Piotr Karasek

Analiza informacji z mediów społecznościowych jako narzędzie wspierające kontrolę bezpieczeństwa w procedurach migracyjnych[1]

Wstęp

Wczesne wykrywanie ataków terrorystycznych, zapobieganie im oraz utrzymywanie właściwego poziomu bezpieczeństwa granic państwowych – to jedne z najaktualniejszych zagadnień w bieżącej debacie publicznej i eksperckiej. Obecnie wzrasta rola mediów społecznościowych we wspieraniu realizacji wyżej wymienionych działań. Chociaż działalność stricte antyterrorystyczna jest domeną poszczególnych wyspecjalizowanych służb państwowych, to w obliczu powagi zagrożeń o charakterze terrorystycznym jest niezbędne szerokie wykorzystanie wszystkich możliwych sposobów przeciwdziałania terroryzmowi. Ma to szczególne znaczenie, gdy bierze się pod uwagę, że współcześni sprawcy aktów terrorystycznych nader często działają samodzielnie i nie utrzymują stałych kontaktów z grupami zorganizowanymi, co czyni zagrożenie z ich strony znacznie trudniejszym do wczesnego wykrycia z wykorzystaniem metod tradycyjnych.

Istotną rolę w szeroko rozumianym zapewnianiu bezpieczeństwa wewnętrznego powinny odgrywać m.in. osoby bezpośrednio odpowiedzialne za przyznawanie wiz wjazdowych. Mając dostęp do prawdziwych, weryfikowalnych danych osób starających się o wizę, w celu wykrycia zagrożenia i podjęcia decyzji dotyczącej ewentualnej odmowy prawa wjazdu, gdy jest to niezbędne do zapewnienia bezpieczeństwa, można wykorzystać informacje ze źródeł otwartych, w tym zwłaszcza z mediów społecznościowych. Co więcej, wykorzystanie tej możliwości w czasie przeprowadzania procedur migracyjnych może pozwolić na uzyskanie wielu innych ważnych informacji na temat starających się o wjazd. Takie narzędzia, jak media społecznościowe, są coraz częściej oficjalnie wykorzystywane przez agencje bezpieczeństwa w różnych krajach, a przede wszystkim w Stanach Zjednoczonych[2], do wczesnego wykrywania zagrożeń. O ile rzeczywiste efekty wykorzystywania informacji z mediów społecznościowych są w chwili obecnej trudne do oszacowania, o tyle istnieje wiele wyraźnych ograniczeń, które należy brać pod uwagę przy projektowaniu rozwiązań opierających się na technikach prowadzenia białego wywiadu.

Niniejszy artykuł, na podstawie danych pochodzących z literatury przedmiotu oraz danych medialnych i pomocniczych wywiadów badawczych z funkcjonariusza-

[1] Artykuł został przygotowany na podstawie materiałów zgromadzonych w ramach realizacji projektu PRIME finansowanego ze środków 7. Programu Ramowego Komisji Europejskiego (umowa grantowa nr 608354).

[2] B.O'Brien, *U.S. visa applicants to be asked for social media history: State Department*, https://www.reuters.com/article/us-usa-immigration-visa/u-s-visa-applicants-to-be-asked-for-social-media-history-state-department-idUSKBN1H611P/ [dostęp: 15 IV 2018].

mi służb różnych państw, ma na celu przedstawienie możliwości, zagrożeń i ograniczeń wynikających ze stosowania technik białowywiadowczych w środowisku mediów społecznościowych w kontekście utrzymywania bezpieczeństwa wewnętrznego państw i bezpieczeństwa procesów migracyjnych.

Państwowe służby bezpieczeństwa, terroryzm, Internet

Możliwości związane z szybkim rozwojem Internetu bywają przedstawiane jako jednoznacznie sprzyjające także rozwojowi przestępczości, w tym terrorystycznej. Takie podejście jednak nie jest prawidłowe. Częściowa anonimowość, zdecentralizowane czarne rynki, przestępcze fora w sieci ukrytej, cała gama niebezpiecznych i niedozwolonych treści, które bez problemu można odnaleźć – wszystkie te elementy współczesnego Internetu rzeczywiście mogą wspierać rozwój działalności przestępczej. Zarazem Internet jest narzędziem pomocnym przy realizacji czynności wykrywczych w odniesieniu do przestępczości kryminalnej i terrorystycznej. Niektórzy badacze twierdzą wręcz, że współczesne technologie komunikacyjne jednak bardziej wspierają działania służb państwowych niż organizacji terrorystycznych[3].

