oraz kontekstualizacja danych, co podkreśla niezastąpioną rolę człowieka w procesie analizy. Dążymy do pozyskania wiedzy absolutnie sprawdzonej.

Zatem, chociaż sztuczna inteligencja jest istotnym narzędziem w procesie gromadzenia i analizy informacji jawnoźródłowych, niezmiennie kluczową rolę odgrywa człowiek. Jego udział jest niezbędny do weryfikacji wiarygodności,

rozumienia kontekstu oraz identyfikacji potencjalnych zniekształceń w przekazywanych danych. Dążenie do pozyskania wiedzy w pełni sprawdzonej wymaga więc połączenia zaawansowanych technologii z niezastąpionym ludzkim osądem i doświadczeniem.

7. Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? Czy wpływają one na zapewnienie bezpieczeństwa państwa?

Analizy jawnoźródłowe są bardzo istotne dla zapewnienia bezpieczeństwa państwa. Obejmują weryfikację i konfrontację uzyskanych informacji z innymi źródłami. Brak profesjonalizmu w tym obszarze może mieć znaczące konsekwencje dla bezpieczeństwa państwa, gdyż może prowadzić do przeoczenia kluczowych informacji, niuansów czy potencjalnych zagrożeń.

W związku z rosnącą popularnością wywiadu jawnoźródłowego i jego zastosowaniem, między innymi podczas konfliktów takich jak wojna w Ukrainie, nasuwa się kwestia ograniczeń etycznych. Profesjonalne podmioty wywiadowcze kierują się kodeksami zawodowymi i etycznymi, które mogą być różnie interpretowane i budzić kontrowersje. Działalność wywiadowcza, zwłaszcza ta prowadzona przez służby specjalne, często balansuje na granicy etyki. Podmioty prywatne natomiast niejednokrotnie kierują się własnymi zasadami, które mogą odbiegać od ogólnie przyjętych norm etycznych, stawiając w centrum swoich działań efektywność i wyniki, co dodatkowo komplikuje ocenę etycznego wymiaru ich działalności.

Ograniczenia w prowadzeniu rozpoznania z otwartych źródeł, takie jak kwestie etyczne i profesjonalizm w weryfikacji informacji, mają wpływ na zapewnienie bezpieczeństwa państwa. Niezbędne jest więc podejście, które łączy wysoką jakość analizy informacji z przestrzeganiem etycznych standardów działania, co stanowi wyzwanie zarówno dla służb specjalnych, jak i podmiotów prywatnych działających w przestrzeni międzynarodowej.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Jeżeli uznajemy, że informacje jawnoźródłowe są kluczowe dla zapewnienia bezpieczeństwa państwa i stanowią podstawę wszelkich analiz, to brak profesjonalizmu w tym obszarze może mieć bardzo poważne konsekwencje. Nieprofesjonalna analiza może prowadzić do przeoczenia kluczowych informacji lub ich kontekstu, co z kolei

może skutkować brakiem dostrzeżenia potencjalnych zagrożeń. Zachowanie profesjonalizmu oraz etycznych standardów jest niezwykle istotne zarówno w działalności służb specjalnych jak i w wywiadzie gospodarczym. Przytoczę przykład firmy z Małopolski, która rozwinęła swój biznes na Ukrainie, a w 2014 roku zmuszona była go zamknąć. Ważne jest, aby pamiętać, że Ukraina to kraj o specyficznych wymaganiach biznesowych, gdzie konieczne jest dokładne, szerokie i dojrzałe podejście do prowadzenia działalności. Przyczyną niepowodzenia firmy był brak solidnych fundamentów wywiadowczych oraz brak adaptacji do lokalnych warunków biznesowych, co skutkowało koniecznością zamknięcia oddziału. Nauka płynąca z tej porażki skłoniła firmę do rozwoju i transformacji jej komórki wywiadowczej, która stała się jedną z kluczowych, jeśli nie najważniejszą, w strukturze tego producenta. To potwierdza, że w dzisiejszych czasach, szczególnie w kontekście międzynarodowym, sukces w biznesie bez wsparcia profesjonalnego wywiadu gospodarczego, jest trudny do wyobrażenia. Jest to istotna lekcja, z której należy wyciągnąć wnioski, mimo że wiąże się to z określonym wysiłkiem, organizacją i kosztami.

9. Czy według Pana procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Oczywiście. Procesy globalizacji, integracji i rozwój cyberprzestrzeni znacząco wpływają na efektywność wywiadu jawnoźródłowego, dynamizują możliwości pozyskania i weryfikacji informacji. I to jest bardzo pożyteczne, pozytywne i ciekawe. Jednakże, nie zastąpią one profesjonalizmu i krytycznego podejścia badacza do analizy. W kontekście bezpieczeństwa państw demokratycznych, istotne jest, aby nie tracić z oczu etycznych i profesjonalnych standardów działania, nawet w obliczy rosnących możliwości technologicznych.

10. Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?

Materiał jawnoźródłowy ma kluczowe znaczenie w określaniu kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach

demokratycznych. Jego wartość zależy jednak od jakości przeprowadzonego postępowania wywiadowczego oraz dokonanej analizy. Z tego względu, jakość i proporcjonalność przeprowadzonego badania jawnoźródłowego będzie stała u podstaw określenia perspektyw bezpieczeństwa. Zawsze podkreślam, że informacje jawnoźródłowe stanowią podstawę analizy, ale konieczne jest ich uzupełnienie o niejawne źródła informacji, co pozwala na uzyskanie kompleksowego obrazu sytuacji bezpieczeństwa.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Kooperacja z sojuszniczymi strukturami, zwłaszcza w kontekście przynależności do Organizacji Traktatu Północnoatlantyckiego (NATO), jest zasadna i niezbędna dla zapewnienia bezpieczeństwa państwa. Polska, będąc członkiem NATO, aktywnie uczestniczy w działaniach służących wzmacnianiu wspólnego bezpieczeństwa. Takie partnerstwo wymaga uwzględnienia różnic w zakresie priorytetów bezpieczeństwa i metod jego zapewniania, co podkreśla wartość lokalnych doświadczeń i unikalnych perspektyw. Relacje w ramach sojuszu powinny bazować na wzajemnej pomocy, przy jednoczesnym poszanowaniu zasad etycznych i profesjonalnych standardów.

Istotna jest odpowiedź na pytanie, czy wszystkie elementy wiedzy, które mogą zapewnić bezpieczeństwo naszemu państwu, interesują głównego sojusznika, czy też nie są one priorytetem dla całego sojuszu. Możemy bowiem mieć do czynienia z zagadnieniami bezpieczeństwa, które są unikatowe lub szczególnie istotne z perspektywy lokalnej, a które mogą być postrzegane inaczej przez głównego sojusznika, mającego inne priorytety, politykę i perspektywę. Mimo tych potencjalnych rozbieżności, zobowiązani jesteśmy do wspierania działań sojuszniczych. Przytoczę przykład z moich badań przeprowadzonych w 2016 roku, które koncentrowały się na roli Wojsk Obrony Terytorialnej w kontekście działań wywiadowczych i kontrwywiadowczych. Nikt nie zna terenu lepiej niż pododdziały Wojsk Obrony Terytorialnej, co historycznie ma swoje uzasadnienie w działaniach podjętych jeszcze podczas drugiej wojny światowej. Armia Krajowa, początkowo funkcjonująca jako Związek Walki Zbrojnej, nie posiadała wydzielonych struktur wywiadowczych działających na szeroką skalę w Europie, w przeciwieństwie do innych organizacji, które od 1939 roku dysponowały szczegółowymi informacjami i później zostały

włączone w struktury Armii Krajowej. Te formacje współpracowały ściśle z sojusznikami, ale przede wszystkim koncentrowały się na działaniach ukierunkowane na bezpośrednie potrzeby polskiego ruchu oporu. Historia ta pokazuje, jak ważna jest lekcja płynąca z przeszłości.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: Profesor Państwowej Akademii Nauk Stosowanych w Krośnie
3. Stopień naukowy: doktor habilitowany
4. Staż pracy zawodowej: 47 lat

Załącznik 10 – Protokół IX wywiadu eksperckiego

przeprowadzonego 9 lutego 2024 r. w Warszawie

Piotr Niemczyk – były Dyrektor Biura Analiz Informacji Urzędu Ochrony Państwa, w latach 1993-1994 zastępca dyrektora Zarządu Wywiadu Urzędu Ochrony Państwa, wieloletni ekspert Komisji do Spraw Służb Specjalnych, ekspert Komisji do spraw przestrzegania praw obywatelskich w działaniach służb specjalnych, wykładowca Centralnego Ośrodka Kadr Agencji Bezpieczeństwa Wewnętrznego, Collegium Civitas i Uniwersytetu Warszawskiego.

1. **Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Wywiad jawnoźródłowy przyczynia się w ogromnym stopniu do zapewnieniabezpieczeństwa państwa. OSINT może naprowadzać na różne kierunki zagrożeń, często z większym wyprzedzeniem i stopniem prawdopodobieństwa niż operacyjne źródła wywiadowcze. Jest to szczególnie cenne dla państw, które nie dysponują wywiadem o zasięgu globalnym, takich jak Polska. W tym kontekście, CIA w Stanach Zjednoczonych prawdopodobnie jest jedynym wywiadem o zasięgu globalnym. Pozostałe agencje wywiadowcze zazwyczaj dostosowują swoje działania do interesów kraju, w którym działają. Amerykanie realizują swoje działania wywiadowcze według konkretnego porządku, opierając się na długoterminowej wizji. Jeżeli więc większość państw nie ma globalnego wywiadu, to ogromna część świadomości pewnych zagrożeń, które narastają pochodzi przede wszystkim z mediów. Przykładowo, rozważając przyszłą falę migracyjną będącą skutkiem ocieplenia klimatu, trudno jest znaleźć źródła operacyjne, które byłyby wcześniej ukierunkowane na analizę tego zagadnienia. W takim kontekście, wywiad jawnoźródłowy umożliwia przewidywanie i zrozumienie tego typu zagrożeń. Na podstawie informacji z wywiadu jawnoźródłowego można następnie projektować inne działania, w tym operacyjne, aby lepiej zidentyfikować i przygotować się na taką sytuację. OSINT dostarcza informacji, które mogą być wykorzystane do projektowania odpowiednich działań prewencyjnych, zwiększając skuteczność tradycyjnych metod wywiadowczych. W porównaniu do źródeł agenturalnych czy technicznych, to właśnie OSINT częściej pełni rolę "*lampek ostrzegawczych*", które uprzedzają o potencjalnych zagrożeniach.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

Uważam, że podstawowym celem wywiadu jawnoźródłowego jest obecnie walka z dezinformacją. Ten priorytet nie ogranicza się jedynie do weryfikacji informacji pozyskiwanych z innych źródeł, ale obejmuje także identyfikowanie i przeciwdziałanie dezinformacji, która może służyć jako narzędzie propagandowe służące do destabilizacji innych państw. Kluczowe jest rozumienie kierunków dezinformacji i opracowanie strategii jej przeciwdziałania, a także analiza wpływu na działalność informacyjną państwa. Niestety, w mojej opinii, polskie służby nie wykorzystują w pełni potencjału wywiadu jawnoźródłowego z powodu braku wykwalifikowanych specjalistów. Dlatego uważam, że utworzenie komórki OSINT ukierunkowanej na dezinformacje jest niezwykle potrzebne. Powstawanie takich jednostek na świecie podkreśla ich znaczenie i potrzebę w obecnym krajobrazie informacyjnym.

3. **Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?**

W mojej pracy podejmowałem decyzje dotyczące analiz, kierując się rekomendacjami przekazywanymi przez decydentów, tj. szefów służb i kierowników jednostek organizacyjnych szczebla rządowego. Decyzje, które podejmowałem, koncentrowały się raczej na szczegółach przedmiotu analizy, będących efektem oceny sytuacji oraz obiektywnych potrzeb konkretnych odbiorców.

4. **Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?**

Obecnie kluczowe znaczenie mają zawansowane wyszukiwarki, które łączą współczesne metody i technologie stosowane w wywiadzie jawnoźródłowym. Są to m.in. wyszukiwarki kontekstowe, które efektywnie operują na różnych, nierzadko niszowych językach.

Na rynku funkcjonują firmy usługowe, głównie o charakterze gospodarczym, specjalizujące się w integrowaniu informacji jawnoźródłowych. Ponadto, istnieją pojedyncze *think tanki*, które analizują trendy polityczne w różnych krajach, choć ich wnioski często odzwierciedlają osobiste poglądy ich autorów. W przypadku jednak analiz dotyczących gospodarki konkretnych firm, kluczowe jest opieranie się na twardych danych. Ciekawym rozwiązaniem jest Moody’s Analytics, oficjalnie znana

jako firma ratingowa, oferuje również doskonałe serwisy analizujące ryzyko gospodarcze, które są jednak bardzo kosztowne. Firma dostarcza zaawansowane rozwiązania analityczne i narzędzia wspierające zarządzanie ryzykiem finansowym, skierowane do instytucji finansowych na całym świecie. Działalność ta obejmuje nie tylko ocenę ryzyka kredytowego, ale i szeroko pojęte zarządzanie ryzykiem gospodarczym. Rozwiązanie to mogłoby być niezwykle użyteczne dla służb odpowiedzialnych za bezpieczeństwo państwa.

Choć Internet jest bogatym źródłem informacji, należy pamiętać, że nie wszystkie dane są dostępne online. Dlatego ważne jest ustalenie kategorii źródeł jawnych, niedostępnych w sieci. W Polsce typowym przykładem są akta KRS, które zawierają cenne informacje o transakcjach gospodarczych, niezbędne do głębokiej analizy ekonomicznej. Podobnie za granicą, konieczne jest dotarcie do informacji z otwartych źródeł, które nie są dostępne w Internecie. I to również jest zadaniem OSINT-u. Z jednej strony kluczowe jest dysponowanie nowoczesnym oprzyrządowaniem, które umożliwia ciągłe śledzenie ważnych informacji dostępnych w Internecie. Z drugiej strony, istotna jest również umiejętność odnajdywania ważnych informacji, które zostały zmarginalizowane. Chodzi o te informacje, które nie pojawiają się w pierwszych kilku tysiącach wyników wyszukiwania. Dlatego kluczowe jest projektowanie i dobór narzędzi w sposób odpowiadający zapotrzebowaniu. W tym kontekście niezwykle istotna jest rola osób monitorujących na bieżąco zmiany w źródłach internetowych, które ewoluują, znikają i pojawiają się, oferując nową jakość. Świat się zmienia, podobnie jak ryzyka i zagrożenia wymagające zarządzania. Ważne jest więc ciągłe monitorowanie zmienności świata i przygotowanie zespołu analityków, który będzie reagował i dysponował aktualnymi źródłami.

5. Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

Informacje jawnoźródłowe są weryfikowane tymi samymi narzędziami, które służą do ich zbierania. Uważam, że weryfikacja informacji opiera się na dwóch kluczowych aspektach, niezależnie od tego, czy dane pochodzą ze źródeł jawnych czy tajnych.

Pierwszy z nich to analiza historii źródła. Obejmuje ocenę wiarygodności i historii publikacji źródła, czy to dziennikarza, działu w gazecie, czy serwisu internetowego. Ważne jest zrozumienie czy źródło miało w przeszłości dostęp do

wiarygodnych informacji oraz czy jego przekazy były wiarygodne. Badana jest również historia źródła, jego zaangażowanie w różne sprawy oraz tendencje społeczne czy polityczne. Sprawdza się, czy informacje podawane wcześniej przez to źródło, szczególnie te dotyczące obszaru zainteresowań, były rzetelne i sprawdzały się w przeszłości.

Drugi aspekt weryfikacji to porównanie z innymi źródłami, uznawanymi za obiektywne. Przy analizie relacji z wydarzeń, takich jak spotkania polityków czy naukowców, sprawdza się, czy dane wydarzenie faktycznie miało miejsce, a następnie porównuje się relacje z różnych źródeł. Pozwala to na ocenę, czy przedstawiane informacje są realne i zgodne z charakterystyką osób biorących udział w wydarzeniu. W kontekście dezinformacji, takie porównanie zazwyczaj nie wymaga tak szczegółowej analizy, ponieważ wystarczy odnieść się do źródeł uznanych za obiektywne i porównać je z treścią potencjalnie nierzetelnych publikacji. Rozbieżności między źródłami mogą wskazywać na nierzetelność lub próbę manipulacji.

Weryfikacja informacji w wywiadzie jawnoźródłowym polega więc na dokładnej analizie historii źródła i porównaniu z innymi, wiarygodnymi źródłami. Te dwa podejścia, pionowe i poziome, są niezbędne do oceny rzetelności informacji i przeciwdziałaniu dezinformacji.

6. Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

Według mnie, rozwój metod i środków technicznych w zakresie pozyskiwania i analizy informacji jawnoźródłowych, kluczowych dla zapewnienia bezpieczeństwa państwa, będzie ukierunkowany na doskonalenie metod wyszukiwania w Internecie oraz doprecyzowanie narzędzi wyszukiwania. Sztuczna Inteligencja (AI) może wesprzeć proces wyszukiwania, umożliwiając uproszczenie kategoryzowania i hierarchizowania struktur informacji. Niemniej jednak, uważam, że jest za wcześnie, aby polegać wyłącznie na metodach sztucznej inteligencji w analizie danych jawnoźródłowych. To zadanie musi wykonać człowiek. Miałbym duże obawy co do wniosków wyciąganych bez bezpośredniego ludzkiego nadzoru. Uważam, że cenne byłoby opracowanie naukowej metody monitorowania zmian z Internecie. Ciągle jednak nieodzowna jest praca kompetentnych, asertywnych analityków, którzy powinni

posiadać umiejętności i wiedzę, aby efektywnie wyszukiwać informacje na całym świecie, w tym te, które nie są dostępne w sieci.

7. Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?

Po pierwsze ograniczony zakres tematyczny dostępnych informacji. Możliwe jest znalezienie informacji o publicznych wydarzeniach czy nastrojach w określonych środowiskach, ale kluczowe decyzje, np. te podejmowane na zamkniętych naradach w warunkach chronionych (np. na Kremlu), pozostają poza zasięgiem OSINT. Drugie ograniczenie dotyczy narzędzi do weryfikacji informacji i identyfikacji dezinformacji, które nie są doskonałe i nie pozwalają na pełne wykorzystanie wszystkich dostępnych źródeł. Po trzecie, skuteczność wywiadu jawnoźródłowego zależy nie tylko od dostępności odpowiednich narzędzi, ale przede wszystkim kompetencji analityków, co jest wspólnym wyzwaniem dla wszystkich rodzajów procesów decyzyjnych w obszarze bezpieczeństwa.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Wykorzystanie informacji jawnoźródłowych bez ich profesjonalnej weryfikacji i analizy może mieć dramatyczne konsekwencje dla bezpieczeństwa państwa. Niepoprawna interpretacja danych może wprowadzić w błąd decydentów w kluczowych kwestiach, prowadząc do katastrofalnych decyzji. Przykładem może być atak na *World Trade Center*, gdzie nieefektywne zintegrowanie informacji jawnoźródłowych ze źródłami operacyjnymi doprowadziło do poważnych zaniedbań. Błędne rozpoznanie ze źródeł jawnych, na podstawie którego zostanie sporządzona „dobrze wyglądająca" i przekonująca analiza, może skutkować nieodpowiednimi decyzjami politycznymi, gospodarczymi, szczególnie w strategicznych obszarach, takich jak produkcja żywności, leków czy sprzętu wojskowego, co ostatecznie zaszkodzi ekonomii kraju.

