Krzysztof Tylutki

Informacja masowego rażenia – OSINT w działalności wywiadowczej

Gdzie jest mądrość, którą straciliśmy w wiedzy?
Gdzie jest wiedza, którą straciliśmy w informacjach?[1]
Gdzie są informacje, które straciliśmy w bitach…

We współczesnym świecie, określanym jako cywilizacja informacyjna, surowcem strategicznym staje się informacja oceniana jako wartość stanowiąca kapitał, nie tylko intelektualny. Nie bez powodu mówi się, że ten ma władzę, kto ma wiedzę, a w węższym rozumowaniu – informacje. Należy zgodzić się z Jamesem Gleickiem, że informacja jest wszędzie, rządzi światem, jest jego krwią i paliwem[2]. Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych w 2016 r. wydało zalecenia w formie rezolucji, aby dostęp do Internetu, który należy uznać za największe źródło informacji, był traktowany na równi z prawem do życia i jako jedno z podstawowych praw człowieka[3]. Informacja staje się elementem wojny informacyjnej, współczesną bronią mającą globalny zakres rażenia, służącą do osiągnięcia przewagi nad przeciwnikiem, określonych celów strategicznych czy w końcu – dominacji w środowisku bezpieczeństwa. Glynn Harmon przyjmuje, że informacja jest rodzajem metaenergii, która porusza większe ilości energii i decyduje o żywiołowości działań podejmowanych przez człowieka[4]. Tę zależność dostrzegł generał John Shalikashvili, który stwierdził, że dopóki wiadomość o zwycięstwie nie pojawi się w źródłach otwartych, w telewizji CNN, dopóty nie uzna, że wygrał wojnę.

Pojęcie informacja jest złożone i występuje w wielu dyscyplinach naukowych. Po raz pierwszy zostało użyte pod koniec XIX wieku przez austriackiego uczonego Ludwiga Boltzmanna do określenia zmian zachodzących w procesach fizycznych. Za ojca teorii informacji uznaje się jednak amerykańskiego matematyka Claude'a E. Shannona, który uważał, że informacja to wybór możliwych opcji. Zdefiniował on jednostkę miary informacji jako **bit**, czyli taką ilość informacji, jaka jest niezbędna do dokonania wyboru między dwiema jednakowo prawdopodobnymi, wzajemnie wykluczającymi się możliwościami. Międzynarodowa norma ISO podaje, że informacja to dane,

[1] Th.S. Eliot, *Choruses from the Rock*, London 1934, https://ww.bayes.it/pdf/Choruses_FromTheRock.pdf [dostęp: 19 VI 2018] – tłum. aut.

[2] J. Gleick, *Informacja – bit, wszechświat, rewolucja*, Kraków 2012, s. 14.

[3] Zob. *Report of the Human Rights Council on its thirty-second session*, General Assembly United Nations, Human Rights Council, Thirty-second session, A/HRC/32/L.20, 14 XI 2016.

[4] Zob. G. Harmon, *The measurement of information*, „Information Processing and Management" 1984, nr 1–2.

które są przetwarzane, organizowane i skorelowane w celu nadania im znaczenia[5]. Dotyczy faktów, pojęć, przedmiotów, zdarzeń, pomysłów oraz procesów[6]. Piotr Sienkiewicz definiuje informację jako zbiór faktów, zdarzeń lub cech zawarty w wiadomości, podany w formie pozwalającej odbiorcy na ustosunkowanie się do zaistniałej sytuacji i podjęcie odpowiednich działań umysłowych lub fizycznch[7]. Informacja, jak słusznie dostrzega się w słowniku Merriam-Webster, to po prostu wiedza uzyskiwana od innych lub na studiach, przez zastosowanie obserwacji czy badań. Zgodnie z definicją *Słownika Języka Polskiego*[8] informacje to w zasadzie dane wywiadowcze. Pełne zrozumienie tego pojęcia jest możliwe dzięki wyjaśnieniu szczególnych funkcji informacji:

- **ilustrującej** – opisującej rzeczywistość (informacja jest jej obrazem);
- **decyzyjnej** – motywującej do działania;
- **sterującej** – budującej systemy informatyczne, bazy wiedzy stanowiące podstawy planowania i podejmowania optymalnych i racjonalnych decyzji;
- **progresywnej** – rozwijającej posiadaną wiedzę;
- **kapitałotwórczej** – uzależniającej od środków finansowych, urządzeń, ludzi oraz ich wiedzy;
- **kulturotwórczej** – zaspokajającej duchowe potrzeby człowieka;
- **komunikacyjnej** – umożliwiającej uczestnictwo w życiu społecznym;
- **integracyjnej** – sprzyjającej rozwojowi relacji międzyludzkich;
- **ideologicznej** – rozwijającej świadomość udziału społeczeństwa w życiu publicznym państwa;
- **opiniotwórczej** – kształtującej poglądy, opinię publiczną na dany temat[9];
- **informacyjnej** – dostarczającej niezbędnej wiedzy, dzięki czemu poprawia się efektywność pracy analitycznej;
- **koordynacyjnej** – porządkującej i harmonizującej realizację równoległych działań;
- **kontrolnej** – weryfikującej oraz oceniającej jakość i spójność danych, ich funkcjonalność – zgodnie z ustalonymi zasadami bezpieczeństwa.

Na podstawie powyższego zestawienia można uznać, że informacja to po prostu towar, przedmiot wyprodukowany jako rezultat ludzkiej pracy, który ma swoją cenę i odbiorcę. Informacja jest elementem składowym wiedzy człowieka oraz głównym czynnikiem uwzględnianym przy podejmowaniu decyzji i organizowaniu procesów w sferze produkcyjnej. Przyczynia się więc do wytwarzania określonego produktu analitycznego[10]. Aby ten produkt był wartościowy, informacja musi być:

---

[5] ISO 22320:2011, *Social security – Emergency management – Requirements for incident response*, November 2011.

[6] ISO 2382-1:1993, *Information technology – Vocabulary*, Part 1: *Fundamental terms*, November 1993.

[7] P. Sienkiewicz, *10 wykładów*, Warszawa 2005, s. 62.

[8] *Słownik Języka Polskiego*, t. 1–3, M. Szymczak (red.), Warszawa 1978–1981, s. 863.

[9] Zob. B. Stefanowicz, *Informacja. Wiedza. Mądrość*, seria: Biblioteka Wiadomości Statystycznych, t. 66, Warszawa 2013, s. 42–45.

[10] Tamże, s. 36.

- **dokładna** – musi w sposób wiarygodny odzwierciedlać rzeczywistość, tak aby stanowiła dla produktu analitycznego realną wartość;
- **aktualna** – dostępna w czasie umożliwiającym właściwe działanie decydenta;
- **kompletna** – musi dostarczać decydentowi wszelkich potrzebnych mu faktów i szczegółów, przedstawiać pełny obraz sytuacji, bez jego zniekształcania;
- **istotna** – przydatna dla decydenta w realizacji konkretnych potrzeb zaistniałych w szczególnych warunkach.

Każde źródło informacji ma właściwe sobie cechy i jest postrzegane indywidualnie przez poszczególne osoby. Informacje, które można znaleźć w internecie, są charakteryzowane jako godne zaufania i dostępne w dowolnym czasie, informacje telewizyjne jako bezstronne i bieżące, a informacje prasowe jako wyważone i rzetelne[11]. Z badań Krystyny Polańskiej wynika, że najważniejszym elementem przy ocenie wiarygodności danej informacji są: zaufanie do źródła, które je podaje, aktualność, logiczne powiązanie informacji z innymi faktami lub wiadomościami oraz przekazywanie takiej samej informacji przez kilka niezależnych źródeł[12]. Oprócz informacji wiarygodnych, rzetelnych i aktualnych pojawiają się także informacje mylące, czasem nawet świadomie wprowadzające w błąd. Należy pamiętać, że ilość informacji może nie mieć nic wspólnego z ich wiarygodnością, a wręcz przeciwnie – zdarza się, że wiele z nich jest nieprawdziwych, dezinformujących[13], przez co zmniejszają swoją wartość. Widoczna jest tutaj manipulacja informacją, która jest wyrażana w jej ocenach, selekcji i doborze, co jest spowodowane tym, że dzięki specyfice Web 2.0 informacje mogą być zamieszczane przez każdego uczestnika wirtualnej społeczności. Anonimowym edytorom Wikipedii zdarzyło się uśmiercić żyjących: senatora Teda Kennedy'ego i polityka Roberta Byrda. Z kolei artykuł o wojnie domowej w Syrii, który ukazał się w 2012 r., ze względu na dynamicznie zmieniającą się sytuację w regionie był ponad 7,5 tys. razy edytowany przez użytkowników Wikipedii, co utrudniało rzetelną ocenę konfliktu. Nie jest to jednak rekord, życiorys prezydenta USA Georga W. Busha był w 2005 r. aktualizowany ponad 20 tys. razy.

Ze względu na czas uzyskania i możliwości wykorzystania informacji w procesie decyzyjnym można wyróżnić:

- **informację relacjonującą** – opisującą zdarzenie, które zaistniało lub dzieje się w chwili obecnej;
- **informację wyprzedzającą** – ukazującą planowane czynności, działania, które

[11] K. Stankiewicz, *Wpływ Internetu na percepcję wiarygodności informacji*, w: L. Haber, *Społeczeństwo informacyjne. Wizja czy rzeczywistość?*, Kraków 2004, s. 409.

[12] Zob. K. Polańska, *Informacja, jej wiarygodność i co z nich dla nas wynika*, w: *Informacja – dobra lub zła nowina*, A. Szewczyk (red.), Szczecin 2004.

[13] Vladimir Volkoff definiuje dezinformację jako czynność podejmowaną z zaangażowaniem wielu środków, powadzoną w sposób systematyczny i fachowy, zawsze za pośrednictwem mass mediów i adresowaną do opinii publicznej. Dezinformacja ma na celu realizację konsekwentnego programu, zmierzającego do zastąpienia w świadomości, a przede wszystkim w podświadomości, mas będących przedmiotem tych działań poglądów uznanych za niekorzystne dla dezinformatora takimi, które uważa za korzystne dla siebie, zob. V. Volkoff, *Dezinformacja: oręż wojny*, Warszawa 1991, s. 6–8.

są w obszarze zainteresowania; jest to najcenniejsza informacja w procesie podejmowania decyzji;

- **informację weryfikującą** – potwierdzającą posiadaną wiedzę na dany temat, zjawisko, zdarzenie.

Zapotrzebowanie na informacje nie jest wartością stałą, w zależności od sytuacji wygląda różnie, jego zróżnicowanie jest szczególnie widoczne na różnych poziomach podejmowania decyzji, począwszy od taktycznego czy operacyjnego, po strategiczny. Im wyższy szczebel zarządzania, tym większa koncentracja informacji i szerszy ich zakres tematyczny. Na niższych poziomach kierowania informacje powinny być bardziej szczegółowe i mieć węższy zakres tematyczny. Taki rozkład informacji jest nazywany „odwróconą piramidą informacyjną". Oznacza on, że piramida informacyjna charakteryzująca ilość, szczegółowość i zakres informacji jest odwrotnością piramidy strukturalnej, opisującej obowiązki, uprawnienia i odpowiedzialności decydentów[14].

