STUDIA POLITOLOGICZNE VOL. 54
DOI: 10.33896/SPolit.2019.54.2

Piotr Sosnowski
ORCID: 0000-0001-6985-4555

Systematyzacja pojęć związanych z metodami i źródłami pozyskiwania informacji w kontekście infobrokeringu

Słowa kluczowe:
infobrokering, pozyskiwanie informacji, źródła informacji, dyscypliny wywiadowcze, dyscypliny rozpoznania

STUDIA I ANALIZY

Wprowadzenie

Zdolność do sprawnego pozyskiwania, przetwarzania i zarządzania informacjami odgrywa dziś kluczową rolę w funkcjonowaniu organizacji. W procesie zarządzania dostęp do informacji pozwala na podejmowanie lepszych decyzji i tym samym na ograniczenie ryzyka związanego z działalnością oraz przeciwdziałanie zagrożeniom pochodzącym z otoczenia podmiotu. Globalna komunikacja i przetwarzanie danych w chmurze wraz z konwergencją sieci poszerzają zakres dostępnych informacji, czego konsekwencją jest dynamiczny rozwój metod ich pozyskiwania, analizy i oceny. Wzrost liczby dostępnych danych oraz szeroka oferta usług stwarzają konieczność uporządkowania terminologicznego i typologicznego chaosu w tym obszarze. Z tej perspektywy celem artykułu uczyniono przegląd i systematyzację pojęć związanych z metodami i źródłami pozyskiwania informacji w kontekście infobrokeringu.

Pierwsza część artykułu stanowi refleksję na temat dynamiki rozwoju technologicznego, która determinuje nowe metody i źródła pozyskiwania informacji. Druga dotyczy podziału ze względu na legalność źródeł pozyskiwanych informacji. Trzecia część jest poświęcona klasycznemu

podziałowi na dyscypliny według Paktu Północnoatlantyckiego[1]. Czwarta – dyscyplinom wspierającym zdefiniowanym w doktrynie amerykańskiej armii (ADP 2-0)[2]. Piąta część dotyczy nowych dyscyplin i subdyscyplin, które zdefiniowano w ostatniej dekadzie. Artykuł zamyka refleksja na temat wykorzystania „klasycznych" i nowych źródeł informacji w pracy brokera informacji.

Rozwój technologiczny jako źródło nowych metod i obszarów pozyskiwania informacji

Informacja jest uważana za najważniejszy czynnik kształtujący rozwój ludzkiej społeczności, a dynamiczne zmiany w dziedzinie jej przekazywania, jak na przykład wynalezienie pisma, druku, telegrafu czy Internetu, prowadziły do cywilizacyjnych przemian. W 1980 roku pierwszy dysk twardy, którego pamięć przekroczyła pojemność 1 GB, ważył 250 kg. Obecnie na rynku są dostępne smartfony dysponujące pamięcią 1 TB. Według danych opublikowanych przez Międzynarodowy Związek Telekomunikacyjny w 1998 roku z sieci Internet korzystało 3% światowej populacji, na koniec 2018 roku ponad połowa ludzkości była online (51,2%), a dziś już niemal cała żyje w zasięgu telefonii komórkowej[3]. W pierwszej połowie 2018 roku analitycy amerykańskiej spółki DOMO[4] oszacowali, że w każdej minucie użytkownicy Twittera przesyłali 473,3 tys. tweetów, a na Instagramie pojawiało się niemal 50 tys. nowych zdjęć. Ludzkość wytwarza ponad 2,5 kwintylion danych dziennie, a do 2020 roku na każdego mieszkańca planety będzie przypadać 1,7 MB wytwarzanych co sekundę[5]. Konsekwencje takiego stanu rzeczy są zbliżone do opisanej przez Alana Turinga koncepcji *infinite computing* i można je nazwać „rewolucją nieogra-

---

1 *AAP-06. NATO Glossary of Terms and Definitions*, NATO 2018, https://nso.nato.int/nso/zPublic/ap/PROM/AAP-06%202018%20EF.pdf (dostęp: 19.02.2019).

2 *Complementary Intelligence Capabilities*, Army Doctrine Publication ADP 2-0 for Army Intelligence Activities, Department of the Army, Waszyngton 2018, https://fas.org/irp/doddir/army/adp2_0.pdf (dostęp: 6.01.2019).

3 International Telecommunication Union, *Measuring the Information Society Report*, 2018, t. 1, s. 2–3, https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx (dostęp: 19.02.2019).

4 DOMO, Inc. – amerykańska spółka specjalizująca się w narzędziach do analizy biznesowej i wizualizacji danych.

5 *Data Never Sleeps* 6.0, infografika, https://www.domo.com/blog/wp-content/uploads/2018/06/18_domo_data-never-sleeps-6verticals.pdf (dostęp: 19.02.2019).

niczonego przetwarzania danych"[6]. Owa rewolucja jest wynikiem wzrostu mocy obliczeniowych oraz coraz szerszego dostępu do danych[7]. Yochai Benkler zauważył, że przetwarzanie i pozyskiwanie informacji przy użyciu zasobów sieci stało się tak relatywnie proste i tanie, że wyzwaniem nie jest już samo odnalezienie informacji, lecz ocena jej wartości i wiarygodności[8]. Podobną opinię wyraził dowódca Dowództwa Strategicznego USA (U.S. Strategic Command) gen. Robert Kehler, który w 2011 roku oświadczył, że w latach 2007–2011 liczba danych zebranych w obszarze rozpoznania geoprzestrzennego (*Geospatial Intelligence*, patrz: tabela 1) wzrosła o 1500%, a zdolność do ich analizy tylko o 30%[9].

W 2011 roku Henning Kagermann[10] wprowadził koncepcję Przemysłu 4.0[11] (*Industrie 4.0*, skrót – I4.0). Przemysł 4.0 opiera się na cyfryzacji *end-to-end*[12] ogółu aktywów fizycznych oraz integracji ekosystemów cyfrowych ze wszystkimi działaniami dotyczącymi produktu[13]. Jego istotą jest powiązanie technologii teleinformatycznych, przemysłu i Internetu rzeczy w celu obniżenia kosztów, poprawy wydajności oraz dostosowania produktu i usług do preferencji i zachowań konsumentów. Opiera się przede wszystkim na przetwarzaniu danych w czasie rzeczywistym z wykorzystaniem nowych technologii, między innymi sztucznej inteligencji, systemów cyberfizycznych, chmur obliczeniowych, robotyki, druku 3D, technologii addytywnych, rozszerzonej rzeczywistości i analityki biznesowej.

Procesy związane z pozyskiwaniem, przetwarzaniem i interpretacją danych od zarania dziejów towarzyszyły działalności handlowej, ale

---

[6] A.M. Turing, *On Computable Numbers, with an Application to the Entscheidungsproblem*, „Proceedings of the London Mathematical Society" 1937, nr 1, s. 230–265.

[7] P. Płoszajski, *Big Data: nowe źródło przewag i wzrostu firm*, „E-mentor" 2013, nr 3(50), s. 6.

[8] Y. Benkler, *Bogactwo sieci. Jak produkcja społeczna zmienia rynki i wolność*, Warszawa 2008.

[9] P.B. de Selding, *Pentagon Struggles with Avalanche of Data*, SpaceNews, 29.11.2011, https://spacenews.com/pentagon-struggles-avalanche-data (dostęp: 19.01.2019).

[10] Profesor fizyki i były prezes zarządu niemieckiego koncernu SAP (Systeme, Anwendungen und Produkte in der Datenverarbeitung).

[11] Inne kraje europejskie podjęły podobne inicjatywy, na przykład *Smart Industry* (Holandia), *Catapults* (Wielka Brytania), *Industrie du Futur* (Francja).

[12] W polskojęzycznej literaturze przedmiotu występuje tłumaczenie „od punktu wyjścia do punktu docelowego".