9. **Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?**

I tak i nie. Z jednej strony globalizacja i rozwój technologiczny zwiększają liczbę dostępnych otwartych źródeł informacji, co może ułatwić identyfikację nowych zagrożeń i trendów w bezpieczeństwie. Procesy te powodują również wzrost liczby różnych środowisk, które należy analizować do celów wnioskowania na temat bezpieczeństwa państwa. Jest to jednocześnie szansa i zagrożenie. Z drugiej strony, procesy te stwarzają ogromne możliwości dezinformacji i kształtowania nastrojów, co ma konkretny wpływ na decyzje polityczne. Co więcej, wzrost ilości informacji może prowadzić do przeciążenia danych i trudności w odróżnieniu informacji ważnych od nieważnych. Stanowi to wyzwanie w skutecznym zarządzaniu ryzykiem w obszarze bezpieczeństwa państwa. Globalizacja, której skutkiem jest ujednolicenie standardów działania poszczególnych krajów, ale i standardów życia, obyczajów i zachowania, może ułatwiać analizę jawnoźródłową, m.in. poprzez lepsze zrozumienie różnić kulturowych.

10. **Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?**

Materiał jawnoźródłowy jest kluczowy dla wyznaczania kierunków działań bezpieczeństwa w państwach demokratycznych i taki jest cel prowadzenia wywiadu jawnoźródłowego. Chciałbym podkreślić, że wykorzystanie OSINT-u wymaga profesjonalnej analizy. Nie wszystkie informacje są dokładnie przeglądane, co może prowadzić do niezrozumienia ich kontekstu lub błędnej interpretacji. Jednocześnie służby niejednokrotnie zajmują w dobrej wierze stanowisko, które jest błędne. Zdolność do właściwej oceny sytuacji gospodarczej, politycznej czy społecznej zależy od głębokiego zrozumienia procesów, wiedzy branżowej oraz strategii decydentów. Dlatego ważne jest, aby opinie i analizy były formułowane przez ekspertów znających dane zagadnienie w sposób rzetelny i obiektywny.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Kooperacja ze strukturami sojuszniczymi w zakresie wykorzystania informacji jawnoźródłowych jest wręcz konieczna. W niektórych aspektach zasadny jest również dialog nawet z krajami o odmiennych interesach, jak Korea Północna czy Rosja (np. w kontekście zagrożeń terrorystycznych, zwalczania przestępczości zorganizowanej czy proliferacji broni ABC). Niezależnie od źródła, kluczowe jest profesjonalne podejście do weryfikacji informacji. Współpraca międzynarodowa może obejmować wymianę danych operacyjnych i jawnych, jednak wymaga ostrożności, by nie ujawniać sojusznikom wszystkich słabych punktów, biorąc pod uwagę zmienne relacje międzynarodowe**.**

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: były funkcjonariusz służb specjalnych
3. Stopień naukowy: kapitan
4. Tytuł: kapitan
5. Staż pracy zawodowej: 40 lat

Załącznik 11 – Protokół X wywiadu eksperckiego

przeprowadzonego 16 lutego 2024 r. w Warszawie

gen. bryg. Mariusz Chmielewski – zastępca Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni ds. IT, Ceniony architekt IT i naukowiec, zajmujący się budową systemów i badaniami z zakresu sztucznej inteligencji, cyberbezpieczeństwa i wspomagania decyzyjnego. Laureat przeszło 100 prestiżowych nagród przyznanych przez środowisko naukowe krajowe i gremia międzynarodowe w obszarze znaczących wynalazków m.in. w dziedzinie biomedycyny i wspomagania dowodzenia. Były zastępca Dyrektora Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni oraz zastępca Dziekana Wydziału Cybernetyki WAT.

1. **Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Oczywiście. Analizując sytuację w Ukrainie można dostrzec, jak ważne jest odpowiednie zarządzanie informacją. Nawet informacja niejawna, która utraciła swoją ważność, jest już informacją jawną, bo jej niejawność została przeterminowana. Dlatego istotna jest terminowość dostarczenia informacji niejawnej. Po zakończeniu operacji, temporalne informacje zwykle publikuje się i stają się ono zasobem ogólnodostępnym, pokazując tym samym pewien aspekt działań wartościowy dla prowadzenia polityki informacyjnej sił zbrojnych oraz państwa. Odpowiednie zarządzanie informacją, czyli prezentowanie tego, co się dzieje w konflikcie, jest również formą pewnego kreowania pozytywnego wizerunku danej armii. Przykładem tego jest ogromny wysiłek włożony w politykę informacyjną na Ukrainie. Działania te są realizowane celowo i z perfekcją, co świadczy o dążeniu do doskonałości w publikowaniu informacji jawnej oraz jej wykorzystywaniu w kreowaniu StratCom, czyli komunikacji strategicznej armii ukraińskiej.

2. **Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?**

Informacje jawnoźródłowe pełnią istotną rolę w weryfikacji innych danych i są kluczowe zarówno dla działań wywiadowczych, jak i kontrwywiadowczych. Wykorzystanie specjalistycznych algorytmów umożliwia narzędziową weryfikację informacji, w tym ocenę ich wiarygodności i pewności.

Bardzo często to właśnie w otwartych źródłach internetowych znajdują się naoczne relacje czy treści publikowane przez użytkowników, które okazują się być cennymi informacjami dla służb. Osoby dokumentujące wydarzenia i dzielące się swoimi obserwacjami, stają się żywymi sensorami przestrzeni informacyjnej, dostarczając danych, które mogą być wykorzystywane w analizie sytuacji.

Informacje jawnoźródłowe zmienia kategorię na niejawną, gdy zostaną wzbogacone o atrybuty analityczne i gdy są wzbogacone o informacje „klauzulowane". Takie informacje, choć pierwotnie publiczne, nabierają nowego znaczenia i wartości, stając się dostępne jedynie dla osób z odpowiednimi uprawnieniami.

Niezwykle istotnym aspektem jest również rola urządzeń cyfrowych, zwłaszcza telefonów komórkowych, które umożliwiają bardzo szybką publikację informacji. W dobie Internetu i mediów społecznościowych, tempo rozprzestrzeniania się danych jest bezprecedensowe. Dodatkowo algorytmy portali internetowych odgrywają znaczącą rolę w propagacji informacji, a powszechna chęć dostępu do często kontrowersyjnych treści w szybki sposób wpływa na dynamikę rozpowszechniania informacji jawnoźródłowych.

3. Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?

Analizy jawnoźródłowe odgrywają istotną rolę w procesie podejmowania decyzji dotyczących bezpieczeństwa państwa.

Po pierwsze, analizy te są niezbędnym elementem w procesie weryfikacji informacji. Ich zastosowanie pozwala na dokładniejsze zrozumienie sytuacji i zapewnienie, że podejmowane decyzje opierają się na rzetelnych danych. Po drugie, kluczowe jest wykorzystanie jak najszerszego spektrum dostępnych źródeł. Im więcej informacji jesteśmy w stanie zgromadzić i skonfrontować, tym dokładniejsza staje się nasza analiza. To z kolei przekłada się na lepszą ogólną percepcję danego problemu. Po trzecie, istotna jest również szybkość dostarczenia informacji. W dynamicznie zmieniającym się środowisku bezpieczeństwa, terminowość jest niezwykle ważna, ponieważ może decydować o skuteczności podjętych działań.

Niezależnie od tego, czy informacja pochodzi ze źródeł jawnych czy niejawnych, jej analiza jest niezbędnym krokiem w procesie decyzyjnym związanym z bezpieczeństwem państwa.

4. Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

W kontekście metod i środków stosowanych w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa, skoncentrowałbym się przede wszystkim na narzędziach i źródłach informacji. W trakcie konfliktów, takich jak w Ukrainie, znaczącą rolę odgrywają komunikatory, które często stanowią pierwsze źródło informacji na temat bieżących wydarzeń. Platformy takie jak Twitter szybko stały się kanałem rozpowszechniania i aktualizowania informacji, jeszcze zanim informacje te dotrą do większego grona odbiorców za pośrednictwem oficjalnych mediów. Należy również podkreślić, że pewne źródła mogą charakteryzować się wyższym poziomem prywatności lub być dostępne wyłącznie dla ograniczonych grup odbiorców, natomiast inne funkcjonują w oparciu o system *multicastu*, dystrybuując dane na dużą skalę. Analitycy polegają na różnorodności tych źródeł, aby zapewnić jak najpełniejszy obraz sytuacji. Ostatecznie, skuteczność wywiadu jawnoźródłowego zależy od umiejętnego wykorzystania tych narzędzi i źródeł w celu zbierania, analizowania i weryfikowania informacji.

W pracy analitycznej istotne jest zarówno samo uzyskanie informacji, ale również dostęp do oryginalnych danych i źródeł. To pozwala na własną interpretację i ocenę autentyczności oraz wiarygodności informacji, co jest nieocenione w kontekście cyberbezpieczeństwa i analizy sytuacji geopolitycznych. Zatem, nie chodzi jedynie o interpretację dostarczonych danych przez innych, ale o bezpośredni dostęp do oryginalnych źródeł, które umożliwiają weryfikację i ocenę potwierdzenia informacji bez ryzyka manipulacji algorytmicznej. Jest to perspektywa techniczna, ponieważ z punktu widzenia metodyki szczególnie cenię sobie algorytmy fuzji danych, które uważam za intuicyjne i niezwykle efektywne w mojej pracy.

5. Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

Weryfikacja informacji pozyskanych za pomocą wywiadu jawnoźródłowego jest bardzo istotna. Proces ten opiera się na trzech podstawowych metodach: fuzji danych, różnicowania oraz kooperacji. Fuzja danych pozwala na integrację informacji pochodzących z różnych źródeł w celu stworzenia spójnego obrazu sytuacji. Fuzja danych umożliwia skorzystanie z różnorodnych perspektyw na ten sam temat, co

zwiększa kompleksowość analizy i pomaga w identyfikacji oraz eliminacji ewentualnych braków lub sprzeczności w danych. Różnicowanie skupia się na porównywaniu i kontrastowaniu informacji pochodzących z dwóch lub więcej źródeł w celu zidentyfikowania różnic. Analiza tych różnic może ujawnić unikatowe cechy lub sprzeczności między źródłami, co jest kluczowe dla oceny wiarygodności i pełności informacji. Różnicowanie pozwala zrozumieć, jak poszczególne źródła przedstawiają daną sytuację, co jest pomocne w wykrywaniu potencjalnej dezinformacji czy stronniczości. Metoda kooperacji jest szczególnie wartościowa, gdy różne źródła oferują uzupełniające się informacje, które razem tworzą spójną całość. Dodatkowo, ważne jest, aby podejść do analizy z ostrożnością, traktując informacje jawnoźródłowe jako niepotwierdzone do momentu zweryfikowania ich wiarygodności. W tym kontekście, ocena ryzyka i poziomu zaufania do poszczególnych źródeł jest nieodzowna, aby zapewnić rzetelność podejmowanych na ich podstawie decyzji. Podstawowe metody fuzji danych, zarówno na poziomie technicznym, jak i analitycznym, są niezwykle wartościowe, ponieważ pozwalają na przemyślane podejmowanie decyzji. Nie należy opierać decyzji wyłącznie na informacji z jednego źródła, dopóki nie zostanie ona zweryfikowana za pomocą innych, niezależnych danych. Ważne jest, aby traktować pojedyncze, niepotwierdzone źródło jako potencjalnie zmanipulowane, a ryzyko takiej manipulacji powinno być zawsze brane pod uwagę przy podejmowaniu decyzji.

Równie ważna jest również analiza samego otwartego źródła informacji. Nie zawsze najbardziej opiniotwórcze gazety gwarantują najwyższą jakość informacji. Jak podkreślił George Washington w jednym ze swoich wywiadów, zadaniem dziennikarza jest dostarczanie prawdziwych, autentycznych i dokładnie sprawdzonych informacji, a nie tych, które są dostępne najszybciej. Ta zasada powinna być stosowana nie tylko w dziennikarstwie, ale w każdym procesie weryfikacji informacji jawnoźródłowych.

6. Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

Metody i środki techniczne pozyskiwania oraz analizy informacji jawnoźródłowej będą ewoluować w kierunku jeszcze większego wykorzystania nowoczesnych technologii. Kluczowym elementem tego rozwoju będzie zwiększona

rola sensorów oraz zaawansowane zastosowania sztucznej inteligencji, które będą miały za zadanie szybką ocenę i porównanie danych. Te technologie zostaną zintegrowane w całościowym środowisku informacyjnym, co pozwoli na efektywniejszą analizę i weryfikację informacji.

Ponadto, znaczącym kierunkiem będzie tworzenie narzędzi analitycznych, takich jak systemy oceny wiarygodności informacji w mediach społecznościowych, wykorzystujące mechanizmy sztucznej inteligencji. W ubiegłym roku miałem przyjemność prowadzić konkurs związany z dezinformacją, gdzie głównym zadaniem było stworzenie narzędzi do analizy treści m.in. z mediów społecznościowych, oceniających wiarygodność informacji przy użyciu sztucznej inteligencji. To doświadczenie ukazało ogromną potrzebę w zakresie edukacji użytkowników w weryfikacji napływających informacji pod kątem ich charakterystyk i prawdziwości. W krajach takich jak Norwegia czy Holandia, obywatele wykazują wysoką świadomość konieczności weryfikacji, czy informacja jest jedno czy wieloźródłowa lub podzielona, co jest wpajane od najmłodszych lat edukacji.

W ramach narzędzi automatyzacji rola sztucznej inteligencji w przetwarzaniu oraz analizie obszernych zbiorów danych generowanych przez systemy informacyjne staje się kluczowa. Pojawia się zatem potrzeba dysponowania zaawansowanymi narzędziami zdolnymi do automatycznej obróbki i weryfikacji tych danych, co umożliwi efektywne wykrywanie potencjalnej dezinformacji. Już teraz powstają portale i narzędzia, wykorzystujące modele AI do analizy językowej i weryfikacji informacji, co w przyszłości będzie istotnym, wspierającym elementem w zapewnieniu bezpieczeństwa informacyjnego państwa. Natomiast, wyniki naszych analiz wskazują, że sztuczna inteligencja nie zastąpi całkowicie człowieka. W kontekście stosowania modeli takich jak Open AI, kluczowe okazuje się stawianie odpowiednich, dobrze przemyślanych i precyzyjnych pytań. Sztuczna inteligencja dostarcza odpowiedzi, ale bez krytycznego podejścia i umiejętności analizy ze strony człowieka, nie zawsze są one wysokiej jakości. Nasze doświadczenia z testowaniem takich rozwiązań utwierdzają mnie w przekonaniu, że przyszłość analizy jawnoźródłowej wykonywanej przez człowieka jest bezpieczna i że wiedza w ludzkim umyśle na swoją przyszłość.

7. Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?

Po pierwsze, występuje naturalna tendencja do pogłębiania wiedzy na temat danej informacji. Dążenie to do weryfikacji źródła informacji może jednak wiązać się z ryzykiem naruszenia norm etycznych i prawnych, w tym aspektów dotyczących prywatności oraz bezpieczeństwa danych.

Największym wyzwaniem jest zapewnienie, że informacje, nawet te pozornie wiarygodne, nie zostały zmanipulowane. W szczególności w kontekście materiałów o słabej jakości, które trudno jest zweryfikować za pomocą dostępnych algorytmów. W takich przypadkach konieczne jest opieranie się na wnioskowaniu opartym na zdrowym rozsądku i krytycznym myśleniu. Zajmowałem się analizą przypadków manipulacji materiałami, które różniły się nie tylko ze względu na aspekty wizualne czy semantyczne, ale także pod kątem metadanych. Z metadanych można bowiem pozyskać kluczowe informacje, takie jak data nagrania, lokalizacja oraz typ urządzenia rejestrującego. Analiza ta umożliwia również weryfikację zdolności urządzenia do rejestracji oraz sprawdzenie, czy przedstawiony obraz środowiska odpowiada rzeczywistości konkretnej lokalizacji w danym czasie. Zwrócić uwagę należy, na fakt, iż materiały cyfrowe często są różnej jakości i cyfrowa ich korekta, augmentacja jest zarówno metodą ulepszenia tych informacji jednocześnie stanowi ryzyko oskarżenia o celową manipulację i ingerencję niszczące autorytarność i niezaprzeczalność tych danych.

Po drugie, z racji powszechności dostępu do informacji jawnoźródłowych, istnieje ryzyko jej manipulacji, w tym cięcia, powielania lub przekręcania danych. Natywna sztuczna inteligencja ułatwia takie działania, co znacznie zwiększa ryzyko dezinformacji. Obserwujemy obecnie w otwartych źródłach informacji praktyki manipulacji, które są alarmujące, szczególnie gdy prowadzą do deprecjacji pozycji i reputacji jednostki lub państwa. Ta sytuacja stwarza poważne zagrożenie i wymaga stanowczej reakcji prawnej. Na szczęście, istnieją już ramy legislacyjne adresujące te wyzwania, co pozwala na podejmowanie działań przeciwko takim praktykom dezinformacyjnym.

W obszarze militarnym, gdzie przetwarzane są informacje niejawne, zazwyczaj obowiązuje zasada zakazu wnoszenia urządzeń rejestrujących. Niemniej jednak,

w warunkach konfliktu, potrzeby operacyjne szybkiego dostępu do informacji pola walki zmuszają do użycia technologii podwójnego zastosowania. Telefony komórkowe okazały się najczęściej używanym narzędziem do przekazywania informacji, a sieć GSM stała się elementem infostruktury krytycznej, która nie jest całkowicie degradowana, a wręcz przeciwnie dba się o nią, gdyż zapewnia kluczowy zasób społeczeństwa. Pojawia się problem, gdy oprogramowanie ofensywne pozwala na manipulację systemami operacyjnymi tych urządzeń, co podważa wiarygodność materiałów z nich pochodzących. Takie działania są nie tylko nieetyczne, ale również zakazane prawnie, mimo to znane są przypadki kwestionowania autentyczności tak pozyskanych danych. Warto również zauważyć, że w niektórych krajach obowiązuje procedura kontroli telefonów przy wjeździe, co świadczy o próbach weryfikacji tożsamości użytkowników opartej na ich cyfrowych śladach. To podkreśla, jak w dzisiejszych czasach cyfrowa identyfikacja i zaufanie stają się kluczowe w ocenie, czy osoby zachowują się zgodnie z oczekiwaniami etycznymi.

