Biały wywiad w zarządzaniu bezpieczeństwem informacji[1]

Open-source intelligence in information security management

MACIEJ WITCZAK

Autor niezależny

https://orcid.org/0009-0002-8199-5865

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 213–240

https://doi.org/10.4467/20801335PBW.24.009.19611

ARTYKUŁ

Abstrakt

Wywiad oparty na źródłach otwartych stanowi zagrożenie systemu bezpieczeństwa informacji w organizacji (biznesie, siłach zbrojnych), a nawet w całym państwie. Celem artykułu jest przybliżenie tego zagadnienia, przedstawienie zagrożeń ze strony białego wywiadu oraz wskazanie sposobów przeciwdziałania im. Część teoretyczna jest uzupełniona praktyczną analizą przypadku i potwierdza postawioną hipotezę: pozyskanie informacji ze źródeł jawnych jest możliwe, jednak nie zawsze pozwala na uzyskanie kompleksowego produktu wywiadowczego. Ponadto zarządzanie bezpieczeństwem informacji pozwala na minimalizowanie ryzyka pozyskania danych ze źródeł otwartych. W drugiej części zawarto rekomendacje i zaproponowano uniwersalny model zarządzania bezpieczeństwem informacji w organizacji.

Słowa kluczowe

biały wywiad, OSINT, zarządzanie bezpieczeństwem informacji, ISM

[1] Artykuł powstał na podstawie pracy magisterskiej pt. *Biały wywiad w zarządzaniu bezpieczeństwem informacji* obronionej na Wydziale Zarządzania Akademii Wojsk Lądowych im. gen. Tadeusza Kościuszki we Wrocławiu. Praca została nagrodzona w XII edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Abstract

Open-source intelligence (OSINT) poses a threat to the information security system in an organisation (business, armed forces) and even in a whole state. The aim of the article is to provide an overview of this issue, to present the threats posed by open source intelligence and to identify ways of countering them. The theoretical part is complemented by a practical case study and confirms the hypotheses: gathering information from the open sources is possible, but it does not always allow for a comprehensive intelligence product. Moreover, the information security management minimises the risk of collecting data from the open sources. The second part provides recommendations and proposes a universal model of information security management in an organisation.

Keywords

open source intelligence, OSINT, information security management, ISM

Ikona myśli strategicznej Sun Tzu już w starożytności zauważył, że (…) *mądrzy władcy i przebiegli dowódcy pokonują przeciwników i dokonują wybitnych czynów, ponieważ z wyprzedzeniem zdobywają wiedzę o wrogu*[2]. Dlatego informacje od zarania dziejów były podstawą zwycięstw w sferze militarnej i cywilnej. Współcześnie można je uzyskać na wiele sposobów, a ich źródła mogą być mniej lub bardziej jawne. W artykule podjęto temat pozyskiwania informacji ze źródeł jawnych, czyli dostępnych i łatwych do zdobycia dla każdego, przedstawiono możliwości i zagrożenia ze strony rozpoznania otwartoźródłowego (ang. *open-source intelligence*, OSINT) oraz nakreślono właściwy kierunek zarządzania bezpieczeństwem informacji (ang. *information security management*, ISM) w kontekście zagrożenia białym wywiadem. Podjęty problem badawczy jest próbą odpowiedzi na pytanie: jak zarządzać bezpieczeństwem informacji w organizacji, aby zminimalizować ryzyko pozyskania ich przez biały wywiad? W tym celu postawiono trzy hipotezy badawcze. Po pierwsze, przypuszcza się, że wywiad otwartoźródłowy pozwala na wejście w posiadanie informacji niejawnej. Po drugie, w niektórych przypadkach kompleksowe rozpoznanie obiektu wyłącznie tą metodą jest niemożliwe. Po trzecie, ryzyko pozyskania informacji przez biały wywiad można redukować odpowiednim ISM. Badania przeprowadzono przy użyciu metody studiów literaturowych oraz studium przypadku.

[2] S. Tzu, *Sztuka wojny. Traktat*, Gliwice 2012, s. 80.

Tematyka wykorzystywania źródeł jawnych oraz używania danych z nich zebranych nieustannie zyskuje na popularności. Terminy „prywatność" i „cyberbezpieczeństwo" pojawiają się coraz częściej w debacie publicznej[3]. W odpowiedzi na to zainteresowanie rynek wydawniczy przedstawia bogatą ofertę pozycji na temat OSINT oraz bezpieczeństwa informacji. Te źródła koncentrowały się jednak na ukazaniu możliwości OSINT, brakowało natomiast rzetelnych i wyczerpujących opracowań na temat zarządzania bezpieczeństwem informacji w kontekście pozyskania ich przez biały wywiad. Niniejszy artykuł powstał w celu wypełnienia choć w pewnym stopniu zaistniałej luki.

Informacja oraz zarządzanie informacją i jej bezpieczeństwem

Pochodzenia terminu „informacja" należy szukać w łacińskim słowie *informatio* – 'wyobrażenie', 'zawiadomienie', 'wyjaśnienie', potocznie 'jakakolwiek wiadomość'[4]. Jej elementami są dane, które rozpatrywane osobno nie mają wartości informacyjnej. Dopiero ich połączenie umożliwia nadanie im miana informacji[5]. Powstało wiele definicji tego pojęcia, niezależnie jednak od ich liczby informację można rozpatrywać w czterech głównych znaczeniach:

1) rzecz – produkt określonego procesu, ma źródło i odbiorcę i można mu przypisać właściwości, takie jak treść, forma, wartość, użyteczność,
2) mierzalna wielkość – wynika z konieczności ilościowej charakterystyki potrzebnej do oceny skuteczności komunikacji,
3) potencjał – zdolność do zmiany na skutek zmniejszenia niepewności wobec rozważanych rzeczy,
4) zmiana – odnosi się do jej roli w procesie kształtowania postaw i zachowań, może dokonywać się bezpośrednio przez odniesienie do zmiany zamierzonej, w postaci zalecenia, instrukcji lub ostrzeżenia albo pośrednio[6].

Informacjom przypisuje się określone cechy. Przede wszystkim istnieją obiektywnie, niezależnie od świadomości ludzi, a ich zbiór jest niewyczerpalny (nie zużywają się w procesie wykorzystania). Muszą być wyrażone wiadomością za pośrednictwem nośników materialnych oraz wymagają ciągłej aktualizacji. Mogą

[3] Na przykład od 2016 r. odbywa się w październiku kampania Europejskiego Miesiąca Cyberbezpieczeństwa. Zob. www.bezpiecznymiesiac.pl [dostęp: 29 XII 2023].

[4] K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010, s. 42.

[5] W. Krztoń, *Zarządzanie informacją w procesach decyzyjnych organizacji*, „Modern Management Review" 2017, nr 3, s. 84.

[6] Za: K. Liedel, *Zarządzanie informacją*…, s. 43–44.

występować w systemie jako czynnik sprawczy, przez odwołanie się do zjawisk niewystępujących w przeszłości i obecnie, ale mogących pojawić się w przyszłości (oraz tych, które nigdy nie istniały i nie zaistnieją). Mogą być przetwarzane, powielane i transportowane w czasie i w przestrzeni, mogą podlegać też celowym lub przypadkowym deformacjom albo fałszowaniu[7].

Informacja może mieć określoną wartość, która opisuje stopień spełnienia potrzeb użytkowników. Składają się na nią dwa czynniki: jakość i użyteczność[8]. Jakość to stopień spełnienia wymagań stawianych przez system decyzyjny w zakresie aktualności (otrzymania informacji w wymaganym czasie), pełności (zawarcia rzeczywistych informacji o stanie rzeczy) i niezawodności (określenia wpływu zakłóceń i zniekształceń na informacje)[9]. Użyteczność to cecha, która określa wpływ informacji na prawidłowość i trafność (zmniejszenie niewiedzy) w podejmowaniu decyzji[10].

Aby zapanować nad coraz większą ilością informacji, jest konieczne odpowiednie zarządzanie nimi. „Zarządzanie informacją" to termin, który pojawił się na początku lat 70. XX w. w czasie rewolucji technologicznej w masowym, komputerowym przetwarzaniu danych, będącym dziś podstawową funkcją zarządzania organizacją[11].

Gromadzenie, przetwarzanie i dystrybucja informacji to typy działalności informacyjnej. Gromadzenie jest elementem procesu decyzyjnego i znajduje zastosowanie w jednej z funkcji zarządzania, czyli planowaniu (w klasyfikacji funkcji zarządzania rozumianego jako planowanie, organizowanie, motywowanie i kontrola). Samo gromadzenie informacji nie wymaga szczegółowego opisywania, należy jednak pamiętać o ryzyku przesytu danych, co może powodować wprowadzenie chaosu informacyjnego i rozproszenie uwagi odbiorcy (ang. *attention crash*). Przetwarzanie to funkcja dostępna dla posiadacza urządzenia mobilnego. W podstawowym pakiecie niemal każdego z nich jest dostępne oprogramowanie do obróbki obrazu, dźwięku i tekstu, zatem modyfikacja informacji nie stanowi problemu. Dystrybucja informacji polega na przekazywaniu ich bez względu na bariery czasu i przestrzeni oraz ponoszenie opłat, przy wykorzystaniu dostępnej technologii[12].

---

[7] K. Liedel, *Zarządzanie informacją*…, s. 45; K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, s. 34–35.