[13] Łańcuch wartości (ang. *value chain*) to w uproszczeniu sekwencja działań podejmowanych przez firmę, aby opracować, wytworzyć, sprzedać i dostarczyć produkt, a następnie świadczyć usługi posprzedażowe. M.E. Porter, *Competitive Advantage: Creating and Sustaining Superior Performance*, Nowy Jork 2008, s. 33.

dopiero współcześnie stały się odrębną i znaczącą gałęzią gospodarki. Przykładem może być ogromny udział w rynku sektora usług bezpłatnych dla konsumentów (jak na przykład media społecznościowe), którego zyski pochodzą w znacznej mierze z monetyzacji danych użytkowników[14]. Główny mechanizm ich funkcjonowania w uproszczeniu można porównać do cyklu wywiadowczego w ujęciu Roberta M. Clarka. Składa się z sześciu elementów: określenia potrzeb, planowania i kierowania, gromadzenia, przetwarzania, analizy i opracowania, rozpowszechniania, którego skutkiem w tym przypadku jest utowarowienie (monetyzacja) danych. Zatem na przykład podmiot z sektora usług marketingowych informuje podmiot administrujący platformą społecznościową o konkretnym zapotrzebowaniu na produkt informacyjny; platforma planuje i kieruje odpowiednie instrumenty, które gromadzą, a następnie przetwarzają dane użytkowników; odpowiednie systemy realizują zadania z zakresu analizy i opracowania zebranych danych. Wyniki trafiają jednocześnie na zewnątrz do klienta w postaci produktu i do wnętrza organizacji jako wnioski dotyczące funkcjonowania całego cyklu. Platforma nieustannie uczy się i rozwija możliwości, na przykład w dziedzinie utrzymania uwagi użytkowników. Im więcej interakcji użytkowników z platformą, tym większa jej wartość.

W sferze marketingu wykorzystanie wielkich zbiorów danych, w tym personalnych, do przygotowania treści reklamowej nazywa się profilowaniem. Można dopatrywać się analogii w dziedzinie wojskowości, w której dokładne uderzenie środków ogniowych na zamierzone cele potocznie nazywa się „precyzyjnym cięciem chirurgicznym". Oba zamierzenia polegają na wykryciu i wejściu w interakcję tylko z obiektem będącym w kręgu zainteresowań organizacji i wymagają zaawansowanych, precyzyjnie zorganizowanych metod pozyskiwania i analizy danych. Jest to tylko jeden z wielu elementów wskazujących na wspólną tożsamość i wzajemne przenikanie się metod i narzędzi procesu rozpoznania realizowanego przez wojsko i wywiadu biznesowego (*Business Intelligence*).

Podział na otwarte i zamknięte źródła informacji

W uproszczeniu źródła informacji dzieli się na jawne i niejawne. Te pierwsze odnoszą się do źródeł otwartych. Dostęp do nich jest

[14] Zob. szerzej: S. Elvy, *Paying for Privacy and the Personal Data Economy*, „Columbia Law Review" 2017, t. 117, nr 6, s. 1369–1459.

powszechny i nie łamie prawa. Pozyskiwanie informacji z tych źródeł w ujęciu procesowym nazywa się białym wywiadem. Drugie nazywane są czarnym wywiadem i dotyczą informacji zbieranych metodami wywiadu operacyjnego przez agenturę lub funkcjonariuszy mających specjalne uprawnienia. Wykorzystuje urządzenia techniczne (podsłuch, podgląd, kontrola korespondencji), dane z satelitów szpiegowskich, skryte pozyskiwanie utajonych informacji itp.[15] Pochodzą ze źródeł zamkniętych. Zdaniem Bartosza Saramaka tym, co odróżnia biały wywiad od czarnego wydaje się być brak konieczności naruszania czyjejś prywatności czy łamania prawa chroniącego poufne bądź tajne informacje. Immamentną cechą czarnego wywiadu jest konieczność utrzymania go w tajemnicy. W przypadku ujawnienia takiej działalności organizacja (rząd, podmiot prywatny) zaprzecza, jakoby ją realizował.

Powyższe rozróżnienie zarysowuje dwa przeciwległe bieguny osi, na której praktyka pozyskiwania informacji oprócz czerni i bieli może też przyjąć najróżniejsze odcienie szarości. Zarysowanie wyraźnej granicy między środkami kwalifikowanymi jako operacyjne a wszelkimi innymi, które można wykorzystać do zbierania informacji, wydaje się niemożliwe. Różne podmioty prywatne (na przykład wywiadownie gospodarcze, firmy detektywistyczne) nie korzystają jedynie z materiałów jawnych i ogólnodostępnych. Pracownicy tych podmiotów mimo braku odpowiednich uprawnień śledczych lub posiadania ich w węższym zakresie niż funkcjonariusze państwowi również stosują techniki operacyjne. Taką działalność podmiotów niepaństwowych nazywa się potocznie szarym wywiadem.

Istotą tej typologii jest rozróżnienie między trzema rodzajami działalności wywiadowczej: legalną i zgodną z normami etycznymi (biały wywiad), legalną, ale wątpliwą etycznie (szary wywiad) oraz nielegalną i nieetyczną (czarny wywiad). Niestety przypisywanie tych pojęć współczesnym niezwykle złożonym problemom staje się coraz trudniejsze. Być może w momencie, kiedy postrzeganie granicy między rzeczywistością wirtualną a fizyczną stało się błędem poznawczym, zaistniała potrzeba konceptualizacji dodatkowych kolorów w tej klasyfikacji. Coraz częściej opinia publiczna dowiaduje się o nieprawidłowościach[16] w funkcjonowa-

[15] T.A. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*, [w:] K. Liedel, P. Piasecka (red.), *Rola mediów w przeciwdziałaniu terroryzmowi*, Warszawa 2009, s. 81; T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, s. 72.

[16] Nieprawidłowości w percepcji opinii publicznej. W percepcji podmiotów świadczących usługę mogą to być funkcjonalności, o których celowo nie informuje się użytkowników w sposób precyzyjny, gdyż przynoszą dochody, np. sprzedaż metadanych firmom marketingowym.

niu technologii, które pozwalają nieprzewidzianym podmiotom na dostęp do prywatnych danych użytkowników. Przykładem mogą być kontrowersje związane z ujawnieniem procederu wykorzystywania precyzyjnych danych lokalizacji smartfonów przez łowców nagród. Firmy telekomunikacyjne sprzedawały dane pochodzące z usługi Assisted-GPS podmiotom zewnętrznym, które z kolei sprzedawały je osobom prywatnym[17]. W tym przypadku jest jasne, że taki proceder nie powinien mieć miejsca i jest społecznie nieakceptowalny. Jednak nie jest do końca jasne, czy którykolwiek z podmiotów złamał prawo. Zakwalifikowanie działań łowców nagród jako szary wywiad lub czarny wywiad zależeć będzie od ewentualnej decyzji amerykańskiego sądu. Ten przykład obrazuje trudność w stosowaniu tej typologii podczas analizy powszechnych dziś zjawisk związanych z pozyskiwaniem informacji pochodzących z urządzeń elektronicznych przez podmioty trzecie, które w założeniu nie powinny mieć do nich dostępu, ale go uzyskują, nie łamiąc przy tym prawa.

Rozróżnienie na biały, szary i czarny wywiad rzadko pojawia się w zagranicznych opracowaniach teoretycznych w znaczeniu wyżej opisywanym[18]. Nie występuje ani w dokumentach doktrynalnych i standaryzacyjnych Sojuszu Północnoatlantyckiego, ani w oficjalnych i publikowanych przez państwa dokumentach i aktach prawnych dotyczących tej dziedziny. Najczęściej stosowana jest typologia ze względu na źródła pozyskanej informacji. Nazywana jest podziałem na dyscypliny wywiadowcze.

Klasyczne dyscypliny wywiadowcze

W amerykańskiej terminologii wojskowo-wywiadowczej ukształtowało się ujęcie procesowe oparte jednocześnie na metodzie i źródle pozyskiwanej informacji oraz na problemie, którego dotyczy. Dyscypliny są nazywane według schematu polegającego na połączeniu dwóch akronimów. Pierwszy pochodzi od określenia problemu, którego dotyczy zakres

[17] M. Giles, *Bounty Hunters Tracked People Secretly Using US Phone Giants Location Data*, „MIT Technology Review", 7.02.2019, https://www.technologyreview.com/the-download/612907/bounty-hunters-tracked-people-secretly-using-us-phone-giants-location-data (dostęp: 8.02.2019).