Ludzkość nieustannie wytwarza coraz więcej informacji. Świat cyfrowy, w którym żyjemy – zdaniem zastępcy dyrektora CIA Andrew Hallmana – podważa zasadę konspiracji działań wywiadowczych. Powoduje, że coraz trudniej jest utrzymać w tajemnicy oficera pod przykryciem, kiedy każdy ma w kieszeni studio telewizyjne[15]. Dynamika wzrostu zbioru danych Big Data[16], tj. zbioru danych o dużej objętości, różnorodności, zmienności i wartości – nieprzerwanie postępuje (od 40 do 60 proc. w ciągu roku). Zbiór osiąga rozmiary, których analiza jest nie lada wyzwaniem dla analityków. W połowie lat 80. XX w., gdy ośrodki naukowe i uniwersytety zaczęły doceniać możliwości płynące z Internetu, jedynie 6 proc. materiałów było zdigitalizowanych. Obecnie już niemal 99 proc. dorobku kultury i życia ma postać cyfrową. Ocenia się, że w 1992 r. powstawało na świecie 100 gigabajtów (GB)[17] danych dziennie, w 1997 r.tyle samo wytwarzano już w godzinę, a w 2002 r. – w ciągu sekundy. Dziś uznaje się, że co sekundę zostaje wytworzonych 50 tys. GB danych. Według szacunków w 2017 r. cyfrowy wszechświat osiągnął rozmiary 16 zettabajtów (ZB), a według prognoz Oracle Corporation do 2020 r. ludzkość wygeneruje w sieci ponad 45 ZB danych. Oznacza to, że na jednego mieszkańca kuli

[14] B. Nogalski, B.M. Surawski, *Informacja strategiczna i jej rola w zarządzaniu przedsiębiorstwem*, w: *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystywanie i ochrona (wybrane problemy teorii i praktyki)*, R. Borowiecki, M. Kwieciński (red.), Kraków 2003, s. 205–206.

[15] P. Tucker, *Meet the Man Reinventing CIA for the Big Data Era*, https://www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453/ [dostęp: 3 I 2018].

[16] Big Data definiuje się za pomocą czterech charakterystycznych czynników opisujących zbiory informacji, zwanych 4 V, tj.: **Volume** (ilość danych), **Variety** (różnorodność analizowanych danych i informacji), **Velocity** (przetwarzanie danych w czasie rzeczywistym) i **Value** (wartość, jaką możemy uzyskać z połączenia wszystkich poprzednio wymienionych czynników wspomagających proces analityczny i decyzyjny). Zob. T. Słoniewski, *Od BI do „Big Data*", w: *Nowa twarz Business Intelligence*, R. Jesionek (red.), http://it-manager.pl/wp-content/uploads/Nowa-twarz-BI1.pdf, s. 8–10, [dostęp: 7 V 2018].

[17] Jednostka używana w informatyce oznaczająca miliard (10^9) bajtów. W tekście występują jednostki używane w informatyce: terabajt, TB (10^{12}), petabajt, PB (10^{15}), eksabajt, EB (10^{18}) i zettabajt, ZB (10^{21}) – przyp. red.

ziemskiej przypadnie ponad 5,2 GB danych. Z kolei The Digital Universe – IDC szacuje, że w 2020 r. zostanie wytworzonych 44–47 ZB danych, a prawie 40 proc. informacji w świecie cyfrowym będzie dostępnych w *cloud computing*[18]. Podaje się ponadto, że w 2021 r. zarządzanie danymi wzrośnie o 50 proc. w stosunku do 2011 r.[19] Obliczono, że do 2025 r. zostanie wygenerowanych 163 ZB informacji.

Ocenia się, że ilość informacji cyfrowych wytworzonych do 2007 r. miała wielkość 281 EB, która na przestrzeni kilku lat nieprzerwanie rosła, i w 2011 r. wyniosła w przybliżeniu 1,8 ZB. Do takich wniosków doszli autorzy raportu[20] opublikowanego w 2014 r. przez Gabinet Prezydenta Stanów Zjednoczonych. W kategoriach ilościowych taka wielkość informacji zapełniłaby 57,5 mld urządzeń iPad z pamięcią 32 GB. Obrazując o zjawisko, można je porównać do zbudowania Wielkiego Muru Chińskiego o dwukrotnie większej średniej wysokości niż oryginał. Można również znaleźć informacje, że w 2011 r. w skali globalnej wytworzono 20 mld razy więcej informacji, czyli 988 EB, niż wszystko, co do tej pory napisano w historii ludzkości[21]. Jest to tyle informacji, ile obecnie obywatel rozwiniętego państwa ma do dyspozycji w ciągu jednej godziny, a dwa pokolenia wstecz – przez całe swoje życie. W 2013 r. wygenerowano już 4 ZB informacji w skali światowej. Ta liczba odpowiada sumie zdjęć zrobionych co sekundę przez każdego mieszkańca Stanów Zjednoczonych przez ponad cztery miesiące życia[22]. Dwa lata później ich wielkość wzrosła do 12 ZB. Amerykanie przeprowadzili badania, które pozwoliły wyliczyć, że w 2008 r. ludzkość wykorzystała średnio 34 GB informacji i 100,500 tys. słów dziennie. Około 35 proc. z nich pochodziło z TV, w tym 10 proc. z filmów, a 55 proc. z gier komputerowych. W stosunku do lat 80. XX w. wykorzystanie słów wzrosło o 140 proc., natomiast przyrost informacji cyfrowych zwiększył się o 350 proc. W 2008 r. media wykorzystały łącznie 3,6 ZB informacji i 1,080 trylionów (czyli ok. 1 EB) słów dziennie[23].

Tempo, w jakim następuje przyrost danych, wynika z potrzeby powszechnej komunikacji i rozwoju obszaru zwanego Internetem rzeczy (ang. *Internet of Things*, IoT), w którego zakresie coraz więcej urządzeń będzie gromadziło i przetwarzało dane w Internecie. W ciągu kilku lat ludzkość czeka eksplozja danych. Sami użytkownicy również uczestniczą w powielaniu informacji, kopiując wszelkiego rodzaju treści i komentarze oraz kwalifikując je jako kolejne, wtórne, źródło in-

[18] Czyli w tzw. chmurze. IBM definiuje to zjawisko jako model wykorzystywania i styl przetwarzania, w którym dane i zasoby IT są dostarczane w formie usług.

[19] Zob. J. Gantz, D. Reinsel, *Extracting Value from Chaos*, w: *IDC analyze the future,* https://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf [dostęp: 4 VI 2018].

[20] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, The White House, Washington DC, May 2014, s. 7–8; informacje podane w raporcie pochodzą z publikacji: J. Gantz, D. Reinsel, *Extracting Value*…; M. Meeker, L. Yu, *Internet Trends*, Washington 2013.

[21] Zob. M. Karnowski, E. Mistewicz, *Anatomia władzy*, Warszawa 2010, s. 114.

[22] *Big Data: Seizing Opportunities*…, s. 8.

[23] R. Bohn, J. Short, *Measuring Consumer Information*, „International Journal of Communication" 2012, nr 6, s. 980–1000.

formacji. Jednocześnie nie podają źródła pierwotnego. To zjawisko jest nazywane „efektem echa" (ang. *echo effect*).

Jak zauważył noblista Herbert Simon, informacja skupia uwagę tych, którzy ją przyjmują. Może się przy tym pojawić stan napięcia, tzw. dysonans poznawczy, jeśli do odbiorcy dotrą informacje niezgodne z jego poglądami czy przekonaniami. Powoduje on, że te informacje się ignoruje, przypisuje się im mniejszą wagę lub je zniekształca. Każdy ma inny poziom absorbowania informacji, zależny w dużym stopniu od ilości i jakości informacji apriorycznych[24]. Z czasem pojawia się syndrom zmęczenia, nazwany z języka angielskiego *attention crash*, który ma związek nie z brakiem umiejętnej selekcji prostych komunikatów, a z ich zrozumieniem. J. Gleick nazywa ten czynnik *Devil of Information Overload*, czyli pojawiającym się natłokiem informacji (albo: *To much information*, TMI)[25]. Dzieje się tak również dlatego, że hipokamp[26], czyli „dysk twardy" ludzkiego mózgu, ma swoje biologiczne ograniczenia. W 1986 r. Thomas K. Landauer w swoich pracach zakładał, że mózg człowieka jest w stanie przechować ok. 11 TB informacji[27]. Według współczesnych badań ekspertów ze StorageCraft mózg człowieka może zapisać od 100 TB do 2,5 PB danych. Dla porównania, gdyby „ludzki dysk twardy" pracował jak cyfrowy rejestrator wideo w telewizorze, to ta wielkość wystarczyłaby do przechowania 3 mln godzin filmów. Aby wykorzystać całą pamięć, należałoby nieprzerwanie przez ponad 300 lat nie wyłączać telewizora. Natomiast badania amerykańskich uczonych pokazują, że biologiczny „komputer" człowieka jest w stanie przechować nie więcej niż około 1 PB danych. Według badań neurologów przeprowadzonych w ostatniej dekadzie przeciętny człowiek ma ponad 30 tys. myśli dziennie.

Nadmiar informacji sprawia ludziom trudności zarówno z ich przetworzeniem, jak i zrozumieniem, przez co przyczynia się do formułowania błędnych ocen. Dlatego trudno jest wybrać odpowiedniego analityka do danego zadania. Ogrom informacji przekazywanych przez pułkownika radzieckiego wywiadu wojskowego (GRU) Olega Pieńkowskiego, który podjął współpracę z Zachodem, spowodował, że Amerykanie (CIA) i Brytyjczycy (MI6) musieli zaangażować łącznie 30 tłumaczy i analityków[28]. Również niedokładny zapis rozmów oficerów CIA z agentem KGB Jurijem Iwanowiczem Nosenką, oferującym pomoc Zachodowi, spowodował, że został on uznany za kłamcę i wykluczony jako potencjalne, cenne źródło informacji. Wnioski zawarte w dokumencie analitycznym nie pozwoliły na dokonanie obiektywnej oceny radzieckiego kapitana. Większość jego zeznań została spisana na podstawie zapamiętanych wypowiedzi, które w połączeniu z brakami lingwistycznymi badających były inter-

[24] S.E. Zločevskij i in., *Informacja w badaniach naukowych*, Warszawa 1972, s. 231.

[25] J. Gleick, *Informacja – bit, wszechświat*…, s. 16.

[26] Element układu limbicznego u człowieka odpowiedzialny za pamięć, odgrywa główną rolę przy przenoszeniu informacji w mózgu, za: https://pl.wikipedia.org/wiki/Hipokamp [dostęp: 11 VI 2018] – przyp. red.

[27] T.K. Landauer, *How Much do People Remember? Some Estimates of the Quantity of Learned Information in Long-Term Memory*, „Cognitive Science" 1986, nr 10, s. 477–493.