Zarówno praktycy, jak i przedstawiciele świata nauk o bezpieczeństwie wskazują na szerokie możliwości związane z poszukiwaniem informacji w publikatorach otwartych. Zwłaszcza media społecznościowe są postrzegane jako źródła danych i de facto stanowią skarbnicę nowego typu szeroko rozumianego „białego wywiadu" (*Open-Source Intelligence* – OSINT), któremu nadają nazwę SOCMINT (*Social Media Intelligence)*[4]. To ostatnie pojęcie zostało wstępnie opisane w literaturze, podobnie jak różnego rodzaju techniki możliwe do wykorzystania w celu prowadzenia rozpoznania za pomocą takich metod. Szczegółowe zastosowania, szanse i zagrożenia związane z prowadzeniem SOCMINT-u wciąż jednak pozostają tematem stosunkowo mało zeksplorowanym. Same zaś media społecznościowe, niezależnie od ich definicji[5], stały się na dobre zjawiskiem globalnym i zawierają ogromną liczbę dobrowolnie publikowanych informacji o jednostkach oraz ich grupach. Skuteczność technik SOCMINT-u wynika częściowo z tego, że użytkownicy mediów społecznościowych, publikując informacje o sobie w Internecie (w celu szeroko pojętej samoekspresji, np. artystycznej czy towarzyskiej), jednocześnie przekazują wiele danych, których by nie przekazali, zapytani o nie wprost[6] (zwłaszcza gdyby byli pytani przez służby państwowe).

[3] D.C. Benson, *Why the Internet is not increasing terrorism,* „Security Studies" 2014, nr 23/2, s. 308, 311, 328.

[4] A.N. Liaropoulos, *The challenge of social media for the Intelligence community,* „Journal of Mediterranean and Balkan Intelligence" 2013, nr 1, s. 6.

[5] Media społecznościowe mogą być definiowane jako (…) *aplikacje internetowe skonstruowane w oparciu o założenia technologiczno-ideowe tzw. Sieci 2.0 i pozwalają użytkownikom na kreowanie i wymianę treści*, w przypadku gdy „strony internetowe" są wykorzystywane wyłącznie w charakterze infrastruktury pozwalającej użytkownikom na dzielenie się własną treścią. Zob. A. Kaplan, M. Haenlein, *Users of the world, Unite!*, „Business Horizons" 2010, nr 53/1, s. 61.

[6] C. Arslan, M. Yanuk, *A New Discipline of Intelligence: Social Media*, Istanbul 2015, s. 69–70.

W przeciwieństwie do forów tematycznych działających w Internecie od wielu lat, media społecznościowe zostały zaprojektowane w taki sposób, aby pobudzać swobodną, publiczną ekspresję użytkowników, szczególnie w zakresie informacji dotyczących stylu życia, tj. zachęcać ich do publikowania własnych myśli, planów, opinii, zdjęć i faktów z ich życia. Wynika z tego obserwowalna tendencja użytkowników mediów społecznościowych do tzw. naddzielenia się (ang. o*ver-sharing)* informacjami prywatnymi. Miewa to groźne konsekwencje, gdyż zwiększa ryzyko stania się ofiarą różnych typów przestępstw[7]. Zwykle w tym właśnie kontekście było to opisywane. Z drugiej jednak strony dokładnie to samo zjawisko wpływa na dużą skuteczność technik SOCMINT-u, które są wykorzystywane do ochrony szeroko rozumianego bezpieczeństwa wewnętrznego.

Media społecznościowe są więc źródłami danych, które mogą służyć pracy wykrywczej. Ponad 81 proc. funkcjonariuszy amerykańskich organów ścigania wykorzystuje tego typu źródła jako narzędzia pozyskiwania informacji na temat osób występujących w prowadzonych przez siebie sprawach. Dzieje się tak pomimo tego, że w 48 proc. przypadków jest to praktyka niezalecana przez przełożonych[8]. Należy podkreślić, że część informacji pochodzących z mediów społecznościowych jest dostępna dla każdego, nawet niezalogowanego użytkownika sieci, bez konieczności występowania z jakimkolwiek wezwaniem czy nakazem sądowym. Wykorzystując specjalistyczne narzędzia, np. oparte na technologii „geofencingu" (choćby Geofeedię, która pozwala na zarządzanie zagrożeniami w czasie niemalże rzeczywistym[9])[10], można pozyskać wiele cennych informacji.