[18] *Grey Intelligence* pojawia się np. jako koncepcja opisująca zjawisko zatarcia granic między działalnością w sferze bezpieczeństwa realizowaną przez państwo a tą realizowaną przez podmioty prywatne. Odnosi się do procesów politycznych, a nie do działań wywiadowczych.

przedsięwzięć, na przykład otwarte źródła informacji – *open source*, a drugi od terminu *intelligence*, co w połączeniu daje OSINT.

Angielskojęzyczny termin *intelligence* jest wieloznaczny i może określać wiedzę, mądrość lub informację. W polskiej literaturze przedmiotu jest tłumaczony najczęściej jako wywiad, gdyż w tym kontekście odnosi się nie do zasobu wiedzy, lecz do procesu, który obejmuje szereg podmiotów włączonych we wspólny łańcuch wymiany informacji[19]. W NATO definiowaniem dyscyplin wywiadowczych zajmuje się Połączona Rada Standaryzacyjna Komitetu Wojskowego (PRSKW)[20]. Według autorów polskiego tłumaczenia słownika terminów NATO z 2014 roku *intelligence* oznacza „[…] produkt wynikający z przetworzenia informacji dotyczących innych państw, wrogich lub potencjalnie wrogich sił lub elementów albo obszarów rzeczywistych lub potencjalnych działań. Termin ten jest stosowany także do określania działania, którego wynikiem jest ten produkt oraz do struktur zaangażowanych w taką działalność"[21]. Zatem może być rozumiany zarówno jako zasób (dane wywiadowcze lub dane rozpoznawcze), jak i czynność (wywiad lub rozpoznanie). Wybór terminu zależy od poziomu prowadzonych działań lub stosowanych procedur. Definicja opublikowana w tym słowniku pochodziła z 1981 roku.

W słowniku z 2018 roku znajduje się definicja PRSKW z 2013 roku, wedle której *intelligence* jest „produktem powstałym wskutek prowadzonego gromadzenia i przetwarzania informacji dotyczących środowiska, możliwości i intencji aktorów w celu identyfikacji zagrożeń i przedstawienia decydentom możliwości do wykorzystania"[22]. W tym samym słowniku środowisko (*environment*) jest zdefiniowane jako otoczenie działania organizacji; obejmuje powietrze, wodę, ląd, zasoby naturalne, florę, faunę oraz ludzi wraz z ich interakcjami[23]. W tej definicji zastanawia brak wyszczególnienia na przykład cyberprzestrzeni jako obszaru, gdzie zachodzą interakcje między urządzeniami.

---

[19] M. Ciecierski, *Wywiad biznesowy w korporacjach transnarodowych. Teoria i praktyka*, Toruń 2009, s. 113.

[20] Military Committee Joint Standardization Board (MCJSB).

[21] *AAP-6. Słownik terminów i definicji NATO. Zawierający wojskowe terminy i ich definicje stosowane w NATO*, 2014, http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf (dostęp: 7.02.2019).

[22] „The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers". Źródło: *AAP-06. NATO Glossary of Terms…*, s. 66.

[23] „The surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans, and their interrelations", tamże, s. 48.

Tabela 1. Dyscypliny wywiadowcze według Paktu Północnoatlantyckiego

Akronim	Nazwa dyscypliny w oryginale	Nazwa dyscypliny w języku polskim	Problem
ACOUSTINT /ACINT	*Acoustical Intelligence*	rozpoznanie akustyczne	Zjawiska akustyczne.
CI	*Counter Intelligence*	kontrwywiad	Zagrożenia związane ze szpiegostwem, sabotażem, działalnością wywrotową i terroryzmem.
COMINT	*Communication Intelligence*	rozpoznanie komunikacyjne	Komunikacja międzyludzka realizowana za pomocą sygnałów elektromagnetycznych
ELINT	*Electronic Intelligence*	rozpoznanie elektroniczne	Sygnały elektromagnetyczne niezwiązane z komunikacją międzyludzką.
GEOINT	*Geospatial Intelligence*	rozpoznanie geoprzestrzenne	Wizualizacja problemu na podstawie powiązania danych geoprzestrzennych z danymi obrazowymi i/lub z danymi pochodzącymi z innych dyscyplin.
HUMINT	*Human Intelligence*	rozpoznanie osobowe	Informacje zbierane i dostarczane przez źródła osobowe.
MASINT	*Measurement and Signature Intelligence*	rozpoznanie pomiarowo-badawcze	Identyfikacja źródła, emitera lub nadawcy na podstawie danych pozyskanych z przyrządów pomiarowych.
MEDINT	*Medical Intelligence*	rozpoznanie medyczne	Dane: z dziedziny nauk biologicznych, medyczne, epidemiologiczne, środowiskowe i inne związane ze zdrowiem ludzi lub zwierząt.
OSINT	*Open Source Intelligence*	rozpoznanie ze źródeł jawnych	Informacje dostępne publicznie lub o ograniczonym dostępie publicznym, ale jawne.
SIGINT	*Signal Intelligence*	rozpoznanie elektromagnetyczne	Sygnały radiowe i elektroniczne. Określenia używa się tylko wtedy, kiedy występują razem.
TECHINT	*Technical Intelligence*	rozpoznanie techniczne	Rozwój zagranicznych technologii oraz wydajność i możliwości zagranicznych materiałów, które mają lub mogą mieć zastosowanie wojskowe.

Źródło: opracowanie własne na podstawie: *AAP-06. NATO Glossary of Terms and Definitions*, NATO 2018, https://nso.nato.int/nso/zPublic/ap/PROM/AAP-06%202018%20EF.pdf [dostęp: 1.02.2019].

Rada standaryzacyjna NATO zdefiniowała 12 dyscyplin wywiadowczych (tabela 1). Według definicji przyjętej i przez NATO, i przez amerykańską armię OSINT „dotyczy danych pochodzących zarówno z publicznie dostępnych informacji, jak i innych jawnych informacji o ograniczonym rozpowszechnianiu lub dostępie"[24]. Jednak amerykańska doktryna wywiadowcza precyzuje, że samo pozyskiwanie i przetwarzanie informacji z otwartych źródeł jest na tyle powszechną czynnością, że nie należy kwalifikować jej jako OSINT, który jest realizowany wyłącznie przez odpowiednio przygotowany personel i ma na celu wsparcie innych dyscyplin rozpoznania, operacji wywiadu oraz decyzji podejmowanych przez dowódców[25]. Szczegółowej charakterystyce tej dyscypliny została poświęcona amerykańska „Army Techniques Publication" – ATP 2-22.9[26].

Definicje występujące w dokumentach doktrynalnych kładą nacisk na ścisły związek produktu informacyjnego ze zgłoszonym wcześniej zapotrzebowaniem oraz na jego weryfikację[27]. Generalnie nie przedstawiają sztywnej metodyki, lecz jedynie zarysowują ogólne ramy, wedle których poszczególne organizacje wypracowują własne standardy[28]. Departament Armii Stanów Zjednoczonych definiuje OSINT jako „pozyskiwanie informacji (publicznie dostępnych, o które każdy może legalnie poprosić, kupić je lub zdobyć w wyniku obserwacji) o dużym znaczeniu, systematycznie gromadzonych w bazach danych, przetwarzanych i analizowanych. Opracowany materiał stanowi zaś odpowiedź na zapytanie wywiadowcze o określonych wymaganiach. Informację jawnoźródłową stanowi każda informacja, którą każdy członek społeczeństwa może legalnie uzyskać na żądanie, za pomocą obserwacji, a także inne nieklasyfikowane jawne informacje o ograniczonym dostępie publicznym. Za informacje ogólnodostępne (publiczne) uznaje się powszechnie dostępne informacje, które spełniają następujące warunki: zostały opublikowane lub zezwolono na ich publiczne wykorzystanie; są dostępne na życzenie, dostępne online, poprzez subskrypcję lub zakup; każdy potencjalny obserwator może je zobaczyć lub usłyszeć; są udostępniane na publicznym spotkaniu lub

---

[24] *Complementary Intelligence Capabilities…*, roz. 4, s. 7–8, https://fas.org/irp/doddir/army/adp2_0.pdf (dostęp: 19.02.2019).