[28] J. Larecki, *W kręgu tajemnic wywiadu*, Warszawa 2007, s. 157–158.

pretowane przez Amerykanów po macoszemu. Zniekształcono nazwę uczelni, której był absolwentem, i zamiast szkoły średniej marynarki wojennej im. gen. Frunzego, sowieckiego bohatera wojennego, wpisali, że ukończył Akademię Wojskową im. Frunzego, czyli sowieckie West Point. Po przeanalizowaniu obszernych akt archiwum CIA jej były funkcjonariusz John L. Hart stwierdził, że badania i analizy kontrwywiadu były tak długie i zawiłe, że niewielu przełożonych miało czas na przeczytanie i przeanalizowanie uzasadnienia dotyczącego rzekomej dwulicowości Nosenki[29]. Generał Robert Kehler, szef Zintegrowanego Dowództwa Operacyjnego Departamentu Obrony Stanów Zjednoczonych (United States Strategic Command), po latach doświadczeń dostrzegł, że Pentagon tonie w zalewie danych wywiadowczych. Coraz sprawniejsze i liczniejsze satelity zwiadowcze dają amerykańskiemu wywiadowi tyle informacji, że analitycy nie są w stanie ich opracowywać. Ilość danych zwiększyła się w ciągu pięciu lat o 1500 proc., a zdolności ich przetwarzania tylko o 30 proc.[30] Do takich samych wniosków doszedł funkcjonariusz NSA William Binney, który dodał, że gromadzenie przypadkowych informacji sprawia, że funkcjonariusze obciążeni nadmierną ilością danych zarzucili analizę kierunkową na rzecz prostego przeszukiwania baz danych po słowach kluczowych. To daje wiele nic nieznaczących „trafień" zamiast wiedzy o istotnych powiązaniach między tymi informacjami[31]. Być może to było powodem zwłoki Amerykańskiego Urzędu Imigracyjnego w poinformowaniu szkoły lotniczej Huffman Aviation International w Venice na Florydzie, że Mohammed Atta i Marwan Alshehi, dwaj późniejsi zamachowcy na World Trade Center, dostali wizy studenckie. Ta informacja dotarła do szkoły dopiero sześć miesięcy po atakach na WTC. Potwierdzeniem tych wniosków jest to, że 10 września 2001 r. NSA przechwyciła dwie informacje w języku arabskim, w których była mowa o tym, co miało się stać następnego dnia. Dopiero jakiś czas po zamachu na WTC informacje, o których mowa, zostały przetłumaczone. Ponadto w okresie letnim w 2001 r., kilka miesięcy przed 11 września, Osama bin Laden wraz ze swoimi dowódcami udzielił obszernego wywiadu dla Centrum Mediów Bliskiego Wschodu, w którym padły ogólne wskazówki dotyczące planowanych na dużą skalę ataków na amerykańskie obiekty[32]. Niektórzy eksperci szacują, że od 50 do 80 proc. informacji będących w kręgu zainteresowań służb specjalnych krajów zachodnich nie jest publikowanych w jęz. angielskim[33].

---

[29] J.L. Hart, *Walka wywiadów. Rosjanie w CIA*, Warszawa 2003, s. 155.

[30] T. Costlow*, Kehler raises trial balloon: Put STRATCOM in charge of all GEOINT PED*, http://defensesystems.com/articles/2011/10/19/geoint-kehler-stratcom-geospatial intelligence.aspx [dostęp: 2 V 2018].

[31] R. Koerner, *William Binney: NSA Claim Not to Be Mining Content Is an "Outright Lie"*, https://www.huffingtonpost.com/robin-koerner/nsa-whisteblower-nsa-clai_b_7837806.html [dostęp: 4 V 2018].

[32] P. Bergen, *Why U.S. can't find Osama bin Laden*, http://edition.cnn.com/2010/OPINION/10/19/bergen.finding.bin.laden/ [dostęp: 2 V 2018].

[33] M.M. Lowenthal, *Open Source Intelligence: New Myths, New Realitties*, w: *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, R.Z. George, R.D. Kline (eds.), Lanham 2006, s. 277.

Informacja to potęga wtedy, gdy może być dostępna tam, gdzie jest potrzebna, temu, komu jest potrzebna, i w celu, w jakim jest potrzebna. Natomiast mankamentem jest zbyt duża ilość informacji nieuporządkowanych. Im większe sukcesy osiąga się w gromadzeniu danych, tym bardziej zaczyna się pływać w ich morzu. David Foster Wallace określa to zjawisko mianem „tsunami dostępnych faktów, kontekstów i perspektyw"[34]. W wyniku operacji przeprowadzonej przez CIA na pograniczu dwóch stref okupacyjnych w Berlinie w latach 1954–1955 Amerykanie zarejestrowali 6 mln godzin ruchu telefonicznego oraz 40 tys. godzin rozmów telefonicznych na linii Moskwa–Karlshorst (w Karlshorst mieściła się główna rezydentura KGB działającego na terenie NRD) i Moskwa–Wünsdorf (w Wünsdorf, zgodnie z dostępną literaturą, znajdowała się kwatera główna wojsk radzieckich). Zgromadzone informacje tłumaczono i analizowano jeszcze przez kolejne dwa lata po zakończonych działaniach. Mimo upływu czasu z nadmiarem informacji borykały się następne służby. Kiedy w 1989 r. Niemiecka Republika Demokratyczna przestawała istnieć, Ministerstwo Bezpieczeństwa Państwowego, znane powszechnie jako Stasi (Ministerium für Staatssicherheit), analizowało materiał pochodzący z podsłuchów rozmów telefonicznych (z kontroli operacyjnej) zebrany w połowie lat 80. XX w.[35]

Podczas gromadzenia informacji ogólnodostępnych łatwo stracić orientację, zwłaszcza jeśli ich źródłem jest Internet, którego rozmiary Eric Schmidt oszacował na 5 mln TB. Systematycznie rosnąca liczba wniosków wizowych składana przez cudzoziemców w urzędach ds. imigracyjnych powoduje chaos przy weryfikacji rzeczywistego powodu, z jakiego decydują się oni na zmianę kraju pobytu. Procedura ma charakter administracyjny i w głównej mierze jest skupiona na kompletowaniu dokumentacji dzięki prowadzeniu wywiadu środowiskowego oraz sprawdzeniu przeszłości (tzw. ang. *background checks*). Brak danych o cudzoziemcu lub pobieżna weryfikacja otwartych źródeł informacji dokonana przez służby imigracyjne i FBI uczestniczące w ocenie pobytu takiej osoby pod kątem zagrożeń bezpieczeństwa wewnętrznego kraju pozwoliły na osiedlenie się w Stanach Zjednoczonych Tashfeen Malik. Emigrantka z Pakistanu od kilku lat otwarcie deklarowała na portalu społecznościowym poparcie dla dżihadu oraz głosiła antyamerykańskie hasła. W dniu 2 grudnia 2015 r. wraz z mężem dokonała ataku w ośrodku pomocy niepełnosprawnym w San Bernardino w Kalifornii, w którym zginęło 14 osób, a ponad 20 zostało rannych[36].

Dziewięćdziesiąt procent informacji wywiadowczych pochodzi z otwartych źródeł. Pozostałe dziesięć, które uzyskuje się w sposób bardziej widowiskowy, z utajnionych. Prawdziwym bohaterem pracy wywiadowczej jest Sherlock Holmes, a nie James Bond [37].

---

[34] J. Gleick, *Informacja – bit, wszechświat*…, s. 374.

[35] P. Żuk, *Demokracja pod kontrolą – czyli podsłuch non stop*, http://www.tygodnikprzeglad.pl/demokracja-pod-kontrola-czyli-podsluch-non-stop/ [dostęp: 15 VI 2018].

[36] M. Apuzzo, M.S. Schmidt, J. Preston, *U.S. Visa Process Missed San Bernardino Wife's Zealotry on Social Media*, http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html [dostęp: 6 V 2018].

[37] Cytat za gen. S.V. Wilsonem, dyrektorem Agencji Wywiadu Obronnego USA.

Możliwości płynące z OSINT-u (ang. *open source intelligence*[38]) – powszechnie rozumianego jako tzw. biały wywiad, czyli ogół publicznie dostępnych, jawnych informacji, które każdy w sposób legalny może pozyskać – były doceniane przez ludzkość od zarania dziejów, od czasów pojawienia się zrębów pierwotnej formy komunikacji[39]. Historia wykorzystywania informacji powszechnie dostępnych sięga okresu powstania wywiadu jako narzędzia gromadzenia istotnej wiedzy w celu wspierania procesu decyzyjnego władcy (rządu) w odniesieniu do bezpieczeństwa narodowego i obronności państwa. Środki wykorzystywane do pozyskiwania danych z otwartych źródeł[40] ewoluowały wraz z postępem technologicznym oraz wydarzeniami, a „National Geographic"[41] słusznie uznał je za te, które zmieniły, a nawet zrewolucjonizowały świat. Dostęp do nich zapoczątkowały i upowszechniły środki masowego przekazu[42] – prasa, radio i telewizja. Jednak największe piętno odcisnęła rewolucja komputerowa oraz internetowa umożliwiająca rozwój sieci, a zwłaszcza mediów społecznościowych[43].

[38] OSINT został zdefiniowany m.in. przez Dyrektora Wywiadu Narodowego USA (Director of National Intelligence, DNI) w: *National Defense Authorization Act for Fiscal Lear 2014* [Public Law 113–66 (26 XII 2013 r.)] oraz Wspólnotę Wywiadów Stanów Zjednoczonych (Intelligence Community), w: *Intelligence Community Directive Number 301*, National Open Source Enterprise 2006.

[39] Można wyróżnić trzy etapy analizowania otwartych źródeł informacji określone jako: ***Open Source Data*** (**OSD**) – **dane jawnoźródłowe**, będące niejako w „stanie surowym", pochodzące z pierwotnego źródła w postaci drukowanej, cyfrowej, mające formę zdjęć, nagrań, obrazów satelitarnych itp; ***Open Source Information*** (**OSIF**) – **informacja jawnoźródłowa**, szeroko opracowana, zebrana w jeden dokument, zredagowana, zweryfikowana, poddana filtracji z uwagi na jej prezentację (np. prasa, książki, publikacje, raporty); ***Validated Open Source Intelligence*** (**OSINT-V**) – **zweryfikowany biały wywiad** mający wysoki stopień wiarygodności dzięki analizie informacji pochodzących ze źródeł niejawnych, przeprowadzonej przez analityka. OSINT można rozszerzyć o następujące terminy: ***Open Source Acquisition*** – **pozyskwanie informacji jawnoźródłowej** z dostępnych źródeł otwartych, które wcześniej zostały zgromadzone i przekazane przez badacza; ***Open Source*** – **źródło otwarte**, którym może być zarówno pojedyncza osoba, jak i grupa dostarczająca informacje, sama zaś informacja oraz relacja łącząca ją z podmiotem, w którego kręgu zainteresowań leży jej uzyskanie, nie są objęte klauzulą tajności. Dane ze źródeł otwartych mogą być publicznie dostępne, ale nie wszystkie upublicznione informacje są źródłem otwartym. Pojęcie źródło otwarte odnosi się do środków publicznie dostępnych i nie należy go ograniczać tylko do osób fizycznych. ***Publicly available information*** – **informacje ogólnodostępne**, dane, fakty, instrukcje, materiały opublikowane bądź transmitowane do ogólnego użytku publicznego, prezentowane na żądanie każdego obywatela, uzyskane dzięki obserwacji, usłyszane bądź przekazane na spotkaniach otwartych dla ogółu społeczeństwa.

[40] W ramach OSINT-u można wyróżnić dwa obszary wywiadowcze: 1) ***Social Media Intelligence*** (**SOCMINT**) – skupiony na rozpoznaniu i monitorowaniu profili użytkowników portali społecznościowych i publikowanych przez nich postów oraz zbieraniu informacji z otwartych i zamkniętych grup społecznych, 2) ***Web Intelligence*** (**WEBINT**) – eksplorację danych oraz wyszukiwanie i magazynowanie informacji w Internecie.

[41] Zob. *100 Events That Changed the World*, „National Geographic" 2015, Special Issue.

[42] Radio potrzebowało 30 lat, aby zyskać 50 mln słuchaczy, telewizja 14 lat, aby zgromadzić taką liczbę widzów, Interent natomiast pozyskał taką liczbę użytkowników w ciągu zaledwie czterech lat.

[43] Zdefiniowane przez Howarda Rheingolda pierwotnie jako społeczności wirtualne, czyli

Biały wywiad jest prowadzony zarówno przez struktury wojskowe, jak i cywilne[44]. Jest domeną głównie instytucji państwowych odpowiedzialnych za zapewnianie bezpieczeństwa, ale coraz częściej jest „doceniany" i przez sektor prywatny, i organizacje terrorystyczne. W celu dokładniejszego zrozumienia istoty białego wywiadu należy określić jego role[45]. Biały wywiad:

- stanowi podstawę informacyjną na każdym etapie prowadzonych działań. Dostarcza tła przekazywanych informacji, które w zależności od kontekstu, m.in. społecznego, kulturowego, politycznego, mają różne znaczenie;
- odpowiada na wymagania wywiadowcze oraz informacyjne stawiane przez instytucje, bez konieczności wsparcia specjalistów czy techniki operacyjnej (metod niejawnych);
- pogłębia i weryfikuje dotychczas uzyskaną wiedzę;
- umożliwia decydentowi korzystanie ze wszystkich dostępnych źródeł informacji. przy podejmowaniu decyzji.