Biorąc pod uwagę wymienione ograniczenia w prowadzeniu rozpoznania z otwartych źródeł, pragnę zaakcentować konieczność przyjęcia krytycznego podejścia do analizy i weryfikacji informacji. Jest to zadanie wymagające zarówno dostępu do zaawansowanych narzędzi technologicznych, jak i świadomości potencjalnych zagrożeń, co jest niezbędne dla skutecznej ochrony przed dezinformacją oraz dla zabezpieczenia interesów państwa.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Wykorzystanie informacji jawnoźródłowych bez odpowiedniej weryfikacji i analizy może mieć tragiczne konsekwencje dla bezpieczeństwa państwa. Po pierwsze, niekontrolowane publikowanie materiałów, zwłaszcza tych o charakterze agresywnym lub drastycznym, dotyczących konfliktów zbrojnych, prowadzi do zjawiska oswajania społeczeństwa z agresją. Takie działanie może mieć na celu mobilizację opinii publicznej, jednak nadmierna ekspozycja na tego typu treści może prowadzić do znieczulicy i osłabienia wrażliwości na przemoc.

Po drugie, niezbędna jest świadomość odpowiedzialności związanej z rozpowszechnianiem informacji, szczególnie w kontekście ich wpływu na percepcję sytuacji bezpieczeństwa. Analitycy, uznawani za autorytety w swojej dziedzinie,

powinni brać na siebie ciężar odpowiedzialności za przekazywane dane, co oznacza konieczność dokładnej weryfikacji i analizy przed ich publikacją. Rola analityka wykracza poza posiadanie odpowiednich umiejętności i obejmuje również świadomość potencjalnych konsekwencji rozpowszechniania niezweryfikowanych danych. W związku z tym, nie każdy z dostępem do Internetu powinien postrzegać się jako analityk. W tym kontekście warto zwrócić uwagę na algorytm PageRank zaprojektowany przez twórców Google, który umożliwia ocenę jakości przekazu i wiarygodności autora (źródła) na podstawie cytowań jego prac przez inne źródła, co jest zgodne z zasadą "Jesteś tak dobry, jak źródła, które ciebie cytują". W kontekście naukowym, oznacza to, że renoma badacza częściowo zależy od tego, kto i jak często powołuje się na jego prace. Tworzy to specyficzną barierę jakościową, którą trzeba przekroczyć, aby zdobyć uznanie w środowisku naukowym i analitycznym.

9. Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Procesy globalizacji i integracji oraz rozwój cyberprzestrzeni bez wątpienia wpływają na efektywność wywiadu jawnoźródłowego oraz podkreślają potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych.

Po pierwsze, należy zauważyć, że globalizacja i rozwój technologii informacyjnych zwiększają dostępność danych, co z jednej strony jest korzystne, ale z drugiej wymaga od osób publikujących informacje o sobie świadomości potencjalnych konsekwencji. Publikując dane w określonych kontekstach, należy być gotowym na to, że mogą one zostać wykorzystane przez obce służby lub inne instytucje.

Z jednej strony, globalizacja i rozwój technologiczny ułatwiają dostęp do szerokiego zakresu informacji, co jest korzystne dla działań wywiadowczych. Z drugiej strony, te same procesy zwiększają ryzyko ekspozycji na ataki ze strony obcych służb czy innych instytucji, zwłaszcza gdy osoby publikują wrażliwe informacje o sobie. Odpowiedzialność za publikowane treści, zwłaszcza w kontekście zawodowym i prywatnym, jest kluczowa, co podkreśla znaczenie cyberhigieny dla osób działających w sferze bezpieczeństwa. Należy mieć świadomość, że łatwość dostępu do mediów cyfrowych i ich publikowania, a także ryzyko niechcącego łączenia kont

i niezamierzonego wysyłania korespondencji służbowej, niesie ze sobą poważne niebezpieczeństwa.

Rozwój cyberprzestrzeni sprawia, że umiejętność korzystania z narzędzi cyfrowych i świadomość, jakie ślady zostawiamy w sieci, stają się kluczowe dla ochrony naszej prywatności i bezpieczeństwa. Podkreślanie zagrożeń wynikających z ekshibicjonizmu informacyjnego oraz uwzględnianie faktu, że Internet nigdy nie zapomina, powinny stać się integralną częścią procesu edukacyjnego już od najwcześniejszych lat życia.

10. Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?

Instytucje państwowe wykorzystują narzędzia oparte na otwartych źródłach do wspomagania działań wywiadowczych i kontrwywiadowczych. Chociaż trudno jest dokładnie określić, jaki procent działań w obszarze bezpieczeństwa państwa opiera się na analizie materiałów jawnych, niewątpliwie obserwuje się rosnącą potrzebę do publikowania i analitycznego przetwarzania takich informacji. To prowadzi do asynchronicznego generowania alertów sygnalizujących potencjalne zagrożenia. Przykładem ekstremalnego wykorzystania takich metod jest społeczeństwo chińskie, które godzi się na wszechobecną analizę behawioralną obywateli z wykorzystaniem sztucznej inteligencji, bez etycznych ograniczeń. I to dla zwykłego obywatela krajów zachodnich jest przerażające. Ta sytuacja ilustruje, jak państwo może kształtować pozytywną trajektorię rozwoju obywateli, zgodnie z linią rozwoju państwa. Jest to obszar inżynierii społecznej, przykład ewidentnej „*kontroli umysłów*", wykorzystywanej do celów politycznych. Dochodzi do pozbawiania obywateli swobód, z ryzykiem nadmiernej kontroli i ograniczania wolności. Dlatego najważniejsze jest znalezienie równowagi między bezpieczeństwem, w tym dążeniem do pełnej transparentności, a ryzykiem inwigilacji. Anonimowość staje się coraz bardziej iluzoryczna w obliczu wszechobecnej cyfryzacji, co zmusza do refleksji nad granicami prywatności w erze Internetu.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Jest podstawą działania w cyberbezpieczeństwie. Cyberbezpieczeństwo opiera się na pracy zespołowej i jest to kluczowy element strategii bezpieczeństwa w domenie cybernetycznej. Dzielenie się informacjami, zarówno jawnymi, jak i niejawnymi, jest niezbędne, ponieważ umożliwia skuteczne reagowanie na zagrożenia oraz buduje wspólną wizję bezpieczeństwa. Istotne jest, aby w przypadku uzyskania krytycznych informacji, niezależnie od tego, czy są one jawne czy tajne, stosować adekwatne kanały do ich przekazywania. Przykładem takiej współpracy są spotkania grup zabezpieczeń cyberbezpieczeństwa, szczególnie w sektorze finansowym. Podczas tych spotkań uczestnicy wymieniają się informacjami o obsługiwanych incydentach i wykrytych zagrożeniach. Brak aktywnego udziału i dzielenia się wartościowymi danymi przez dwa kolejne spotkania skutkuje wykluczeniem z dalszego uczestnictwa. Ważny jest więc wkład wynikający z kompetencji strony, między innymi w zakresie wykrywania podatności, określania wektorów ataków, ale także jej otwartości i gotowości do dzielenia się informacjami jawnoźródłowymi. Zastosowanie znajdzie podejście oparte na zasadzie "najsłabszego ogniwa".

Odpowiedzialność za bezpieczeństwo i rozwój technologiczny nie powinna spoczywać wyłącznie na barkach jednego dostawcy czy kraju. Polska, dzięki rozwiniętemu rynkowi IT, jest mocnym partnerem na arenie międzynarodowej i może być dumna ze swoich osiągnięć w dziedzinie informatyki. Nasze zaangażowanie w realizację usług w dziedzinie technologii informacyjnych dla innych krajów buduje wizję polskiego IT oraz specjalisty, z którego wiedzy możemy korzystać. Suwerenność technologiczna, kluczowe pojęcie dla naszego kraju, powinna gwarantować, że posiadamy zdolność samodzielnego tworzenia narzędzi i technologii, nawet jeśli w pewnych aspektach nie jest to bezwzględnie konieczne.

Cytując doktora Łukasza Przybyło, mojego serdecznego kolegę, Polska jako państwo średniej wielkości dysponuje unikalną wartością. Moim zdaniem, ta wyjątkowość jest widoczna w potencjale do kreowania międzynarodowej współpracy i innowacji w dziedzinie technologii informacyjnych. Powinniśmy identyfikować technologie krytyczne dla naszego bezpieczeństwa i niezależności, a także dbać o to, aby nasze działania były wspierane przez solidną wiedzę i kompetencje wewnętrzne.

To podejście umożliwi nie tylko zabezpieczenie kluczowych przepływów informacyjnych i technologicznych, ale także pozwoli na utrzymanie pozycji Polski jako cenionego partnera na międzynarodowym rynku IT.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: zastępca Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni ds. IT
3. Stopień naukowy: doktor
4. Tytuł: generał brygady
5. Staż pracy zawodowej:

Załącznik 12 – Protokół XI wywiadu eksperckiego

przeprowadzonego w dniu 19 lutego 2024 r. w Warszawie

Bartosz Pastuszka – Prezes Zarządu NaviRisk, specjalizuje się w zarządzaniu ryzykiem i bezpieczeństwem, wywiadzie gospodarczym, audytach śledczych i sprawdzaniu przeszłości. Był pierwszym dyrektorem Pinkerton, najstarszej na świecie agencji detektywistycznej w Polsce i Europie Środkowo-Wschodniej.

1. Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?

Obecne wykorzystanie wywiadu jawnoźródłowego odgrywa ważną rolę w zapewnieniu bezpieczeństwa państwa, jednak jego potencjał nie jest wykorzystywany w pełni. Chociaż agencje wywiadowcze i analityczne korzystają z OSINT-u jako podstawy do gromadzenia informacji, często skupiają się one na aspektach śledczych, poszukiwaniu przestępców czy nadużyciach, zamiast wykorzystywać te informacje do identyfikacji szans (*opportunities*) dla państwa i jego gospodarki. Przykład współpracy ze Szwedami nad systemem zarządzania kryzysowego opartym o dostęp do systemu Bloomberg pokazuje, że informacje jawnoźródłowe mogą być wykorzystywane nie tylko do reagowania na kryzysy, ale również do wypracowywania przewagi konkurencyjnej. Informacje jawnoźródłowe o wydarzeniach międzynarodowych mogą być kluczowe dla logistyki, bezpieczeństwa oraz identyfikacji szans biznesowych wynikających z niespodziewanych zmian w globalnym środowisku. Te informacje umożliwiają państwu ekspansję produkcji i zdobycie nowych rynków.

W kontekście bezpieczeństwa państwa, polskie służby i inne państwowe agencje powinny, według tej perspektywy, bardziej skoncentrować się na analizowaniu informacji jawnoźródłowych pod kątem wykorzystania szans dla rozwoju kraju. Oznacza to permanentne analizowanie globalnego środowiska biznesowego, technologicznego, politycznego i społecznego, aby identyfikować tendencje, które mogą wpłynąć na strategiczne pozycjonowanie państwa na arenie międzynarodowej. W Polsce i niektórych innych krajach wydaje się, że brakuje takiej aktywności. Skupienie się tylko na aspekcie śledczym jest pewną niedoskonałością, która może ograniczać potencjał rozwojowy kraju. Istnieje potrzeba tworzenia i utrzymania struktur analitycznych, które będą w stanie nie tylko reagować na zagrożenia, ale również

proaktywnie wykorzystywać dostępne informacje do budowania siły i stabilności państwa oraz wspierania rozwoju gospodarczego.

W kontekście współczesnych konfliktów kluczową rolę ogrywa ekonomia. Wojna gospodarcza trwa już od wielu lat. Jesteśmy jej uczestnikami, a kluczowe znaczenie ma budowanie przewagi ekonomicznej, pozwalającej na bogacenie się kraju, generowanie środków finansowych, efektywną produkcję i akumulację zasobów. Bez solidnej podstawy gospodarczej, nawet jeśli produkcja amunicji jest możliwa, zakup broni staje się problematyczny z powodu braku funduszy. Przykład Ukrainy pokazuje, że pomimo możliwości werbowania żołnierzy, brak środków finansowych uniemożliwia odpowiednie ich wyposażenie.

2. Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?

Ocena przydatności informacji jawnoźródłowych w kontekście weryfikacji innych źródeł informacji wymaga złożonego podejścia. Obecnie obserwujemy przesunięcie z deficytu informacji, który był problemem jeszcze pięć lat temu, do nadmiaru danych dostępnych w przestrzeni publicznej. To zmienia sposób, w jaki analitycy muszą podchodzić do procesu weryfikacji.

Współcześnie, kluczową umiejętnością jest zdolność do selekcjonowania i oceny informacji, identyfikowania danych relewantnych i wiarygodnych w morzu dostępnych treści. Wyzwanie to jest potęgowane przez ogólnodostępność Internetu i mediów, które stały się źródłem rozległej dezinformacji. Trudność w wyłowieniu wartościowych informacji wynika także z intensyfikacji wojny informacyjnej, gdzie stosowane są różnorodne techniki mające na celu zaciemnienie prawdy, w tym działalność farm trolli czy tworzenie fałszywych narracji. Weryfikacja informacji jawnoźródłowych staje się kluczowym elementem krzyżowej weryfikacji danych, choć nie brak tutaj problemów związanych z oceną wiarygodności tych danych. niezbędna jest zatem nie tylko szeroka wiedza ekspercka i doświadczenie analityczne, ale też zdolności krytycznego myślenia.

W kontekście informacyjnym, gdzie wielokrotnie powtarzane kłamstwo może zacząć być postrzegane jako prawda, istotne jest poleganie na wysokiej jakości ekspertyzach i długoterminowym doświadczeniu. To podkreśla wagę inwestycji w rozwój umiejętności analityków i budowanie zespołów eksperckich zdolnych do efektywnej nawigacji w złożonym świecie informacji jawnoźródłowych.

3. Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?

Analiza informacji jawnoźródłowych odgrywa kluczową rolę w podejmowaniu decyzji dotyczących bezpieczeństwa państwa, jak również w kształtowaniu przewagi konkurencyjnej w różnych sferach działalności. Z doświadczenia wynika, że dokładny research na temat osób czy instytucji przed spotkaniami czy negocjacjami pozwala budować strategiczną przewagę, dostarczając wiedzy o preferencjach, sytuacji życiowej, zawodowej czy biznesowej danego podmiotu.

Współczesny świat zarządzania i biznesu coraz częściej korzysta z analizy informacji jawnoźródłowych. Nie chodzi już tylko o pojedyncze działania, ale o stałe monitorowanie sytuacji, które pozwala na szybką adaptację do zmieniających się warunków. Dostęp do odpowiednich informacji i ich efektywne wykorzystanie przekłada się na budowanie przewagi konkurencyjnej, trafność podejmowanych decyzji oraz optymalizację ryzyka.

W obliczu rosnącej konkurencji i skomplikowanej sytuacji geopolitycznej, trafne decyzje oparte na rzetelnych danych jawnoźródłowych stają się fundamentem skutecznego działania. Wymaga to jednak od decydentów nie tylko intuicji, ale przede wszystkim umiejętności analitycznych i dostępu do wiarygodnych źródeł. Współczesne wyzwania wymagają od państw i ich struktur umiejętności szybkiego adaptowania się do zmieniających się okoliczności oraz wykorzystywania dostępnych informacji w sposób strategiczny.

4. Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

Znacząca ewolucja narzędzi i metod stosowanych w wywiadzie jawnoźródłowym, od drogich i trudno dostępnych do tych oferowanych za niewielką opłatą lub nawet za darmo, znacznie poszerzyła możliwości analizy i zbierania danych. Dostępne obecnie narzędzia analityczne umożliwiają szeroki zakres działań – od wychwytywania twarzy po głębokie analizy w mediach społecznościowych.

Mimo ogromnego postępu technologicznego i dostępności narzędzi, kluczowym elementem nadal pozostaje wiedza i doświadczenie analityków. To właśnie one pozwalają na efektywne odsiewanie i interpretację gromadzonych informacji. W przeszłości, dostęp do danych był bardziej ograniczony i często wymagał

np. odwiedzin w bibliotekach czy archiwach. Obecnie, większość informacji jest dostępna online, co z jednej strony ułatwia pracę, a z drugiej generuje wyzwania związane z nadmiarem danych.

5. Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

Informacje pozyskane drogą wywiadu jawnoźródłowego są weryfikowane przy użyciu zaawansowanych technologii. Mimo to, kluczową rolę odgrywają analitycy, których zadaniem jest krytyczna analiza i ocena wiarygodności informacji, uwzględniająca kontekst kulturowy i specyfikę tematu. Doświadczenie i wiedza analityczna są niezbędne do rozróżnienia prawdziwych danych od dezinformacji. W tym kontekście, synergia między możliwościami technologicznymi a ekspertyzą ludzką stanowi fundament skutecznego wykorzystania wywiadu jawnoźródłowego w działaniach na rzecz bezpieczeństwa państwa.

6. Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?

Pierwszym z kierunków rozwoju metod i środków technicznych w wywiadzie jawnoźródłowym będzie koncentracja na ocenie i weryfikacji informacji. Narzędzia analityczne muszą ewoluować, by skuteczniej identyfikować fałszywe dane i dezinformację. Mimo potencjału sztucznej inteligencji (AI) i automatyzacji, które usprawniają analizę danych, kluczowa pozostaje rola człowieka w ostatecznej ocenie informacji. Sztuczna inteligencja, choć niezwykle pomocna, może być ograniczona przez dane, na których została wytrenowana. Uważam, że kluczową rolę w ocenie i wykorzystaniu informacji jawnoźródłowych będzie nadal odgrywać doświadczenie i umiejętności analityków. W przyszłości możemy spodziewać się dalszego rozwoju narzędzi AI i metod automatyzacji, które będą jeszcze skuteczniej wspierać procesy pozyskiwania i analizy danych jawnoźródłowych. Jednocześnie, wzrośnie zapotrzebowanie na wyszkolonych analityków zdolnych do pracy z tymi narzędziami, interpretacji ich wyników i podejmowania na ich podstawie trafnych decyzji.

Drugim z kierunków będzie dalszy rozwój i integracja zaawansowanych technologii, takich jak sztuczna inteligencja czy uczenie maszynowe oraz tworzenie narzędzia do głębokiej analizy danych, aby wspierać procesy identyfikacji i segregacji

danych. To umożliwi szybsze i bardziej efektywne przetwarzanie ogromnych zbiorów danych.

7. Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?

Prowadzenie rozpoznania z otwartych źródeł napotyka na szereg ograniczeń, które mają wpływ na zapewnienie bezpieczeństwa państwa. Jednym z nich są ograniczenia kosztowe związane z dostępem do cennych baz danych. Coraz częściej obserwujemy, że dostęp do ważnych informacji jest utrudniony z powodu wysokich kosztów subskrypcji, ponieważ stanowią one źródło dochodu dla ich właścicieli.

W niektórych krajach, jak na przykład w Szwecji, obserwujemy dużą transparentność życia publicznego, co ułatwia dostęp do informacji o zarobkach, nieruchomościach czy opinii publicznej danej osoby. Takie podejście sprzyja otwartości i dostępności informacji, ale rodzi pytania o granice prywatności i bezpieczeństwa danych osobowych.

Kolejnym aspektem są ograniczenia prawne dotyczące ochrony danych osobowych. Choć istnieją przepisy mające na celu ochronę prywatności, w praktyce często okazują się one niewystarczające lub łatwe do obejścia dla osób zdeterminowanych do zdobycia pewnych informacji. To wskazuje na lukę między intencją ochrony a rzeczywistą skutecznością przepisów.