[25] Tamże.

[26] *Open Source Intelligence*, „Army Techniques Publication" No. 2-22.9 (FMI 2-22.9), Department of the Army, Waszyngton 2012, https://fas.org/irp/doddir/army/atp2-22-9.pdf (dostęp: 20.01.2019).

[27] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, s. 21.

[28] Tamże, s. 20–21.

uzyskiwane przez odwiedzanie dowolnego miejsca albo uczestnictwo w każdym wydarzeniu otwartym dla publiczności. Publicznie dostępne informacje obejmują także informacje ogólnie dostępne dla społeczności wojskowej, chociaż społeczność wojskowa nie jest otwarta dla ludności cywilnej. Otwarte informacje mogą występować na przykład w formie interakcji społecznych, materiałów drukowanych, przekazu medialnego, Internetu, otwartego forum. Pozyskiwanie takich informacji powinno być nieinwazyjne (ang. *nonintrusive*)[29].

Niezależnie od terminologii wojskowej sfera cywilna interpretuje OSINT w sposób tożsamy z polskim białym wywiadem, czyli po prostu jako wykorzystanie otwartych (jawnych) źródeł informacji. W tym ujęciu informacje mogą mieć różne źródło i charakter, przez co cywilny OSINT przenika się z innymi dyscyplinami, które w nomenklaturze wojskowej mogłyby zostać uznane za odrębne.

Armia amerykańska definiuje HUMINT (ang. *Human Intelligence*, pol. rozpoznanie osobowe) jako pozyskiwanie informacji ze źródeł osobowych i multimediów przez wyszkolonego w tym zakresie specjalistę w celu identyfikacji: obcych podmiotów, ich intencji, części składowych, sił, zadań, taktyki, wyposażenia i możliwości. Źródłem osobowym (osobą dostarczającą informacji) mogą być na przykład więźniowie, jeńcy wojenni, uchodźcy, przesiedleńcy, lokalni mieszkańcy, siły przeciwnika, członkowie zagranicznych organizacji rządowych i pozarządowych. Proces pozyskiwania informacji może być zarówno jawny jak i niejawny, opiera się na metodach związanych z monitorowaniem, prowadzeniem przesłuchań, rozpytywaniem, przetwarzaniem informacji nieosobowych (na przykład multimediów) dotyczących źródeł osobowych oraz na współpracy łącznikowej z organizacjami państwowymi i pozarządowymi[30].

Dyscyplina MASINT (ang. *Measurement and Signature Intelligence*, pol. rozpoznanie pomiarowo-badawcze) dotyczy produktu informacyjnego powstałego w wyniku analizy naukowej i technicznej danych pochodzących z przyrządów pomiarowych. Dzięki rozpoznaniu charakterystycznych cech związanych ze źródłem, emiterem lub nadawcą możliwa jest jego identyfikacja[31]. Często dotyczy tych samych problemów co inne dyscypliny, ale różni się od nich stosowaniem metod naukowych. Na przykład SIGINT (ang. *Signal Intelligence*, pol. rozpoznanie radioelek-

[29] *Complementary Intelligence Capabilities*…, roz. 4, s. 4–8.

[30] *FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations Headquarters*, Department of The Army, Waszyngton 2006, https://fas.org/irp/doddir/army/fm2-22-3.pdf (dostęp: 20.01.2019).

[31] *AAP-06. NATO Glossary of Terms*…

troniczne) koncentruje się na samym przechwytywaniu i przetwarzaniu danych, a MASINT na szczegółowej analizie opartej na metodach jakościowych i ilościowych. W dużym uproszczeniu można to zobrazować przykładem: analityk SIGINT na podstawie podobieństwa przechwyconych sygnałów do posiadanych wzorów określa typ urządzenia, które je emituje. Odpowiednio dobrany analityk MASINT może na przykład dojść do wniosku, że ma do czynienia z dezinformacją (na podstawie przyczyn nieznanych analitykowi SIGINT), a ponadto może być zdolny do umieszczenia danego zdarzenia w szerszym kontekście. W przypadku wywiadu naukowo-technicznego ocena danych jest realizowana przez ekspertów z danej dziedziny. Amerykańska doktryna wywiadu z 2018 roku podaje praktyczne przykłady zastosowania tej dyscypliny, na przykład wykrywanie i penetracja kamuflażu, wykrywanie zmian na powierzchni ziemi, identyfikacja swój–obcy, wykrywanie broni masowego rażenia. Matthew M. Aid wyróżnił sześć subdyscyplin składających się na MASINT[32]:

1. rozpoznanie radiooptyczne (*Radiooptical Intelligence*, EOINT), w ramach którego wyróżnia się dyscypliny podrzędne:
   a. rozpoznanie promieniowania podczerwieni (*Infrared Intelligence*, IRINT);
   b. rozpoznanie optyczne (*Optical Intelligence*, OPTINT) dotyczy fal elektromagnetycznych widzialnych – na przykład ultrafiolet, bliska podczerwień;
   c. rozpoznanie promieniowania laserowego (*Laser Intelligence*, LASINT) dotyczy systemów komunikacji laserowej, naprowadzania laserowego itp.;
2. rozpoznanie radiolokacyjne (*Radar Intelligence*, RADINT);
3. rozpoznanie fal radiowych (*Radio-frequency Intelligence*, RF), w ramach którego wyróżnia się dyscypliny podrzędne:
   a. rozpoznanie fal radiowych (RF) i/lub impulsów elektromagnetycznych (*Electro-magnetic Pulse*, EMP);
   b. rozpoznanie niezamierzonego promieniowania (*Unintentional Radiation Intelligence*, RINT);
4. rozpoznanie geofizyczne (*Geophysical Intelligence*, GEOINT)[33];
5. rozpoznanie materiałowe (*Materials Intelligence*);
6. rozpoznanie jądrowe (*Nuclear Intelligence*, NUCINT).

---

[32] M.M. Aid, *Measurement and Signature Intelligence*, [w:] R. Dover, M.S. Goodman, C. Hillebrand, *Routledge Companion to Intelligence Studies*, Londyn 2014, s. 121.

[33] Dokumenty NATO AAP-06 (2018) i ADP 2-0 (2019) używają tego samego akronimu do opisu rozpoznania geoprzestrzennego (*Geospatial Intelligence*).

Amerykańska doktryna wywiadu oprócz powyższych obszarów MASINT wyróżnia też metody pozyskiwania danych dotyczących broni chemicznej, biologicznej i radiologicznej. Specyfika tych subdyscyplin wynika z umieszczenia ich w kontekście wywiadu pomiarowo-badawczego. W zależności od uwarunkowań doktrynalnych, organizacyjnych czy specyfiki problemu powyższe subdyscypliny MASINT mogą występować jako samodzielne dyscypliny.

Słownik terminów i definicji NATO definiuje również rozpoznanie akustyczne (ang. *Acoustic Intelligence*, ACINT, dawniej ACOUSINT[34]). W literaturze i w brytyjskiej doktrynie jest ono kwalifikowane jako subdyscyplina MASINT[35]. Dotyczy pozyskiwania i przetwarzania informacji generowanych przez zjawiska akustyczne[36]. Brytyjska doktryna definiuje również rozpoznanie obrazowe (*Imagery Intelligence*, IMINT) i kwalifikuje je jako subdyscyplinę rozpoznania geoprzestrzennego. Niektórzy autorzy przyporządkowują IMINT jako subdyscyplinę TECHINT (*Technical Intelligence*)[37] lub jako samodzielną dyscyplinę. Dotyczy ona obrazów (zdjęć) dostarczonych na przykład przez samoloty, satelity, pojazdy itp.