[8] K. Liedel, *Zarządzanie informacją*…, s. 51.

[9] Tamże, s. 49.

[10] Tamże, s. 50.

[11] W. Krztoń, *Zarządzanie informacją w procesach decyzyjnych*…, s. 91.

[12] M. Nowina-Konopka, *Infomorfoza. Zarządzanie informacją w nowych mediach*, Kraków 2017, s. 81.

Informacja w kontekście bezpieczeństwa osób fizycznych i organizacji (w tym przedsiębiorstw i całych państw) odgrywa obecnie olbrzymią rolę. Rozpatrując zagadnienie bezpieczeństwa informacyjnego państwa, należy uwzględnić:

- informacje jako zasób strategiczny oraz podstawowy czynnik wytwórczy, generujący część dochodu narodowego[13],
- uzależnienie procesów decyzyjnych w sektorach gospodarki od systemów przesyłania i przetwarzania informacji,
- fakt, że współczesna rywalizacja między adwersarzami przenosi się na poziom walki informacyjnej, a mass media mogą być wykorzystywane do zakłócania informacyjnego[14].

Dlatego stwierdzenie, że (…) *bez racjonalnie ukształtowanej sfery informacyjnej nie może efektywnie funkcjonować współczesne społeczeństwo, państwo – jego administracja, nauka i szkolnictwo, kultura, gospodarka narodowa, siły zbrojne*[15], jest zgodne z prawdą. Informacja to kluczowy element współczesnych konfliktów, wykorzystuje się ją zarówno jako broń, jak i cel, a sfera informacyjna jest traktowana jako odrębne środowisko walki[16]. W 2014 r. podczas szczytu NATO w Newport w Walii przyjęto przełomową wówczas deklarację o możliwości przywołania art. 5 traktatu północnoatlantyckiego w razie najpoważniejszych cyberataków. Podczas kolejnego szczytu w Warszawie w 2016 r. cyberprzestrzeń uznano za współczesne pole walki, obok ziemi, powietrza, morza i przestrzeni kosmicznej. Ponadto, według Bolesława Balcerowicza walka informacyjna może być (…) *zjawiskiem autonomicznym, komponentem wspierającym działania militarne bądź głównym, wpieranym działaniami militarnymi*[17]. Koncepcja walki informacyjnej, mimo militarnego rodowodu, znajduje zastosowanie także w sferze politycznej, gospodarczej, kulturalnej, naukowej, sektorze publicznym i prywatnym[18].

Polityka bezpieczeństwa informacji wymusza zatem korzystanie z mechanizmów, które będą zabezpieczać prawidłowe przetwarzanie informacji (zapewnią bezpieczeństwo informacyjne). W celu stosowania właściwych zabezpieczeń opracowano System Zarządzania Bezpieczeństwem Informacji (SZBI), którego wdrożenie i użytkowanie zgodnie z wymaganiami międzynarodowej normy *ISO/IEC 27001*

[13] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 18.

[14] Zob. tamże; K. Liedel, *Zarządzanie informacją*…, s. 55.

[15] Za: K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 9.

[16] Tamże, s. 16–17.

[17] Tamże, s. 21.

[18] Tamże.

stanowi podstawę certyfikacji systemu bezpieczeństwa[19]. W rozumieniu wskazanej normy bezpieczeństwo informacyjne obejmuje:

1) poufność – dostęp wyłącznie dla uprawnionych osób,
2) spójność – monitorowanie procesu przetwarzania informacji w celu uniemożliwienia nieautoryzowanej modyfikacji,
3) dostępność – zawsze, gdy osoba uprawniona tego potrzebuje[20],
4) niezaprzeczalność – możliwość udowodnienia, że zdarzenia lub działania miały miejsce i wywołał je określony podmiot,
5) niezawodność – zamierzone, spójne i zachowane skutki[21].

Głównym celem SZBI jest takie zarządzanie ryzykiem, aby zminimalizować możliwość wystąpienia incydentów i zagrożeń. Poza wskazaną normą w polskim systemie prawnym istnieje jeszcze kilka pozycji, które poruszają tematykę bezpieczeństwa informacji (nie ma bowiem jednego aktu prawnego obejmującego to zagadnienie). Najistotniejsze z nich to:

- *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*,
- *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*,
- *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych*.

Ważne są również m.in.: *Ustawa z dnia 29 września 1994 r. o rachunkowości*, *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne*. Bezpieczeństwo informacyjne na szczeblu państwowym reguluje także *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* oraz *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*[22]. W dalszej części artykułu omówiono najważniejsze pozycje.

Konstytucja jako ustawa zasadnicza kodyfikuje powszechne prawodawstwo kraju. W jej zapisach można znaleźć fragmenty związane z bezpieczeństwem informacji oraz z prawem do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o życiu osobistym (art. 47). W art. 51 jest wskazane, że:

[19] J. Krawiec, *System Zarządzania Bezpieczeństwem Informacji – zabezpieczenia*, „Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie" 2017, nr 1 (38), s. 46.

[20] J. Łuczak, M. Tyburski, *Systemowe Zarządzanie Bezpieczeństwem Informacji ISO/IEC 27001*, Poznań 2009, s. 12–17.

[21] Dodatkowe dwa atrybuty wyróżniono w normie *PN-ISO/IEC 27000:2014*. Za: S. Stanek, *Podejmowanie decyzji w warunkach zagrożenia bezpieczeństwa informacyjnego organizacji*, Wrocław 2016, s. 30.

[22] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 19 XII 2023].

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Szczególnej ochronie podlegają informacje niejawne. Zgodnie z ustawą o ochronie informacji niejawnych (OIN) informacje niejawne to takie, (…) *których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania* (art. 1). Inne, pozanormatywne definicje wskazują, że ujawnienie informacji niejawnej osobie nieuprawnionej może mieć negatywny wpływ na organizację, jej członków albo na osoby z nią współpracujące (akcjonariuszy, partnerów, pracowników, klientów) oraz może obejmować informacje handlowe, marketingowe, finansowe, specyfikacje techniczne i inne o szczególnym znaczeniu dla funkcjonowania organizacji[23].

Obowiązująca ustawa określa zasady OIN rozumiane jako: klasyfikowanie i przetwarzanie informacji niejawnych, organizowanie ich ochrony, zasady organizacji kontroli stanu ich zabezpieczenia i stosowania środków bezpieczeństwa fizycznego. Ustawa definiuje kolejne klauzule niejawności: zastrzeżone, poufne, tajne, ściśle tajne (art. 5). W celu prawidłowego przetwarzania informacji niejawnych są organizowane szkolenia w zakresie OIN (art. 19–20) oraz jest przeprowadzana procedura sprawdzająca dotycząca rękojmi zachowania tajemnicy (art. 2 pkt 2). Zajmują się tym Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego. Służby te realizują zadania w zakresie OIN, w tym prowadzenie kontroli przestrzegania przepisów ustawy, postępowań sprawdzających, doradztw i szkoleń czy zapewnianie OIN wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi (art. 10 ust. 1).

Kolejnym ważnym dokumentem jest *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2020*. Określono w nim cele strategiczne, takie jak cyberbezpieczeństwo i bezpieczeństwo przestrzeni informacyjnej, oraz sposoby ich realizacji. Cele te obejmują (…) *zwiększenie poziomu ochrony informacji w sektorze publicznym,*

[23] K. Mitnick, W. Simon, *Sztuka podstępu. Łamałem ludzi, nie hasła*, Gliwice 2016, s. 297.

militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji[24] przez m.in.:

- zbudowanie (…) *zdolności do ochrony przestrzeni informacyjnej*,
- stworzenie jednolitego systemu komunikacji strategicznej państwa, (…) *którego zadaniem powinno być prognozowanie, planowanie i realizowanie spójnych działań komunikacyjnych, przy wykorzystaniu szerokiej gamy kanałów komunikacji i mediów*,
- aktywne przeciwdziałanie dezinformacji przez (…) *stworzenie procedur współpracy z mediami informacyjnymi oraz społecznościowymi, przy zaangażowaniu obywateli i organizacji pozarządowych*,
- dążenie do (…) *zwiększenia świadomości społecznej o zagrożeniach związanych z manipulacją informacją poprzez edukację w zakresie bezpieczeństwa informacyjnego*[25].

Armie różnych państw świata także dostrzegają zarówno korzyści ze sprawnego zarządzania informacją w organizacji, jak i potrzebę bezpieczeństwa w tym zakresie. Wojsko Polskie dba o bezpieczeństwo informacji o żołnierzach i wykonywanych przez nich zadaniach. Kampania pod hasłem „#ŚwiadomiZagrożeń" zwraca uwagę na problem udostępniania w sieci danych personalnych, zdjęć infrastruktury krytycznej lub jednostek wojskowych, geolokalizacji czy terminów ćwiczeń wojskowych.