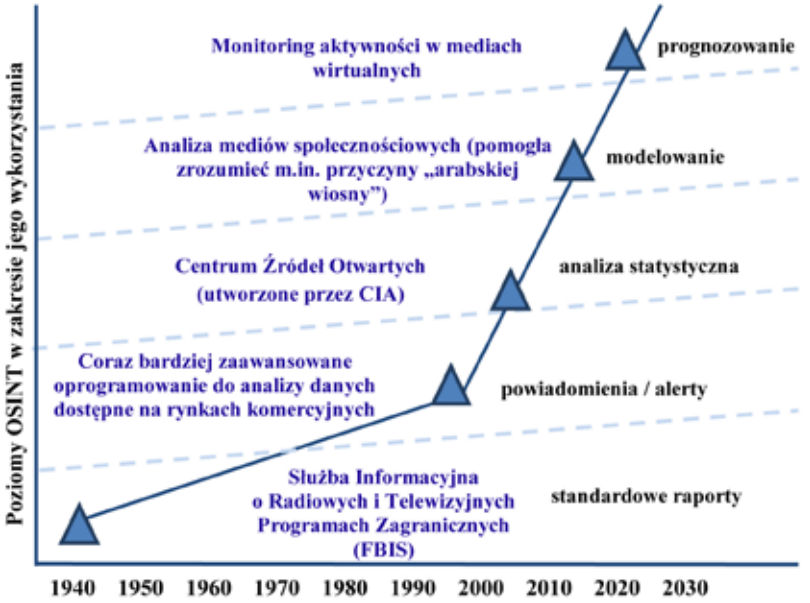
Historia wykorzystywania OSINT-u wiąże się w zasadzie z historią wywiadu Stanów Zjednoczonych. Ten typ wykorzystywania informacji był jednym z głównych źródeł informacji na temat zdolności wojskowych przeciwników oraz ich zamiarów politycznych (wczesne ostrzeganie i prognozowanie zagrożeń). Amerykanie byli pionierami w gromadzeniu danych dzięki rozwojowi zdolności samodzielnego monitorowania, filtrowania, tłumaczenia oraz archiwizacji wiadomości pochodzących z zagranicznych mediów. W monitorowaniu otwartych źródeł informacji, które w początkowej fazie oznaczało śledzenie doniesień prasowych, sektor komercyjny wyprzedzał działania rządowe. Przed profesjonalizacją i formalną instytucjonalizacją wywiadu jako niezbędnego elementu narodowego aparatu bezpieczeństwa w drugiej połowie XX wieku zbieranie i analizowanie otwartych źródeł przez rząd ewoluowało od procesu mało uporządkowanego do czynności o znaczeniu strategicznym, wymagających użycia określonych metod i narzędzi. Na schemacie przedstawiono kierunek zmian OSINT-u oraz wykorzystywanie jego głównych obszarów, pozwalające na opracowanie odpowiedniego produktu analitycznego w działalności wywiadowczej Stanów Zjednoczonych na przestrzeni wieków XX i XXI.

---

grupy ludzi, którzy mogą lub nie mogą spotkać się twarzą w twarz i którzy wymieniają myśli (idee) za pośrednictwem klawiatury i sieci. Ich cechą charakterystyczną jest to, że każdy ich uczestnik może stać się jednostką aktywną, przywódczą czy destrukcyjną. Nieobowiązująca zasada więzi sprzyja wolności słowa, debacie oraz ekshibicjonizmowi życia prywatnego czy zawodowego na forum publicznym. Zob. H. Rheingold, *The Virtual Community. Homesteading on the Electronic Frontier*, New York 1994.

[44] Poza tradycyjnymi otwartymi źródłami informacji należą do nich także: komercyjne bazy danych, takie jak informatory gospodarcze, statystyczne, publiczne rejestry, tzw. szara literatura, czyli raporty robocze, nieoficjalne dokumenty rządowe, przedruki, studia i badania rynkowe, raporty badawcze, indywidualni eksperci, wykładowcy akademiccy, literatura naukowa, materiały z konferencji i sympozjów, opracowania ośrodków badawczych.

[45] *Open Source Intelligence*, Headquarters, Department of Army, Army Techniques Publication, ATP 2-22.9, Washington, 2012, s. 2-2.



Schemat. Ewolucja wykorzystania możliwości OSINT.

Źródło: Opracowanie własne na podstawie: *Disruptive innovation*. *Case study: Intelligence – Open-source data analytics*, Washington, DC 2012, s. 3.

Wartość źródeł otwartych została dostrzeżona przez Georga Washingtona już w XVIII wieku podczas rewolucji amerykańskiej. Czerpał on aktualne informacje o sile brytyjskich wojsk i aktywności szpiegów z publikacji prasowych oraz wiadomości ogólnie dostępnych[46]. Kilkadziesiąt lat później, w 1808 r., brytyjski książę Wellington w bitwie prowadzonej przeciwko armii Napoleona na Półwyspie Iberyjskim zalecał swoim generałom lekturę codziennej prasy, m.in. dziennika „The Times", w której szeroko opisywano sposób organizacji nowych struktur francuskiej piechoty[47]. W 1863 r. w czasie kampanii gettysburskiej wywiad generała Roberta Lee monitorował ruchy wojsk Unii na północy dzięki śledzeniu doniesień prasowych[48]. W latach 1899–1902 podczas wojny filipińskiej amerykańscy stratedzy wojskowi opierali się na raportach wywiadowczych, które w zasadzie były kopiami artykułów z encyklopedii[49]. W czasie dwóch wojen światowych książki i gazety były źródłem cennych informacji wykorzystywanych przez wywiad wojskowy. Podczas ofensywy we Francji wojska generała

[46] *A Look Back … George Washington: America's First Military Intelligence Director*, https://www.cia.gov/news-information/featured-story-archive/2007-featured-storyarchive/george-washington.html [dostęp: 5 V 2018].

[47] S.D. Gibson, *Exploring the Role and Value of Open Source Intelligence*, w: *Open Source Intelligence in Twenty-First Century*, Ch. Hobbes, D. Sailsbury (eds.), New York 2014, s. 13.

[48] E.B. Coddington, *The Gettysburg Campaign: A Study in Command*, New York 1968, s. 19.

[49] B. McAllister Linn, *The Philippine War: 1899–1902*, Lawrence 2000.

George'a Pattona w celu rozpoznania geoprzestrzennego używały map Michelin dostępnych na stacjach benzynowych[50].

W 1939 r. brytyjski rząd zwrócił się do BBC o utworzenie komercyjnego serwisu podsumowującego zagraniczną prasę i audycje radiowe pod nazwą *Digest of Foreign Broadcasts* (*Przegląd Audycji Zagranicznych*), który w późniejszym czasie był nazywany *Summary of World Broadcasts* (*Podsumowanie Wiadomości ze Świata*), a obecnie jest emitowany jako *BBC Monitoring*. W podręczniku BBC z 1940 r. wskazano, że powstanie serwisu miało na celu stworzenie (…) *nowoczesnej Wieży Babel, gdzie słuchano głosów zarówno przyjaciół, jak i wrogów*[51]. W połowie 1943 r. BBC monitorowało dziennie 1,25 mln transmisji. Formalne partnerstwo między BBC i jego amerykańskim odpowiednikiem ustanowiono na przełomie lat 1947/1948 na podstawie porozumienia o pełnej wymianie informacji. W 1948 r. z Lotniczej Jednostki Badawczej (Aeronautical Research Unit) utworzono oddział Amerykańskiej Biblioteki Kongresu (US Library of Congress), który miał zapewnić niestandardowe badania i usługi analityczne wykorzystujące rozległe zasoby biblioteki. Obecnie funkcjonuje on jako Federalny Oddział Badawczy (Federal Research Division)[52].

W 1941 r. decyzją prezydenta Franklina Delano Roosevelta utworzono w USA Służbę Monitoringu Nadawców Zagranicznych (Foreign Broadcast Monitoring Service). Była ona odpowiedzialna za monitorowanie, tłumaczenie, transkrypcję i analizę informacji pochodzących z audycji radiowych państw Osi. Do końca 1942 r. służba osiągnęła sporą wydajność. Tłumaczyła ponad 500 tys. słów dziennie, które pochodziły z 25 stacji radiowych nadających w 15 językach[53]. W ramach powołanego Międzyresortowego Komitetu Nabywania Zagranicznych Publikacji (Interdepartmental Committee for the Acquisition of Foreign Publications) Amerykanie monitorowali i analizowali także prasę i książki ukazujące się w czasie wojny poza granicami kraju. Pod koniec wojny przesyłano tygodniowo do analizy astronomiczną liczbę 45 tys. stron tekstu. W ostatnich dniach wojny w Komitecie zgromadzono 300 tys. fotografii, 350 tys. numerów czasopism, 50 tys. książek oraz ponad milion map i 300 tys. innych dokumentów[54].

W okresie zimnowojennym amerykańskie Biuro Badań Strategicznych (Office of‒Strategic Research) uzyskiwało informacje na temat zagranicznych możliwości jądrowych innych państw (w kręgu zainteresowań znalazły się głównie ZSRR, Chiny i Francja). Te dane pochodziły z oficjalnych, ogólnodostępnych raportów rządów wymienionych krajów oraz z publikacji naukowców[55]. W tym samym okresie Biuro

[50] R.A. Norton, *Guide to Open Source Intelligence. A Growing Window into the World*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2011, nr 2, s. 66.

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

[52] Tamże.

[53] K. Leetaru, *The Scope of FBIS and BBC Open-Source Media Coverage*, 1979–2008, „Studies in Intelligence" 2010, nr 1, s. 19.

[54] A. Olcott, *Open Source Intelligence in a Networked World*, London–New York 2012, s. 16.

[55] T.T. Stafford, *The U.S. Intelligence Community*, [b.m.w.] 1983, s. 58–60.

Badań Ekonomicznych (Office of Economic Research) wykorzystywało informacje jawne, ogólnodostępne, dotyczące m.in. produkcji ropy przez kraje OPEC, produkcji zboża w Związku Radzieckim, siły nabywczej obcych walut czy wartości nabycia zagranicznych firm[56]. Rozwój radzieckiego programu kosmicznego był również monitorowany przez CIA i Siły Powietrzne Stanów Zjednoczonych przy wykorzystaniu dostępnej literatury fachowej na ten temat[57].

W czasie zimnej wojny Stasi analizowało miesięcznie około tysiąca zachodnich czasopism i 100 książek, dziennie zaś – 12 godzin audycji emitowanych przez radio i telewizję w RFN[58]. Niemieckie służby do tej pory doceniają wartość białego wywiadu. W Departamencie BND uchodzącym za jego analityczne serce większą część analizowanego materiału (85 proc.) stanowią źródła otwarte (gazety, audycje radiowe, komunikaty medialne, ulotki, Internet). Zaledwie 10 proc. informacji pochodzi z rozpoznania technicznego, a tylko 5 proc. ze źródeł osobowych[59].