W nomenklaturze wojskowej rozróżnia się trzy subdyscypliny wchodzące w skład SIGINT: rozpoznanie elektroniczne (*Electronic Intelligence*, ELINT), wywiad radiowy[38] (*Communications Intelligence*, COMINT) oraz *Foreign Instrumentation Signals Intelligence* (FISINT). Mimo takiego przyporządkowania ELINT i COMINT występują w literaturze przedmiotu jako samodzielne dyscypliny[39]. FISINT zaś zazwyczaj jest kwalifikowany jako subdyscyplina SIGINT lub MASINT, w zależności od podejścia podmiotu, który realizuje działanie i zastosowanych technik. FISINT dotyczy informacji technicznych i danych wywiadowczych pochodzących z przechwycenia emisji elektromagnetycznych związanych z testami i rozmieszczaniem operacyjnym obcych systemów w powietrzu, na lądzie i pod wodą.

---

34 OPSEC, *Intelligence Threat Handbook*, 1996, s. 1–2 (dostęp: 12.06.2019).

35 Ministry of Defence, *Joint Doctrine Publication 2-00 (JDP 2-00) Understanding and Intelligence Support to Joint Operations*, 3rd ed., 2011, s. 11, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf (dostęp: 19.01.2019).

36 *AAP-06. NATO Glossary of Terms…*

37 L.K. Johnson, *Introduction*, [w:] L.K. Johnson (red.), *Handbook of Intelligence Studies*, Nowy Jork 2016, s. 6.

38 Polskie tłumaczenie na podstawie: *AAP-6. Słownik terminów…*, s. 102.

39 A.D.M. Svendsen, *Collective Intelligence (COLINT)*, [w:] *Encyclopedia of U.S. Intelligence*, Nowy Jork 2015, s. 114.

COMINT dotyczy „pozyskiwania danych wywiadowczych (rozpoznawczych) za pomocą środków i systemów łączności radiowej przez osoby nie będące właściwymi odbiorcami lub użytkownikami”[40]. Amerykańska doktryna wywiadu rozróżnia informacje techniczne od wywiadowczych i uwzględnia je jako obszar zainteresowania tej dyscypliny. Ponadto zwraca uwagę, że COMINT obejmuje też zbieranie danych pochodzących z systemów zautomatyzowanych oraz sieci informatycznych przeciwnika. Może również dotyczyć zdjęć, jeśli są przetwarzane za pomocą sieci komputerowych lub urządzeń radiowych[41].

ELINT jest definiowany jako potencjał rozpoznawczy oraz proces pozyskiwania danych i informacji rozpoznawczych z systemów niekomunikacyjnych przechwyconych przez innych odbiorców niż tych, do których są one adresowane. Amerykańska doktryna wywiadu wskazuje, że dotyczy informacji technicznych i geolokalizacyjnych, których źródłem jest promieniowanie elektromagnetyczne, które jednocześnie nie stanowi komunikacji międzyludzkiej ani nie jest skutkiem promieniowania lub eksplozji nuklearnej. W jego skład wchodzą dwie subkategorie: operacyjna i techniczna. Pierwsza z nich dotyczy informacji istotnych dla operacji, są to na przykład lokalizacja, ruch, wykorzystanie, taktyka i działalność obcych emiterów i systemów uzbrojenia niesłużących komunikacji. Druga dotyczy technicznych cech emitowanych sygnałów, jak na przykład charakterystyka sygnału, tryb, funkcje, powiązania, możliwości, ograniczenia, luki w zabezpieczeniach i poziom technologii.

Zwraca uwagę multidyscyplinarne podejście do analizy wywiadowczej, które jest efektem integracji dyscyplin wywiadowczych. Wykorzystanie wszystkich dostępnych źródeł i metod jest nazywane „wywiadem ze wszystkich źródeł” (*all source intelligence*). Mimo iż proces rozpoznania, fuzji i produkcji informacji w tym podejściu jest bardziej skomplikowany i czasochłonny, to produkt informacyjny jest lepszy jakościowo i bardziej wiarygodny niż uzyskany w ramach pojedynczej dyscypliny.

---

[40] *AAP-6. Słownik terminów…*, s. 102.

[41] „Communications intelligence is technical information and intelligence derived from foreign communications by other than the intended recipients (JP 2-0). Communications intelligence includes collecting data from target or adversary automated information systems or networks. It also may include imagery when pictures or diagrams are encoded by a computer network or radio frequency method for storage or transmission. The imagery can be static or streaming”, *AAP-06. NATO Glossary of Terms…*

Dyscypliny wspierające

Doktryna wywiadu armii amerykańskiej z 2018 roku (*Army Doctrine Publication 2.0 Intelligence*) wymienia siedem dyscyplin wywiadowczych: CI (*Competitive Intelligence*), GEOINT, HUMINT, MASINT, OSINT[42], SIGINT i TECHINT. Oprócz nich definiuje również cztery dyscypliny wspierające (tabela 2).

Tabela 2. Dyscypliny wspierające

Akronim	Nazwa dyscypliny w oryginale	Nazwa dyscypliny w języku polskim	Problem
BEI	*Biometrics-enabled Intelligence*	Wywiad umożliwiony biometrią	Ustalenie tożsamości na podstawie danych biometrycznych.
_	*Cyber-enabled Intelligence*	Wywiad umożliwiony cyberprzestrzenią i spektrum elektromagnetycznym	Cyberprzestrzeń oraz spektrum elektromagnetyczne.
DOMEX	*Document and Media Exploitation*	Wywiad umożliwiony wykorzystaniem dokumentów i mediów	Zbiory dokumentów i mediów elektronicznych będących w posiadaniu rządu USA, ale niedostępnych publicznie.
FEI	*Forensic-enabled Intelligence*	Wywiad umożliwiony analizą kryminalistyczną	Analiza kryminalistyczna w celu ustalenia relacji między osobami, zdarzeniami, miejscami i przedmiotami.

Źródło: opracowanie własne na podstawie *Complementary Intelligence Capabilities*, Army Doctrine Publication (ADP 2-0) for Army Intelligence Activities, Department of the Army, Waszyngton 2018, https://fas.org/irp/doddir/army/adp2_0.pdf (dostęp: 19.02.2019).

Wywiad umożliwiony cyberprzestrzenią dotyczy zarówno pozyskiwania i przetwarzania danych z cyberprzestrzeni, jak i spektrum elektromagnetycznego. Mogą one dotyczyć środowiska informacyjnego i przestrzeni fizycznej (na przykład infrastruktury).

[42] Niekiedy opisywany jako *Digital Intelligence* (DIGINT), zob. szerzej: S.C. Mercado, *Sailing the Sea of OSINT in the Information Age*, „Studies in Intelligence" (CIA Journal) 2004, t. 48, nr 3, s. 45–55. W niektórych dokumentach i publikacjach DIGINT jest utożsamiany z CYBINT (*Cybespace Intelligence*).

Istotą wywiadu umożliwionego wykorzystaniem dokumentów i mediów (DOMEX) jest wsparcie zespołu lingwistów, których zadaniem jest archiwizacja, tłumaczenie i wstępna ocena dokumentów i materiałów multimedialnych. Produkt informacyjny może zostać wykorzystany zarówno na szczeblu taktycznym, jak i strategicznym.

Wywiad umożliwiony biometrią (BEI) polega na połączeniu informacji biometrycznych z innymi danymi wywiadowczymi, informacjami o zagrożeniach lub dotyczącymi innych aspektów środowiska operacyjnego w celu uzyskania odpowiedzi na pytania wywiadowcze. Sama biometria jest definiowana jako proces potwierdzania tożsamości na podstawie mierzalnych cech anatomicznych, fizjologicznych i behawioralnych. Warto zauważyć, że w otoczeniu współczesnego człowieka znajduje się coraz więcej urządzeń, które takie dane zbierają (na przykład monitoring miejski, urządzenia mobilne).