Obecnie nie tylko organizacje są zainteresowane tematyką bezpieczeństwa informacji. To zagadnienie nurtuje zwykłych ludzi, do czego przyczynił się efekt Snowdena[26]. Tajne dokumenty National Security Agency (NSA), które zostały upublicznione w 2013 r. przez Edwarda Snowdena, ujawniły, że służby specjalne przy wykorzystaniu technologii są w stanie prowadzić inwigilację obywateli, większą niż można było przypuszczać. Innymi słowy (…) *NSA była w stanie podsłuchiwać niemal wszystko i każdego, w kraju i za granicą, za zgodą sądu i bez niej*[27]. Te informacje spowodowały zmianę na niemal wszystkich poziomach społecznych – począwszy od stosunków dyplomatycznych, przez ustawodawstwo krajowe i międzynarodowe, aż do sposobu myślenia przeciętnych ludzi. Pytano, kto kontroluje kontrolujących. Efekt Snowdena wywołał dyskusję o publikowaniu własnych danych w sieci oraz zweryfikował mit anonimowości w internecie. Była to nauka także dla agencji wywiadowczych.

---

[24] *Strategia Bezpieczeństwa Narodowego*…, s. 20.

[25] Tamże, s. 21.

[26] Edward J. Snowden (ur. 1983) – amerykański sygnalista (ang. *whistleblower*), były pracownik CIA i zleceniobiorca NSA oraz informatyk samouk, który według szacunków upublicznił ok. 1,7 mln dokumentów poufnych, tajnych i ściśle tajnych, co uznano za największy wyciek informacji niejawnych w historii Stanów Zjednoczonych. Za: M. Nowina-Konopka, *Infomorfoza*…, s. 238–242.

[27] T. Aleksandrowicz, „*Efekt Snowdena*", Wszystko Co Najważniejsze, 7 VI 2014 r., https://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-efekt-snowdena/ [dostęp: 11 IV 2022].

Przekonały się, że powszechna inwigilacja i gromadzenie niezliczonej ilości informacji nie mają sensu, gdyż (…) *trzeba wiedzieć, co się chce wiedzieć i co musimy wiedzieć. Inaczej będziemy wiedzieć wszystko – i nic*[28].

Biały wywiad – charakterystyka, potencjał i ograniczenia, źródła OSINT

Przypomniane na początku artykułu słowa Sun Tzu nie tracą na aktualności. Organy państwa od dawna poszukiwały informacji pomocnych w podejmowaniu decyzji, od których zależało bezpieczeństwo wewnętrzne i zewnętrzne. W tym celu wykorzystywano agentów i informatorów (źródła osobowe), przechwytywano dokumenty oraz stosowano metody przypisywane dziś białemu wywiadowi. Początkowo opierały się one na czytaniu materiałów pisanych, co znacznie ułatwił druk wynaleziony w połowie XV w. Kolejne źródła otwarte, pierwowzór dzisiejszych gazet, pojawiły się w XVII w. W późniejszych latach rosła liczba wynalazków, które wpłynęły na dostępność informacji. Dzięki telegrafowi, radiu, telefonowi, telewizji, a następnie komputerowi można dziś przesyłać szybko i na duże odległości niezliczone ilości informacji[29].

Zagraniczne instytucje wywiadowcze określały te działania początkowo jako wywiad jawny (ang. *overt intelligence*). Rodzime pojęcie białego wywiadu było używane znacznie wcześniej niż angielskojęzyczny akronim OSINT[30]. W polskiej literaturze biały wywiad jest przeciwieństwem czarnego – twardego i operacyjnego, który zdobywa informacje w sposób tajny, a czasem nawet nielegalny. Biały wywiad wyróżnia się brakiem konieczności naruszania prywatności lub łamania prawa. Przymiotnik „biały" sugeruje, że ta metoda jest na swój sposób niewinna[31]. Praktyka udowadnia jednak, że między tymi dwoma sposobami działania istnieje szerokie spektrum szarości[32].

Współczesny OSINT jest domeną przede wszystkim cywilną, a jego głównym beneficjentem pozostają wciąż służby specjalne. Jak podaje Andrzej Nowosad, według stanu wiedzy na 2005 r. wywiady obcych państw pozyskiwały 95% informacji

---

[28] Tamże.

[29] Za: A. Wojciulik, *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków*, w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski, W. Mądrzejowski (red.), Warszawa 2011, s. 46–47.

[30] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, s. 15.

[31] W. Filipkowski, W. Mądrzejowski, *Wstęp*, w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski, W. Mądrzejowski (red.), Warszawa 2011, s. 14.

[32] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 16–17.

ze źródeł jawnych, 4% z półjawnych i jedynie 1% ze źródeł tajnych[33]. Wydaje się, że wraz z postępem technologicznym stosunek udziału poszczególnych dziedzin wywiadowczych zmienił się na korzyść białego wywiadu. Informacje ze źródeł otwartych analizuje się dziś według czterech następujących po sobie etapów i są one klasyfikowane jako:

1) *Open Source Data* – surowe dane ze źródła nieobjętego klauzulą tajności,
2) *Open Source Information* – dane po wstępnej analizie, zgrupowane i przekazane osobom zarządzającym,
3) *Open Source Intelligence* – wybrane dane przekazane wyselekcjonowanej grupie odbiorców według założeń określonych przez składającego zapytanie (ang. *request for information*),
4) *Validated Open Source Intelligence* – dane zweryfikowane, z przypisanym wysokim poziomem pewności[34].

Informacje zebrane z wykorzystaniem OSINT przynoszą wiele korzyści związanych z rozpoznaniem celu. Wyróżnia się trzy najważniejsze funkcje OSINT: podstawową, naprowadzającą i komplementarną. Funkcja podstawowa oznacza użycie technik białego wywiadu w przypadku niedostępności źródeł operacyjnych albo braku konieczności ich wykorzystania. Funkcja naprowadzająca może sygnalizować zagrożenia i potrzebę objęcia danego podmiotu zainteresowaniem operacyjnym. Funkcja komplementarna wobec źródeł operacyjnych pozwala na uzupełnianie informacji zdobytych różnymi metodami, dzięki czemu można zbudować kompleksowy obraz analizowanego problemu[35]. Biały wywiad zapewnia ponadto takie korzyści, jak:

- łatwa dostępność informacji,
- szybkość pozyskiwania informacji,
- ilość, różnorodność, jakość i przejrzystość informacji,
- niskie koszty analizy uzyskanych informacji[36].

Biały wywiad pozwala na znacznie szybsze pozyskiwanie informacji w porównaniu z działaniami operacyjnymi. Nie wymaga odbywania spotkań czy dostarczania zdobytych informacji. Otwarte źródła zapewniają niemal nieograniczoną ilość

[33] A. Nowosad, *Metody i techniki pozyskiwania i przetwarzania informacji medialnej na potrzeby białego wywiadu*, „Państwo i Społeczeństwo" 2005, nr 2, s. 59.

[34] B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5, s. 149.

[35] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*, w: *Rola mediów w przeciwdziałaniu terroryzmowi*, K. Liedel, P. Piasecka (red.), Warszawa 2009, s. 85–86.

[36] Por. B. Saramak, *Wykorzystanie otwartych źródeł informacji…*, s. 31; *Rozpoznanie ze źródeł otwartych DD-2.9(A),* Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2020, s. 2-2.

informacji, a w związku ze swoją specyfiką są dużo tańsze niż ich odpowiedniki, takie jak źródła osobowe czy systemy techniczne, np. satelitarne[37]. Zalety OSINT zostały dostrzeżone przez służby specjalne oraz policyjne. Masowe pozyskiwanie danych przy użyciu OSINT pozwala skuteczniej wypełniać zadania ustawowe tych służb. Podejmują one działania mające na celu zapewnienie bezpieczeństwa struktur państwa, porządku publicznego oraz obywateli. Jednymi z największych zagrożeń są współcześnie terroryzm i organizacje o charakterze przestępczym. Dzięki OSINT można realizować zadania przeciwdziałania organizacjom tego typu. W ocenie ekspertów korporacji RAND[38] 70–80% kluczowych dla antyterroryzmu informacji pochodzi ze źródeł otwartych, pozostałą część pozyskuje się przez wywiad operacyjny[39]. Tomasz Aleksandrowicz zauważył, że terroryści z powodzeniem wykorzystują internet „w walce o medialność", ponieważ jest on bardziej efektywnym narzędziem niż tradycyjne media[40]. Według stanu wiedzy na 2012 r. Al-Kaida publikowała swoje informacje na niemal 6000 stron internetowych[41]. Sieć zapewnia terrorystom nieskrępowany dostęp do odbiorców ze środowiska opiniotwórczego oraz daje możliwość publikowania treści pozbawionych kontroli, obróbki redakcyjnej czy cenzury[42]. Działania propagandowe terrorystów mogą koncentrować się na uzyskaniu rezultatów pozytywnych (pozyskanie sympatyków) lub negatywnych (skutki psychologiczne – wywołanie strachu i poczucia zagrożenia)[43]. Źródła otwarte można wykorzystać w walce z organizacjami terrorystycznymi w kilku obszarach. Po pierwsze, OSINT pozwala poznać historię, manifesty i oświadczenia organizacji, na ich podstawie określić jej strategię, a następnie przygotować odpowiedni sposób postępowania. Po drugie, wykorzystanie źródeł jawnych daje możliwość przeciwdziałania mechanizmom pozyskiwania nowych członków i zwolenników organizacji. Dzięki funkcji naprowadzającej zdobyte informacje mogą być wskazówką do podejmowania działań antyterrorystycznych. Po trzecie, OSINT może stanowić uzupełnienie i/lub weryfikację źródła operacyjnego w celu kompleksowego rozpracowania organizacji. Długotrwała aktywność służb, która prowadzi m.in. do ustalenia

[37] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 85.