W latach 50. XX w. Sherman Kent, twórca amerykańskiej szkoły analizy wywiadowczej, zamówił u swoich uniwersyteckich kolegów historyków raport na temat stanu amerykańskich sił zbrojnych. Miał on być sporządzony wyłącznie na podstawie źródeł otwartych i dotyczyć wszystkich rodzajów broni, ich liczebności, stanu uzbrojenia oraz dyslokacji jednostek do poziomu dywizji włącznie. Po trzech miesiącach pracy Kent otrzymał kilkaset stron danych i analiz poprzedzonych 30-stronicowym streszczeniem. Okazało się, że raport w 90 proc. dawał właściwy obraz armii amerykańskiej, co spowodowało natychmiastowe utajnienie tego dokumentu[60].

Korzyści płynące z OSINT-u w działalności wywiadowczej oprócz Amerykanów i Europejczyków docenili także Chińczycy. W 1958 r. otworzyli oni Chiński Instytut Informacji Naukowo-Technicznej – centralny organ odpowiedzialny za koordynację pozyskiwania, przetwarzania i dystrybucji zagranicznych materiałów pochodzących ze źródeł otwartych. Przez osiem lat zbudowano ogromną jak na tamte czasy bazę informacji o charakterze naukowo-technicznym, pochodzących z ponad 50 krajów, która mieściła: 11 tys. różnych zagranicznych periodyków, 500 tys. raportów badawczych, publikacji rządowych, materiałów pokonferencyjnych i prac naukowych, ponad 5 mln zagranicznych patentów oraz kilka milionów próbek produktów przydatnych dla chińskiego przemysłu[61].

Znaczenie informacji pochodzących z białego wywiadu doceniały również sowieckie służby specjalne, o czym mogło się przekonać FBI po aresztowaniu w 1957 r. Williama Fishera, szpiega KGB, który działał pod zmienionymi personaliami jako Rudolf Abel. Po przeanalizowaniu materiałów dostarczanych przez niego do ZSRR okazało się,

---

[56] J.T. Richelson, *The U.S. Intelligence Community*, 4 wyd., Boulder 1999, rozdział 12.

[57] J.J. Bagnall, *The Exploitation of Russian Scientific Literature for Intelligence Purposes*, „Studies in Intelligence" 1958, nr 2, s. 45–49.

[58] F. Schaurer, J. Störger, *Guide to the Study of Intelligence*…

[59] U. Ulfkotte, *Pod osłoną mroku. Wielkie wywiady bez tajemnic*, Warszawa 2008, s. 292.

[60] W. Zajączkowski, *Zrozumieć innych. Metoda analityczna w polityce zagranicznej*, Warszawa 2011, s. 14.

[61] W.C. Hannas, J. Mulvenon, A.B. Puglisi, *Chinese industrial espionage: Technology acquisition and military modernization*, London–New York 2013, s. 19–20.

że ich podstawą były w znacznej mierze wiadomości zaczerpnięte z otwartych źródeł informacji: dziennika „The New York Times" oraz miesięcznika „Scientific American", i tylko w niektórych miejscach były uzupełnione informacją agenturalną[62].

Na gruncie polskim przykładem wykorzystania białego wywiadu w pracy wywiadowczej jest działalność płk. Mieczysława Wyżła-Śnieżyńskiego, attaché wojskowego w Czechosłowacji. Podstawą sporządzanych przez niego raportów operacyjnych kierowanych do Oddziału II Sztabu Generalnego WP były głównie prasa i katalogi czechosłowackich firm zbrojeniowych[63].

John L. Hart, były oficer operacyjny CIA mający kilkudziesięcioletnie doświadczenie w kierowaniu operacjami wywiadowczymi w różnych częściach świata, po przeanalizowaniu dokumentacji operacyjnej z archiwów amerykańskiej służby przyznał, że oficerowie wywiadu nauczyli się, że przekazanie swoim przełożonym „kartki papieru" z jakąkolwiek treścią jest lepsze niż nieprzekazanie niczego[64]. Jeden ze szpiegów, sowiecki oficer Piotr Popow, usłyszał od swoich przełożonych, że jego praca wywiadowcza nie przynosi efektów, ponieważ więcej można dowiedzieć się z gazet[65]. W 1983 r. japoński dziennikarz przeprowadził wywiad z oficerem KGB Stanisławem Lewczenką pracującym pod przykryciem reportera w Japonii, który w 1979 r. zbiegł do Stanów Zjednoczonych. Podczas 20 godzin rozmów przekazał on informacje na temat agentów oraz omówił warsztat pracy operacyjnej. Na ich podstawie powstała książka, odbywały się również konferencje prasowe z jego udziałem, na których, według oficera amerykańskiego wywiadu, ujawniał on więcej informacji, niż było ich zawartych w jego aktach zgromadzonych przez CIA[66].

Współcześnie „arabska wiosna" jest dowodem na to, że ogólnodostępne informacje, poglądy i oceny publikowane w Internecie są potężnymi narzędziami, które mogą wpływać na losy krajów i społeczeństw. Zastępca dyrektora CIA Christopher Sartinsky po latach doświadczeń w pracy wywiadowczej wyraził zdziwienie i jednocześnie zachwyt tym, że ludzie dobrowolnie ujawniają w Internecie wiedzę o sobie, swoim życiu prywatnym i najbliższych, dzięki czemu ułatwiają pracę agentom[67]. Eben Moglen w wywiadzie pt. *Who Needs the KGB when we have Facebook?*, powołując się na źródła w rosyjskiej służbie specjalnej, odpowiada na to pytanie pytaniem retorycznym: (…) *komu teraz potrzebna Łubianka* (potoczna nazwa siedziby Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej – dop. aut.), *skoro teraz mamy Facebook? Kiedyś wsadzano ludzi*

[62] W. Zajączkowski, *Zrozumieć innych. Metoda…* s. 14.

[63] A. Wojciulik, *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków*, w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipowski, W. Mądrzejowski (red.), Warszawa 2012, s. 48.

[64] J.L. Hart, *Walka wywiadów, Rosjanie w CIA*, Warszawa 2008, s. 58.

[65] Tamże, s. 52.

[66] S.C. Mercado, *A Venerable Sailing the Sea of OSINT in the Information Age. A Venerable Source in a New Era*, „Studies in Intelligence" 2004, nr 3, s. 51, na podstawie książki S. Lewczenki, *On the Wrong Side: My Life in the KGB*, Washington 1988.

[67] J. Ortega Sim, *Facebook The Social Filter of World Intelligence*, http://thedailyjournalist.com/theinvestigative/facebook-the-social-filter-of-world-intelligence/ [dostęp: 2 V 2018].

do więzienia i próbowano uzyskać od nich informacje. Było to drogie i okrutne. W obecnych czasach jest to o wiele tańsze i łatwiejsze, ponieważ każdy może być szpiegiem, zbierać informacje o swoich znajomych. Trudno teraz wskazać w tej grze, kto jest wygranym, a kto przegranym, skoro wszyscy nawzajem mogą się szpiegować [68].

Wychodząc naprzeciw wyzwaniom, analitycy amerykańskiego Open Source Center, określani jako „wścibscy bibliotekarze", poza monitoringiem mediów i prasy, czytają codziennie nawet 5 mln postów na portalach społecznościowych. Sporządzają z nich raporty zawierające opisy bieżących nastrojów społecznych w wybranych krajach na świecie oraz przewidują możliwości wystąpienia danego zagrożenia[69].

Brytyjskie Rządowe Centrum Łączności również nie ustępuje w tym swojemu sojusznikowi dzięki Network Analysis Center, które codziennie gromadzi ponad 50 mld rekordów dotyczących wizyt użytkowników Internetu w serwisach informacyjnych i portalach z audycjami radiowymi online na całym świecie, powiązanych w większości z islamem[70]. Szef niemieckiego BfV Hans-Georg Maassen podkreśla, że chińskie służby wywiadowcze wykorzystują portale społecznościowe, m.in. Linkedln, za których pośrednictwem nawiązują kontakty rzekomo zawodowo-biznesowe, aby dotrzeć do pracowników niemieckich agencji rządowych[71]. Skuteczne wykorzystanie mediów społecznościowych obrazują chociażby działania izraelskiej służby Szin Bet, która dzięki śledzeniu wiadomości na komunikatorach internetowych udaremniła ataki terrorystyczne na Międzynarodowe Centrum Konferencyjne w Jerozolimie oraz na Ambasadę USA w Tel Awiwie[72]. Również europejskie służby odnoszą sukcesy na tym polu. Francuska Centralna Dyrekcja Wywiadu Wewnętrznego (Direction Centrale du Renseignement Intérieur, DCRI, a od 2014 r. Dyrekcja Generalna Bezpieczeństwa Wewnętrznego, Direction Générale de la Sécurité Intérieure, DGSI) zatrzymała w 2013 r. Romaina Letelliera, francuskiego konwertytę, moderatora dżihadystycznego forum internetowego Ansar Al-Haqq, posługującego się pseudonimem Abu Siyad Al-Normandy, który usłyszał zarzuty podżegania do terroryzmu i szerzenia propagandy terrorystycznej. Był on pierwszym francuskim dżihadystą skazanym na mocy nowej regulacji prawnej z 2012 r. mającej na celu zahamowanie zjawiska samoradykalizacji za pośrednictwem Internetu.

---

[68] A. Schechter, *Who Needs the KGB when we have Facebook? An Interview with Eben Moglen*, http://moglen.law.columbia.edu/publications/Who-needs-KGB-when-we-have-Facebook Schechter.pdf [dostęp: 1 V 2018].

[69] D. Goodin, *CIA 'Open Source Center' monitors Facebook, Twitter*, http://www.theregister.co.uk/2011/11/04/cia_open_source_center [dostęp: 7 V 2018].

[70] Zob. Broadcast/Internet Radio Exploitation and Analysis, 6 November 2009 – UK TOP SECRET/COMINT, https://theintercept.com/document/2015/09/25/broadcast-analysis/ [dostęp: 10 IV 2018].

[71] K. Grieshaber, *German intelligence warns of increased Chinese cyberspying*, https://www.seattletimes.com/business/german-intelligence-warns-of-increased-chinese-cyberspying [dostęp: 2 V 2018].

[72] M. Peck, *Israel Thwarts Al Qaeda Plot to Blow Up U.S. Embassy*, https://www.forbes.com/sites/michaelpeck/2014/01/22/israel-thwarts-al-qaeda-plot-to-blow-up-u-s-embassy/1 [dostęp: 2 V 2018].

Mohammed Emwazi, występujący jako Jihadi John, który skupiał uwagę mediów i służb w związku z tym, że był egzekutorem zakładników przetrzymywanych przez dżihadytów z Państwa Islamskiego, został zidentyfikowany, gdy robił zakupy w Internecie. Służby ustaliły jego personalia i miejsce pobytu w Syrii po podaniu przez niego swojego spersonalizowanego kodu, z którego korzystał jeszcze za czasów studiów[73]. Monitorowanie śladu cyfrowego w Internecie pozwala dotrzeć do jego źródła – użytkownika. W ocenie Paula Moore'a przerwy między naciskaniem poszczególnych klawiszy klawiatury komputera lub długość ich przyciskania są wartościami stałymi i unikatowymi, co czyni je cechą behawioralną człowieka. Dzięki takiej obserwacji i analizie można dokonać oceny profilu konkretnego użytkownika komputera. Z podobnych metod w czasie II wojny światowej miał korzystać brytyjski wywiad. Nasłuchiwał on niemieckich telegrafistów, a następnie na podstawie szybkości nadawania i charakterystycznych błędów, które ci żołnierze popełniali[74],tworzył profile niemieckich żołnierzy.

Twórczość literacka poza dostarczaniem wiedzy poszerzającej horyzonty i pobudzającej wyobraźnię swoich czytelników może także inspirować. Scenariusz stworzony dla widzów światowego kina może zostać przekuty w rzeczywistość, o czym świadczą wydarzenia z 11 września 2001 r. Porwanie samolotu przez terrorystę i dokonanie samobójczego ataku na amerykański parlament – Kapitol – w Waszyngtonie już pięć lat wcześniej opisał Tom Clancy na łamach swojej powieści *Dekret*. Również Timothy McVeigh, skazany za podłożenie bomby w rządowym budynku w Oklahoma City w 1995 r., inspirował się filmem *Red Dawn* (*Czerwony świt*, 1984 r.) oraz *Dziennikami Turnera* autorstwa Andrewa Macdonalda, członka Amerykańskiej Partii Nazistowskiej.