Wywiad umożliwiony analizą kryminalistyczną (FEI) ma na celu ustalenie relacji między osobami, zdarzeniami, miejscami i przedmiotami. Jego istotą jest integracja materiałów poddanych naukowej analizie z innymi danymi (na przykład biometrycznymi: odciski palców, DNA). Może obejmować między innymi badanie pochodzenia na przykład dokumentów, dokumentacji miejsca incydentów czy analizę przebiegu wydarzeń itd. W doktrynie brytyjskiej występuje dyscyplina będąca połączeniem analizy kryminalistycznej i biometrii (*Forensic and Biometric Intelligence*, FABINT)[43].

Podobnie jak w przypadku innych zdefiniowanych przez wojsko klasyfikacji, o przynależności do konkretnej dyscypliny decydują wewnętrzne przepisy i wytyczne. Narzędzia (na przykład technologie informatyczne) i źródła informacji mogą być wspólne dla wielu dyscyplin i dyscyplin wpierających. Powyższe zestawienie jest jedynie pewnym skrótowym omówieniem nomenklatury obowiązującej w NATO i Armii USA. Stanowi ważne źródło inspiracji i wyznacza istotne trendy w literaturze przedmiotu. Z racji swojej specyfiki sfera cywilna wypracowuje pojęcia, które nie muszą być kompatybilne z wojskowymi. Jest to zależne od konkretnego podmiotu oraz jego specyficznych potrzeb i możliwości.

[43] Ministry of Defence, *Joint Doctrine Publication 2-00 (JDP 2-00)…*

Nowe dyscypliny

Dynamicznie zmieniająca się rzeczywistość, a przede wszystkim tzw. Gospodarka 4.0, przyczyniła się do zdefiniowania nowych dyscyplin dotyczących pozyskiwania informacji. Są one oparte na źródłach i problemach, które albo wcześniej nie występowały (jak Internet rzeczy), albo brakowało odpowiednich technologii pozwalających na ich wyodrębnienie.

Tabela 3 wymienia dyscypliny, które zostały zdefiniowane w literaturze przedmiotu, ale nie zostały uwzględnione jako samodzielne dyscypliny we wspomnianych wyżej dokumentach doktrynalnych.

Tabela 3. Nowe dyscypliny pozyskiwania informacji

Akronim	Nazwa dyscypliny w oryginale	Nazwa dyscypliny w języku polskim	Problem
ADINT	*Advertising-based Intelligence*	Wywiad oparty na technologiach kierowania (targetowania) reklam w aplikacjach mobilnych	Realizowany z wykorzystaniem sieci reklamowych (infrastruktury, której zadaniem jest łączyć reklamodawców z miejscem wyświetlania reklamy, jak na przykład aplikacja mobilna).
COLINT	*Collective Intelligence*	Wywiad zbiorowy	Współpraca i/lub rywalizacja podmiotów z zakresu wszystkich dyscyplin wywiadowczych[a].
IoTINT	*Internet of Things Intelligence*	Wywiad oparty na Internecie rzeczy	Dane zebrane przez sensory urządzeń Internetu rzeczy.
MARKINT/ MI	*Market Intelligence*	Wywiad rynkowy	Dane dotyczące działalności rynkowej i konkurencji.
RESINT[b]	*Research Intelligence*	Wywiad naukowy	Informacja i wiedza wywodząca się z działalności badawczej.
SOCMINT	*Social Media Intelligence*	Wywiad oparty na mediach społecznościowych	Interakcje międzyludzkie w mediach społecznościowych.

[a] COLINT różni się od wywiadu ze wszystkich źródeł (*all source intelligence*) tym, że jego immamentną cechą jest głęboka współpraca między podmiotami specjalizującymi się w różnych dyscyplinach.

[b] A.D.M. Svendsen, *Introducing RESINT: A Missing and Undervalued „INT" in All-Source Intelligence Efforts*, „International Journal of Intelligence and CounterIntelligence" 2013, nr 26, s. 777–794.

Źródło: opracowanie własne.

Wywiad rynkowy (*Market Intelligence*, MARKINT[44]) jest definiowany jako proces, którego zadaniem jest ciągłe generowanie wiedzy ze źródeł rozproszonych na użytek zarządzania strategicznego organizacją. Celem jest wsparcie procesu podejmowania decyzji odnoszących się do konkurowania w środowisku biznesowym[45]. W gestii zainteresowania tej dyscypliny znajdują się dane dotyczące na przykład pozycji rynkowej, działalności konkurencji, strategii sprzedaży itp.

Adam D.M. Svendsen definiuje dwie nowe dyscypliny: COLINT i RESINT. Pierwsza polega na ustanowieniu w instytucjonalnej formie głębokiej współpracy między podmiotami specjalizującymi się we wszystkich możliwych dyscyplinach. Określa produkt informacyjny, który powstał w wyniku pracy z zakresu różnych dyscyplin oraz we współpracy i/lub konkurencji wszystkich możliwych podmiotów[46]. W tym zakresie jest tożsamy z wywiadem opartym na wszystkich źródłach (*all source intelligence*). Ponadto odnosi się do instytucji zajmującej się pozyskiwaniem i analizą informacji, która powstała z inicjatywy kilku różnych podmiotów i jest przez nie utrzymywana. Druga dyscyplina (*Research Intelligence*, RESINT) dotyczy informacji, które powstają w wyniku analizy badań naukowych[47]. Wywiad naukowy może być realizowany na przykład w celu dostarczenia odpowiedniego opracowania wyników badań do odbiorcy, który jest zainteresowany ich wykorzystaniem. A.D.M. Svendsen wskazuje, że RESINT dotyka szerszego obszaru niż OSINT ze względu na możliwość wykorzystania go do optymalizacji całego procesu pozyskiwania, przetwarzania, dystrybucji i wykorzystania informacji[48].

W 2016 roku amerykańska Rada Naukowa Armii (Army Science Board) dyskutowała na temat nowej dyscypliny specjalizującej się w pozyskiwaniu informacji za pomocą Internetu rzeczy[49]. Zidentyfikowanie tego obszaru ma prowadzić do zwiększenia świadomości sytuacyjnej żołnierzy operujących na terenie zurbanizowanym. Może on dostarczyć informacji

---

[44] Niektórzy autorzy stosują określenie *Competitive Intelligence*, CI.

[45] G.L. Jamil, L.H.R. Santos, M.L. Alves, L. Furbino, *A Design Framework for a Market Intelligence System for Healthcare Sector: a Support Decision Tool in an Emergent Economy*, [w:] *Handbook on Research of ICTs for Social Services and Healthcare: Developments and Applications*, Hershey 2012.

[46] A.D.M. Svendsen, *Collective Intelligence…*, s. 114–119.

[47] A.D.M. Svendsen, *Introducing RESINT: A Missing and Undervalued „INT" in All-Source Intelligence Efforts*, „International Journal of Intelligence and Counter Intelligence" 2013, nr 26, s. 778.

[48] Tamże, s. 780–781.

[49] M.L. Loper, *Situational Awareness in Megacities*, [w:] M.E. Kosal (red.), *Technology and the Intelligence Community Challenges and Advances for the 21st Century*, Cham 2018, s. 226.

o: lokalizacji, ładunku i pasażerach pojazdów; budynkach wraz z identyfikacją osób, które w nich przebywają; zasobach (na przykład żywności); informacjach medycznych dotyczących populacji miasta itp. Może również pomóc rozróżnić cywili od żołnierzy przeciwnika.

Dostęp do danych publikowanych za pośrednictwem portali społecznościowych spowodował zdefiniowanie odpowiedniej dyscypliny – *Social Media Intelligence* (SOCMINT)[50]. W odróżnieniu do choćby HUMINT (rozpoznania osobowego) pozwala na opracowanie informacji o konkretnych grupach osób odnoszących się do konkretnych wydarzeń w czasie rzeczywistym (jak trendy zachowań użytkowników Twittera)[51]. Zdaniem publicystów rosyjski wywiad wykorzystał głównie dane zebrane za pośrednictwem mediów społecznościowych w celu wywarcia wpływu na wybory prezydenckie w Stanach Zjednoczonych w 2016 roku[52]. Teoretycy kwalifikują SOCMINT jako subdyscyplinę OSINT-u[53].