Należy również zwrócić uwagę na kwestie etyczne związane z gromadzeniem i wykorzystywaniem informacji z otwartych źródeł. Współczesny ekshibicjonizm i publikowanie przez osoby prywatne szerokiej gamy danych osobistych w mediach społecznościowych stawiają pytania o odpowiedzialność za ochronę tych informacji, jak również o konsekwencje ich nieodpowiedniego wykorzystania.

W kontekście bezpieczeństwa państwa, te ograniczenia mogą mieć znaczący wpływ. Koszty dostępu do kluczowych informacji mogą ograniczać zdolności analityczne państwa, podczas gdy różnice w dostępności danych publicznych na świecie utrudniają globalne działania wywiadowcze. Dodatkowo, kwestie prawne i etyczne wymagają ciągłego zastanowienia nad granicami i metodami pozyskiwania danych, aby nie naruszać prywatności jednostek i nie podważać zaufania publicznego. Wymaga to od państwa nie tylko inwestycji w narzędzia i technologie, ale również rozwijania

kompetencji etycznych i prawnych osób zajmujących się analizą danych jawnoźródłowych.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy może mieć bardzo poważne konsekwencje dla bezpieczeństwa państwa. Niekontrolowane rozpowszechnianie kluczowych informacji gospodarczych czy politycznych może służyć nie tylko jako źródło wiedzy, ale również jako potencjalny cel lub narzędzie dla obcych wywiadów.

Pierwszą kwestią jest ryzyko nadużycia informacji. Dostęp do szczegółowych danych o problemach finansowych firm czy osób publicznych może stać się łatwym celem dla działań szpiegowskich lub manipulacji. W kontekście bezpieczeństwa państwa, takie informacje, jeśli są niepoprawnie zarządzane lub eksponowane, mogą być wykorzystywane przeciwko państwu przez obce mocarstwa.

Drugim aspektem jest wpływ na życie publiczne i prywatność obywateli. Nieumiejętne obchodzenie się z danymi jawnoźródłowymi może prowadzić do nieautoryzowanego ujawnienia informacji prywatnych, co z kolei może mieć negatywne konsekwencje zarówno dla jednostek, jak i dla funkcjonowania całego systemu państwowego.

Kolejną konsekwencją jest możliwość dezinformacji i manipulacji. W erze cyfrowej, gdzie informacje rozprzestrzeniają się błyskawicznie, niezweryfikowane źródła mogą być świadomie wykorzystywane do kreowania fałszywych narracji, co może prowadzić do destabilizacji społecznej, polaryzacji opinii publicznej oraz podważania zaufania do instytucji państwowych.

Ponadto, brak profesjonalnej analizy i weryfikacji może prowadzić do nieefektywnego wykorzystania zasobów, zarówno ludzkich, jak i finansowych, przez państwo. Zamiast koncentrować się na realnych zagrożeniach i szansach, służby mogą nieefektywnie wykorzystywać czas, monitorując zagrożenia, które zostały zmanipulowane lub sfabrykowane.

Zapewnienie bezpieczeństwa państwa wymaga profesjonalnego zarządzania i analizy informacji jawnoźródłowych. Rozpowszechnianie danych przez osoby nieświadome potencjalnych konsekwencji lub przez nieautoryzowane źródła może

przynieść korzyści przeciwnikom państwa. W związku z tym kluczowe jest wprowadzenie systemowych rozwiązań, które ograniczą dostęp do istotnych informacji oraz wspomogą rozwój kultury odpowiedzialności informacyjnej wśród obywateli i instytucji.

9. Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Każdy medal ma dwie strony, co doskonale ilustruje rozważanie tego tematu Z jednej strony, globalizacja i rozwój cyberprzestrzeni umożliwiają dostęp do szerokiego spektrum informacji, co może być wykorzystane do lepszego zrozumienia i reagowania na globalne zagrożenia oraz do budowania i utrzymywania sojuszy. Z drugiej strony, te same procesy mogą prowadzić do destabilizacji i zwiększenia zagrożeń, takich jak cyberataki czy dezinformacja, co wymaga skuteczniejszego i bardziej zintegrowanego podejścia do wywiadu jawnoźródłowego. W związku z tym, trudno jednoznacznie określić, czy wpływ tych zjawisk jest pozytywny czy negatywny, podkreślając skomplikowanie i wielowymiarowość współczesnych wyzwań.

Procesy globalizacji i integracji oraz rozwój cyberprzestrzeni są stale monitorowane przez zarówno naszych wrogów, jak i sojuszników z NATO, w celu identyfikacji stref wpływów oraz liderów, zarówno formalnych, jak i nieformalnych. Jednak pojawia się obawa, że państwo jako system nie analizuje i nie zarządza tymi procesami w sposób wystarczająco skuteczny, co może prowadzić do niekontrolowanych sytuacji.

Na przykład, obecne działania Ukrainy, polegające na blokowaniu polskich firm transportowych, wskazują na pewien rodzaj wrogości, który może eskalować do bardziej poważnych konfliktów. Takie sytuacje, gdzie przeszłość historyczna może wpływać na obecne napięcia, wymagają od państwa aktywnej kontroli i zarządzania, aby zapobiec eskalacji konfliktu. Istnieje obawa, że bez odpowiedniej analizy i zarządzania tymi procesami przez państwo, mogą one być wykorzystywane przez polityków lub nieformalnych liderów do własnych celów, potencjalnie kosztem bezpieczeństwa państwa.

Kluczowym wyzwaniem jest zarządzanie i analiza ogromnych ilości danych, które są generowane przez procesy globalizacji i działania w cyberprzestrzeni. Państwa

muszą rozwijać odpowiednie narzędzia analityczne i kompetencje, aby móc efektywnie wykorzystywać dostępne informacje jawnoźródłowe w celu identyfikacji szans i zagrożeń dla bezpieczeństwa narodowego.

Oprócz aspektów technologicznych, istotne są również kwestie zarządzania i koordynacji na poziomie międzynarodowym. Współpraca międzynarodowa i wymiana informacji między sojusznikami są kluczowe dla skutecznego adresowania globalnych wyzwań bezpieczeństwa.

10. Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?

Materiał jawnoźródłowy jest fundamentem, który umożliwia obserwację szerokiego spektrum wydarzeń nie tylko wewnątrz kraju, ale również u sojuszników, przeciwników oraz sąsiadów. Dzięki temu, odpowiednie komórki mogą w dynamicznej sytuacji geopolitycznej wyciągać wnioski i kierunki działań.

W kontekście obecnego kryzysu elit politycznych, materiał jawnoźródłowy powinien służyć jako narzędzie inspiracji i dostarczać raporty oraz rekomendacje politykom, aby ich działania były bardziej racjonalne i mniej emocjonalne. Skupienie się na rzeczywistych priorytetach, takich jak bezpieczeństwo i dobrostan społeczeństwa, jest kluczowe. Informacje jawnoźródłowe mogą przyczynić się do unikania zajmowania się kwestiami, które, mimo że ważne, nie są priorytetowe w kontekście bezpieczeństwa państwa

Ponadto, istotna jest rola think tanków i innych ośrodków analitycznych w analizowaniu pozyskanego materiału i formułowaniu rekomendacji dla decydentów. Bez takich instytucji i strategicznego podejścia do bezpieczeństwa, państwa demokratyczne mogą znaleźć się w sytuacji, gdzie będą jedynie "*płynąć z nurtem*", zamiast aktywnie kształtować rzeczywistość i wpływać na globalne procesy.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Uważam, że kooperacja w zakresie pozyskiwania i wykorzystywania informacji jawnoźródłowych jest niezbędna, ale powinna opierać się na zasadach równości, a nie zależności czy proszeniu się o dostęp do baz danych. W obliczu obecnych zagrożeń,

kluczowe jest budowanie sojuszy i aliansów, w ramach których moglibyśmy wspólnie analizować informacje. Często informacje, które mogą być bagatelizowane przez naszych sojuszników np. z Wielkiej Brytanii czy Stanów Zjednoczonych, w rzeczywistości okazują się nieocenione po dokładnej analizie przez naszych analityków, dzięki znajomości lokalnego kontekstu kulturowego i specyfiki. Dostęp do szerokiej gamy danych i analiz pozwala na lepsze zrozumienie globalnych trendów i zagrożeń, a także na bardziej skuteczne działanie w ramach wspólnych struktur, takich jak NATO.

Niestety, obecnie działamy w ramach sojuszy, które wydają się być iluzoryczne, w których brakuje zaufania między państwami członkowskimi, co osłabia skuteczność współpracy. Patrząc na globalny rozwój, Europa zdaje się znajdować na schyłkowym etapie. Mimo przekonania o dobrym stanie rzeczy, w rzeczywistości od kilkunastu lat nie udało się jej osiągnąć znaczącego postępu w porównaniu do dynamicznego rozwoju takich potęg jak Chiny, Indie czy rosnących aspiracji Rosji. To uwydatnia brak w Europie solidnych centrów analitycznych, które mogłyby efektywnie wykorzystywać wywiad jawnoźródłowy w ramach struktur europejskich, transatlantyckich czy nawet na poziomie lokalnym, Niezbędne jest więc budowanie silnych, opartych na wzajemnym zaufaniu relacji, które umożliwią efektywną wymianę informacji i analiz. Współpraca międzynarodowa w zakresie wywiadu jawnoźródłowego powinna również prowadzić do tworzenia specjalistycznych grup roboczych i centrów analitycznych, które będą wspierać decyzje strategiczne na różnych poziomach zarządzania bezpieczeństwem. Tylko poprzez zintegrowane działania i wykorzystanie zaawansowanej analizy informacji możemy zmierzyć się z wyzwaniami, które stawia przed nami współczesny świat.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: Prezes Zarządu Navi Risk
3. Stopień naukowy: magister
4. Tytuł: –
5. Staż pracy zawodowej: 21 lat

Załącznik 13 – Protokół XII wywiadu eksperckiego

przeprowadzonego 22 marca 2024 r. w Warszawie

Łukasz Wojewoda – Dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji. Oficer z wieloletnim doświadczeniem w obszarze cyberbezpieczeństwa, łączności i informatyki, a w szczególności w organizowaniu i prowadzeniu procesów obsługi incydentów bezpieczeństwa teleinformatycznego oraz testów bezpieczeństwa systemów teleinformatycznych. Aktywnie uczestniczył w projektowaniu i wdrażaniu systemów teleinformatycznych na potrzeby zapewnienia wymaganego poziomu cyberbezpieczeństwa jak również w organizowaniu i prowadzeniu *cyber threat intelligence* (CTI). Współtworzył i zarządzał Security Operation Center (SOC) w Służbie Kontrwywiadu Wojskowego. Reprezentując resort obrony narodowej współtworzył Krajowy System Cyberbezpieczeństwa. Posiada m.in. Certyfikat GIAC Information Security Professional (GISP) oraz Certyfikat Certified Ethical Hacker (CEH).

1. **Czy obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa?**

Uważam, że obecne wykorzystanie wywiadu jawnoźródłowego przyczynia się do zapewnienia bezpieczeństwa państwa. Kluczowym elementem, na który warto zwrócić uwagę, jest fakt, iż ludzie pozostawiają znaczące ilości informacji w różnych formach aktywności online, w tym na platformach społecznościowych. Te ostatnie, dzięki swojej powszechności i dostępności, stają się bogatym źródłem danych dla struktur państwowych odpowiedzialnych za bezpieczeństwo. Platformy społecznościowe gromadzą informacje o relacjach i interakcjach między użytkownikami, ich poglądach, spostrzeżeniach oraz różnych formach aktywności online. Dzięki temu, wywiad jawnoźródłowy może wykorzystywać te dane do budowania profilów osób, co jest szczególnie istotne w kontekście identyfikowania działań mogących wprowadzać zamieszanie lub niepokój społeczny. Pozwala na weryfikację, czy dana osoba lub grupa działa w sposób prawdziwy, sponsorowany, czy też dąży do manipulacji społecznej. Przykłady z przeszłości, jak te dotyczące referendum w Wielkiej Brytanii o wyjściu z Unii Europejskiej, pokazują, jak media społecznościowe mogą być wykorzystane do wpływania na opinię publiczną, często w sposób manipulacyjny. Dzięki OSINT-owi możliwe jest wczesne identyfikowanie

takich zagrożeń i odpowiednie reagowanie na nie, co ma kluczowe znaczenie dla bezpieczeństwa państwa.

Wywiad jawnoźródłowy bezwzględnie wpływa na bezpieczeństwo państwa, ale pojawia się pytanie o przyszłość i definicję otwartości źródeł takich jak Darknet czy *deep web*. Istnieją dwa główne podejścia do tej kwestii. Pierwsze uważa, że Darknet nie jest źródłem otwartym, ponieważ jego treści nie są łatwo dostępne dla przeciętnego obywatela. Z punktu widzenia bezpieczeństwa, drugie podejście sugeruje, że te zasoby można uznać za otwarte, gdyż dostęp do nich nie wymaga specjalistycznych, trudnych do wykonania zabiegów. Założenie, że Deep Dark Web stanowi również źródło informacji, prowadzi do konkluzji, że jest to istotny element w monitorowaniu aktywności potencjalnie związanych z przestępczością czy terroryzmem. Na forach dostępnych przez sieć Tor pojawiały się na przykład ogłoszenia dotyczące zleceń zabójstw ważnych osób w państwie. Tego typu informacje są kluczowe dla zabezpieczenia najważniejszych osób w kraju, a co za tym idzie bezpieczeństwa państwa.

2. Jak ocenia Pan przydatność informacji jawnoźródłowych w weryfikacji innych źródeł informacji w działaniach ofensywnych i defensywnych państwa?

Informacje jawnoźródłowe odgrywają istotną rolę w weryfikacji innych źródeł informacji w ramach działań ofensywnych i defensywnych państwa. Nie jest łatwo porównać jedno źródło z drugim, szczególnie kiedy mówimy o otwartych zasobach informacyjnych. Zawsze istotne jest sprawdzenie wiarygodności informacji jawnoźródłowych, gdyż niektóre z nich mogą być celowo zmanipulowane w celu destabilizacji państwa. Z drugiej strony, informacje potwierdzone klauzulą poufności stanowią zupełnie inny zasób wiedzy. Dane te są często pozyskiwane w sposób operacyjny, nadawane są im odpowiednie klauzule oraz istnieją określone procedury dotyczące sposobu ich pozyskania, wykorzystania i atrybucji. Kluczowe jest to, że informacje z obu źródeł – otwartych i klasyfikowanych – często okazują się być komplementarne. Połączenie tych dwóch rodzajów informacji pozwala na głębsze zrozumienie sytuacji, potwierdzając lub zaprzeczając różnym zjawiskom. Dzięki synergii między informacjami jawnoźródłowymi a danymi objętymi klauzulą poufności, możliwe jest budowanie pełniejszego obrazu dotyczącego adwersarzy, ich motywacji, planowanych działań, taktyk, technik oraz procedur. W takim kontekście nie można

jednoznacznie określić, które źródło jest lepsze, ponieważ oba wzajemnie się uzupełniają.

3. Jakie znaczenie ma dokonywanie analiz jawnoźródłowych w podejmowanych przez Pana decyzjach dotyczących bezpieczeństwa państwa?

W naszym departamencie utworzyliśmy specjalną komórkę analiz cyberbezpieczeństwa. Z racji samego faktu komplementarności, o której mówiłem wcześniej, naturalną konsekwencją jest wykorzystywanie informacji jawnoźródłowych. Po pierwsze jest to jeden z kanałów, którym zasilamy nasze kierownictwo w informacje. Po drugie pozyskane przez nas informacje jawnoźródłowe uzupełniają lub potwierdzają informacje pozyskane z innych, w tym niejawnych źródeł. Często w analizach bezpieczeństwa nie potrzebujemy dodatkowych źródeł danych. Informacje jawnoźródłowe, odpowiednio zweryfikowane i zebrane świadomie, wystarczają, aby potwierdzić lub zaprzeczyć danym hipotezom. Dlatego też osoby odpowiedzialne za przeprowadzanie tych analiz jawnoźródłowych muszą być dobrze przygotowane i przeszkolone, co pozwala na efektywne wykorzystanie materiałów pozyskanych z Internetu, dostępnych teoretycznie dla każdego. Starannie przygotowany materiał wynikowy staje się solidną bazą, na podstawie której można wskazywać kierunki działań, przewidywać pozytywne lub negatywne skutki poszczególnych działań, a także decydować o niewprowadzaniu niektórych rozwiązań z powodu zbyt wysokich ryzyk. Każdy element analizy jest ważny, ale kluczowym jest wiedza ekspercka osoby, która tę analizę wykorzystuje. Dlatego dbałość o kompetencje analityków jest nieodzowna w procesie zapewnienia bezpieczeństwa państwa.

W naszym departamencie przykładamy dużą wagę do podnoszenia kompetencji pracowników. Jeżeli mówimy stricte o komórkach analitycznych, istotne są specjalnie szkolenia dla osób zajmujących się pozyskiwaniem i wykorzystaniem informacji jawnoźródłowych. Rozwój umiejętności naszych pracowników jest dla nas priorytetem, choć oczywiście napotykamy na ograniczenia budżetowe typowe dla instytucji centralnych, które wpływają na możliwości organizacji szkoleń. Mimo tych ograniczeń, staramy się zapewnić naszym pracownikom odpowiednie szkolenia, uwzględniając ich chęci do nauki i rozwijania się w wybranej dziedzinie. To właśnie pasja do pracy, a nie tylko obowiązek, jest kluczowym kryterium, które bierzemy pod uwagę przy wyborze osób do konkretnych zadań. Pracowników zachęcamy do samokształcenia, oferując im możliwość podnoszenia własnych kompetencji w ramach czasu pracy. W ten sposób

tworzymy przestrzeń dla ich rozwoju, co z kolei przekłada się na ich efektywność i satysfakcję z pracy. Nie zawsze jest to związane z formalnymi kursami. Często wystarczy zapewnienie pracownikom czasu na samodzielne zdobywanie wiedzy, co jest równie cenione. To nie będzie postrzegane jako zaniedbywanie innych obowiązków, lecz jako sposób na sprawniejsze wykonywanie kolejnych zadań. Takie podejście pozwala pracownikom mieć poczucie, że są wspierani przez pracodawcę w budowaniu swojej wiedzy, co z kolei przekłada się na lepsze wykonanie ich zadań. Promowanie takiego podejścia w każdym miejscu pracy uważam za kluczowy element wspierający rozwój zarówno indywidualny, jak i całego zespołu.