[38] RAND Corporation – amerykański think tank i organizacja badawcza non profit, założona 14 maja 1948 r. na potrzeby Sił Zbrojnych Stanów Zjednoczonych. Obecnie RAND zatrudnia ok. 1600 pracowników w sześciu siedzibach w USA oraz w Europie. Prowadzi badania w dziedzinach obronności i terroryzmu, stosunków międzynarodowych, edukacji czy zdrowia publicznego. Za: Wikipedia, https://pl.wikipedia.org/wiki/RAND_Corporation [dostęp: 29 XII 2023].

[39] Za: T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 86.

[40] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 25.

[41] Tamże.

[42] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 87.

[43] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 25.

korelacji zjawisk, jest możliwa dzięki wykorzystaniu źródeł otwartych, w tym naukowych, w ramach outsourcingu wywiadowczego[44].

Potencjał OSINT został zauważony także w sferze biznesu, który rozwinął dziedzinę wywiadu gospodarczego. Ocenia się, że wielkie korporacje mogą dysponować dziś większym i bardziej efektywnym aparatem wywiadowczym niż służby wywiadowcze mniej zamożnych państw[45]. Biznes korzysta w tym celu z usług wywiadowni gospodarczych, które cieszą się już międzynarodową popularnością. Mają one charakter przedsiębiorstw wykonujących zadania z zakresu wywiadu gospodarczego, takie jak sporządzanie raportów o podmiotach gospodarczych, opracowywanie rankingów wiarygodności firm, określanie bezpiecznego poziomu finansowania przedsięwzięć gospodarczych. Dodatkowo zajmują się określaniem trendów w sektorach gospodarczych, tworzeniem baz danych i wykazów dłużników, oferują wsparcie przy windykacji i współpracują z bankami i firmami ubezpieczeniowymi w ramach analizy ryzyka[46]. Wywiadownie gospodarcze (również agencje detektywistyczne) bazują na informacjach pozyskanych często ze źródeł otwartych. Wskazują przy tym na etykę i zgodność z prawem swoich działań, a także na zachowanie dyskrecji cenionej w biznesie. Źródła jawne wykorzystywane w wywiadzie gospodarczym to m.in. publiczne wypowiedzi (np. przedstawicieli zarządów), serwisy społecznościowe (w tym branżowe, np. LinkedIn), sondy społeczne, dokumentacje i rejestry z otwartym dostępem czy ogłoszenia sądowe.

Istnieją jednak ograniczenia OSINT. Są to m.in.:

1) **zbyt duża ilość danych** – zdobywanie olbrzymiej liczby informacji wiąże się z pozyskiwaniem również tych nieistotnych z wywiadowczego punktu widzenia. To zjawisko powoduje czasochłonność prowadzenia analizy, a wyselekcjonowanie wiarygodnych informacji wymaga fachowej wiedzy, umiejętności oraz sporego doświadczenia. Innymi słowy, największa zaleta OSINT jest jednocześnie jego wadą;
2) **nieprecyzyjne informacje** – pozyskane dane mogą być nieprecyzyjne, stronnicze albo wprowadzać dezinformację. Informacje w internecie są często wielokrotnie kopiowane, zwykle bez podawania pierwotnego źródła, co komplikuje ocenę ich przydatności, aktualności i rzetelności. Weryfikacja źródeł, choć może ograniczyć problemy, nie wyeliminuje ich całkowicie;

[44] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 88–90.

[45] Tamże, s. 92.

[46] P. Niemczyk, *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu"*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 147.

3) **ograniczenia prawne** – istnieje wiele złożonych kwestii prawnych związanych z pozyskiwaniem, przechowywaniem i niszczeniem danych pochodzących ze źródeł otwartych. W polskim prawie ograniczenia wynikają z praw człowieka (obejmujących prawo do prywatności, wolności słowa, ochrony danych osobowych i własności intelektualnej) oraz aktów prawa międzynarodowego[47];
4) **ograniczenia językowe** – problem bariery językowej zawsze towarzyszy działalności wywiadowczej. Chociaż język angielski dziś jest jednym z najpowszechniej używanych na świecie, to informacje z części globu stanowiących najsilniejsze punkty zapalne nie są publikowane w sieci w tym języku na tyle często, by było możliwe efektywne pozyskiwanie danych. Szacuje się, że nawet 50–80% informacji dotyczących krajów wywiadowczego zainteresowania państw zachodnich nie jest publikowane w języku angielskim[48]. Brak specjalistów posługujących się językami, takimi jak arabski, chiński czy rosyjski, znacznie ogranicza przydatność białego wywiadu, nawet przy wykorzystaniu elektronicznych translatorów. Wskazuje się też na konieczność posiadania wiedzy kulturowej w zakresie rozpatrywanego zagadnienia – znajomość realiów historycznych, społecznych i politycznych pozwala na prawidłową interpretację informacji oraz ocenę wiarygodności źródeł[49];
5) **rozwój technologiczny** – dynamiczny rozwój sprawia, że technologie wykorzystywane do pozyskiwania danych mogą się szybko zdezaktualizować. Duże nadzieje pokłada się w inteligentnych, samouczących się algorytmach, jednak wizja zrobotyzowanego białego wywiadu wydaje się wciąż odległa. Szybkość przyrostu informacji znacznie przewyższa możliwości współczesnych programów przeznaczonych do ich analizy[50]. Dlatego analitycy OSINT muszą ciągle aktualizować swoją wiedzę i podnosić swoje kwalifikacje;
6) **konieczność przestrzegania bezpieczeństwa operacji** (ang. *operations security*, OPSEC) – pozyskiwanie informacji ze źródeł otwartych wymaga

[47] Zob. art. 12 *Powszechnej Deklaracji Praw Człowieka z dnia 10 grudnia 1948 r.*, https://www.bb.po.gov.pl/images/Prawa/PNZ/PDPCZ.pdf [dostęp: 13 XII 2023]; art. 17 *Międzynarodowego Paktu Praw Obywatelskich i Politycznych otwartego do podpisu w Nowym Jorku dnia 19 grudnia 1966 r.*; art. 8 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2*; art. 7–8 *Karty praw podstawowych Unii Europejskiej*.

[48] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 36.

[49] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 91.

[50] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 35.

działania w zgodzie z OPSEC, rozumianym jako (…) *proces zapewniający odpowiedni poziom bezpieczeństwa operacjom lub działaniom* (…) *w celu ukrycia przed przeciwnikiem możliwości i zamiarów sił własnych*[51];

7) **niska przydatność w niektórych obszarach** – biały wywiad nie zawsze będzie uniwersalny i wszechstronny. Terroryści działający w pojedynkę (ang. *lone wolves*) są np. niemożliwi do zlokalizowana i – ze względu na brak podejrzanych powiązań – zapobieganie ich działalności jest trudne[52]. Przywódcy najgroźniejszych grup terrorystycznych wykorzystują internet do celów propagandowych bardzo profesjonalnie i nie zostawiają cyfrowych śladów (ang. *digital footprint*). Przez większość czasu znajdują się w miejscach odciętych zarówno od sieci, jak i od świadków. W takich przypadkach zdobycie danych jest możliwe jedynie dzięki działalności źródeł osobowych (ang. *human intelligence*, HUMINT)[53].

Najpopularniejsza i najbardziej odpowiednia klasyfikacja źródeł białego wywiadu wyodrębnia:

1) wystąpienia publiczne,
2) dokumenty publiczne,
3) programy nadawane publicznie,
4) szarą literaturę,
5) komercyjne bazy danych,
6) internet i media społecznościowe[54].

Wystąpienia publiczne to przekazywanie informacji drogą ustną podczas wydarzeń otwartych i odbywających się w miejscach publicznych. Obejmują one m.in.: dokumentację sądową, wyniki kontroli organów do tego uprawnionych, konferencje prasowe, wiece polityczne, posiedzenia rządu, wykłady, debaty akademickie, kazania religijne, wystawy naukowe i komercyjne. Przyjmuje się, że podczas wystąpień publicznych mówca i słuchacze nie oczekują prywatności[55].

Dokumentami publicznymi są rzeczowe świadectwa danego zjawiska sporządzone w formie właściwej dla danego miejsca i czasu, np.: książki i podręczniki,

[51] *AAP-6 Słownik terminów i definicji NATO*, 2017, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf, s. 336 [dostęp: 24 II 2021].

[52] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 115.

[53] Taka sytuacja zaistniała podczas ustalania miejsca pobytu Osamy bin-Ladena w 2011 r. Zob. B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 36.

[54] Klasyfikacja na podstawie: *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 47–50.

[55] Tamże, s. 47.

czasopisma fachowe, ulotki i broszury marketingowe, mapy, fotografie[56], materiały publikowane przez rządy (raporty, dane statystyczne, projekty legislacyjne)[57].

Program nadawany publicznie należy rozumieć jako (…) *jednoczesną transmisję informacji dla użytku ogólnego do odbiorników (przekaźników) w ramach sieci komputerowej, radiowej, telekomunikacyjnej lub telewizyjnej*[58]. Można tu wyszczególnić źródła radiowe i telewizyjne, a z tej klasyfikacji wyodrębnić radiowe rozgłośnie informacyjne, filmy (programy) dokumentalne, materiały filmowe oraz programy radiowe inne niż rozrywkowe[59].