Na szczególną uwagę zasługują wyniki badań naukowców z Uniwersytetu Waszyngtonu. W celu zwrócenia uwagi na zagadnienie prywatności przeprowadzili oni eksperyment, w którym wykazali, że istnieje możliwość pozyskania danych wrażliwych użytkowników urządzeń mobilnych przy wykorzystaniu środowiska reklam internetowych. Zakupili usługę wyświetlania reklam w aplikacji mobilnej i za jej pomocą uzyskali dane lokalizacji urządzenia należącego do określonej osoby[54]. Zdefiniowali *Adware-based Intelligence* (ADINT) jako metodę wykorzystywania ekosystemu reklamowego przez nabywcę reklam do zbierania informacji o osobach docelowych. Przy użyciu podobnego mechanizmu nabywca reklam może uzyskać też inne dane zbierane i udostępniane sieciom reklamowym przez aplikacje – na przykład lista zainstalowanych aplikacji może wskazać zainteresowania obiektu, płeć, styl życia, światopogląd czy orientację seksualną. Aplikacje często mają też dostęp do kontaktów, czujników, mikrofonu, aparatu itp. Te dane są zanonimizowane, ale jak

[50] D. Omand, J. Bartlett, C. Miller, *Introducing Social Media Intelligence (SOCMINT)*, „Intelligence and National Security" 2012, nr 27(6), s. 801–823.

[51] K.P. Jani, A. Soni, *Promise and Perils of Big Data Science for Intelligence Community*, [w:] M.E. Kosal (red.), *Technology and the Intelligence*…, s. 192.

[52] Źródło: S. Shane, *These are the Ads Russia Bought on Facebook in 2016*, „The New York Times", 1.11.2017, https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html (dostęp: 19.02.2019).

[53] A.N. Liaropoulos, *The Challenge of Social Media for the Intelligence Community*, „Journal of Mediterranean and Balkan Intelligence" 2013, nr 1(1), s. 6.

[54] P. Vines, F. Roesner, T. Kohno, *Exploring ADINT: Using Ad Targeting for Surveillance on a Budget – or – How Alice Can Buy Ads to Track Bob*, Waszyngton 2017, https://adint.cs.washington.edu/ADINT.pdf (dostęp: 15.07.2018).

pokazuje wynik wyżej wspomnianego eksperymentu, dysponując odpowiednimi informacjami (na przykład dotyczącymi miejsca pracy i miejsca zamieszkania) możliwe jest powiązanie ich z konkretną osobą. Opisana metoda wykorzystuje ekosystem reklamowy urządzeń mobilnych. Zatem można ją uznać za charakterystyczną dla IoTINT. Zakwalifikowanie jej jako oddzielnej dyscypliny powinno być poprzedzone badaniami dotyczącymi wykorzystywania tej metody oraz dyskusją.

Użytkownicy urządzeń mobilnych, korzystając z ich szerokich możliwości, zostawiają na nich pewnego rodzaju cyfrową kopię swojej świadomości. Jacek Dukaj nazwał to „protezą umysłu"[55], co jest kontynuacją idei przedstawionej w pracy *The Extended Mind* z 1998 roku, której autorzy próbowali zdefiniować granicę ludzkiej świadomości[56]. Trudno wykluczyć, że w niedalekiej przyszłości broker informacji będzie w stanie nie tylko precyzyjnie udzielić odpowiedzi na pytanie, kim jest dana osoba, ale również kim będzie i jak postąpi w przyszłości.

Podsumowanie

Twórca koncepcji społeczeństwa informacyjnego Manuel Castells wysnuł tezę, że wytwarzanie, przetwarzanie i transmisja informacji stanowią podstawowe źródło produktywności i bogactwa[57]. Wraz ze wzrastającą ilością różnych urządzeń w naszym otoczeniu wzrasta też liczba przetwarzanych danych, by – teoretycznie – lepiej nam służyć. Zebrane dane są przetwarzane i wykorzystywane nie tylko po to, by usprawnić urządzenia w naszym otoczeniu, ale by zdobyć naszą uwagę i zasugerować pewne wybory. W obecnie rozwijającym się modelu gospodarczym coraz bardziej widoczny jest proces masowego utowarowienia intymnych aspektów ludzkiego życia. Na masową skalę rynek eksploruje obszary ludzkiej osobowości, emocji i życia intymnego[58]. Zjawisko monetyzacji

---

55 *Smartfon jest protezą naszego umysłu – Jacek Dukaj*, „Rozmowy o Przyszłości", Onet News (wideo), https://www.youtube.com/watch?v=UuEPplXAtJQ (dostęp: 19.01.2019). Prawdopodobnie J. Dukaj użył tego terminu w nawiązaniu do badania: N. Barr, G. Pennycook, J.A. Stolz, J.A. Fugelsang, *The Brain in Your Pocket: Evidence that Smartphones are Used to Supplant Thinking*, „Computers in Human Behavior" 2015, nr 48, s. 473–480.

56 Zob. szerzej: A. Clark, D. Chalmers, *The Extended Mind*, „Analysis" 1998, t. 58, nr 1, s. 7–19.

57 M. Castells, *The Rise of the Network Society. The Information Age. Economy, Society and Culture. Volume 1*, Oxford 1996, s. 17.

58 Zob. E. Illouz, *Uczucia w dobie kapitalizmu*, przekł. Z. Simbierowicz, Warszawa 2010.

uwagi starają się wyjaśnić koncepcje kapitalizmu kognitywnego[59] i ekonomii uwagi[60].

Zwiększenie możliwości pozyskiwania informacji poszerza obszary zainteresowania informacyjnego i powoduje wzrost wymagań wobec systemów przetwarzania wielkich zbiorów danych. Wielość codziennych czynności, które człowiek wykonuje w asyście lub przy pomocy urządzeń mających możliwość zbierania danych i komunikacji z użytkownikiem (jak smartfony), umożliwiła oddziaływanie w czasie rzeczywistym na jego wybory poprzez sprzężenie zwrotne systemów profilowania z algorytmami dokonującymi wyboru wyświetlanych treści w mediach społecznościowych.

Charakter rynku opartego na informacji powoduje, że te powszechnie dostępne są zazwyczaj powierzchowne, a dostawcy usług informacyjnych coraz częściej dostarczają odbiorcy gotową interpretację zamiast produktu informacyjnego, analizę dokonywaną z własnego punktu widzenia i wynikające z niej wnioski. Wykorzystanie danych surowych jest coraz bardziej skomplikowane i wymaga specjalistycznej wiedzy[61]. Analiza takich danych jest ogromnym wyzwaniem dla brokerów informacji, a podmioty projektujące systemy zbierania danych na przykład z określonej rodziny urządzeń będą coraz częściej utrudniać pracę niezależnych infobrokerów w celu choćby skłonienia ich do zakupu dedykowanego oprogramowania do analizy lub udziału w kosztownych szkoleniach. Jednak z drugiej strony analiza danych w pewnych obszarach stała się obecnie dostępna dla każdego. To generuje też wyzwania terminologiczne, gdyż coraz trudniej zakwalifikować działalność na przykład aktywistów dokonujących triangulacji danych zebranych z otwartych źródeł i zamkniętych grup dyskusyjnych, którzy następnie poddają je wielowarstwowej analizie (na przykład obraz, dźwięk, metadane, artefakty[62]) do określonego obszaru[63].

---

[59] Termin zaproponował Lorenzo Cillario: *Il capitalismo cognitivo: Saper, sfruttamento e accumulazione dopo la rivoluzione informatica*, [w:] L. Cillario i in. (red.), *Trasformazione e persistenza. Saggi sulla storicità*, Mediolan 1990. Koncepcję rozwinął m.in.: Y. Moulier Boutang, *Cognitive Capitalism*, Amsterdam 2011.