Ekspert w dziedzinie bezpieczeństwa powinien uzupełniać swoją wiedzę. Obecnie, dzięki szerokiej dostępności informacji w otwartych źródłach, to zadanie nie stanowi dużego wyzwania. Istotne jest jednak zapewnienie odpowiednich warunków, które pozwolą pracownikowi na rozwijanie swoich umiejętności. Dając pracownikom możliwość samokształcenia, osiągamy szybsze i jakościowo lepsze efekty pracy, co przekłada się na podwójne korzyści: lepszego pracownika i lepszy materiał analityczny. Nierzadko okazuje się, że czas potrzebny na zrealizowanie całego zadania, wliczając w to czas na podnoszenie kwalifikacji, jest ostatecznie krótszy. Wynika to z faktu, że pracownik poświęca chwilę na rozwój swoich umiejętności, co z kolei przyspiesza końcowe wykonanie pracy. Chociaż inwestycja w samokształcenie wydaje się zwiększać całkowity czas pracy, w praktyce umożliwia ona znacznie szybsze i efektywniejsze wykonywanie zadań. Takie inwestowanie w rozwój pracownika przynosi korzyści wszystkim stronom. Warunkiem efektywności tego podejścia jest znalezienie odpowiedniego balansu pomiędzy jakością a nakazem. Ważne jest, aby pracownik rozumiał cel swojego rozwoju i widział w nim swoje wyzwanie, a nie tylko kolejne zadanie narzucone odgórnie. Działanie w ten sposób buduje w zespole kulturę lidera, który wskazuje kierunki, zamiast dowódcy, który wydaje rozkazy. Takie podejście nie tylko motywuje pracowników, ale również przyczynia się do ich lepszego rozwoju i efektywniejszego wykorzystania ich potencjału w pracy.

4. Jakie znane są Panu metody i środki stosowane w wywiadzie jawnoźródłowym dla zapewnienia bezpieczeństwa państwa?

Praca analityczna jest złożona. W naszym podejściu wykorzystujemy doświadczenia służb w zakresie prowadzenia wywiadu jawnoźródłowego. Proces ten można usystematyzować, zachowując odpowiednią hierarchię działań. Zaczynamy od

planowania. Na początku określamy nasze potrzeby informacyjne: jakie informacje są nam potrzebne, skąd zamierzamy je pozyskać i w jaki sposób. Planujemy również serię działań, które musimy przeprowadzić, aby te dane uzyskać. To obejmuje zdefiniowanie źródeł, takich jak media społecznościowe czy, w bardziej zaawansowanych przypadkach, *deep web* czy Dark Web. Następnie określamy sposób kontroli i monitorujemy efektywność tych działań, co jest równoznaczne z zaplanowaniem całego szeregu czynności, które chcemy przeprowadzić. Kolejnym etapem jest analiza zgromadzonych danych. Potrzebujemy takiej analizy, aby mieć pewność, że informacje, które udało nam się zgromadzić, są wystarczające do osiągnięcia postawionego celu. Jeśli naszym celem jest potwierdzenie lub zaprzeczenie jakiejś tezy, to właśnie w tym momencie sprawdzamy czy posiadamy wystarczająco dużo danych, czy może jeszcze potrzebujemy poszukać dodatkowych źródeł, jak na przykład *deep web* czy *dark web*. Po potwierdzeniu lub odrzuceniu naszych hipotez, stajemy przed pytaniem: czy te działania rzeczywiście przyczyniły się do zwiększenia bezpieczeństwa państwa? Czy osiągnęliśmy nasz główny, wysoko poziomowy cel?

Ostatnim krokiem jest weryfikacja efektywności całego procesu przez sprzężenie zwrotne. To właśnie ta kontrola, często postrzegana jako najwyższa forma zaufania, pozwala nam zmierzyć i ocenić skuteczność naszej pracy. Przygotowaliśmy plan, przeprowadziliśmy analizę, mamy wyniki i oceny. Na koniec kontrolujemy łańcuch działań, czy wszystko przebiegło zgodnie z naszymi założeniami i czy nie poświęciliśmy na coś za dużo czasu, aby móc jeszcze bardziej usprawnić cały proces w przyszłości. Wszystko to tworzy skonsolidowaną metodologię działania, którą stosujemy w naszym departamencie.

W zakresie metod i środków stosowanych w wywiadzie jawnoźródłowym naszym Departamencie nie ukierunkowujemy się na konkretne narzędzia czy techniki. Zamiast tego korzystamy z różnorodnych metod dostosowanych do bieżących potrzeb i celów. Przykładowo do badania zależności pomiędzy informacjami publikowanymi w mediach społecznościowych możemy skorzystać m.in. z programu Maltego. W zależności od sytuacji, mogą wystarczyć również podstawowe działania takie jak przeglądanie forów internetowych czy analiza wpisów w mediach społecznościowych. Jednakże, gdy mierzymy się z bardziej złożonymi zagadnieniami, jak na przykład weryfikacja informacji z potencjalnego wycieku danych czy działania grup przestępczych, konieczne jest użycie bardziej zaawansowanych technologii. W takich przypadkach korzystamy z platform typu Cyber Threat Intelligence, które umożliwiają

analizę dużych zbiorów danych pochodzących nie tylko z jawnych, ale i ukrytych źródeł, takich jak *dark web* czy *deep web*. Te zaawansowane narzędzia działają jako agregatory danych, co pozwala na szybką i efektywną analizę informacji, która może potwierdzić lub zaprzeczyć naszym hipotezom. Istotne jest, aby zrozumieć, że nasze metody muszą być elastyczne – nie zamykamy się na stałe w ramach jednego środka czy metody. Zamiast tego, staramy się adaptować i wykorzystywać różne opcje, w zależności od tego, jaki jest cel naszego działania i jakie zasoby są aktualnie dostępne.

5. Czy i w jaki sposób weryfikowane są informacje pozyskiwane drogą wywiadu jawnoźródłowego?

W naszym procesie weryfikacji informacji pozyskanych drogą wywiadu jawnoźródłowego, pierwszym i podstawowym krokiem jest zawsze identyfikacja źródła informacji. Nie istnieje złoty środek, który gwarantowałby stuprocentową pewność w *fact checkingu*. Naszym celem jest ustalenie, kto opublikował daną informację i ocena czy źródło to jest wiarygodne. Analizujemy również kontekst i możliwe powiązania z innymi faktami, aby zrozumieć podstawy, dla których informacja została opublikowana. Sprawdzamy również historię aktywności źródła, na przykład w mediach społecznościowych, aby zobaczyć, czy jego poprzednie posty były zgodne z rzeczywistością czy też stanowiły manipulację. Jeżeli informacja odnosi się do jakiegoś artykułu, sprawdzamy w Internecie, czy ten artykuł rzeczywiście istnieje. Sprawdzamy również, czy został napisany przez daną organizację lub firmę, czy też jest to tylko próba wywołania sensacji lub dezinformacji. Proces ten jest coraz bardziej skomplikowany ze względu na rosnącą ilość informacji i różnorodność ich źródeł. Często spotykamy się z próbami wprowadzenia zamieszania w przestrzeni medialnej, które mają na celu osiągnięcie korzyści przez konkretne osoby czy grupy. Weryfikacja takich informacji wymaga więc gruntownej analizy i niejednokrotnie użycia zaawansowanych narzędzi analitycznych. Pierwszym z kierunków rozwoju metod i środków technicznych w wywiadzie jawnoźródłowym będzie koncentracja na ocenie i weryfikacji informacji. Narzędzia analityczne muszą ewoluować, by skuteczniej identyfikować fałszywe dane i dezinformację. Mimo potencjału sztucznej inteligencji (AI) i automatyzacji, które usprawniają analizę danych, kluczowa pozostaje rola człowieka w ostatecznej ocenie informacji. Sztuczna inteligencja, choć niezwykle pomocna, może być ograniczona przez dane, na których została wytrenowana. Uważam,

że kluczową rolę w ocenie i wykorzystaniu informacji jawnoźródłowych będzie nadal odgrywać doświadczenie i umiejętności analityków. W przyszłości możemy spodziewać się dalszego rozwoju narzędzi AI i metod automatyzacji, które będą jeszcze skuteczniej wspierać procesy pozyskiwania i analizy danych jawnoźródłowych. Jednocześnie, wzrośnie zapotrzebowanie na wyszkolonych analityków zdolnych do pracy z tymi narzędziami, interpretacji ich wyników i podejmowania na ich podstawie trafnych decyzji.

Drugim z kierunków będzie dalszy rozwój i integracja zaawansowanych technologii, takich jak sztuczna inteligencja czy uczenie maszynowe oraz tworzenie narzędzia do głębokiej analizy danych, aby wspierać procesy identyfikacji i segregacji danych. To umożliwi szybsze i bardziej efektywne przetwarzanie ogromnych zbiorów danych.

W procesie weryfikacji informacji pozyskanych drogą wywiadu jawnoźródłowego, kluczowe jest ustalenie pochodzenia danych. Przede wszystkim należy zidentyfikować źródła informacji. Badamy, kto pierwszy ją opublikował i czy źródło to jest uznawane za wiarygodne. Nie istnieje uniwersalna metoda, która gwarantowałaby stuprocentową pewność co do prawdziwości informacji, dlatego skupiamy się na analizie dostępnych danych, aby jak najlepiej ocenić ich autentyczność. Przykładowo, jeżeli informacja pochodzi z mediów społecznościowych, sprawdzamy historię aktywności konta, które ją rozpowszechnia. Analizujemy, czy poprzednie posty były zgodne z rzeczywistością czy stanowiły próbę manipulacji. Jeśli informacja odnosi się do jakiegoś artykułu, staramy się zweryfikować, czy artykuł faktycznie istnieje, czy został opublikowany przez renomowaną organizację, a nie jest tylko tzw. "*clickbaitem*" mającym na celu wywołanie sensacji. Dodatkowo, rozpatrujemy kontekst, w jakim informacja się pojawiła oraz motywacje, które mogły doprowadzić do jej publikacji. W dzisiejszych czasach, gdy jakość dziennikarstwa może być różna, nawet informacje pochodzące z pozornie solidnych źródeł wymagają dokładnej weryfikacji. Często zdarza się, że osoby lub organizacje publikujące informacje mogą być motywowane chęcią osiągnięcia sukcesu medialnego, co może prowadzić do wprowadzania zamieszania. Proces weryfikacji jest coraz bardziej skomplikowany i wymaga skrupulatności oraz ciągłej czujności, aby efektywnie oddzielić informacje prawdziwe, od tych wprowadzających w błąd.

6. **Według Pana w jakich kierunkach będą się rozwijały metody i środki techniczne pozyskiwania i analizy jawnoźródłowej dla zapewnienia bezpieczeństwa państwa?**

Zaawansowane technologie takie jak *machine learning*, szeroko rozumiana jako sztuczna inteligencja, są kluczowymi narzędziami w wywiadzie jawnoźródłowym, które umożliwiają automatyzację różnorodnych procesów. Te technologie są dla nas niezbędne, zwłaszcza ze względu na ograniczone zasoby ludzkie. W przyszłości możemy spodziewać się jeszcze większej roli automatyzacji, która będzie obejmować nie tylko aktualne metody, ale i te, które będą tworzone. Algorytmy będą decydować o wielu aspektach bez konieczności ciągłej interwencji człowieka. Część działań mimo wszystko nadal będzie wymagać ludzkiej uwagi. Istnieje jednak wyzwanie związane z zaufaniem do sztucznej inteligencji. Na przykład, w sytuacji, gdy potrzebujemy zweryfikować dużą ilość danych, jak logi systemów czy inne zasoby tekstowe, algorytmy mogą analizować je szybciej i efektywniej niż ludzie. Jednak kluczowe jest, abyśmy mogli zaufać tym procesom, rozumiejąc jak są one skonstruowane i na jakich zasadach działają. Z drugiej strony, nie możemy ignorować potrzeby weryfikacji informacji generowanych przez AI. Algorytmy mogą sugerować rozwiązania na podstawie dostępnych danych, które nie zawsze są pełne lub dokładne. To wymaga od nas czujności i umiejętności krytycznego myślenia, aby nie przyjmować za pewnik wszystkiego, co sugeruje system. Rozwój metod i środków technicznych w wywiadzie jawnoźródłowym będzie niewątpliwie szedł w kierunku dalszej automatyzacji i integracji sztucznej inteligencji. Musimy jednak pamiętać o konieczności zachowania kontroli nad tymi procesami i odpowiedniego poziomu weryfikacji informacji, które są przez nie generowane. To podejście pozwoli na maksymalnie wykorzystanie potencjału nowych technologii przy jednoczesnej minimalizacji ryzyka błędów i nadużyć.

7. **Jakie ograniczenia dostrzega Pan w prowadzeniu rozpoznania z otwartych źródeł? W jakim stopniu wpływają one na zapewnienie bezpieczeństwa państwa?**

Otwarte źródła nie są pełnią wiedzy. Jak wspomniałem wcześniej, postrzegam je przez pryzmat komplementarności. Mogą służyć jako potwierdzenie pewnych informacji, jako ich rozszerzenie, lub nawet jako dobry punkt startowy do dalszego pogłębiania danego tematu. Nie należy oczekiwać, że w otwartych źródłach znajdziemy

informacje, które z punktu widzenia bezpieczeństwa państwa są opatrzone klauzulami. Jeśli takie informacje się tam pojawią, jest to zazwyczaj naruszenie przepisów prawa, co jest niedopuszczalne. Czasem w debatach pojawia się argument, że pewne informacje z materiałów analitycznych, które formalnie są opatrzone klauzulą, mogłyby być znalezione w Internecie. W naszych wewnętrznych dyskusjach często analizujemy, czy cała zawartość materiału jest dostępna publicznie. Na przykład, ostatni akapit lub dwa ostatnie akapity dodane do informacji, które są już dostępne w otwartych źródłach, mogą całkowicie zmienić postrzeganie danego problemu czy wyzwania.

Otwarte źródła nie są jedynym miejscem, z którego czerpiemy informacje niezbędne do budowania bezpieczeństwa państwa; stanowią one jednak bardzo ważny zasób. Często to właśnie od nich zaczyna się analiza, ze względu na to, że przestępcy czy grupy sponsorowane z oczywistych względów nie przestrzegają przepisów dotyczących klauzul.

Koszty, czyli brak zasobów na realizację jakiegoś zagadnienia, są jednym z aspektem naszej pracy. Chciałbym, aby brak środków nigdy nie był powodem, dla którego rezygnujemy z realizacji ważnych operacji, które są niezbędne dla sprawnego budowania bezpieczeństwa państwa. Koszt, w takich przypadkach, powinien być akceptowany jako niezbędny. Zawsze powinniśmy podejmować decyzje oparte na starannej analizie ryzyka. Przykładowo, jeśli musimy zakupić bazę danych od cyberprzestępców, aby mieć pełny obraz potencjalnych zagrożeń, powinniśmy rozważyć, czy korzyści z uzyskanych informacji przewyższają koszty i potencjalne ryzyko wspierania przestępczości. To jest kluczowe dla oceny, czy możemy sobie pozwolić na takie wydatki i czy są one uzasadnione z punktu widzenia bezpieczeństwa narodowego. Jednakże, musimy również rozważyć etyczne i prawne konsekwencje takich działań, jak płacenie okupu cyberprzestępcom. Taka decyzja może potencjalnie sponsorować dalszą działalność przestępczą. W ramach międzynarodowej inicjatywy Counter Ransomware, której Polska jest członkiem, staramy się zachęcać organizacje, które padły ofiarą ataku typu ransomware, aby nie płaciły okupów, aby nie finansować przestępców. Niezależnie od tego, każda sytuacja wymaga indywidualnej oceny – na przykład, w przypadku ataku na infrastrukturę krytyczną, jak szpital, decyzja o zapłacie może zaważyć na życiu i zdrowiu ludzi. Ostatecznie, wszystkie te decyzje powinny wynikać z przemyślanej analizy ryzyka i odpowiedzialności, zawsze mając na uwadze długoterminowe konsekwencje dla bezpieczeństwa państwa.

Decyzje dotyczące płacenia okupu w przypadku ataków ransomware nie są czarno-białe i zależą od wielu czynników. Przykładowo, rozważaliśmy sytuację ataku na szpital zapewniający podstawową lub interwencyjną opiekę zdrowotną, gdzie podczas skomplikowanej, wielogodzinnej operacji dochodzi do cyberataku. W takiej sytuacji, kiedy pacjent leży na stole operacyjnym i czas jest ograniczony, decyzja o zapłaceniu okupu – lub jej braku może decydować o życiu lub śmierci pacjenta. Z drugiej strony, koszt takiej decyzji nie zawsze jest łatwy do określenia. Początkowo może wydawać się, że wystarczy zapłacić określoną kwotę, ale w miarę pogłębiania analizy koszty mogą rosnąć. Każda decyzja o zapłacie okupu powinna być poprzedzona dokładną analizą ryzyka. Musimy ocenić, czy potencjalna strata informacji i jej wartość są warte wydatkowania środków finansowych. Ostatecznie, każda sytuacja wymaga indywidualnej oceny. W przypadkach krytycznych, gdzie na szali leży życie ludzi, decyzje muszą być szybkie i świadome, biorąc pod uwagę wszystkie możliwe konsekwencje.

8. Według Pana, jakie konsekwencje dla bezpieczeństwa państwa ma wykorzystanie informacji jawnoźródłowych bez profesjonalnej weryfikacji i analizy?

Jeśli zamierzamy wykorzystywać informacje jawnoźródłowe bez odpowiedniej weryfikacji, nie powinniśmy tego robić w kontekście bezpieczeństwa państwa! Konsekwencje takich działań mogą wahać się od banalnych do tragicznych. Na poziomie trywialnym, mogliśmy na przykład nie udzielić patronatu dla konferencji tylko dlatego, że ktoś nie sprawdził wszystkich faktów i zasugerował się jednym negatywnym postem mówiącym, że coś jest źle zorganizowane. Innym razem, nie uczestniczyliśmy w ważnym przedsięwzięciu, ponieważ ktoś nie zweryfikował historii wydarzenia i zdecydował na podstawie jednego negatywnego emaila, który przybył ze źródeł zewnętrznych. Podkreślam, że niezweryfikowane informacje jawnoźródłowe nie powinny być brane pod uwagę przy decyzjach dotyczących bezpieczeństwa państwa, ponieważ mogą być równie dobrze całkowicie nieprawdziwe. Zamiast poprawiać stan bezpieczeństwa, takie działanie może go znacząco pogorszyć**.**

9. Czy, według Pana, procesy globalizacji i integracji oraz rozwój cyberprzestrzeni wpływają na efektywność wywiadu jawnoźródłowego oraz potrzebę jego wykorzystania dla zapewnienia bezpieczeństwa w państwach demokratycznych?

Uważam, że te zagadnienia są trudne i złożone. Globalizacja powoduje z jednej strony łatwiejszy dostęp do różnorodnych źródeł informacji, co poszerza nasz horyzont i zakres wiedzy, co jest niewątpliwym atutem. Jednakże, ta sama otwartość sprawia, że zakres niepewności, w którym działamy, również się rozszerza, co czyni proces weryfikacji informacji jawnoźródłowych bardziej złożonym i wymagającym.