Opublikowanie w „The Washington Post" i „The New York Times" tzw. manifestu Kaczyńskiego dotyczącego zagrożeń wynikających z rozwoju technologicznego stało się przyczyną zatrzymania w 1996 r. przez FBI Theodora Johna Kaczynskiego. Amerykański terrorysta, znany jako „Unabomber", w ciągu prawie 18 lat zabił trzy osoby, a wiele ranił, 29 własnoręcznie wykonanymi bombami. Jego brat David rozpoznał w opublikowanym manifeście myśli swojego brata Theodora, o czym poinformował amerykańską służbę i tym samym przyczynił się do przerwania śledztwa nieprzynoszącego żadnych efektów.

Źródłem informacji zbieranych w ramach białego wywiadu są także metadane, czyli dane o danych, pozwalające na zidentyfikowanie i opisanie informacyjnego obiektu cyfrowego. Można w nich przechowywać informacje m.in. na temat okoliczności i lokalizacji wykonania zadania oraz praw autorskich. Metadane zdjęcia zamieszczonego na Instagramie przez rosyjskiego żołnierza w wojskowym transporterze ujawniły jego miejsce pobytu na Ukrainie, w okresie, gdy Rosja zaprzeczała swojej

[73] J. Murray, *Jihadi John exposed by web error: Killer downloaded software using student ID*, http://www.express.co.uk/news/uk/561135/Jihadi-John-Mohammed-Emwazi-identified-web-error-student-ID-Westminster-university [dostęp: 26 III 2018].

[74] Zob. P. Moore, *Behavioral Profiling: The password you can't change*, https://paul.reviews/behavioral-profiling-the-password-you-cant-change/ [dostęp: 8 IV 2018].

obecności na wschodzie tego kraju. Upublicznienie na Twitterze zdjęcia terrorysty z Państwa Islamskiego na tle jednego z centrów dowodzenia tej organizacji pozwoliło amerykańskim siłom lotniczym na lokalizację i zbombardowanie tego miejsca w ciągu 24 godzin od momentu pojawienia się fotografii w Internecie[75]. Powszechnie wiadomo, że są aplikacje, które dzięki funkcji geolokalizacji umożliwiają precyzyjne zapisywanie pokonywanych tras przez sportowców. Ich aktywność z opisem dystansu, jaki pokonali, jest odzwierciedlana na mapie, którą później chętnie dzielą się z innymi użytkownikami portali społecznościowych. Jak pokazuje przykład aplikacji Strava, analiza metadanych udostępnionych ścieżek biegaczy ujawniła lokalizację tajnych obiektów wojskowych, w tym obiektów służb specjalnych, w których służbę pełnili owi sportowcy.

Organizacje terrorystyczne również chętnie wykorzystują otwarte źródła[76] informacji w działalności, a zwłaszcza w procesie rekrutacji członków[77], ich radykalizacji, szkolenia, planowania zamachów[78] lub cyberataków[79]. W podręczniku Al-Kaidy oceniono, że (…) *publiczne, jawne źródła pozwalają zebrać co najmniej 80% informacji o wrogu*[80]. Peter Bergan doszedł do wniosku, że walka z Al-Kaidą i jej sojusznikami jest w rzeczywistości pierwszą wojną źródeł otwartych[81]. Do tej pory żadna organizacja terrorystyczna nie wykorzystywała mediów społecznościowych w takim stopniu, jak Państwo Islamskie. W ocenie dyrektora FBI Jamesa Comeya członkowie

[75] W. Castillo, *Air Force intel uses ISIS* 'm*oron' post to track fighters*, CNN, https://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html [dostęp: 13 IV 2018].

[76] Idąc z duchem czasu, organizacje terrorystyczne stosowały różne narzędzia medialnej aktywności. Od połowy lat 80. XX w. były to transmisje i nagrania VHS z kazaniami, wykładami, zdjęciami z walk oraz artykuły w magazynach i gazetach, w połowie lat 90. XX w. – strony internetowe tworzone i kontrolowane przez prominentnych działaczy organizacji, na początku XXI wieku fora internetowe, a obecnie media społecznościowe. Zob. A.Y. Zelin, R. Borow Fellow, *The State of Globar Jihad Online*, Washington Institute for Near East Policy, January 2013.

[77] W ocenie Elizabeth Kendall istotnym narzędziem rekrutacji może być poezja, która porusza emocje arabskich słuchaczy i czytelników, tworząc aurę tradycji, autentyczności i prawomocności opartej na ideologii. Nawet Osama bin Laden skomponował odę, w której opiewał zniszczenie przez Al-Kaidę okrętu USA „Cole" w 2000 r.

[78] Za pierwszy rozkaz dla terrorystów wydany w Internecie uznaje się wypowiedź członka Al-Kaidy Abu Muhammada al-Hilali, który 25 października 2005 r. wezwał do przeprowadzania zamachów na półwyspie Synaj. Ale już wcześniej, w 1995 r., stwierdzono, że Abd-al-Rahman Zaydan, zatrzymany aktywista Hamasu, przy którym znaleziono komputer, kontaktował się przez Internet z innymi członkami tej organizacji, zob. K. Soo-Hoo, S. Goldman, L. Greenberg, *Information Technology and the Terrorist Threat*, „Survival" 1997, nr 3, s. 139.

[79] Otwarte źródła informacji są narzędziem umożliwiającym rozgłos, który niezależnie, czy jest formą gloryfikacji, czy pogardy dla aktów terrorystycznych, zawsze przynosi pożądany efekt i wpisuje się w scenariusz strategii terrorystów (tzw. terror medialny). Ponadto pozwalają na prowadzenie operacji psychologicznych, dezinformacyjnych i kampanii propagandowych w Internecie.

[80] Zob. podręcznik Al-Kaidy *Al Qaeda Training Manual* z XII 2001 r. Wspomniał o nim m.in. sekretarz obrony USA Donald Rumsfeld w przemówieniu z 15 I 2003 r.

[81] P. Bergen, *Why U.S. can't find Osama bin Laden*…

tej organizacji opanowali Internet[82] do perfekcji i tym samym zrewolucjonizowali zjawisko terroryzmu[83]. Stworzyli tzw. Open Source Jihad[84], czyli szeroko dostępne i łatwe do wyszukania informacje związane z działalnością terrorystyczną. Wzmożone działania islamskich ekstremistów odnotowała również niemiecka BND, według której i Al-Kaida, i Państwo Islamskie prowadzą propagandową wojnę internetową na niespotykaną wcześniej skalę. W niektórych analizach podkreśla się, że nawet 90 proc. treści tworzonych przez terrorystów w Internecie jest rozprzestrzenianych za pośrednictwem mediów społecznościowych[85]. W Internecie znajduje się mnóstwo darmowych książek[86], które są przewodnikami oraz instrukcjami dla potencjalnych zamachowców – „samotnych wilków".

Amerykański wywiad informował, że Osama bin Laden w swojej siedzibie w afgańskich górach miał centrum komputerowe, z którego – wykorzystując czat oraz grupy dyskusyjne – przekazywał informacje członkom Al-Kaidy[87]. Internet prawdopodobnie służył do opracowania szczegółów ataku z 11 września 2001 r. i jego koordynacji. Po aresztowaniu w marcu 2002 r. Abu Zubaydaha, uznawanego za szefa operacyjnego Al Kaidy, w jego komputerze znaleziono prawie 2300 zaszyfrowanych wiadomości i plików ściągniętych z islamskiej strony internetowej. Analiza danych wykazała, że informacje były systematycznie wymieniane pomiędzy członkami ugrupowania od maja 2000 r. do 9 września 2011 r., a częstotliwość korespondencji wzrosła miesiąc przed zamachem[88]. Saudyjski terrorysta doceniał także wartość mediów. W 2002 r. w liście do przywódcy talibańskiego mułły Muhammeda Omara pisał: *Jest oczywiste, że w tym wieku walka przy użyciu mediów jest jedną z najmocniejszych*

[82] Za ojca internetowego dżihadu uznaje się Brytyjczyka z pakistańskimi korzeniami – Babara Ahmada. W 1996 r. ten wówczas 22-letni student jednego z londyńskich uniwersytetów założył pierwszą stronę internetową dla islamskich ekstremistów i dedykował ją Osamie bin Ladenowi oraz jednemu z założycieli Al-Kaidy, Abdullahowi Azzamowi.

[83] J. Ax, *No evidence California attackers were part of terrorist cell – FBI head*, https://in.reuters.com/article/usa-security-idINKBN0TZ29G20151216 [dostęp: 17 IV 2018].

[84] Analiza aktywności terrorystów na portalach społecznościowych, przeprowadzona przez Brytyjskie Międzynarodowe Centrum Studiów nad Radykalizacją i Przemocą Polityczną, wskazuje, że są one wykorzystywane do informowania (raportowania) o bieżącej sytuacji (w rzeczywistym czasie) na froncie walki.

[85] Zob. D. Bieda, E. Riddle, *Cyberspace: A Venue for Terrorism*, „Issues in Information Systems" 2015, nr 16.

[86] Zob. *The Terrorist's Handbook* oraz *The Anarchist Cookbook* – podręczniki, w których opisano, jak skonstruować ładunki wybuchowe przy użyciu domowych środków chemicznych; *Military Studiem in the Jihad Against the Tytants* oraz *How to survive in the west* – analizy zasad organizowania i prowadzenia działań zbrojnych według dżihadystycznej myśli wojskowej; *The Mijahedeen Poisons Handbook* – procedury wytwarzania trucizn; *Safety and Security guidelines for Lone Wolf Mujahideen and small cells* – informacje dotyczące szyfrowania wiadomości w Internecie, metod wywiadowczych i kontrwywiadowczych oraz tworzenia tajnych komórek dzihadu.

[87] D.E. Denning, *Ativism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, w: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica 2001, s. 259.

[88] J. Kelly, *Militants wire Web with links to jihad*, „USA Today" z 10 lipca 2002 r., http://usatoday30.usatoday.com/news/world/2002/07/10/web-terror-cover.htm [dostęp: 20 IV 2018].

metod, właściwie może ona stanowić 90 proc. przygotowań do walk. Przygotowując zamachy w Bombaju w listopadzie 2008 r., terroryści korzystali z wyszukiwarki Google Earth – uczyli się na pamięć topografii miasta, nazw ulic i rozmieszczenia najważniejszych obiektów ataku. W 2009 r. w Pakistanie zatrzymano grupę mężczyzn z Waszyngtonu, nazwanych później „Virginia Five", którzy chcieli dołączyć do bojowników walczących przy granicach z Afganistanem. Ich przyjazd zainspirował talibański rekrut, który znalazł na YouTube komentarz jednego z tych mężczyzn do filmu o ataku na amerykańskie wojska, który miał dla talibów wydźwięk pozytywny. Osoby, które napotykają ograniczenia w bezpośrednim procesie komunikacji, chociażby ze względu na uwarunkowania społeczno-kulturowe, w środowisku wirtualnym mogą je obejść. Aktywność internetowa holenderskich muzułmanek nie umknęła uwadze grup terrorystycznych, które rekrutowały te kobiety jako tłumaczki, programistki i twórczynie holenderskich stron internetowych dotyczących dżihadu[89].