[60] M.H. Goldhaber, *The Attention Economy and the Net*, „First Monday" 1997, t. 2, nr 4.

[61] T.R. Aleksandrowicz, *Podstawy walki…*, s. 53.

[62] Wady powstające najczęściej podczas kompresji lub zmiany formatu danych. Ich analiza pozwala wykryć, czy np. zdjęcie satelitarne lub nagranie zostało poddane manipulacji.

[63] Przykładem takiej działalności jest założony przez brytyjskiego dziennikarza Eliota Higginsa portal bellingcat.com. Jedną z najbardziej znanych opublikowanych analiz jest dotycząca zestrzelenia holenderskiego samolotu pasażerskiego MH17 przez rosyjskie wojska nad Ukrainą w 2014 r. Źródło: https://www.bellingcat.com/news/uk-and-europe/2017/07/17/mh17-open-source-investigation-three-years-later/ (dostęp: 19.02.2019).

Dzięki nowym obszarom i narzędziom pozyskiwania informacji rola brokera może znacząco wzrosnąć w najbliższej przyszłości. Z jednej strony zaawansowane algorytmy będą mogły odpowiadać na coraz bardziej abstrakcyjne zapytania, ale nie oznacza to, że zastąpią człowieka, który dzięki swojej wiedzy i umiejętnościom dobierze odpowiednie narzędzia, zweryfikuje i dokona ostatecznej obróbki produktu informacyjnego. Umiejętność doboru narzędzi i zdolność do weryfikacji są już dziś kluczowymi kompetencjami. Nie sposób jednak określić precyzyjnie, jak infobrokering będzie rozwijać się w przyszłości – można założyć, że jednym z istotnych kierunków będzie ten wyznaczony przez nanotechnologie, biotechnologie, informatykę i kognitywistykę, które wspólnie podążają kierunkiem modyfikacji ludzkiego mózgu.

STRESZCZENIE

Dynamiczny rozwój technologii stwarza potrzebę uporządkowania istniejących i konceptualizacji nowych metod pozyskiwania informacji. Aktualna typologia zawarta w dokumentach doktrynalnych NATO i Armii Stanów Zjednoczonych częściowo koresponduje z możliwościami, jakie dają nowe technologie. Na uwagę zasługują również propozycje nowych dyscyplin, które w ostatnich latach pojawiły się w literaturze przedmiotu. Analizie towarzyszy refleksja na temat nowych trendów w pracy brokera informacji.

Piotr Sosnowski

SYSTEMATISATION OF CONCEPTS RELATED TO METHODS AND SOURCES OF GATHERING INFORMATION FOR THE INFOBROKERING

The dynamic development of technology causes the need to organize existing and conceptualize new methods of gathering information. Current typology contained in the doctrinal documents of NATO and the United States Army partially corresponds to the possibilities offered by new technologies. Noteworthy are also the proposals for new disciplines, which in recent years appeared in the literature. The analysis includes reflection about the new trends in the work of the information broker.

KEY WORDS: *information brokering, information gathering, information sources, intelligence collection*

Bibliografia

Aid M.M., *Measurement and Signature Intelligence*, [w:] R. Dover, M.S. Goodman, C. Hillebrand (red.), *Routledge Companion to Intelligence Studies*, Londyn 2014.

Aleksandrowicz T.R., *Podstawy walki informacyjnej*, Warszawa 2016.

Aleksandrowicz T.A., *Biały wywiad w walce z terroryzmem*, [w:] K. Liedel, P. Piasecka (red.), *Rola mediów w przeciwdziałaniu terroryzmowi*, Warszawa 2009.

Barr N., Pennycook G., Stolz J.A., Fugelsang J.A., *The Brain in Your Pocket: Evidence that Smartphones are Used to Supplant Thinking*, „Computers in Human Behavior" 2015, nr 48.

Castells M., *The Rise of the Network Society. The Information Age. Economy, Society and Culture. Volume 1*, Oxford 1996.

Ciecierski M., *Wywiad biznesowy w korporacjach transnarodowych. Teoria i praktyka*, Toruń 2009.

Cillario L., *Il capitalismo cognitivo: Saper, sfruttamento e accumulazione dopo la rivoluzione informatica*, [w:] L. Cillario i in. (red.), *Trasformazione e persistenza. Saggi sulla storicità*, Mediolan 1990.

Clark A., Chalmers D., *The Extended Mind*, „Analysis" 1998, t. 58, nr 1.

Dukaj J., *Smartfon jest protezą naszego umysłu*, „Rozmowy o Przyszłości", Onet News, (wideo), https://www.youtube.com/watch?v=UuEPplXAtJQ (dostęp: 19.01.2019).

Elvy S., *Paying for Privacy and the Personal Data Economy*, „Columbia Law Review" 2017, t. 117, nr 6.

Favarel-Garrigues G., Godefroy T., Lascoumes P., *Reluctant Partners? Banks in the Fight against Money Laundering and Terrorism Financing in France*, „Security Dialogue" 2011, nr 42(2).

Giles M., *Bounty Hunters Tracked People Secretly Using US Phone Giants Location Data*, „MIT Technology Review", 7.02.2019, https://www.technologyreview.com/the-download/612907/bounty-hunters-tracked-people-secretly-using-us-phone-giants-location-data (dostęp: 8.02.2019).

Hurley M.M., *For and from Cyberspace Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance*, „Air and Space Power Journal" 2012, nr 26(6).

Jamil G.L., Santos L.H.R., Alves M.L., Furbino L., *A Design Framework for a Market Intelligence System for Healthcare Sector: a Support Decision Tool in an Emergent Economy*, [w:] *Handbook on Research of ICTs for Social Services and Healthcare: Developments and Applications*, Hershey 2012.

Jani K.P., Soni A., *Promise and Perils of Big Data Science for Intelligence Community*, [w:] M.E. Kosal (red.), *Technology and the Intelligence Community Challenges and Advances for the 21st Century*, Cham 2018.

Liaropoulos A.N., *The Challenge of Social Media for the Intelligence Community*, „Journal of Mediterranean and Balkan Intelligence" 2013, nr 1(1).

Loper M.L., *Situational Awareness in Megacities*, [w:] M.E. Kosal (red.), *Technology and the Intelligence Community Challenges and Advances for the 21st Century*, Cham 2018.

Mercado S.C., *Sailing the Sea of OSINT in the Information Age*, „Studies in Intelligence" (CIA Journal) 2004, t. 48, nr 3.

Murch R., *A Perspective on the Strategy of Intelligence*, [w:] V. Radosavljevic, I. Banjari, G. Belojevic (red.), *Defence Against Bioterrorism. Methods for Prevention and Control*, Dordrecht 2018.

Omand D., Bartlett J., Miller C., *Introducing Social Media Intelligence (SOCMINT)*, „Intelligence and National Security" 2012, nr 27(6).

Płoszajski P., *Big Data: nowe źródło przewag i wzrostu firm*, „E-mentor" 2013, nr 3(50).

Porter M.E., *Competitive Advantage: Creating and Sustaining Superior Performance*, Nowy Jork 2008.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015.

Selding P.B. de, *Pentagon Struggles with Avalanche of Data*, SpaceNews, 29.11.2011, https://spacenews.com/pentagon-struggles-avalanche-data (dostęp: 19.10.2011).

Shane S., *These are the Ads Russia Bought on Facebook in 2016*, „The New York Times", 1.11.2017, https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html (dostęp: 19.02.2019).

Svendsen A.D.M., *Collective Intelligence* (*COLINT*), [w:] *Encyclopedia of U.S. Intelligence*, Nowy Jork 2015.

Svendsen A.D.M., *Introducing RESINT: A Missing and Undervalued „INT" in All-Source Intelligence Efforts*, „International Journal of Intelligence and CounterIntelligence" 2013, nr 26.

Vines P., Roesner F., Kohno T., *Exploring ADINT: Using Ad Targeting for Surveillance on a Budget – or – How Alice Can Buy Ads to Track Bob*, Waszyngton 2017, https://adint.cs.washington.edu/ADINT.pdf (dostęp: 15.07.2018).