Rozwój technologii i integracja systemów informacyjnych pozwalają na szybszą wymianę danych, co z jednej strony ułatwia dostęp do informacji. Obecnie, gdy systemy są zintegrowane, informacje z różnych obszarów mogą być łatwiej dostępne i połączone. Na przykład, jeśli w jednym systemie mamy informacje od A do C, a w innym od D do G, integracja tych systemów może pozwolić na uzyskanie pełniejszego obrazu od A do G. Z drugiej strony, każdy z tych aspektów wymaga dogłębnej analizy i weryfikacji, aby uniknąć manipulacji i błędów. W miarę jak systemy stają się bardziej złożone i połączone, zadania te są bardziej skomplikowane, ale równocześnie narzędzia analityczne dostosowują się do nowych wyzwań, oferując ogromne możliwości kumulacji i analizy danych na dużą skalę. Globalizacja i rozwój cyberprzestrzeni zwiększają zarówno potencjał, jak i wyzwania związane z wywiadem jawnoźródłowym. Zwiększają one zakres dostępnej wiedzy, ale jednocześnie wymagają bardziej zaawansowanych metod weryfikacji, aby zapewnić wiarygodność i dokładność informacji niezbędnych dla bezpieczeństwa państwa.

Często korzystamy z informacji dostępnych w otwartych źródłach. Pierwszym krokiem w naszym procesie weryfikacyjnym jest sięgnięcie do tego, co jest dostępne publicznie – co mówią o danej organizacji, osobie czy stowarzyszeniu dostępne zasoby internetowe. To jest nasz punkt wyjścia. Następnie, dla zapewnienia komplementarności informacji, możemy sięgnąć po dodatkowe źródła, aby potwierdzić lub zaprzeczyć danym doniesieniom. Korzystamy z tego na dużą skalę, cross-instytucjonalnie, by zbadać historię organizacji czy osoby, badać motywy ich działań czy prawdziwość wypowiedzi. Globalizacja i integracja cyfrowych zasobów danych czynią tę komplementarność jeszcze bardziej istotną. Jeśli miałbym to ocenić, stwierdziłbym, że zasoby internetowe będą miały coraz większe znaczenie w naszym codziennym

dostępie do informacji. Internet stał się naszym głównym medium przekazu i wymiany informacji, zastępując tradycyjne metody jak książki telefoniczne czy encyklopedie. Na przykład, kiedyś, by znaleźć numer telefonu, używaliśmy książek telefonicznych, a wiedzę czerpaliśmy z encyklopedii. Dziś wszystko to znajdujemy w Internecie. Z tego względu, ważne jest, gdzie i jak dokonujemy weryfikacji informacji, aby nie ulec manipulacji. W miarę jak zasoby informacyjne rosną, tak samo rośnie potrzeba ich odpowiedniej weryfikacji, niekiedy nawet automatycznie, aby ochronić przeciętnego użytkownika przed dezinformacją.

10. Czy pozyskany materiał jawnoźródłowy przyczynia się do określenia kierunków szans i zagrożeń oraz podejmowanych działań na rzecz bezpieczeństwa w państwach demokratycznych?

Absolutnie, materiał jawnoźródłowy odgrywa kluczową rolę w określaniu kierunków szans i zagrożeń dla bezpieczeństwa w państwach demokratycznych. Dzięki informacjom pozyskanym z otwartych źródeł możemy szybko reagować na zmieniające się warunki globalne, analizując szeroki zakres danych, co pozwala na bieżącą ocenę potencjalnych ryzyk i możliwości. Informacje jawnoźródłowe, po odpowiedniej weryfikacji, są podstawą do podejmowania strategicznych decyzji w obszarze bezpieczeństwa. Poprzez integrację i komplementarność różnorodnych źródeł, jesteśmy w stanie zbudować kompleksowy obraz sytuacji, co jest niezbędne do skutecznego planowania i działania. Warto zaznaczyć, że bez szczegółowej analizy i potwierdzenia danych jawnoźródłowych, ryzykujemy podejmowanie decyzji opartych na niepełnych lub błędnych informacjach, co może prowadzić do nieadekwatnych działań z punktu widzenia bezpieczeństwa państwa.

11. Czy, według Pana, zasadna jest kooperacja ze strukturami sojuszniczymi pozyskującymi i wykorzystującymi informacje jawnoźródłowe na rzecz bezpieczeństwa państwa?

Oczywiście, kooperacja ze strukturami sojuszniczymi w zakresie wykorzystywania informacji jawnoźródłowych jest zasadna i przynosi wiele korzyści. Informacje, które możemy pozyskać z otwartych źródeł, w tym z *deep web* czy *dark web*, stanowią tylko część tego, co jest dostępne. Niektórzy porównują to do wierzchołka góry lodowej. Pamiętajmy, że zbadanie tych wszystkich zasobów przez jedną organizację czy osobę wiąże się z pewnym nakładem czasu i możliwości.

Dodatkowo niektóre zasoby informacyjne są ograniczone geograficznie. Sojusznicy mogą mieć dostęp do różnych informacji i mogą już posiadać informacje zweryfikowane, które są dla nas wartościowe. Nie ma więc sensu powtarzać już wykonanej pracy. Współpraca pozwala na oszczędność zasobów i wykorzystanie sprawdzonych danych, co zwiększa efektywność działania w zakresie bezpieczeństwa. Chyba nikt teraz nie powie, że posiada zasoby w nadmiarze – ani osobowe, ani finansowe. Na pewno nie my. Dlatego powinniśmy skorzystać z pracy już wykonanej przez innych. Integracja ze strukturami sojuszniczymi umożliwia również dostęp do analiz przeprowadzanych na szeroką skalę przez różne zespoły analityczne, co obejmuje informacje z różnych krajów i źródeł. To pozwala na bardziej kompleksowe i pewne badanie pozyskanych informacji.

Istotnym aspektem współpracy z sojusznikami w zakresie wykorzystywania analiz jawnoźródłowych jest weryfikacja czy wnioski wynikające z tych analiz są zgodne z naszymi potrzebami. Nawet jeśli analiza pochodzi od kraju sojuszniczego, musimy upewnić się, że pierwsze wyniki – wstępny *fact checking* – oraz dalsze interpretacje są spójne z naszymi oczekiwaniami. Wartościowanie i interpretacja tych informacji mogą się różnić w zależności od kraju i kontekstu, w jakim dane były analizowane. Dlatego zawsze powinniśmy sprawdzić, czy wnioski wyciągnięte przez sojuszników są odpowiednie dla naszych specyficznych potrzeb i czy warunki brzegowe są zgodne z naszymi oczekiwaniami, aby uniknąć nieporozumień czy błędnych decyzji. Ostatecznie, bezpieczeństwo państwa jest priorytetem, dlatego konieczne jest dokładne sprawdzenie wszystkich wniosków przed ich akceptacją, aby uniknąć potencjalnych nieporozumień czy błędów, które mogłyby zagrażać naszym interesom narodowym.

Metryczka:

1. Wykształcenie: wyższe
2. Stanowisko: Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji
3. Stopień naukowy: magister
4. Tytuł: pułkownik
5. Staż pracy zawodowej: 24 lat

Załącznik 14 – Zgody na publikację wywiadu

gen. bryg. Paweł Pruszyński — Warszawa, 10 stycznia 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 07.12.2023 r. w Warszawie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Paweł Pruszyński

Sylwester Sawicki — Warszawa, 22 stycznia 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 18.12.2023 r. w Warszawie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Sylwester Sawicki

Dariusz Trojszczak — Bielsko-Biała, 16 lutego 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 17.01.2024 r. w Bielsku-Białej autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Dariusz Trojszczak

Artur Szachno — Warszawa, 16 lutego 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 15.01.2024 r. w Warszawie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Artur Szachno

Stanisław Ignaciuk

Warszawa, 12 lutego 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 16.01.2024 r. w Warszawie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Stanisław Ignaciuk

Piotr Caliński

Warszawa, 26 lutego 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 26.01.2024 r. w Warszawie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Piotr Caliński

ppłk dr inż. Przemysław Kornacki

Łódź, 12 lutego 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 25.01.2024 r. w Łodzi, autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Przemysław Kornacki

dr hab. Mirosław Kwieciński

Kraków, 22 marca 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 07.02.2024 r. w Krakowie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Mirosław Kwieciński

Piotr Niemczyk Warszawa, 5 kwietnia 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 09.02.2024 r. w Warszawie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Piotr Niemczyk

gen. bryg. Mariusz Chmielewski Warszawa, 5 kwietnia 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 16.02.2024 r. w Warszawie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Bartosz Pastuszka Warszawa,28 marca 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 19.02.2024 r. w Warszawie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Bartosz Pastuszka

Łukasz Wojewoda Warszawa, 15 kwietnia 2024 r.

W związku z udzieleniem mgr Annie Nastule wywiadu w dniu 22.03.2024 r. w Warszawie autoryzuję go i wyrażam zgodę na jego publikację w jej pracy doktorskiej.

Łukasz Wojewoda

BIBLIOGRAFIA

Książki i rozdziały

1. Aleksandrowicz T.R., *Biały wywiad w walce z terroryzmem*, [w:] K. Liedel, P. Piasecka (red.), *Rola mediów w przeciwdziałaniu terroryzmowi*, Collegium Civitas Press, Warszawa 2009.
2. Aleksandrowicz T.R., *Podstawy walki informacyjnej*, Editions Spotkania, Warszawa 2016.
3. Aleksandrowicz T.R., *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*, Difin, Warszawa 2021.
4. Arystoteles, *Etyka nikomachejska*, Wydawnictwo Naukowe PWN, 2023.
5. Arystoteles, *Polityka*, t. 7, Wydawnictwo PWN, Warszawa 1964.
6. Babbie E., *Badania społeczne w praktyce*, Wydawnictwo Naukowe PWN, Warszawa 2005.
7. Baker R., *Prawdziwa głębia OSINT. Odkryj wartość danych Open Source Intelligence*, Helion, Gliwice 2024.
8. Bazzell M., *Open Source Intelligence Techniques. Resources for searchning and analyzing online information*, Sixth Edition, CreateSpace Independent Publishing Platform 2018.
9. Bernays E.I., *Propaganda*, Wydawnictwo Ig Publishing, New York 2004.
10. Brzeziński M., *Rodzaje bezpieczeństwa państwa*, [w:] S. Sulowski, M. Brzeziński (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa 2009.
11. Buzan B., Waever O., J. de Wilde, *Security: A New Framework for Analysis*, Boulder 1998.
12. Chałubińska-Jentkiewicz K., *Prawna ochrona treści cyfrowych*, Wolters Kluwer, Warszawa 2022.
13. Clark R.M., *Intelligence Analysis. A Target-Centric Approach*, Sage, 2013.
14. Czaputowicz J., *Bezpieczeństwo międzynarodowe. Współczesne koncepcje*, Wydawnictwo PWN, Warszawa 2012.
15. Czaputowicz J., *Kryteria bezpieczeństwa międzynarodowego – aspekty teoretyczne*, [w:] S. Dębski, B. Górska-Winter (red.), *Kryteria bezpieczeństwa międzynarodowego państwa*, PISM, Warszawa 2003.
16. Dobrowolski G., Filipkowski W., Kisiel-Dorohinicki M., Rakoczy W., *Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu*, [w:] L. Paprzycki, Z. Rau (red. nauk.), *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, Wyd. Wolters Kluwer, Warszawa 2009.
17. Dziubek I.T., *Media a współczesny terroryzm*, [w:] K. Jałoszyński, T. Aleksandrowicz, K. Wiciak (red.), *Bezpieczeństwo państwa a zagrożenie terroryzmem. Terroryzm na przełomie XX i XXI wieku*, t. 1. WSPol, Szczytno 2016.
18. Fehler W., *Podstawy bezpieczeństwa informacyjnego*, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, 2021.
19. Frankfort-Nachmias Ch., Nachmias D., *Metody badawcze w naukach społecznych*, Zysk i S-ka, Poznań 2001.
20. Fukuyama F., *Budowanie państwa. Władza i ład międzynarodowy w XXI wieku,* Rebis 2005.
21. Gibson H., Ramwell S., T. Day, *Analysis, Interpretation and Validation of Open Source Data*, [w:] B. Akhgar, P.S. Bayerl, F. Sampson (eds.), *Open Source Intelligence: Investigation From Strategy to Implementation*, Springer, 2023.
22. Gibson S.D., *Open source intelligence*, [w:] R. Dover, M.S. Goodman, C. Hillebrand (eds.), *The Routledge Companion to Intelligence Studies*, London 2014.

23. Gierszewski J., Pieczywok A., *Metodologiczne podstawy badania problemów bezpieczeństwa*, Wydawnictwo Difin, Warszawa 2020.
24. Gierszewski J., *Wokół uniwersum nauk o bezpieczeństwie*, Difin, Warszawa 2022.
25. Górski S., *O metodach badawczych w naukach społecznych*, [w:] A. Czupryński, B. Wiśniewski, J. Zboina (red.), *Nauki o bezpieczeństwie. Wybrane problemy badań*, Wydawnictwo CNBOP-PIB, 2017.
26. Graham D.G., *Etyczny haking. Praktyczne wprowadzenie do hakingu*, Helion, Gliwice 2021.
27. Hall W.M., Citrenbaum G., *Intelligence Analysis: How to Think in Complex Environments*, Praeger Security International, 2010.
28. Hariharan B., *Reverse Engineering*, [w:] M. Augier, D.J. Teece (eds.), *The Palgrave Encyclopedia of Strategic Management*, Palgrave Macmillan, London 2018, https://doi.org/10.1057/978-1-137-00772-8_249.
29. Hassan N.A., Hijazi R., *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, Apress, 2018.
30. Heuer R.J., Pherson R.H., *Structured Analytic Techniques for Intelligence Analysis*, CQ Press, Thousand Oaks, 2021.
31. Hickey M., Arcuri J., *Warsztat Hakera. Testy penetracyjne i inne techniki wykrywania podatności*, Helion, Gliwice 2022.
32. Hinsley F., *British Intelligence in the Second World War: Vol. 2*, HMSO, London 1981.
33. Jagusiak B., Żukowski P., *Zagrożenia procesów informacyjnych w systemie bezpieczeństwa państwa. Zagadnienia wybrane*, Wojskowa Akademia Techniczna, Warszawa 2019.
34. Janjeva A., Harris A., J. Byrne, *The Future of Open-Source Intelligence for UK National Security*, Royal United Services Institute for Defence and Security Studies, 2022.
35. Jardins E.A., *Open Source Intelligence*, [w:] M.M. Lowenthal, R.M. Clark, *The Five Disciplines of Intelligence Collection*, SAGE Publications, 2015.
36. Jelinek G., *Ogólna nauka o państwie*, Wydawnictwo F. Hoesicka, Warszawa 1921.
37. Jemioło T., Sienkiewicz P., *Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analiza zagrożeń i ryzyka*, t. 1, *Raport z badań*, AON, Warszawa 2004.
38. Johnson L.K., *The Oxford Handbook of National Security Intelligence*, Oxford Handbooks, 2010.
39. Johnston R., *Analytic Culture in the U.S. Intelligence Community. An Ethnographic Study*, Washington, DC, 2005.
40. Kamiński M.A., *Ewolucja wywiadu jako instytucji państwa*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2021.
41. Karciarz M., Dutko M., *Informacja w Internecie*, Wydawnictwo PWN, Warszawa 2010.
42. Kelsen H., *General Theory of Law and State,* The Lawbook Exchange, Ltd., Clark, New Jersey 2007.
43. Konieczny J. (red.), *Analiza informacji w służbach policyjnych i specjalnych*, Wydawnictwo C.H. Beck, Warszawa 2012.
44. Konieczny J., *Analiza informacji w dziedzinie bezpieczeństwa państwa*, ABW, Warszawa 2014.
45. Konieczny J., *Kryminalistyczny leksykon śledztwa*, Wydawnictwo Uniwersytetu Opolskiego, Opole 2020.
46. Kozera A., Żebrowski A., *Agentura wywiadu i kontrwywiadu II Rzeczypospolitej Polskiej uczestnikiem walki informacyjne. Wybrane aspekty*, [w:] H. Ćwięk, M. Siewier (red.), *Wywiad i kontrwywiad a bezpieczeństwo Polski odrodzonej po 1918 roku*, ABW i IPN, Warszawa 2019.
47. Kuźniar R., *Między polityką a strategią*, Wydawnictwo PWN, Warszawa 1994.
48. Larecki J.H., *Wielki leksykon tajnych służb świata*, wyd. 2, Oficyna Wydawnicza RYTM Sp. z o.o., 2017.
49. *Leksykon wiedzy wojskowej*, Ministerstwo Obrony Nardodowej, Warszawa 1979.
50. Liderman K., *Bezpieczeństwo informacyjne. Nowe wywzania*, PWN SA, Warszawa 2017.

51. Lieberthal K., *The U.S. Intelligence Community and Foreign Policy: Getting Analysis Right*, „John L. Thornton China Center Monograph Series" no. 2, „Foreign Policy Paper Series" no. 18, 2009.
52. Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011.
53. Long J., Gardner B., Brown J., *Google hacking for penetration testers*, vol. 2, Elsevier 2011.
54. Lowenthal M.M., Clark R.M., *The Five Disciplines of Intelligence Collection*, SAGE Publications, 2016.
55. Lowenthal M.M., *From Secrets to Policy* (4th ed.), CQ Press, Washington 2009.
56. Messier R., *Kali Linux. Testy bezpieczeństwa. Testy penetracyjne i etyczne hakowanie*, Helion, Gliwice 2019.
57. Michalik M., *Społeczne przesłanki, swoistość i funkcje etyki zawodowej*, [w:] A. Sarapata, *Etyka zawodowa*, Warszawa 1971.
58. Minkina M., *Sztuka wywiadu w państwie współczesnym*, Oficyna Wydawnicza RYTM, Warszawa 2022.
59. Moch N., *Bezpieczeństwo państwa*, [w:] J. Itrich-Drabarek, A. Misiuk, S. Mitkow, P. Bryczek-Wróbel (red.), *Encyklopedia bezpieczeństwa narodowego*, Wydział Bezpieczeństwa, Logistyki i Zarządzania. Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Dom Wydawniczy i Handlowy ELIPSA, Warszawa 2023.
60. Motylińska P., *Manipulacja informacją*, [w:] Vademecum Bezpieczeństwa informacyjnego, 2020, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/manipulacja-informacja/ [dostęp: 12.04.2024].
61. Nicoll J., *Task Definition*, [w:] J.H. Ratcliffe (red.), *Strategic Thinking in Criminal Intelligence*, The Federation Press, Sydney 2009.
62. Oleński J., *Ekonomika informacji. Metody*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2003.
63. Oleński J., *Ekonomika informacji. Podstawy*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2001.
64. Omand D., Miller C., J. Bartlett, *Towards the Discipline of Social Media Intelligence*, [w:] C. Hobbs, M. Moran, D. Salisbury (eds.), *Open Source Intelligence in the Twenty-First Century. New Security Challenges*, Palgrave Macmillan, London 2014.
65. Phytian M., *Beyond the Intelligence Cycle?*, [w:] M. Phytian (ed.), *Understanding the Intelligence Cycle*, Routledge, London-New York 2013.
66. Platon, *Państwo*, t. 1, Wydawnictwo PWN, Warszawa 1994.
67. Pogorzelski J.D., *Wykorzystanie otwartych źródeł informacji w pracy prokuratora,* [w:] W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Wydawnictwo C.H. Beck, Warszawa 2011.
68. Ramwell S., Day T., H. Gibson, *Use Case and Best Practise for LEAs*, [w:] B. Akghar, S. Bayerl, F. Sampson (eds.), *Open Source Intelligence Investigation. From Strategy to Implementation*, Springer, 2016.
69. Ratcliffe J., *Intelligence-Led Policing*, Routledge, London 2016.
70. Richards J., *The Art and Science of Intelligence Analysis*, Oxford University Press 2019.
71. Rojszczak M., *Ochrona prywatności w cyberprzestrzeni*, Wolters Kluwer, Warszawa 2019.
72. Sienkiewicz P., *Analiza systemowa. Podstawy i zastosowania*, Wydawnictwo BELLONA, Warszawa 1994.
73. Soule M.H., Ryan R.P., *Grey Literature. Technical Briefing*, [w:] *NATO Open-Source Intelligence Reader*, 2002.
74. Stańczyk J., *Formułowanie kategorii pojęciowych bezpieczeństwa*, Wydawnictwo FNCE, 2017.
75. Szafrański B., *Analiza danych w warunkach niepewności źródeł danych*, [w:] G. Szpor, K. Czaplicki (red.), *Internet. Analityka danych*, Wydawnictwo C.H. Beck, Warszawa 2019.