Pomiędzy białym wywiadem a działalnością terrorystyczną można zauważyć synergię[90]. Już w 1976 r. Walter Laquer w magazynie „Harpers" wyraził opinię, że media są najlepszym przyjacielem terrorystów, akt terroru sam w sobie zaś nic nie znaczy bez nagłośnienia całego wydarzenia. To media dostarczają im tlen, od którego są uzależnieni, jak mawiała ponad 30 lat temu Margaret Thatcher. Słusznie określił to Ted Kepel: (…) *bez telewizji terroryzm przypomina drzewo w środku lasu: jeśli runie, nikt tego nie zauważy*[91]. Chciałoby się powiedzieć, że media wykreowały terrorystów, robiąc z nich gwiazdy. Świadczy o tym to, że w ciągu 10 tygodni od wydarzeń z 11 września „Times" na swoich okładkach trzy razy umieścił podobiznę bin Ladena, a tyko dwa razy wizerunek ówczesnego prezydenta USA George'a W. Busha.

W jaki sposób można wykorzystać biały wywiad, pokazuje brytyjski bloger Eliot Higgins, który śledząc aktywność na portalach internetowych, wyciąga zaskakujące wnioski. Po analizie filmu, na którym bojownicy Państwa Islamskiego dokonują egzekucji brytyjskiego dziennikarza Jamesa Foleya, wskazał, że miejscem, w którym to się stało, były wzgórza w pobliżu Ar-Rakka, choć tłem było zupełne pustkowie[92]. Kiedy w sierpniu 2013 r. na syryjskie miasta spadły pociski, a inspektorzy ONZ nie mieli możliwości ich zbadania, w tym samym dniu kiedy to się wydarzyło, Higgins opublikował zdjęcia i filmy odnalezione na YouTubie, na których było widać, że rakiety nie eksplodowały od razu, ale padały nienaruszone, uwalniając z głowic gaz (jak się potem okazało – sarin). Podobnie było w przypadku wschodniej Ukrainy. Wystarczyło przejrzeć portale społecznościowe, aby znaleźć zdjęcia z tego terenu umieszczone

[89] *Jihadis and the Internet. 2009 update*, National Coordinator for Counterterrorism (NCTb), V 2010 r., s. 65–66.

[90] Według raportu United States Institute of Peace w 1998 r. zaledwie co trzecia organizacja terrorystyczna miała własną stronę interentową, a już w 2002 r. miały ją w zasadzie wszystkie.

[91] P. Rees, *Kolacja z terrorystą. Spotkania z najbardziej poszukiwanymi bojownikami na świecie*, Kraków 2008, s. 27.

[92] J. Ensor, *Is this where James Foley was beheaded?*, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11053544/Is-this-where-James-Foley-was-beheaded.html [dostęp: 4 V 2018].

przez żołnierzy 53 Rakietowej Brygady Przeciwlotniczej z obwodu kurskiego, na których były widoczne rakiety Buk. Dowodziły one, że separatystów regularnie wspierały siły zbrojne Federacji Rosyjskiej. Higgins dowiódł również, że pasażerski samolot linii lotniczych Malaysia Airlines został zestrzelony nad Ukrainą przez rakietę Buk należącą do rosyjskiego wojska[93].

Jak ogromnymi zasobami wiedzy są otwarte źródła informacji, w których można odnaleźć również wiadomości ściśle tajne, pokazuje kuriozalna wpadka agenta FBI, pełniącego wcześniej funkcję szefa wydziału antyterrorystycznego. W 2010 r. postanowił on zastrzec prawa autorskie do podręcznika napisanego dla agentów przesłuchujących podejrzanych. Nie zdawał sobie jednak sprawy, że wraz z wpisem do rejestru ten dokument zostanie udostępniony szerokiemu gronu odbiorców. W celu zarejestrowania podręcznika złożył w urzędzie patentowym jego kopię, z którą obecnie każdy może się zapoznać w Bibliotece Kongresu[94]. Błąd popełniony przez funkcjonariusza służb specjalnych, pomimo że wydaje się, że nie był celowy z punktu widzenia zasad ochrony informacji niejawnych, niczym się nie różni od przecieku dokonanego przez Edwarda Snowdena – informacje niejawne zostały udostępnione osobom nieupoważnionym. Wniosek z tego jest jeden: najsłabszym ogniwem w zapewnianiu bezpieczeństwa informacji przed ich nieuprawnionym wyciekiem jest nie technika, ale człowiek. Przykładem tego może być zdekonspirowanie przez Biały Dom swojego szpiega w Afganistanie. Ze względu na pełnioną funkcję dysponował on z pewnością wiedzą, której ujawnienie mogło rodzić niebezpieczne w skutkach konsekwencje dla bezpieczeństwa USA oraz ich sojuszników. Nazwisko i funkcja „Chief of Stadion" (szefa placówki CIA) pojawiło się na liście rozesłanej dziennikarzom w związku z wizytą Baracka Obamy w bazie Bagram w Afganistanie. Ta informacja natychmiast trafiła na Twittera, gdzie była głośno komentowana[95].

Nawet osoby świadome wartości OSINT w działalności wywiadowczej mają konta na portalach społecznościowych, a ich identyfikacja, mimo jakichkolwiek prób ukrywania się, nie jest trudna, wymaga jedynie czasu i determinacji. Przekonał się o tym sam dyrektor FBI James Comey, którego konta na Twitterze i Instagramie zostały ujawnione w krótkim czasie po tym, jak publicznie wspomniał, że z nich korzysta. Dziennikarka Ashley Feinberg zaczęła od prób zlokalizowania kont jego rodziny, które – jak słusznie założyła – są łatwiejsze do odnalezienia. Za główny cel wybrała jego syna Briena, koszykarza drużyny uniwersyteckiej. Pośród opublikowanych tweetów jego drużyny znalazła odniesienia do konta Briena i jego zdjęcia wraz z linkiem do tego zdjęcia na Instagramie, które – jak się okazało – było zablokowane. Korzystając

[93] *The lost digit – Buk 3x2*, „A bell¿ngcat Investigation" 2014, https://www.bellingcat.com/wp-content/uploads/2016/05/The-lost-digit-BUK-3x2_EN_final-1.pdf, s. 2 [dostęp: 1 V 2018].

[94] Zob. J. Baumann, *You'll Never Guess Where This FBI Agent Left a Secret Interrogation Manual*, http://www.motherjones.com/politics/2013/12/fbi-copyrightedinterrogation-manual-unredacted-secrets/ [dostęp: 1 V 2018].

[95] G. Miller, *White House to investigate inadvertent naming of CIA officer*, http://www.washingtonpost.com/world/national-security/white-house-to-investigate-inadvertent-naming-of-cia-officer/2014/05/27/5d5f41f0-e5e6-11e3-afc6-a1dd9407abcf_story.html [dostęp: 4 IV 2018].

z fikcyjnego konta, poprosiła o dodanie jej do znajomych. Portal automatycznie zaproponował kolejne konta osób, które może znać dziennikarka. Wśród nich znalazła kilku krewnych dyrektora FBI, w tym jego żonę, Patrice Comby, oraz tajemniczego Reinholda Niebuhra. Ten ostatni miał tylko kilku znajomych na swoim koncie, a o takiej możliwości Comey wspominał podczas wywiadu. Po przeszukaniu zasobów Internetu Feinberg ustaliła, że Comey na studiach pisał pracę na temat teologa Reinholda Niebuhra, co utwierdziło ją w przekonaniu, że zidentyfikowała konto Comeya. Po tym samym pseudonimie „Reinhold Niebuhr" pośród kilku kont na Twitterze wyszukała jedno, którego nick: projectexile7 nawiązywał do projektu realizowanego przez Comeya w poprzedniej pracy[96], co ostatecznie potwierdziło jej przypuszczenia.

Podsumowując rozważania o OSINT i płynących z niego wymiernych korzyściach w działalności wywiadowczej, autor chciałby zaznaczyć, że dzięki postępowi technologicznemu i nieustającemu rozwojowi infrastruktury informatycznej otwarte źródła informacji, a zwłaszcza wirtualne, coraz silnej oddziałują na globalną rzeczywistość. Amerykanie dostrzegają ten trend, dlatego w strukturach Biura Dyrektora Wywiadu Krajowego, podmiotu odpowiedzialnego za opracowanie i badanie projektów w zakresie działalności wywiadowczej, uruchomili w 2011 r. projekt *Open Source Indicators*. W ramach tego projektu jest monitorowana aktywność w wirtualnych, ogólnie dostępnych źródłach otwartych. To pozwala na łączenie wspólnych wskaźników w sieci, a następnie – na prognozowanie i wczesne wykrycie istotnych zdarzeń społecznych, które mogą nieść za sobą niebezpieczeństwo.

Dyrektor Wywiadu Narodowego USA James R. Clapper w lutym 2016 r. podczas posiedzenia senackiej komisji ds. wywiadu, oceniając globalne zagrożenia w dzisiejszych czasach, wskazał, że poza OSINT-em służby mogą zacząć wykorzystywać w działalności wywiadowczej wspomniany już tzw. *Internet of Things*, czyli monitorować i pozyskiwać informacje z urządzeń podłączonych do Internetu. Robert Steele poszedł dalej w swoich przemyśleniach i stwierdził, że służby w XXI wieku będą skoncentrowane w dużej mierze na każdym dostępnym źródle – *Open Source Everythings*.Tego typu źródła mogą dostarczać drobnych, szczątkowych informacji, ale dających punkt zaczepienia, odpowiadających na pytania, które z perspektywy prowadzonych działań są nie tylko podstawą analizy, jej „chlebem i masłem" – jak uważał Arthur S. Hulnick[97], lecz także priorytetowym narzędziem w działalności wywiadowczej na każdym etapie jej realizacji. Pozwalają też zarówno zweryfikować i pogłębić dotychczasową wiedzę, jak i szerzej spojrzeć na badane zjawisko.

[96] A. Feinberg, *This Is Almost Certainly James Comey's Twitter Account*, https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641 [dostęp: 10 IV 2018].

[97] A.S. Hulnick, *The Downside of Open Source Intelligence*, „International Journal of Intelligence and Counter Intelligence" 2002–2003, nr 4, s. 565.

Bibliografia:

100 Events That Changed the World, „National Geographic" 2015, Special Issue.

A Look Back… George Washington: America's First Military Intelligence Director, https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/george-washington.html [dostęp: 5 V 2018].

Apuzzo M., Schmidt M.S., Preston J., *U.S. Visa Process Missed San Bernardino Wife's Zealotry on Social Media*, http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html [dostęp: 6 V 2018].

Ax J., *No evidence California attackers were part of terrorist cell – FBI head*, http://in-.reuters.com/article/usa-security-idINKBN0TZ29G20151216 [dostęp:17 IV 2018].

Bagnall J.J., *The Exploitation of Russian Scientific Literature for Intelligence Purposse*, „Studies in Intelligence" 1958, nr 2.

Baumann J., *You'll Never Guess Where This FBI Agent Left a Secret Interrogation Manual*, http://www.motherjones.com/politics/2013/12/fbi-copyrighted-interrogation-manual-unredacted-secrets/ [dostęp: 12 VIII 2017].

Bergen P., *Why U.S. can't find Osama bin Laden*, http://edition.cnn.com/2010/OPINION/10/19/bergen.finding.bin.laden/ [dostęp: 2 VIII 2017].

Bieda D., Riddle E., *Cyberspace: A Venue for Terrorism*, „Issues in Information Systems" 2015, nr 16, International Association of Computer Investigative Specialists (IACIS), Leesburg 2015.

Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, The White House, Washington DC, V 2014 r., s. 7–8.

Bohn R., Short J., *Measuring Consumer Information*, „International Journal of Communication" 2012, nr 6, University of California, s. 980–1000.