Trzeba też zaznaczyć, że wszystkie metody pracy stosowane przy zwalczaniu zwykłej przestępczości kryminalnej są przydatne również w zwalczaniu przestępstw terrorystycznych i zapobieganiu im. Dotyczy to zwłaszcza tzw. monitoringu Internetu. Podczas badań prowadzonych w ramach projektu 7. Programu Ramowego Komisji Europejskiej „PRIME"[11] ustalono, że metody stosowane przez organy ścigania i służby bezpieczeństwa w celu zwalczania terroryzmu sprawców indywidualnych właściwie nie różnią się w sposób istotny od tych stosowanych przeciwko grupom terrorystycznym czy zorganizowanym grupom przestępczym o charakterze kryminalnym[12]. Na podstawie wyników badań ankietowych przeprowadzonych z doświadczonymi

[7] K. Paullet, J. Pinchot, *Cybercrime: the unintentional effects of oversharing information on Facebook,* Proceedings of the Conference on Information Systems Applied Research, New Orleans 2012, s. 1–7.

[8] *Social media use in law enforcement: crime prevention and investigative activities continua to driver usage*, https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf [dostęp: 15 IV 2018].

[9] K. Cooke, *US Police used Facebook, Twitter data to track protesters*, http://www.reuters.com/article/social-media-data-idUSL4N1CH4J1 [dostęp: 15 IV 2018].

[10] M.D. Dabhi, *Geofencing: a generic approach to Real time location based tracking system*, „International Journal of Computer Networks and Wireless Communications" 2016, nr 6, s. 35–37.

[11] http://www.fp7-prime.eu/home_page [dostęp: 15 IV 2018].

[12] FP7 PRIME WP7 Deliverable D7.1, *Counter-measures review report*, niepubl.

funkcjonariuszami służb (policji, agencji antyterrorystycznych właściwych w danym kraju i służb ochrony granic) w Europie, Ameryce Północnej oraz w Indiach utworzono hierarchiczne zestawienie najskuteczniejszych i zarazem najmniej kosztownych metod zwalczania zagrożeń terrorystycznych[13]. Monitoring Internetu został przy tym określony przez respondentów jako najbardziej przydatna, skuteczna i zarazem najtańsza metoda pracy (takiej odpowiedzi udzieliło 94 proc. badanych praktyków).

Przy omawianiu i ocenie skuteczności metod zwalczania zagrożeń terrorystycznych w kontekście Internetu i monitoringu mediów społecznościowych istotne jest także zrozumienie specyficznego charakteru przestępczości terrorystycznej tzw. samotnych wilków oraz tego, w jaki sposób treści zamieszczone w mediach społecznościowych mogą wskazywać na przyszłe zagrożenia. Mimo że sformułowanie ścisłej definicji „samotnego wilka" przez kryminologów wciąż napotyka ogromne trudności, to osoby określane w ten sposób bywają na ogół opisywane jako pojedynczy sprawcy działający bez formalnych powiązań z jakąkolwiek grupą terrorystyczną, dokonujący (lub planujący dokonanie) aktu terrorystycznego, będąc zmotywowanymi przez ideologię ekstremistyczną. Wzorcowy „samotny wilk" realizuje schemat działania w kolejnych etapach: od fazy radykalizacji, przez przygotowanie ataku, aż po sam atak – bez pomocy z zewnątrz. Sprawcy takich czynów często (choć niekoniecznie świadomie czy celowo) komunikują otoczeniu swoje intencje na kilka godzin, dni czy nawet tygodni przed dokonaniem ataku. Według części badaczy spośród wszystkich tego typu aktów dokonanych lub planowanych w Stanach Zjednoczonych po 11 września 2001 r. aż w 76 proc. sprawca publikował informację o przyszłym zamachu (niekiedy więcej niż jednokrotnie) z wykorzystaniem mejla, wiadomości tekstowych, ale również mediów społecznościowych – za pośrednictwem Facebooka czy Twittera[14]. Nawet wtedy, gdy zamiar ataku nie był przez sprawcę wskazany wprost, jego zachowanie w mediach społecznościowych często wskazywało na radykalizację w jakimś kierunku. Niestety, tego typu informacje nie zawsze są właściwie odczytywane[15].

Media społecznościowe a procedura wizowa

Przy uwzględnieniu wspomnianych powyżej zalet zastosowania technik SOCMINT-u w zwalczaniu przestępczości kryminalnej i terrorystycznej warto rozważyć, czy i ewentualnie w jaki sposób mogłyby one być wykorzystywane przy wzmacnianiu bezpieczeństwa w ramach procedur migracyjnych. Lub też szerzej: w jaki sposób OSINT, a zwłaszcza SOCMINT, mogą wspomóc rolę procedur migracyjnych w zapewnianiu i utrzymywaniu bezpieczeństwa wewnętrznego.

---

[13] Tamże.

[14] M. Hamm, R. Spaaij, *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies*, Waszyngton 2015, s. 9.