76. Sztumski J., *Wstęp do metod i technik badań społecznych*, „Śląsk" Sp. z o.o. Wydawnictwo Naukowe, Katowice 2010.
77. Tatarkiewicz W., *Historia filozofii*, t. 2, Wydawnictwo Naukowe PWN, Warszawa 1993.
78. Velu V.K., *Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite*, Helion, Gliwice 2023.
79. Volkoff V., *Psychosocjotechnika, dezinformacja, oręż wojny*, Wydawnictwo Antyk, Komorów 1999.
80. Weber M., *Racjonalność, władza, odczarowanie*, Wydawnictwo Poznańskie, Poznań 2011.
81. Wells D., Gibson H., *OSINT from a UK Perspective: Considerations from the Law Enforcement and Military Domains*, [w:] Proceedings Estonian Academy of Security Sciences, 16: *From Research to Security Union*, Estonian Academy of Security Sciences, 2017.
82. Williams P.D., *Security Studies: An Introduction*, [w:] P.D. Williams (ed.), *Security Studies: An Introduction*, London–New York 2008.
83. Wojciulik A., *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków*, [w:] W. Filipkowski, W. Mądrzejewski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, C.H. Beck, Warszawa 2012.
84. Wojtaszczyk K.A., *Bezpieczeństwo państwa – konceptualizacja pojęć*, [w:] A. Materska-Sosnowska, K.A. Wojtaszczyk (red.), *Bezpieczeństwo państwa. Wybrane problemy*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2009.
85. Wróblewski R., *Podstawowe pojęcia z dziedziny polityki bezpieczeństwa, strategii i sztuki wojennej*, AON, Warszawa 1993.
86. Wrzosek M., *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, NASK Państwowy Instytut Badawczy, Warszawa 2019.
87. Żebrowski A., Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000.
88. Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego*, Warszawa 2007.
89. Ziembiński Z., *Podstawy nauki o moralności*, Uniwersytet im. Adama Mickiewicza, Poznań 1981.
90. Ziembiński Z., Wronkowska S., *Państwo i inne struktury społeczne*, [w:] M. Zmierczak, S. Wronkowska (red.), *Kompendium wiedzy o społeczeństwie, państwie i prawie*, PWN, Warszawa-Poznań 1993.

Artykuły w czasopismach

1. Bast H., Buchhold B., E. Haussmann, *Semantic Search on Text and Knowledge Bases*, „Foundations and Trends in Information Retrieval" 2016, vol. 10, no. 2-3.
2. Benito-Osorio D., Peris-Ortiz M., Armengot C.R., Colino A.C., *Web 5.0: the future of emotional competences in higher education*, „Global Business Perspectives" 2013, vol. 1, no. 3, https://doi.org/10.1007/s40196-013-0016-5 [dostęp: 1.02.2021].
3. Bergman M.K., *The Deep Web: Surfacing Hidden Value*, „Journal of Electronic Publishing" 2001, vol. 7, no. 1.
4. Berners-Lee T., Cailliau R., R. Luotonen, A. Nielsen, A. Secret, *The World-Wide Web*, „Communications of the ACM" 1994, vol. 37, no. 8, http://dx.doi.org/10.1145/179606.179671 [dostęp: 3.03.2021].
5. Calkins L.M., *Patrolling the Ether: US-UK Open-Source Intelligence Cooperation and the BBC's Emergence as an Intelligence Agency*, 1939–1948, „Intelligence and National Security" 2011, vol. 26, no. 1.
6. Childress E., Jul E., *Going Gray: Gray Literature and Metadata*, „Journal of Internet Cataloging" 2003, vol. 6, no. 3.
7. Cuijpers C., *Legal aspects of open source intelligence – Results of the VIRTUOSO project*, „Computer Law & Security Review" 2013, vol. 29, no. 6, https://doi.org/10.1016/j.clsr.2013.09.002 [dostęp: 20.11.2023].

8. Davis P., *Analyze This: OPSEC is Key in the War on Terrorism*, „Journal of Counterterrorism & Homeland Security International" 2002, vol. 8, no. 2.
9. Devine J., Egger-Sider F., *Beyond Google: The Invisible Web in the Academic Library*, „The Journal of Academic Librarianship" 2004, vol. 30.
10. Elak L., Śliwa Z., *Hybridity – a 'new' method to accomplish dominance,* „Security and Defence Quarterly" 2019, vol. 23, no. 1.
11. Ferreira W.D., C.B.R. Ferreira, G. da Cruz Júnior, F. Soares, *A review of digital image forensics,* „Computers & Electrical Engineering" 2020, vol. 85, 106685, https://doi.org/10.1016/j.compeleceng.2020.106685 [dostęp: 10.06.2024].
12. Fleszer D., *Wokół problematyki bezpieczeństwa informacji*, „Roczniki Administracji i Prawa" 2018, nr 1.
13. Gontar B., Papińska-Kacperek J., *Semantyczne wyszukiwarki internetowe, (Semantic Search Engines)*, „Acta Universitatis Lodziensis. Folia Oeconomica" 261, 2011.
14. Goodchild M.F., *Citizens as Voluntary Sensors*: Spatial *Data Infrastructure in the World of Web 2.0,* „International Journal of Spatial Data Infrastructures Research" 2007, vol. 2, no. 1.
15. Hendrickson N., *Critical Thinking in Intelligence Analysis*, „International Journal of Intelligence and Counterintelligence" 2010, vol. 21, no. 4.
16. Herman M., *Ethics in Intelligence after September 2001*, „Intelligence and National Security" 2004, vol. 19, no. 2.
17. Heuer R.J. Jr., *Limits of Intelligence Analysis*, „Orbis" 2005, vol. 49, no. 1.
18. Hoc S., *Przestępstwo dezinformacji wywiadowczej w kodeksie karnym*, „Przegląd Sądowy" 2000, nr 5.
19. Ivan A.L., Iov C.A., R.C. Lutai, M.N. Grad, *Social Media Intelligence: Opportunities and Limitations*, „CES Working Papers" 2013, vol. 7, no. 2A.
20. Konieczny J., *Bezpieczeństwo państwa a bezpieczeństwo biznesu. Studium metodologiczne*, „Bezpieczeństwo: teoria i praktyka" 2015, nr 4.
21. Lapid E., *OSINT: A Major Source of Up-to-Date Information*, „National Security and the Future" 2016, vol. 17, nr 1–2.
22. Liaropoulos A.N., *The Challenge of Social Media for the Intelligence Community*, „Journal of Mediterranean and Balkan Intelligence" 2013, nr 1(1).
23. Lowenthal M.M., *OSINT the State of Art, The Artless State*, „Studies in Intelligence" 2001, vol. 45, no. 3.
24. Maslow A., *A Theory of Human Motivation*, „Psychological Review" 1943, vol. 50.
25. Matela K., *Wybrane aspekty systemów wywiadu, obserwacji i rozpoznania (ISR),* „Wiedza Obronna" 2021, vol. 276, no. 3.
26. Mider D., *Sztuka wyszukiwania w Internecie – autorski przegląd wybranych technik i narzędzi*, „Studia Politologiczne" 2019, nr 54.
27. Mukhopadhyay A., Venkatagiri S., K. Luther, *OSINT Research Studios: A Flexible Crowdsourcing Framework to Scale Up Open Source Intelligence Investigations*, „Proc. ACM Hum.-Comput. Interact." 2024, vol. 8, issue CSCW1, art. 105, https://doi.org/10.1145/3637382 [dostęp: 5.07.2024].
28. Niemczyk P., *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu",* „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5).
29. Ogiński M., *Dezinformacja w dobie cyfryzacji*, „Zeszyty Naukowe Zbliżenie Cywilizacyjne" 2023, vol. 19, no. 1.
30. Ohm P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (August 13, 2009), „UCLA Law Review" 2010, vol. 57, https://ssrn.com/abstract=1450006 [dostęp: 20.08.2024].
31. Pastor-Galindo J., Nespoli P., F. Gómez Mármol, G. Martínez Pérez, *The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends*, „IEEE Access" 2020, vol. 8.
32. Pozen D.E., *The Mosaic Theory, National Security, and the Freedom of Information Act*, „Yale Law Journal" 2005, vol. 115.

33. Schaurer F., Störger J., *The Evolution of Open Source Intelligence (OSINT)*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2012, vol. 19, no. 3.
34. Sherman C., Price G., *The Invisible Web: Uncovering Sources Search Engines Can't See*, „Library Trends" 2003, vol. 52, no. 2.
35. Svendsen A.D.M., *Introducing RESINT: A Missing and Undervalued "INT" in All-Source Intelligence Efforts*, „International Journal of Intelligence and CounterIntelligence" 2013, vol. 26, nr 4.
36. Tarakeswar K., Kavitha D., *Search engines: a study*, „Journal of Computer Applications (JCA)" 2011, vol. 4, no. 1.
37. Tversky A., Kahneman D., *Judgment under Uncertainty: Heuristics and Biases*, „Science. New Series" 1975, vol. 185, no. 4157.
38. Wason P.C., *Reasoning about a rule*, „Quarterly Journal of Experimental Psychology" 1968, vol. 20, no. 3.
39. Westin A.F., *Privacy and Freedom*, „Washington and Lee Law Review" 1968, vol. 25, no. 1.
40. Wolfe H.B., *Computer forensics*, „Computers & Security" 2003, vol. 22, no. 1, https://doi.org/10.1016/S0167-4048(03)00105-6 [dostęp: 10.06.2024].
41. Zaskórski P., Zaskórski W., *Big-Data systems in improving modern organizations*, „Nowoczesne Systemy Zarządzania" 2017, z. 12, nr 2.
42. Zięba R., *O tożsamości nauk o bezpieczeństwie*, „Zeszyty Naukowe AON" 2012, nr 1(86).
43. Zięba R., *Pojęcie i istota bezpieczeństwa państwa w stosunkach międzynarodowych*, „Sprawy Międzynarodowe" 1989, nr 10.

Inne źródła

Akty prawne (Polska)

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. nr 78, poz. 483 ze zm.).
2. Ustawa o ochronie prywatności z 1981 r., Protection of Privacy Law, 5741-1981, Official Gazette of Israel, No. 990, 23.12.1981.
3. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2020 r. poz. 2176).
4. Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 r. nr 62, poz. 558).
5. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2002 r. nr 74, poz. 676).
6. Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. z 2002 r. nr 113, poz. 985).
7. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2002 r. nr 156, poz. 1301).
8. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r. nr 64, poz. 565).

Akty prawne (międzynarodowe)

1. *Data Protection Act 2018*, c. 12, Wielka Brytania, uchwalony 23 maja 2018 r., https://www.legislation.gov.uk/ukpga/2018/12/contents [dostęp: 5.12.2024].
2. Decyzja Komisji Europejskiej z dnia 31 stycznia 2011 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniego poziomu ochrony danych osobowych w Państwie Izrael w odniesieniu do zautomatyzowanego przetwarzania danych osobowych, C(2011) 332 (Dz.Urz. UE L 27 z 1.2.2011, s. 39–42).

3. *Gramm-Leach-Bliley Act (GLBA)*, Public Law 106-102, uchwalona przez Kongres Stanów Zjednoczonych, 12 listopada 1999 r.
4. *Health Insurance Portability and Accountability Act (HIPAA)*, Public Law 104-191, uchwalona przez Kongres Stanów Zjednoczonych, 21 sierpnia 1996 r.
5. *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3638 (2004).
6. *National Defense Authorization Act for Fiscal Year 2006*, Pub. L. No. 109-163, 119 Stat. 3136 (2006).
7. *Regulation of Investigatory Powers Act 2000*, Wielka Brytania.
8. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE z 2016 r., L 119).
9. Rzymski Statut Międzynarodowego Trybunału Karnego sporządzony w Rzymie dnia 17 lipca 1998 r. (Dz.U. z 2003 r. nr 78, poz. 708).

Dokumenty

1. ACPO, *Good Practice Guide for Digital Evidence*, 2012.
2. ACPO, *Online Research and Investigation Guidance*, Version 1.2, 2013.
3. *ATP 2-22.9: Open-Source Intelligence*, DC: Headquarters, Department of the Army, Waszyngton, 2012.
4. Bar S., *7 October – The Unlearning of the Lessons of 1973*, National Institute for Public Policy, Information Series, no. 589, June 11, 2024.
5. *Berkeley Protocol on Digital Open-Source Investigations*, HR/PUB/20/2, Nowy Jork–Genewa 2022.
6. Department of Defense, *Department of Defense Instruction 3115.12, Open Source Intelligence (OSINT)*, August 24, 2010.
7. Europol, *Strategia zarządzania informacjami. Wsparcie wdrożenia rozporządzenia Europolu i Strategii Europolu 2020+*, Europol, Haga 2018.
8. *IC OSINT Strategy 2024-2026*, dokument jawny, Biuro Dyrektora Wywiadu Narodowego, 2024.
9. International Telecommunication Union, *Next Generation Networks – Framework and functional architecture models – Overview of the Internet of things*, ITU-T Y.2060, 06/2012.
10. *Israel International Cyber Strategy: International Engagement for Global Resilience*, National Cyber Directorate, Prime Minister's Office, 2021.
11. *Israel National Cyber Security Strategy in Brief*, National Cyber Directorate, Prime Minister's Office, 2017.
12. Ministerstwo Obrony Narodowej Wielkiej Brytanii, *UK Defence Doctrine (JDP 0-01)*, 2011.
13. Ministerstwo Spraw Wewnętrznych Wielkiej Brytanii, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, 2011, CP 8134.
14. National Police Chiefs' Council, 2015, *NPCC Guidance On Open Source Investigations*.
15. National Police Chiefs' Council, 2019, *Internet Intelligence & Investigations Strategy*.
16. National Police Chiefs' Council, 2023, *NPCC Internet Intelligence & Investigations Guidance On Covert Profiles*.
17. *NATO Open-Source Intelligence Handbook*, Norfolk 2001.
18. NATO Standardization Office, *AAP-6: Słownik terminów i definicji NATO*, NATO, 2017, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf [dostęp: 5.02.2024].
19. NATO, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, AJP-2, wyd. A, wersja 2, NATO Standardization Office, 2016.
20. NATO, *Intelligence Exploitation of the Internet*, Brussels, October 2002.
21. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, February 5, 2024.

22. *Operations Security Guide*, RCC dokument 600-11, kwiecień 2011, Secretariat, Range Commanders Council, U.S. Army White Sands Missile Range, New Mexico, USA.
23. OSINT Foundation, *OSINT Collection Methodologies*, Document Number: 20231120-01, 2023.
24. UK College of Policing, *UK College of Policing Intelligence Report Breakdown*, 2015.
25. Unver A., *Digital open-source intelligence and international security: a primer*, EDAM Research Reports, Cyber Governance and Digital Democracy, 2018.

Źródła internetowe

1. A Free and Open Source Geographic Information System, https://www.qgis.org [dostęp: 5.06.2024].
2. Acunetix, https://www.acunetix.com/ [dostęp: 5.03.2024].
3. African Network Information Centre, https://www.afrinic.net [dostęp: 10.03.2024].
4. Akademia Wywiadu, *Podstawy inżynierii wstecznej w cyberbezpieczeństwie*, 2023, https://akademiawywiadu.pl/podstawy-inzynierii-wstecznej-w-cyberbezpieczenstwie/ [dostęp: 12.07.2024].
5. *Al-Qaeda Targeting US Embassy, Jerusalem Convention Center*, The Times of Israel, 2014, https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/, [dostęp: 25.04.2024].
6. American Registry for Internet Numbers, https://www.arin.net [dostęp: 10.03.2024].
7. Asia Pacific Network Information Centre, https://www.apnic.net [dostęp: 10.03.2024].
8. Baidu, https://www.baidu.com/ [dostęp: 2.01.2023].
9. Bellingcat – brytyjska witryna dziennikarstwa śledczego, https://www.bellingcat.com/ [dostęp: 10.06.2024].
10. Bellingcat Investigation Team, *Hospitals Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine*, 2022, https://www.bellingcat.com/news/2022/03/17/hospitals-bombed-and-apartments-destroyed-mapping-incidents-of-civilian-harm-in-ukraine/ [dostęp: 22.08.2024].
11. Bellingcat, https://www.bellingcat.com/ [dostęp: 8.10.2023].
12. Bing, https://www.bing.com/ [dostęp: 2.01.2023].
13. Blackdot Solutions – ODIN: Open Source Intelligence Discovery & Investigation, https://blackdotsolutions.com/events/odin/ [dostęp: 5.06.2023].
14. Blackdot Solutions, *Leveraging OSINT for Public-Private Partnerships*, https://blackdotsolutions.com/blog/leveraging-osint-for-public-private-partnerships/ [dostęp: 20.01.2024].
15. *BodyNet Sensor System for Wearable Electronics*, Stanford University, https://techfinder.stanford.edu/technology/bodynet-sensor-system-wearable-electronics [dostęp: 14.05.2024].
16. Brytyjska społeczność OSINT, https://www.osint.uk/ [dostęp: 5.06.2024].
17. BuiltWith – Technology Lookup & Market Analysis, https://www.builtwith.com [dostęp: 4.03.2024].
18. Central Intelligence Agency, *Factbook on Intelligence*, https://irp.fas.org/cia/product/facttell/index.html [dostęp: 1.02.2021].
19. CENTRIC, *OSINT Hub*, https://centric-research.co.uk/projects/osint-hub [dostęp: 28.12.2023].
20. Cerre M., Sagalyn D., *Private companies track the war in Ukraine in real time*, PBS Newshour, 2022, https://www.pbs.org/newshour/show/private-companies-track-the-war-in-ukraine-in-real-time [dostęp: 22.08.2024].
21. Cisek S., *Szara literatura jako źródło informacji biznesowej. Zarys problematyki*, „EBIB Elektroniczny Biuletyn Informacyjny Bibliotekarzy" 2002, nr 11 (40), http://www.ebib.pl/2002/40/cisek.php [dostęp: 4.03.2023].
22. Commission on the Roles and Capabilities of the U.S. Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, William J. Clinton