Pod pojęciem szarej literatury kryją się informacje niezastrzeżone, a równocześnie niedostępne komercyjnie. Obejmują one m.in.:

- książki (opracowania) nieobjęte rejestracją bibliograficzną,
- niepublikowane tłumaczenia,
- projekty i rysunki techniczne,
- sprawozdania i raporty naukowe (techniczne, ekonomiczne, społeczne),
- dokumenty dotyczące standardów technicznych (normy, zalecenia, ekspertyzy),
- materiały promocyjne i reklamowe,
- dysertacje magisterskie i doktorskie,
- wewnętrzne materiały metodyczne i szkoleniowe[60].

Źródła szarej literatury są dostępne dzięki specjalistycznym kanałom lub przez bezpośredni kontakt z organizacjami je wytwarzającymi. Przykładami mogą być: agencje rządowe, organizacje pozarządowe, ośrodki akademickie, biblioteki, profesjonalne towarzystwa branżowe oraz ośrodki badawcze statutowo nieprowadzące działalności wydawniczej[61]. Szara literatura jest kolportowana w ograniczonej liczbie egzemplarzy, jednak dostęp do niej jest utrudniony tylko pozornie. W wielu krajach oraz wspólnotach funkcjonują elektroniczne bazy danych, które umożliwiają dotarcie do tego typu dokumentów za pomocą wyszukiwarki. W Europie taką bazą jest OpenGrey (www.opengrey.eu), w Polsce – serwis Nauka Polska (www.nauka-polska.pl), który umożliwia dostęp do baz zawierających raporty i sprawozdania z badań naukowych, informacje o pracach badawczo-rozwojowych, materiały konferencyjne oraz spisy nazwisk osób związanych z danymi dziedzinami nauki[62].

---

[56] Tamże.

[57] K. Liedel, *Zarządzanie informacją*…, s. 65.

[58] *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 47.

[59] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 58.

[60] Zob. *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 50; B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 70.

[61] Tamże.

[62] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 71–72.

Profesjonalne bazy, do których dostęp można uzyskać po opłaceniu abonamentu, takie jak Factiva (www.factiva.com), LexisNexis (www.lexis-nexis.com), Dialog (www.dialog.com), komercyjne bazy fotografii i obrazów (np. z dostępem do zdjęć satelitarnych powierzchni Ziemi), znajdują się na pograniczu otwartości źródeł[63].

Najważniejszym i wymagającym odrębnego omówienia źródłem jest internet. Samą sieć internetową porównuje się do góry lodowej. Jej mały, widoczny wierzchołek stanowi jawna, zindeksowana część, pod powierzchnią wody znajduje się zaś niezmierzona ilość treści o ograniczonym dostępie[64]. Internet dzieli się na trzy poziomy:

1) sieć zindeksowaną (ang. *surface web*), czyli używaną powszechnie, jawną część,
2) sieć głęboką (ang. *deep web*), której treści są niedostępne przy użyciu darmowych i powszechnych wyszukiwarek, obejmującą prywatne strony, na których jest konieczna rejestracja w celu uzyskania dostępu,
3) sieć ciemną (ang. *dark web*), która jest częścią sieci głębokiej, stanowiącą zbiór niewidocznych publicznie stron. Tego typu strony są zakodowane (zaszyfrowane) i dostęp do nich wymaga konkretnej konfiguracji lub autoryzacji albo specjalnego oprogramowania[65].

Szacuje się, że niemal połowa populacji świata ma dostęp do internetu. Co roku do użytkowników sieci dołączają setki milionów nowych. W 2014 r. ogólna liczba stron internetowych przekroczyła 1 mld[66]. Pięć lat później oceniano, że średnio co minutę na portalu Facebook pojawiało się ok. 500 000 nowych komentarzy, 293 000 postów oraz 450 000 zdjęć[67]. Media społecznościowe są ważnym elementem internetu z punktu widzenia białego wywiadu. Przykładami takich mediów są sieci:

- społecznościowe,
- fachowe (branżowe),
- networkingowe,
- do publicznego udostępniania treści wideo (wideoblogi), audio (podcasty) oraz zdjęć (hosting),
- z blogami i mikroblogami.

---

[63] K. Liedel, *Zarządzanie informacją*…, s. 65.

[64] Zawartość sieci zindeksowanej szacuje się na 4%, sieci głębokiej na 90%, a sieci ciemnej na 6% objętości treści w całym internecie. Za: T. Leżoń, *Głęboko pod powierzchnią jest miejsce, o którym wolałbyś nie wiedzieć*, Magazyn TVN24, https://tvn24.pl/magazyn-tvn24/gleboko-pod-powierzchnia-jest-miejsce-o-ktorym-wolalbys-nie-wiedziec,95,1850 [dostęp: 12 III 2021].

[65] *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 48–49.

[66] P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny. Media społecznościowe jako broń*, Kraków 2019, s. 76.

[67] Tamże, s. 86.

Media społecznościowe zawdzięczają popularność przemianom społeczno-kulturowym oraz technologicznym w zakresie upowszechnienia internetu mobilnego i urządzeń mobilnych[68]. Pozyskiwanie informacji z social mediów przez biały wywiad może być uznane dziś za subdyscyplinę OSINT, która w literaturze anglojęzycznej ma nazwę SOCMINT (ang. *social media intelligence*)[69]. Jej cel to identyfikacja i zrozumienie węzłów sieci oraz relacji między nimi[70]. SOCMINT jest przydatny szczególnie w pracy organów ścigania oraz prokuratury. Portale społecznościowe dostarczają materiałów dowodowych dotyczących popełnienia czynów zabronionych, takich jak zniesławienia, zniewagi, stalking, rozpowszechnianie pornografii, naruszenie prawa wyborczego czy nawet handel ludźmi[71]. Brak autorefleksji podczas publikowania informacji osobistych w sieci albo wyrażanie opinii w sposób widoczny dla wszystkich użytkowników jest ułatwieniem dla służb i organów ścigania.

Zdjęcia publikowane w sieci często zawierają metadane, czyli informacje o pliku, takie jak np. jego wielkość, data wykonania, autor, w przypadku zdjęcia urządzenie, jakim je zrobiono, a nawet dane na temat lokalizacji urządzenia w momencie wykonania fotografii[72]. Amerykańskie rządowe oprogramowanie RIOT (ang. *Rapid Information Overlay Technology*) zaprezentowane w 2010 r. wyszukuje i łączy metadane. Ten system służy do profilowania obywateli na podstawie informacji z serwisów społecznościowych. Potrafi wskazać lokalizacje i przeanalizować aktywność w miejscach, w których dana osoba przebywała, a także stworzyć sieć powiązań z innymi użytkownikami social mediów[73]. Podobne zastosowanie ma oprogramowanie Maltego, które wyszukuje relacje między publicznie dostępnymi treściami oraz pozwala je skonwertować i przedstawić siatkę powiązań za pomocą grafu. Istotnym elementem analizy OSINT przy użyciu metadanych jest wykorzystanie geolokalizacji. Metadane zapisywane automatycznie przez urządzenie, którym wykonuje się fotografię (nagranie), pozwalają zwykle na późniejsze zlokalizowanie użytkownika.

---

[68] Szacuje się, że liczba urządzeń mobilnych już w 2012 r. zrównała się z liczbą ludności świata. Za: M. Nowina-Konopka, *Infomorfoza*…, s. 106.

[69] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 84.

[70] *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 49.

[71] B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce*…, s. 162.

[72] Tamże, s. 152.

[73] *RIOT – rządowy system inwigilacji i profilowania przez serwisy społecznościowe*, Niebezpiecznik, 17 II 2013 r. https://niebezpiecznik.pl/post/riot-rzadowy-system-inwigilacji-przez-serwisy-spolecznosciowe/ [dostęp: 16 III 2021].

Możliwości białego wywiadu są zauważane i doceniane przez coraz większą liczbę służb specjalnych[74] i policyjnych. Współcześnie nawet sądy przychylnie patrzą na dowody zgromadzone w ten sposób. Punktem zwrotnym w tym zakresie była sprawa libijskiego zbrodniarza Mahmuda al-Werfallego. W sierpniu 2017 r. Międzynarodowy Trybunał Karny w Hadze wydał nakaz jego aresztowania na podstawie dowodów opartych niemal wyłącznie na informacjach z mediów społecznościowych[75]. Wykorzystanie w procesie sądowym materiałów pochodzących z OSINT jest jednak skomplikowane z uwagi na niezbędną rzetelność informacji i ich źródeł, a także potrzebę utrwalania takich materiałów w specjalnych bazach danych. To kluczowe w kontekście trwałości i równocześnie ulotności treści internetowych. Z jednej strony, informacje raz udostępnione w sieci są niemal niemożliwe do usunięcia, z drugiej strony, w gąszczu informacji trudno odnaleźć taką, która zwróci uwagę odbiorcy.

Tematem OSINT są zainteresowani także dziennikarze śledczy. Narzędzia białego wywiadu umożliwiają im uzyskanie informacji na temat np. konfliktów zbrojnych, wpływowych osób, działalności skrajnych światopoglądowo grup, brutalności resortów siłowych czy degradacji środowiska naturalnego[76]. Pojedynczy obywatele, w tym hobbyści i pasjonaci[77], również korzystają z OSINT, a z roku na rok rośnie liczba otwartych szkoleń, organizowanych głównie przez instytucje związane z cyberbezpieczeństwem[78].