Broadcast/Internet Radio Exploitation and Analysis, 6 November 2009 – UK TOP SECRET/COMINT, https://theintercept.com/document/2015/09/25/broadcast-analysis/ [dostęp: 10 IV 2018].

Castillo W., *Air Force intel uses ISIS 'moron' post to track fighters*, https://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html [dostęp: 13 IV 2018].

Church G.M., Gao Y., Konsuri S., *Next-Generation Digital Information Storage in DNA*, Sciencexpress, 16 VIII 2012 r., [dostęp: 4 IV 2018].

Coddington E.B., *The Gettysburg Campaign: A Study in Command*, New York 1968, Charles Scribner's Sons.

Costlow T., *Kehler raises trial balloon: Put STRATCOM in charge of all GEOINT PED*, http://defensesystems.com/articles/2011/10/19/geoint-kehler-stratcom-geospatial intelligence.aspx [dostęp: 9 VII 2017].

Denning D.E., *Ativism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, w: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica 2001.

Disruptive innovation. Case study: Intelligence – Open-source data analytics, Washington, 2012, Deloitte.

Ensor J., *Is this where James Foley was beheaded?*, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11053544/Is-this-where-James-Foley-was-beheaded.html [dostęp: 4 VIII 2017].

Feinberg A., *This Is Almost Certainly James Comey's Twitter Account*, https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641 [dostęp: 10 IV 2018].

Gantz J., Reinsel D., *Extracting value from chaos*, w: *IDC analyze the future,* https://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf [dostęp: 4 VI 2018].

Gibson S.D., *Exploring the Role and Value of Open Source Intelligence*, w: *Open Source Intelligence in Twenty-First Century*, Ch. Hobbes, D. Sailsbury (eds.), New York 2014.

Gleick J., *Informacja – bit, wszechświat, rewolucja*, Kraków 2012.

Goodin D., *CIA 'Open Source Center' monitors Facebook, Twitter*, http://www.theregister.co.uk/2011/11/04/cia_open_source_center [dostęp: 7 VIII 2017].

Grieshaber K., *German intelligence warns of increased Chinese cyberspying*, https://www.seattletimes.com/business/german-intelligence-warns-of-increased-chinese-cyberspying/ [dostęp: 2 V 2018].

Hannas W.C., Mulvenon J., Puglisi A.B., *Chinese industrial espionage: Technology acquisition and military modernization*, London–New York 2013.

Harmon G., *The measurement of information*, „Information Processing and Management" 1984, nr 1–2.

Hart J.L., *Walka wywiadów, Rosjanie w CIA*, Warszawa 2008, Bellona.

Hulnick S., *„The Downside of Open Source Intelligence"*, „International Journal of Intelligence and Counter Intelligence", 2002–2003, nr 4.

Intelligence Community Directive Number 301, NATIONAL OPEN SOURCE ENTERPRISE 2006, https://www.fas.org/irp/dni/icd/icd-301.pdf [dostęp: 6 VII 2017].

ISO 22320:2011, *Societal security – Emergency management – Requirements for incident response*, November 2011.

ISO 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*, November 1993.

Karnowski M., Mistewicz E., *Anatomia władzy*, Warszawa 2010, Czerwone i Czarne.

Kelly J., *Militants wire Web with links to jihad*, „USA Today" z 10 lipca 2002 r., http://usatoday30.usatoday.com/news/world/2002/07/10/web-terror-cover.htm [dostęp: 20 IV 2018].

Koemer R., *William Binney: NSA Claim Not to Be Mining Content Is an* "*Outright Lie*", https://www.huffingtonpost.com/robin-koerner/nsa-whisteblower-nsa-clai_b_7837806.html [dostęp: 4 V 2018].

Landauer T.K., *How Much do People Remember? Some Estimates of the Quantity of Learned Information in Long-Term Memory*, „Cognitive Science" 1986, nr 10, s. 477–493.

Larecki J., *W kręgu tajemnic wywiadu*, Warszawa 2007, WNT.

Leetaru K., *The Scope of FBIS and BBC Open-Source Media Coverage*, *1979–2008*, „Studies in Intelligence" 2010, nr 1, s. 17–37.

Levinson P., *Nowe nowe media*, Kraków 2010, Wydawnictwo WAM.

Lowenthal M.M., *Open Source Intelligence: New Myths, New Realitties,* w: *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, R.Z. George, R.D. Kline (eds.), Lanham 2006.

McAllister Linn B., *The Philippine War, 1899–1902*, Lawrence 2000, University Press of Kansas.

Meeker M., Yu L., *Internet Trends*, Washington 2013, Kleiner Perkins Caulfield Byers.

Mercado S.C., *Sailing the Sea of OSINT in the Information Age. A Venerable Source in a New Era*, „Studies in Intelligence" 2004, nr 3; na podstawie książki S. Lewczenki, *On the Wrong Side: My Life in the KGB*, Washington 1988, Pergamon-Brassey's,

Miller G., *White House to investigate inadvertent naming of CIA officer*, http://www.washingtonpost.com/world/national-security/white-house-to-investigate-inadvertent-naming-of-cia-officer/2014/05/27/5d5f41f0-e5e6-11e3-afc6-a1dd9407abcf_story.html [dostęp: 4 IV 2018].

Moore P., *Behavioral Profiling: The password you can't change*, https://paul.reviews/behavioral-profiling-the-password-you-cant-change/ [dostęp: 8 IV 2018].

Murray J., *Jihadi John exposed by web error: Killer downloaded software using student ID*, http://www.express.co.uk/news/uk/561135/Jihadi-John-Mohammed-Emwazi-identified-web-error-student-ID-Westminster-university [dostęp: 26 III 2018].

National Coordinator for Counterterrorism (NCTb), Jihadis and the Internet, 2009.

National Defense Authorization Act for Fiscal Year 2014, Public Law 113–66 (26 XII 2013 r.).

Nogalski B., Surawski M.B., *Informacja strategiczna i jej rola w zarządzaniu przedsiębiorstwem*, w: *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystywanie i ochrona (wybrane problemy teorii i praktyki)*, R. Borowiecki, M. Kwieciński (red.), Kraków 2003.

Norton R.A., *Guide to Open Source Intelligence. A Growing Window into the World*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2011, nr 2.

Olcott A., *Open Source Intelligence in a Networked World*, London–New York 2012, The Continuum International Publishing Group.

Open Source Intelligence, Headquarters, Department of Army, Army Techniques Publication, ATP 2-22.9, Washington 2012.

Ortega Sim J., *Facebook The Social Filter of World Intelligence*, http://thedailyjournalist.com/theinvestigative/facebook-the-social-filter-of-world-intelligence/ [dostęp: 26 V 2018].

Peck M., *Israel Thwarts Al Qaeda Plot to Blow Up U.S. Embassy*, https://www.forbes.com/sites/michaelpeck/2014/01/22/israel-thwarts-al-qaeda-plot-to-blow-up-u-s-embassy/1 [dostęp: 2 V 2018].

Polańska K., *Informacja, jej wiarygodność i co z nich dla nas wynika*, w: *Informacja – dobra lub zła nowina*, A. Szewczyk (red.), Szczecin 2004, Uniwersytet Szczeciński.

Rees P., *Kolacja z terrorystą*. *Spotkania z najbardziej poszukiwanymi bojownikami na świecie*, Kraków 2008, Uniwersum.

Report of the Human Rights Council on its thirty-second session, General Assembly United Nations, Human Rights Council, Thirty-second session, A/HRC/32/L.20, 14 XI 2016 r.

Rheingold H., *The Virtual Community. Homesteading on the Electronic Frontier*, New York 1994.

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

Schechter A., *Who Needs the KGB when we have Facebook? An Interview with*

Eben Moglen, http://moglen.law.columbia.edu/publications/Who-needs-KGB-when-we-have-Facebook-Schechter.pdf [dostęp: 1 V 2018].

Sienkiewicz P., *10 wykładów*, Warszawa, 2005, AON.

Słoniewski T., *Od BI do „Big Data*", w: *Nowa twarz Business Intelligence*, R. Jesionek (red.), http://it-manager.pl/wp-content/uploads/Nowa-twarz-BI1.pdf [dostęp: 7 V 2018].

Soo Hoo K., Goodman S., Greenberg L., *Information Technology and the Terrorist Threat*, „Survival" 1997, nr 3.

Stafford T.T., *The U.S. Intelligence Community*, [b.m.w] 1983, University Press of America.

Słownik języka polskiego, t. 1–3, M. Szymczak (red.), Warszawa 1978–1981, PWN.

Stankiewicz K., *Wpływ Internetu na percepcję wiarygodności informacji*, w: *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, L.H. Haber (red.), Kraków 2003, Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie.

Stefanowicz B., *Informacja. Wiedza. Mądrość*, seria: Biblioteka Wiadomości Statystycznych, t. 66, Warszawa 2013, GUS.

Taycher L., *Books of the world, stand up and be counted! All 129,864,880 of you*, booksearch.blogspot.com/.

The lost digit – Buk 3x2, „A bellingcat Investigation" 2014, https://www.bellingcat.com/wp-content/uploads/2016/05/The-lost-digit-BUK-3x2_EN_final-1.pdf [dostęp: 1 V 2018].

Tucker P., *Meet the Man Reinventing CIA for the Big Data Era*, http://www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453/ [dostęp: 3 I 2018].

Ulfkotte U., *Pod osłoną mroku. Wielkie wywiady bez tajemnic*, Warszawa 2008, KiW.

Volkoff V., *Dezinformacja: oręż wojny*, Warszawa 1991, Antyk.

Wojciulik A., *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków*, w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipowski, W. Mądrzejowski (red.), Warszawa 2012, C.H. Beck.

Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analogia zagrożeń i ryzyka, t. 1: *Raport z badań*, T. Jemioło, P. Sienkiewicz (red.), Warszawa 2004, AON.

Zajączkowski W., *Zrozumieć innych. Metoda analityczna w polityce zagranicznej*, Warszawa 2011, KSAP.

Zelin A.Y., Borow Fellow R., *The State of Global Jihad Online*, Washington Institute for Near East Policy, I 2013.

Zločevskij S.E. i in., *Informacja w badaniach naukowych*, Warszawa 1972, WKiŁ.

Żuk P., *Demokracja pod kontrolą – czyli podsłuch non stop*, http://www.tygodnikprzeglad.pl/demokracja-pod-kontrola-czyli-podsluch-non-stop/ [dostęp: 15 VI 2018].

Abstrakt

Artykuł jest poświęcony istocie, funkcji i wartości informacji pochodzących ze źródeł otwartych w kontekście działalności wywiadowczej. Analiza wybranych przykładów wykorzystania informacji ogólnodostępnych pokazuje, że niezależnie od zmieniających się czasów w sposób wymierny uzupełniają one wiedzę uzyskaną innymi metodami, określanymi jako niejawne. Autor dochodzi do wniosku, że w obecnych czasach zdobycie pożądanych informacji jest coraz trudniejsze ze względu na ich ilość, która systematycznie rośnie. Lawinowy wzrost informacji wielośródłowych powoduje przeciążenie możliwości analitycznych, którym te informacje są poddawane, oraz chaos informacyjny, przez co wymagają one dodatkowej weryfikacji i oceny ich wiarygodności. Zasadne wydaje się stwierdzenie, że z uwagi na swoją właściwość, po uwzględnieniu wyzwania dzisiejszych czasów, informacja stanowi „broń masowego rażenia". Może ona być wykorzystywana dwojako: albo jako narzędzie dezinformujące wobec przeciwnika, albo – w przypadku jej pozytywnej weryfikacji – może przyczyniać się do podjęcia działań wyprzedzających, dających przewagę w środowisku bezpieczeństwa.

Słowa kluczowe: informacja, OSINT, otwarte źródła informacji, media społecznościowe, biały wywiad, działalność wywiadowcza, terroryzm.