Presidential Library & Museum, 1996, https://clinton.presidentiallibraries.us/items/show/36064 [dostęp: 12.03.2024].
23. Common Crawl , https://commoncrawl.org/ [dostęp: 2.07.2024].
24. Crowdsourced Street-Level Imagery, https://www.mapillary.com [dostęp: 5.06.2024].
25. Cyotek WebCopy, https://www.cyotek.com/cyotek-webcopy [dostęp: 4.03.2024].
26. DCMA, *OPSEC history: from ancient origins to modern challenges*, 2023, https://www.dcma.mil/News/Article-View/Article/3258274/opsec-history-from-ancient-origins-to-modern-challenges/ [dostęp: 5.02.2024].
27. Defense Advanced Research Projects Agency, *Darpa Network Challenge Project Report*, 2010, https://www.eecs.harvard.edu/cs286r/courses/fall10/papers/ProjectReport.pdf [dostęp: 3.07.2024].
28. Department of the Army, *Complementary Intelligence Capabilities, Army Doctrine Publication (ADP 2-0) for Army Intelligence Activities*, rozdz. 4, 2018, https://irp.fas.org/doddir/army/adp2_0.pdf [dostęp: 25.06.2023].
29. DISARM Red Framework, https://www.disarm.foundation/framework [dostęp: 10.07.2024].
30. DNSdumpster, https://dnsdumpster.com/ [dostęp: 10.03.2024].
31. DuckDuckGo, https://duckduckgo.com/ [dostęp: 2.01.2023].
32. Exploit Database – Google Hacking Database, https://www.exploit-db.com/google-hacking-database [dostęp: 5.03.2024].
33. FAS Intelligence Resource Program, *Operations Security Intelligence Threat Handbook*, https://irp.fas.org/nsa/ioss/threat96/part01.htm [dostęp: 5.02.2024].
34. Federation of American Scientists, Intelligence Resource Program, *Measurement and Signature Intelligence (MASINT)*, https://irp.fas.org/program/masint.htm [dostęp: 25.06.2023].
35. Flickr , https://www.flickr.com [dostęp: 5.06.2024].
36. FOCA, https://foca.softonic.pl/ [dostęp: 12.07.2024].
37. Forensic Architecture, https://forensic-architecture.org/ [dostęp: 10.06.2024].
38. Freenet Project , https://freenetproject.org/ [dostęp: 20.08.2024].
39. Gibson S.D., *Open-Source Intelligence (OSINT): A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, Appendices: Interview EUROPOL 4, 2007, https://dspace.lib.cranfield.ac.uk/handle/1826/6524 [dostęp: 22.01.2023].
40. GNU Wget – Free Software Foundation, https://www.gnu.org/software/wget/ [dostęp: 5.03.2024].
41. Google Earth, https://www.google.com/earth [dostęp: 5.06.2024].
42. Google Maps , https://www.google.com/maps [dostęp: 5.06.2024].
43. Gretel K., *The Israel-Hamas war highlights the power (and the limits) of open-source reporting*, 2023, https://reutersinstitute.politics.ox.ac.uk/news/israel-gaza-war-highlights-power-and-limits-open-source-reporting [dostęp: 22.08.2024].
44. Hadarem Y., *The IDF's Not-So-Secret Unit*, 2015, https://www.israelhayom.co.il/article/306247 [dostęp: 20.04.2024].
45. Hasło „państwo", [w:] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/szukaj/państwo.html [dostęp: 26.05.2023].
46. Hasło „prasa", [w:] Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/prasa;3961726.html [dostęp: 4.03.2023].
47. Her Majesty's Government, *BBC Monitoring: Evidence to the Defence and Foreign Affairs Committees*, 2016, https://committees.parliament.uk/writtenevidence/74950/pdf/ [dostęp: 8.10.2023].
48. HTTrack Website Copier, https://www.httrack.com [dostęp: 5.03.2024].
49. Hugill J., *Introducing INDEX – A Cross-Government Digital Information and Data Exchange*, PUBLIC, 2021, https://www.public.io/introducing-index-a-cross-government-digital-information-and-data-exchange/ [dostęp: 22.11.2023].
50. Human Rights Watch Digital Investigations Lab, https://www.hrw.org/topic/technology-and-rights/digital-investigations-lab [dostęp: 10.06.2024].
51. I2P – The Invisible Internet Project, https://geti2p.net/ [dostęp: 20.08.2024].

52. ICANN, https://www.icann.org [dostęp: 10.03.2024].
53. *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en [dostęp: 6.07.2024].
54. Institut des Hautes Études de Défense Nationale (IHEDN), *Aubaines et limites de l'OSINT: le nouveau nerf de la guerre*, https://ihedn.fr/en/2023/06/08/aubaines-et-limites-de-losint-le-nouveau-nerf-de-la-guerre/ [dostęp: 2.01.2023].
55. *Israel Downgrades Its Open-source Military Intelligence Unit*, Haaretz, 2016, https://www.haaretz.com/israel-news/2016-10-30/ty-article/israel-downgrades-its-open-source-military-intelligence-unit/0000017f-e351-d75c-a7ff-ffddb17b0000 [dostęp: 12.03.2024].
56. Israel Internet Crime Center, https://www.iicc.org.il/?module=articles&item_id=4&article_id=188&art_category_id=3&q=%D7%90%D7%95%D7%A1%D7%99%D7%A0%D7%98 [dostęp: 12.08.2024].
57. *Kodeks dobrych praktyk. Wspólnie przeciw dezinformacji*, 2023, https://www.nask.pl/pl/wlaczweryfikacje/kodeks-dobrych-praktyk/4991,Kodeks-Dobrych-Praktyk.html [dostęp: 11.07.2024].
58. Kodeks etyczny Infobrokerów stworzony przez The Association of Independent Information Professionals, https://aiip.org/About/Professional-Standards [dostęp: 20.07.2023].
59. Kodeks etyczny organizacji „Strategic and Competitive Intelligence Professionals", https://www.scip.org/page/Ethical-Intelligence [dostęp: 20.07.2023].
60. Latin American and Caribbean Internet Addresses Registry, https://www.lacnic.net [dostęp: 10.03.2024].
61. Maltego, https://www.maltego.com/ [dostęp: 12.07.2024].
62. Markoff J., *Entrepreneurs See a Web Guided by Common Sense*, „The New York Times" 2006, https://www.nytimes.com/2006/11/12/business/12web.html [dostęp: 1.02.2021].
63. *Military Intelligence Directorate*, Israel Defense Forces, https://www.idf.il/en/mini-sites/directorates/military-intelligence-directorate/military-intelligence-directorate/ [dostęp: 22.04.2024].
64. Millet E., *Deploying OSINT in armed con ict settings: law, ethics, and the need for a new theory of harm*, 2023, https://blogs.icrc.org/law-and-policy/2023/12/05/deploying-osint-in-armed-conflict-settings-law-ethics-theory-of-harm/ [dostęp: 24.08.2024].
65. Minas H., *Can the Open-Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the Twenty-First Century*, RIEAS, 2010, https://rieas.gr/publications/1119-harris-minas-can-the-open-source-intelligence-emerge-as-an-indispensable-discipline-for-the-intelligence-community-in-the-21st-century-rieas-research-paper-no-139-january-2010 [dostęp: 27.03.2025].
66. *Mossad Trains European Intel Agents in Open-Source Spy Tools & Analysis*, Intelligence Online, 2022, https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra [dostęp: 30.03.2024].
67. Mossad, https://www.mossad.gov.il/ [dostęp: 8.07.2024].
68. NASA Earthdata, „GeoTIFF", 2023, https://www.earthdata.nasa.gov/esdis/esco/standards-and-practices/geotiff [dostęp: 5.06.2024].
69. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, U.S. Government Printing Office, Washington, D.C. 2004, https://www.9-11commission.gov/report/911Report.pdf [dostęp: 12.03.2024].
70. Niles Riddel J., *The Role of the Foreign Broadcast Information Service in Open Source Intelligence*, 1992, https://irp.fas.org/fbis/riddel.html [dostęp: 3.11.2023].
71. NISO, *Understanding Metadata*, 2017, https://www.niso.org/publications/understanding-metadata-2017 [dostęp: 7.06.2022].
72. *Nowe podejście do walki z dezinformacją,* 2024, https://www.gov.pl/web/cyfryzacja/nowe-podejscie-do-walki-z-dezinformacja [dostęp: 20.05.2024].

73. Octoparse, https://www.octoparse.com/ [dostęp: 2.07.2024].
74. Office of the Director of National Intelligence – United States of America, *U.S. National Intelligence – An Overview 2011*, 2011, https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf [18.11.2021].
75. Onyphe, https://www.onyphe.io/ [dostęp: 10.07.2024].
76. OpenStreetMap, https://www.openstreetmap.org [dostęp: 5.06.2024].
77. OSINT Foundation, *Mediums of Publicly Available Information*, 2023, Document Number: 20230304-01a, https://www.osintfoundation.com/osint/Standards.asp [dostęp: 4.03.2023].
78. OSINT Framework, https://osintframework.com/ [dostęp: 2.07.2024].
79. Oxford English Dictionary, https://www.oed.com/?tl=true [dostęp: 20.04.2024].
80. Pace S., Frost G.P., Lachow I., Frelinger D.R., Fossum D., Wassem D., Pinto M.M., *The Global Positioning System: Assessing National Policies*, RAND Corporation, 1995, https://www.rand.org/pubs/monograph_reports/MR614.html.
81. Pearson J., Zinets N., *Deepfake footage purports to show Ukrainian president capitulating*, 2022, https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/ [dostęp: 12.04.2024].
82. Praescient Analytics, *Why OSINT Matters to the Intelligence Community*, https://praescientanalytics.com/why-osint-matters-to-the-intelligence-community/ [dostęp: 23.01.2024].
83. Pratt N., *An Historical Overview of the 2011 Egyptian Revolution and its Aftermath*, Politics, Popular Culture and the 2011 Egyptian Revolution, 2020, https://egyptrevolution2011.ac.uk/exhibits/show/overview/overview [dostęp: 5.06.2024].
84. *Prime Minister Benjamin Netanyahu Announces Creation of CyberSpark in Beer-Sheva,* Americans for Ben-Gurion University, 2014, https://americansforbgu.org/prime-minister-benjamin-netanyahu-announces-creation-of-cyberspark-in-beer-sheva/ [dostęp: 8.10.2023].
85. Projekt TOR, https://www.torproject.org/ [dostęp: 20.08.2024].
86. Recon-ng, https://github.com/lanmaster53/recon-ng [dostęp: 12.07.2024].
87. Réseaux IP Européens Network Coordination Centre, https://www.ripe.net [dostęp: 10.03.2024].
88. Reverse Lookup, https://mxtoolbox.com/ReverseLookup.aspx [dostęp: 10.07.2024].
89. Robtex , https://www.robtex.com/ [dostęp: 3.07.2024].
90. *Rozpoznanie geoprzestrzenne*, Vademecum Bezpieczeństwa Informacyjnego, 2020, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/rozpoznanie-geoprzestrzenne/ [dostęp: 5.06.2024].
91. SHABAK, https://www.shabak.gov.il/en/about/values/ [dostęp: 8.07.2024].
92. Shodan, https://www.shodan.io/ [dostęp: 5.07.2024].
93. SiteSucker, https://ricks-apps.com/osx/sitesucker/ [dostęp: 4.03.2024].
94. SoftByte Labs, https://www.softbytelabs.com [dostęp: 4.03.2024].
95. Spamhaus, https://check.spamhaus.org/ [dostęp: 10.07.2024].
96. SpiderFoot , https://github.com/smicallef/spiderfoot [dostęp: 12.07.2024].
97. SpiderFoot, https://www.spiderfoot.net/attack-surface-monitoring/ [dostęp: 12.07.2024].
98. The Association of British Investigators, [https://www.theabi.org.uk/ [dostęp: 5.06.2024].
99. Thomas E., *Project Nemesis, Doxxing and the New Frontier of Informational Warfare,* 2022, https://www.isdglobal.org/digital_dispatches/project-nemesis-and-the-new-frontiers-of-informational-warfare/ [dostęp: 25.08.2024].
100. U.S. Cyber Command, *Private Sector Partnerships*, https://www.cybercom.mil/Partnerships-and-Outreach/Private-Sector-Partnerships/ [dostęp: 23.01.2024].
101. VirusTotal, https://www.virustotal.com/gui/home/upload [dostęp: 10.03.2024].
102. Wappalyzer, https://www.wappalyzer.com/ [dostęp: 4.03.2024].
103. WhatRuns , https://www.whatruns.com/ [dostęp: 4.03.2024].
104. Whois.com , https://www.whois.com/ [dostęp: 3.07.2024].
105. Whoisology, https://whoisology.com/ [dostęp: 3.07.2024].
106. Wikimapia, https://www.wikimapia.org [dostęp: 5.06.2024].

107. Williams H.J., Blum I., *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, Rand Corporation, 2018, https://www.rand.org/pubs/research_reports/RR1964.html [dostęp: 27.03.2025].
108. WINTESS, https://www.witness.org/ [dostęp: 10.06.2024].
109. Yandex, https://yandex.com/ [dostęp: 2.01.2023].

WYKAZ RYSUNKÓW

WYKAZ TABEL

STRESZCZENIE

Tytuł rozprawy: „Znaczenie wywiadu jawnoźródłowego w bezpieczeństwie państwa”
Autor: Anna Nastuła

W ramach badań zrekapitulowanych w rozprawie doktorskiej podjęto problematykę związaną z rolą wywiadu jawnoźródłowego realizowanego w obszarze bezpieczeństwa państwa.

Głównym celem pracy jest określenie znaczenia wywiadu jawnoźródłowego w bezpieczeństwie państwa. Celem badań w ujęciu teoretycznym jest zidentyfikowanie możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa. Wynikiem pracy są wnioski i rekomendacje dotyczące usprawnienia wykorzystania wywiadu jawnoźródłowego na rzecz bezpieczeństwa państwa.

Główny problem badawczy niniejszej rozprawy sformułowano następująco: *Jakie znaczenie ma wywiad jawnoźródłowy w zapewnieniu bezpieczeństwa państwa?* Przyjęto następującą główną hipotezę badawczą: *Dynamiczny rozwój otwartych źródeł informacji oraz technologii związanych z możliwością pozyskiwania i masowej dystrybucji informacji, a także coraz szersze wykorzystanie nowych technologii do pozyskiwania i analizy informacji jawnoźródłowych powodują wzrost możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa. Informacje dostarczone w wyniku działań wywiadu jawnoźródłowego: a) uzupełniają informacje pozyskane drogą operacyjną, b) skracają czas konieczny do podjęcia decyzji, przez co c) poprawiają jakość i skuteczność działań ofensywnych i defensywnych państwa***.***

W celu udzielenia odpowiedzi na postawione pytania badawcze oraz weryfikacji hipotez – oprócz badań teoretycznych przeprowadzono badania empiryczne w formie pogłębionych wywiadów eksperckich z osobami posiadającymi duży dorobek zawodowy oraz specjalistyczną wiedzę w zakresie wywiadu jawnoźródłowego i jego wykorzystania w sektorze bezpieczeństwa państwa.

Rozprawa doktorska składa się ze wstępu, sześciu rozdziałów, zakończenia, bibliografii, wykazu rysunków, wykazu tabel oraz załączników, które obejmują: scenariusz wywiadu eksperckiego, transkrypcje przeprowadzonych wywiadów z ekspertami oraz zgody na publikację wywiadów w pracy doktorskiej. Struktura dysertacji przedstawia się następująco:

– rozdział I – przedstawienie założeń metodologicznych, uzasadnienie potrzeby podjęcia badań oraz omówienie podstawowych pojęć występujących w pracy;
– rozdział II – analiza charakterystyki wywiadu jawnoźródłowego;
– rozdział III – naukowa eksploracja metod i środków stosowanych w wywiadzie jawnoźródłowym;
– rozdział IV – badania dotyczące prawnych i pozaprawnych aspektów prowadzenia wywiadu jawnoźródłowego;
– rozdział V – analiza wykorzystania wywiadu jawnoźródłowego w wybranych państwach demokratycznych;
– rozdział VI – podsumowanie badań dotyczących znaczenia wywiadu jawnoźródłowego w bezpieczeństwa państwa;

W zakończeniu rozprawy dokonano podsumowania przeprowadzonych badań oraz odniesiono się do postawionej hipotezy i zidentyfikowanych problemów badawczych.

Niniejsza dysertacja dostarcza kompleksowej oceny znaczenia wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa państwa oraz formułuje konkretne rekomendacje mające na celu zwiększenie jego efektywności w dynamicznie zmieniającym się środowisku bezpieczeństwa.

Słowa kluczowe: wywiad jawnoźródłowy, bezpieczeństwo państwa, informacje jawnoźródłowe, OSINT.

Summary

Title of doctoral dissertation: „The importance of open-source intelligence in state security".

Author: Anna Nastuła

The research summarized in the doctoral dissertation addressed issues related to the role of open-source intelligence implemented in the area of state security.

The primary aim of the dissertation is to determine the significance of open-source intelligence in state security. The theoretical objective of the research is to identify the possibilities of uses of open-source intelligence in ensuring the security of the state. The result of the work includes conclusions and recommendations aimed at improving the use of open-source intelligence for state security.

The main research question of the dissertation is formulated as follows: What is the importance of open source intelligence in ensuring state security? The following main research hypothesis was adopted: The dynamic development of open information sources and technologies related to the acquisition and mass distribution of information, as well as the increasingly widespread use of new technologies for the acquisition and analysis of open-source information, contribute to the enhanced potential of open-source intelligence in ensuring state security. Information obtained through open-source intelligence: (a) complements intelligence gathered through operational methods, (b) reduces the time required for decision-making, thereby (c) improving the quality and effectiveness of the state's offensive and defensive actions.

In order to address the research questions and verify the hypotheses, in addition to theoretical research, empirical research was conducted in the form of in-depth expert interviews with individuals with extensive professional backgrounds and expertise in open source intelligence and its use in the state security sector.

The doctoral dissertation consists of an introduction, six chapters, a conclusion, bibliography, list of figures, list of tables, and appendices, which include: the expert interview scenario, transcriptions of the interviews with the experts, and consent forms for the publication of the interviews in the doctoral dissertation. The dissertation is structured as follows:

– Chapter I – presentation of the methodological assumptions, justification for the need to undertake the research, and discussion of the key concepts used in the study
– Chapter II – analysis of the characteristics of open-source intelligence

– Chapter III – scientific exploration of the methods and means used in open-source intelligence
– Chapter IV – research into the legal and extralegal aspects of conducting open-source intelligence
– Chapter V – analysis of the use of open-source intelligence in selected democratic states
– Chapter VI – summary of the research on the importance of open-source intelligence in state security.

In the conclusion, the results of the research were summarized, and reference was made to the hypothesis and research problems identified.

This dissertation provides a comprehensive assessment of the importance of open-source intelligence in ensuring state security and formulates specific recommendations aimed at enhancing its effectiveness in an increasingly dynamic security environment.

Keywords: open source intelligence, state security, publicly available information, OSINT