OSINT w zarządzaniu bezpieczeństwem informacji – studium przypadku

Rozwój technologii i mediów społecznościowych doprowadził do tego, co można nazwać złotym wiekiem OSINT[79]. Punktem zwrotnym oraz krokiem w kierunku budowania społeczeństwa odpornego na dezinformację były obserwacje m.in. Eliota

[74] Zob. wykład Agencji Wywiadu pt. *OSINT – nie lekceważ białego wywiadu*, zorganizowany 12 I 2022 r. we współpracy ze studenckimi kołami naukowymi Uniwersytetu Warszawskiego, www.facebook.com/events/1035173887046324/ [dostęp: 16 I 2022].

[75] E. Higgins, *Bellingcat. Ujawniamy prawdę w czasach postprawdy*, Katowice 2021, s. 277.

[76] Tamże, s. 293.

[77] Zob. *OSINT Quest Challenge* organizowany z inicjatywy pasjonatów analizy źródeł otwartych, www.osintquest.pl/category/challenge [dostęp: 16 I 2022].

[78] Zob. m.in. szkolenie *OSINT: zaawansowane pozyskiwanie szczegółowych informacji na temat ludzi i firm* organizowane przez redakcję portalu Niebezpiecznik czy seria „OSINT master" zespołu portalu Sekurak.

[79] *The Golden Age of OSINT is over*, Key Findings, 4 I 2019 r., https://keyfindings.blog/2019/01/04/the-golden-age-of-osint-is-over/ [dostęp: 6 II 2022].

Higginsa, który odkrywał zagrożenia i potencjał źródeł otwartych. Jak stwierdził w swojej książce pt. *Bellingcat. Ujawniamy prawdę w czasach postprawdy*, natrafił na lukę w systemie informacji i postanowił codziennie ją zapełniać[80].

Brytyjczyk Eliot Higgins (ur. w 1979 r.) pierwsze kroki w obywatelskim dziennikarstwie śledczym stawiał w 2012 r. na blogu „Brown Moses", na którym skupiał się na wyjaśnianiu przypadków użycia broni chemicznej w Syrii. Nie znał języka arabskiego, więc po arabskojęzycznej części sieci poruszał się przy użyciu internetowego translatora. Prowadzone śledztwa przysporzyły mu popularności, a wraz z wyjaśnianiem kolejnych spraw zyskiwał coraz większą liczbę fanów, współpracowników i wolontariuszy. W konsekwencji tego powstała grupa Bellingcat. Dziś funkcjonuje ona jako globalna społeczność internetowa, której zadaniem jest prowadzenie śledztw, zwalczanie dezinformacji i tropienie zbrodni wojennych na podstawie danych ze źródeł otwartych.

Bellingcat ma charakter społeczny i egalitarny; funkcjonuje jako (…) *agencja wywiadowcza dla wszystkich*[81]. Motto organizacji opiera się na trzech filarach: odkrywanie (spraw, które pominięto lub które można wyśledzić w internecie), weryfikowanie (dowodów) i nagłaśnianie (uzyskanych informacji)[82]. Zespół składa się z zawodowych dziennikarzy śledczych oraz ze stałych współpracowników i wolontariuszy. Swoją działalność finansuje ze zbiórek publicznych, z grantów i płatnych szkoleń[83]. Unika przy tym finansowania przez rządy państw, co ma zapewnić organizacji niezależność. Uzyskane wyniki prezentuje na stronie internetowej (www.bellingcat.com) w formie raportów, artykułów i podcastów. Wśród sukcesów grupy można wymienić: udowodnienie użycia broni chemicznej w Syrii (2012 r.), zidentyfikowanie sympatyków Państwa Islamskiego w Europie (2016 r.), rozpracowanie neonazistowskiej grupy odpowiedzialnej za zamieszki w Charlottesville w Stanach Zjednoczonych (2017 r.), ujawnienie udziału rosyjskich agentów w otruciu w Anglii Siergieja Skripala (2018 r.), współuczestnictwo w demaskowaniu dezinformacji związanej z pandemią SARS-CoV-2 (od 2019 r.).

W niniejszym artykule przedmiotem analizy przypadku będzie zestrzelenie samolotu Boeing 777-00ER, lot nr MH17 linii lotniczych Malaysia Airlines z Amsterdamu do Kuala Lumpur 17 lipca 2014 r., do którego doszło w przestrzeni powietrznej obwodu donieckiego w Ukrainie kontrolowanego przez prorosyjskich separatystów.

---

[80] E. Higgins, *Bellingcat. Ujawniamy prawdę*…, s. 69.

[81] Tamże, s. 17.

[82] Tamże, s. 91.

[83] B. Biel, *Internet pełen jest dowodów na zbrodnie. Trzeba wiedzieć, gdzie ich szukać*, Magazyn TVN24, https://tvn24.pl/magazyn-tvn24/internet-pelen-jest-dowodow-na-zbrodnie-trzeba-wiedziec-gdzie-ich-szukac,158,2754 [dostęp: 26 I 2022].

Zginęły wszystkie osoby będące na pokładzie – 283 pasażerów i 15-osobowa załoga[84]. Portal Bellingcat zaczął działalność dwa dni przed tym zdarzeniem. Przez kolejne lata grupa pracowała nad wykryciem przyczyn tragedii i osób za nią odpowiedzialnych oraz demaskowaniem manipulacji przekazów dotyczących przebiegu katastrofy. Efektem tego były szczegółowe raporty prezentowane w latach 2014–2019.

W jednym z pierwszych raportów można prześledzić drogę, jaką przebył wojskowy konwój przewożący system kierowanych pocisków Buk M1. Zdjęcie opublikowane 25 lipca 2014 r. przez „Paris Match" przedstawia system transportowany na samochodzie ciężarowym. Analiza fotografii pozwoliła wskazać miejsce oraz czas jej wykonania (określony przez położenie słońca, co ustalono na podstawie cienia rzucanego przez pojazd). Późniejsze posty i nagrania w sieci dostarczały kolejnych informacji dotyczących trasy konwoju. W następnych dniach system Buk był transportowany już nie na samochodzie ciężarowym, lecz poruszał się na gąsienicach.

Kilka dni wcześniej, 17 lipca, miejscowi dziennikarze informowali o wyrzutni z załadowanymi czterema pociskami rakietowymi SA-11. Według lokalnych informacji ok. godziny 16.20 dało się słyszeć huk, po którym zaobserwowano szczątki samolotu spadające z nieba. Kilka godzin później w sieci opublikowano zdjęcie dymu charakterystycznego dla momentu po wystrzeleniu pocisku. Na tej podstawie, a także przy użyciu zdjęć satelitarnych wywiadu Stanów Zjednoczonych oraz fotografii i zeznań świadków, metodą wcięć ustalono dokładne miejsce wystrzelenia pocisku[85]. Ostatni z analizowanych materiałów wideo z 18 lipca ukazywał system Buk podczas ponownego transportu prawdopodobnie tym samym samochodem ciężarowym. Wyrzutnia przewoziła wówczas już tylko trzy pociski[86].

Do przeprowadzenia dalszego śledztwa Bellingcat wykorzystał, oprócz fotografii, nagrań i relacji świadków, posty rosyjskich żołnierzy opublikowane w mediach społecznościowych (VK, Instagram, Odnoklassniki). Niejednokrotnie to oni sami bezrefleksyjnie ogłaszali, gdzie znajdują się w danym momencie, albo wykonywali fotografie, na których detale widoczne w tle zdradzały ich lokalizację[87]. Z uzyskanych dowodów wynikało, że system Buk do strefy walk został dostarczony przez 53 Rakietową Brygadę Przeciwlotniczą z Kurska. Analiza z wykorzystaniem wyszukiwarek,

---

[84] M. Miśko, *Gdyby nie Internet dowodów na tę zbrodnię być może by nie było*, GeekWeb, https://www.geekweb.pl/magazyn-dobrych-tresci/item/1788-proces-o-zestrzelenie-mh17-w-2014-roku [dostęp: 26 I 2022].

[85] *MH17. The Open Source Evidence. A Bellingcat Investigation*, Bellingcat, https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf [dostęp: 6 II 2022].

[86] *MH17: Source of Separatists' Buk. A Bellingcat Investigation*, Bellingcat, https://www.bellingcat.com/app/uploads/2014/11/Origin-of-the-Separatists-Buk-A-Bellingcat-Investigation1.pdf [dostęp: 6 II 2022].

[87] B. Biel, *Internet pełen jest dowodów na zbrodnie…*

forów i mediów społecznościowych (w tym ponad 200 profili żołnierzy) umożliwiła odtworzenie siatki powiązań oraz zrekonstruowanie całej struktury brygady wraz z jej uzbrojeniem i nazwiskami żołnierzy niemal wszystkich szczebli. W ten sposób ustalono role osób odpowiedzialnych za zestrzelenie malezyjskiego samolotu, w tym tych z kręgów rosyjskiej armii, wywiadu wojskowego oraz prorosyjskich separatystów.

Krótko po zestrzeleniu samolotu strona rosyjska starała się stworzyć narrację, zgodnie z którą odpowiedzialność za katastrofę ponosi Ukraina. Przedstawiano spreparowane dowody, a w kampanię były zaangażowane zarówno rosyjskie Ministerstwo Obrony, jak i portale Russia Insider, Sputnik, RT (dawna Russia Today) oraz pracownicy Agencji Badań Internetowych (potocznie nazywanej fabryką trolli), którzy w ciągu trzech dni od katastrofy tylko na portalu Twitter opublikowali łącznie 111 486 dezinformacyjnych postów[88]. Proces dezinformacji wzmocniono dyskredytowaniem Bellingcat. Ataki były przeprowadzane przez portale i blogi pozornie niezwiązane ze sobą, które jednak mają źródła w rosyjskich ośrodkach wpływu. Przeciwko Higginsowi i jego zespołowi używano też socjotechnik w celu przejęcia ich kont mailowych. Pomimo to zespół Bellingcat sukcesywnie publikował wyniki śledztwa oraz zwalczał manipulacje, dzięki czemu w kolejnych latach wszczęto oficjalne śledztwo.

W 2016 r. Połączony Zespół Śledczy (Joint Investigation Team, JIT) pod przewodnictwem prokuratury holenderskiej ogłosił, że poszukuje informacji o rosyjskich wojskowych i separatystach, których rozmowy telefoniczne przechwyciła Służba Bezpieczeństwa Ukrainy. Bellingcat uznał te osoby za kluczowe dla śledztwa w sprawie lotu MH17 i zidentyfikował je[89]. W maju 2017 r. JIT oficjalnie potwierdził, że system Buk wykorzystany do zestrzelenia samolotu został sprowadzony z Rosji, a jego właścicielem jest brygada z Kurska[90]. W czerwcu 2019 r. ogłoszono, że zarzuty zostaną postawione trzem Rosjanom: Siergiejowi Dubinskiemu, Igorowi Girkinowi i Olegowi Pułatowowi oraz Ukraińcowi Leonidowi Charczence. Na konferencji potwierdzono wszystkie dowody i ustalenia zgromadzone wcześniej przez Bellingcat[91]. Postępowanie karne rozpoczęło się w 2020 r. w Holandii i przebiegło na podstawie lokalnego prawa, ponieważ 193 ofiary katastrofy spośród wszystkich 298 pochodziły właśnie z tego kraju. Oskarżeni byli sądzeni zaocznie. Proces uważany za kulminację (…) *najbardziej skomplikowanego śledztwa w historii prawnej Niderlandów*[92] zakończył się w listopadzie 2022 r. Wyrokiem sądu okręgowego w Hadze Dubinski, Girkin oraz Charczenko zostali skazani na karę dożywotniego pozbawienia wolności oraz

[88] E. Higgins, *Bellingcat. Ujawniamy prawdę*…, s. 114.

[89] B. Biel, *Internet pełen jest dowodów na zbrodnie*…

[90] Tamże.

[91] M. Miśko, *Gdyby nie Internet*…

[92] Tamże.

zobowiązani do wypłacenia krewnym ofiar 16 mln euro odszkodowania. Pułatowa uniewinniono z powodu braku dowodów[93].

Śledztwo grupy Bellingcat udowadnia, że informacje niejawne mogą stać się jawnymi dzięki wykorzystaniu OSINT. Zespołowi udało się odtworzyć drogę rosyjskiego konwoju, a przy okazji także strukturę rosyjskiej brygady, wyłącznie na podstawie danych ze źródeł otwartych. Dziennikarze odkryli dowody, które jednoznacznie wskazywały na zaangażowanie Rosji w konflikt na wschodzie Ukrainy, kilka lat wcześniej niż oficjalne organy państw europejskich[94].

Wnioski

W literaturze przedmiotu podkreśla się, że bezpieczeństwo organizacji nie jest produktem, lecz ciągłym procesem[95]. Myśl tę rozwinął Kavin Mitnick: bezpieczeństwo (…) *nie jest problemem technologicznym, tylko problemem związanym z ludźmi i zarządzaniem*[96]. Zarządzanie bezpieczeństwem informacji opiera się jednak na wszystkich filarach związanych z zarządzaniem ludźmi, odpowiednimi procedurami oraz technologią. Skuteczność ISM zależy od tego, czy środki bezpieczeństwa zostaną odpowiednio wyodrębnione oraz sklasyfikowane. Zgodnie z przyjętym podziałem dzielą się one na: personalne, techniczne, fizyczne oraz organizacyjno-proceduralne.

Personalne środki bezpieczeństwa powinny obejmować wszystkie osoby w organizacji, a szczególnie kierownictwo i tych, którzy mają dostęp do informacji niejawnych[97]. Jak zauważa Mitnick, (…) *firma może dokonać zakupu najlepszych i najdroższych technologii bezpieczeństwa, wyszkolić personel tak, aby każda poufna informacja była trzymana w zamknięciu, wynająć najlepszą firmę chroniącą obiekty i wciąż pozostać niezabezpieczoną.* (…) *Dlaczego? Ponieważ to czynnik ludzki jest piętą achillesową systemów bezpieczeństwa*[98]. Istotne jest szkolenie pracowników na wszystkich szczeblach hierarchii, ze szczególnym uwzględnieniem nowo zatrudnionych. Dodatkowo należy skupić się na budowaniu świadomości na temat tego, jak dużo informacji można uzyskać ze źródeł otwartych, zarówno wśród

[93] *Malezyjski Boeing 777 zestrzelony przez Rosjan w 2014 r. Sąd w Hadze przedstawił stanowisko*, Dziennik Gazeta Prawna, 17 XI 2022 r., https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8590126,holandia-sad-zestrzelenie-2014-malezyjski-boeing-777-ukraina.html [dostęp: 9 X 2023].

[94] *About*, Bellingcat, https://www.bellingcat.com/about/ [dostęp: 2 II 2022].

[95] K. Mitnick, W. Simon, *Sztuka podstępu*…, s. 24.

[96] Tamże.

[97] K. Liedel, *Zarządzanie informacją*…, s. 83.

[98] K. Mitnick, W. Simon, *Sztuka podstępu*…, s. 23–24.

zatrudnionych w organizacji użytkowników sieci, jak i ich rodziny i przyjaciół. Kolejnym środkiem powinno być uniemożliwienie dostępu do informacji niejawnych osobom nieuprawnionym. Należy zapewnić prewencyjne wykrywanie osób, których zatrudnienie może naruszyć bezpieczeństwo informacyjne (postępowanie sprawdzające). Warto przeprowadzać rutynowe kontrole osób mających dostęp do koszy na śmieci i niszczarek dokumentów (ekipy sprzątające lub osoby uprawiające tzw. *dumpster diving*), ponieważ mogą one wejść w posiadanie zdezaktualizowanych informacji niejawnych, jednak wartościowych z punktu widzenia np. konkurencji[99].

W zakresie stosowania **technicznych środków bezpieczeństwa informacyjnego** należy przestrzegać również zasady powszechności. Powinny zostać nią objęte wszystkie nośniki oraz urządzenia służące do przetwarzania informacji. Przechowywanie danych dotyczących organizacji i jej członków w odpowiednio zabezpieczonej bazie danych jest obligatoryjne.

Fizyczne środki bezpieczeństwa powinny obejmować wydzielenie stref bezpieczeństwa poddanych kontroli wejść i wyjść oraz stref administracyjnych służących do kontroli osób i pojazdów[100]. Należy to zastosować wobec wszystkich pomieszczeń, w których informacje niejawne są lub będą przechowywane. Organizacja powinna zapewnić dostęp do sieci intranet z organizacyjnymi środkami komunikacji (własnymi lub zewnętrznymi). Istotne jest certyfikowanie systemów i sieci używanych w organizacji przez uprawnione podmioty. Systemom tym należy zapewnić techniczne wsparcie oraz ochronę fizyczną, kryptograficzną i elektromagnetyczną, a także niezawodność transmisji[101].

W zakresie **proceduralno-organizacyjnym** najważniejszym elementem wydaje się zapewnienie odpowiednich zarobków osobom odpowiedzialnym za bezpieczeństwo organizacji. O ile w dużych przedsiębiorstwach ten problem praktycznie nie występuje, o tyle w tych z mniejszym budżetem rzadko zdarza się możliwość korzystania z profesjonalnej infrastruktury i z bieżącego monitorowania bezpieczeństwa. Podobną barierę napotykają instytucje związane z bezpieczeństwem państwa[102] oraz jego administracją[103]. Powoduje to olbrzymie różnice płacowe niekorzystne dla pracowników sektora publicznego. Organizacja powinna przeprowadzać

[99] Tamże, s. 185.

[100] K. Liedel, *Zarządzanie informacją*…, s. 85.

[101] Tamże, s. 86.

[102] M. Janik, *Wojska Obrony Cyberprzestrzeni stać najwyżej na studentów. „Z płaceniem zawsze był problem"*, INN Poland, 14 II 2019 r., https://innpoland.pl/150265,wojska-obrony-cyberprzestrzeni-place-w-wojsku-roznia-sie-znacznie-od-it [dostęp: 4 IV 2022].

[103] M. Kicka, *Tak zarabiają. Pensja zasadnicza na wybranych stanowiskach urzędników samorządowych*, Serwis Samorządowy PAP, 21 VIII 2019 r., https://samorzad.pap.pl/kategoria/archiwum/tak-zarabiaja-pensja-zasadnicza-na-wybranych-stanowiskach-urzednikow [dostęp: 4 IV 2022].

obowiązkowe szkolenia w zakresie celów polityki bezpieczeństwa informacji oraz postępowania z informacjami niejawnymi. Należy stosować odpowiednie klauzule niejawności oraz wyraźnie określić zakres odpowiedzialności za naruszenie zasad OIN. Po opracowaniu tych procedur i szkoleń kierownictwo powinno dać podwładnym wystarczająco dużo czasu na zapoznanie się z wytycznymi. Planowanie takiego szkolenia w czasie ponadnormatywnym lub wolnym od pracy negatywnie wpływa na przyswajanie informacji. Polityka bezpieczeństwa informacyjnego powinna być regularnie uaktualniana.

Bezpieczeństwo jest procesem, który powinien być stale monitorowany i usprawniany, jeżeli dana organizacja ceni sobie bezpieczeństwo informacyjne. Należy jednak pamiętać, że wszelkie zalecenia dotyczące bezpieczeństwa nie gwarantują całkowitej ochrony przed OSINT. Konieczne jest odpowiednie zarządzanie ryzykiem pozyskania informacji ze źródeł otwartych i zmniejszenie go do akceptowalnego poziomu. Ocena ryzyka powinna pozwolić na określenie, jakie informacje mają podlegać szczególnej ochronie, jakie występują wobec nich zagrożenia oraz jakie szkody może spowodować pozyskanie informacji chronionych (niejawnych). Odpowiednie ISM znacznie przyczyni się do ochrony zasobów w organizacji, a tym samym zostaną zapewnione korzyści wewnętrzne i zewnętrzne, w tym marketingowe, biznesowe oraz dla klientów i innych stron trzecich.

Myśl przytoczona na początku artykułu nie traci na aktualności. Współcześnie są ważne jednak dane nie tylko o nieprzyjacielu, lecz także o potencjalnym partnerze. Techniki i narzędzia OSINT znacznie ułatwiają ich uzyskanie. Dlatego z punktu widzenia organizacji pozyskanie informacji niejawnych działa zawsze na jej niekorzyść. Istotne jest więc wprowadzenie polityki bezpieczeństwa o charakterze prewencyjnym. Nieliczni komentatorzy argumentują, że złoty wiek OSINT, w którym analitycy mogli korzystać z niezliczonej ilości źródeł przy niskiej świadomości użytkowników sieci, dobiegł końca[104]. Jednak zainteresowanie białym wywiadem rośnie i nie przestaje być on zagrożeniem. Problematyka OSINT stwarza możliwość stawiania kolejnych pytań i nowych problemów badawczych. Wyniki tych badań i analiz poprawią bezpieczeństwo informacji będące bardzo ważnym zasobem organizacji. W przyszłości, dzięki zwiększeniu świadomości społecznej oraz poziomu rozwoju technologicznego, może to mieć pozytywny wpływ na działalność organizacji o charakterze społecznym i gospodarczym, jak również na bezpieczeństwo całego państwa.

[104] *The Golden Age of OSINT is over…*

Bibliografia

Aleksandrowicz T., *Biały wywiad w walce z terroryzmem*, w: *Rola mediów w przeciwdziałaniu terroryzmowi*, K. Liedel, P. Piasecka (red.), Warszawa 2009, s. 81–92.

Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki, W. Filipkowski, W. Mądrzejowski (red.),Warszawa 2011.

Higgins E., *Bellingcat. Ujawniamy prawdę w czasach postprawdy*, Katowice 2021.

Krawiec J., *System Zarządzania Bezpieczeństwem Informacji – zabezpieczenia*, „Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie" 2017, nr 1 (38), s. 46–59.

Krztoń W., *Zarządzanie informacją w procesach decyzyjnych organizacji*, „Modern Management Review" 2017, nr 3, s. 83–94.

Liedel K., *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010.

Liedel K., Piasecka P., Aleksandrowicz T., *Analiza informacji. Teoria i praktyka*, Warszawa 2012.

Łuczak J., Tyburski M., *Systemowe Zarządzanie Bezpieczeństwem Informacji ISO/IEC 27001*, Poznań 2009.

Mitnick K., Simon W., *Sztuka podstępu. Łamałem ludzi, nie hasła*, Gliwice 2016.

Niemczyk P., *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu"*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 147–166.

Nowina-Konopka M., *Infomorfoza. Zarządzanie informacją w nowych mediach*, Kraków 2017.

Nowosad A., *Metody i techniki pozyskiwania i przetwarzania informacji medialnej na potrzeby białego wywiadu*, „Państwo i Społeczeństwo" 2005, nr 2, s. 59–69.

Rozpoznanie ze źródeł otwartych DD-2.9(A), Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2020.

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

Singer P.W., Brooking E.T., *Nowy rodzaj wojny. Media społecznościowe jako broń*, Kraków 2019.

Stanek S., *Podejmowanie decyzji w warunkach zagrożenia bezpieczeństwa informacyjnego organizacji*, Wrocław 2016.

Stromczyński B., Waszkiewicz P., *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5, s. 146–170.

Tzu S., *Sztuka wojny. Traktat*, Gliwice 2012.

Wojciulik A., *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków,* w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski, W. Mądrzejowski (red.),Warszawa 2011, s. 43–55.

Źródła internetowe

AAP-6 Słownik terminów i definicji NATO, 2017, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf [dostęp: 24 II 2021].

About, Bellingcat, https://www.bellingcat.com/about/ [dostęp: 2 II 2022].

Aleksandrowicz T., *„Efekt Snowdena"*, Wszystko Co Najważniejsze, 7 VI 2014 r., https://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-efekt-snowdena/ [dostęp: 11 IV 2022].

Biel B., *Internet pełen jest dowodów na zbrodnie. Trzeba wiedzieć, gdzie ich szukać*, Magazyn TVN24, https://tvn24.pl/magazyn-tvn24/internet-pelen-jest-dowodow-na-zbrodnie-trzeba-wiedziec-gdzie-ich-szukac,158,2754 [dostęp: 26 I 2022].

Janik M., *Wojska Obrony Cyberprzestrzeni stać najwyżej na studentów. „Z płaceniem zawsze był problem"*, INN Poland, 14 II 2022 r., https://innpoland.pl/150265,wojska-obrony-cyberprzestrzeni-place-w-wojsku-roznia-sie-znacznie-od-it [dostęp: 4 IV 2022].

Kicka M., *Tak zarabiają. Pensja zasadnicza na wybranych stanowiskach urzędników samorządowych*, Serwis Samorządowy PAP, 21 VIII 2019 r., https://samorzad.pap.pl/kategoria/archiwum/tak-zarabiaja-pensja-zasadnicza-na-wybranych-stanowiskach-urzednikow [dostęp: 4 IV 2022].

Leżoń T., *Głęboko pod powierzchnią jest miejsce, o którym wolałbyś nie wiedzieć*, Magazyn TVN24, https://tvn24.pl/magazyn-tvn24/gleboko-pod-powierzchnia-jest-miejsce-o-ktorym-wolalbys-nie-wiedziec,95,1850 [dostęp: 12 III 2021].

Malezyjski Boeing 777 zestrzelony przez Rosjan w 2014 r. Sąd w Hadze przedstawił stanowisko, Dziennik Gazeta Prawna, 17 XI 2022 r., https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8590126,holandia-sad-zestrzelenie-2014-malezyjski-boeing-777-ukraina.html [dostęp: 9 X 2023].

MH17: Source of Separatists' Buk. A Bellingcat Investigation, Bellingcat, https://www.bellingcat.com/app/uploads/2014/11/Origin-of-the-Separatists-Buk-A-Bellingcat-Investigation1.pdf [dostęp: 6 II 2022].

MH17. The Open Source Evidence. A Bellingcat Investigation, Bellingcat, https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf [dostęp: 6 II 2022].

Miśko M., *Gdyby nie Internet dowodów na tę zbrodnię być może by nie było*, GeekWeb, https://www.geekweb.pl/magazyn-dobrych-tresci/item/1788-proces-o-zestrzelenie-mh17-w-2014-roku [dostęp: 26 I 2022].

RIOT – rządowy system inwigilacji i profilowania przez serwisy społecznościowe, Niebezpiecznik, 17 II 2013 r. https://niebezpiecznik.pl/post/riot-rzadowy-system-inwigilacji-przez-serwisy-spolecznosciowe/ [dostęp: 16 III 2021].

The Golden Age of OSINT is over, Key Findings, 4 I 2019 r., https://keyfindings.blog/2019/01/04/the-golden-age-of-osint-is-over/ [dostęp: 6 II 2022].

www.bezpiecznymiesiac.pl [dostęp: 29 XII 2023].

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (t.j. DzU z 1997 r. nr 78 poz. 483, ze zm.).

Powszechna deklaracja praw człowieka (Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana 10 grudnia 1948 r.).

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (DzU z 1993 r. nr 61 poz. 284).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (DzU z 1977 r. nr 38 poz. 167).

Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 303/1 z 14 XII 2007 r.).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2023 r. poz. 913, ze zm.).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. DzU z 201 r. poz. 1781).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. DzU z 2023 r. poz. 756, ze zm.).

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. DzU z 2024 r. poz. 34).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. DzU z 2020 r. poz. 344).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. DzU z 2022 r. poz. 902).

Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. DzU z 2023 r. poz. 120, ze zm.).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. DzU z 2022 r. poz. 2509).

Inne dokumenty

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 19 XII 2023].

Maciej Witczak

Absolwent Akademii Wojsk Lądowych im. gen. Tadeusza Kościuszki we Wrocławiu.

Kontakt: maciejwitczak1995@gmail.com