[15] Na przykład: George Sodini (znany jako „the Gym Killer") szczegółowo opisywał plan swojego ataku na osobistym blogu przez wiele miesięcy pomiędzy 2008 a 2009 rokiem. Zob. *Full text of Gym Killer's blog,* http://nypost.com/2009/08/05/full-text-of-gym-killers-blog/ [dostęp: 15 IV 2018].

Znaczenie prawidłowej weryfikacji osób starających się o wjazd na teren danego państwa dobrze ilustruje zamach w San Bernardino z grudnia 2016 r. Wkrótce po dokonaniu ataku podano informację, że kobieta – napastnik, Tashfeen Malik, przebywała w Stanach Zjednoczonych na podstawie wizy narzeczeńskiej. Jednocześnie publikowała ze swojego konta w mediach społecznościowych dżihadystyczną propagandę jeszcze zanim tę wizę otrzymała[16]. Należy podkreślić, że ta informacja okazała się później nie w pełni prawdziwa[17], chociaż doskonale ilustruje to, jakie problemy mogą wyniknąć w przypadku nieprawidłowego lub niepełnego sprawdzenia osób starających się o wizy pobytowe[18].

Dokonywanie bieżącej weryfikacji kandydatów do otrzymania wizy co prawda nie powinno należeć do najważniejszych zadań głównych instytucji zajmujących się bezpieczeństwem państwa, ale nie koliduje z ich kompetencjami. W praktyce udział tych struktur w procedurze wizowej jest ograniczony. Dostępne dane wywiadowcze na temat osób starających się o wizę są dostarczane decydentom przez narodowe służby bezpieczeństwa (np. w formie odpowiednich list czy baz danych prowadzonych przez wyspecjalizowane jednostki, takie jak np. Terrorist Screening Center w Stanach Zjednoczonych[19] lub System Informacyjny Schengen w Europie[20]). Jednak ze względu na decentarlizację współczesnego terroryzmu, zwłaszcza indywidualnego, oparcie systemu bezpieczeństwa na jednym, scentralizowanym źródle informacji nie jest wystarczające. O ile bowiem sukcesy organów zapewniających bezpieczeństwo w wykrywaniu powiązań jednostek z grupami zorganizowanymi oraz w ich ramach są niezaprzeczalne, o tyle pojedynczy zradykalizowani sprawcy mogą ujść ich uwadze. Co więcej, jest wiele innych elementów niebędących domeną organów ścigania i organów ochrony bezpieczeństwa, które należy brać pod uwagę podczas weryfikacji podania wizowego. Dotyczy to np. weryfikacji specyficznych wymogów wizowych w zakresie podania informacji o niekaralności czy stanie zdrowia. Takie dane mogą mieć istotne znaczenie dla podjęcia decyzji w sprawie wydania wizy, gdyż mają związek z szeroko rozumianym bezpieczeństwem publicznym. Niekoniecznie jednak mają jakiekolwiek znaczenie dla instytucji zajmujących się bezpieczeństwem państwa.

Wykorzystywanie technik tzw. białego wywiadu, zwłaszcza OSINT, może więc być postrzegane jako element szerokiego zarządzania bezpieczeństwem i zostać

[16] M. Apuzzo, M.S. Schmidt, J. Preston, *U.S. Visa Process Missed San Bernardino Wife's Online Zealotry*, 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?_r=0 [dostęp: 15 IV 2018].

[17] R.A. Serrano, *FBI chief: San Bernardino shooters did not publicly promote jihad on social media*, http://www.latimes.com/nation/la-ln-fbi-san-bernardino-social-media-20151216-story.html [dostęp: 15 IV 2018].

[18] Por. B. Ross i in., *Secret US Policy blocks agents from looping at social media of visa applicants, former official says,* http://abcnews.go.com/US/secret-us-policy-blocks-agents-social-media-visa/story?id=35749325 [dostęp: 15 IV 2018].

[19] Zob. *Terrorist Screening Center,* https://www.fbi.gov/about-us/nsb/tsc/tsc [dostęp: 15 IV 2018].

[20] Zob. *Schengen Information System*, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm [dostęp: 15 IV 2018].

uwzględnione w procedurach migracyjnych, tak aby w ten sposób móc realizować przynajmniej dwa cele: 1 – wcześnie wykrywać jednostki zradykalizowane i ekstremistów skłonnych do popełniania przestępstw, w tym terrorystycznych, 2 – wykrywać inne okoliczności, które mogą stanowić podstawę do odmowy prawa wjazdu na dany teren lub pobytu na tym terenie. Istnieje jednak wiele ograniczeń i zagrożeń, które należy uwzględniać przy ewentualnym wykorzystaniu tego rodzaju narzędzi. Pozyskiwanie i analiza informacji ze źródeł otwartych powinny być prowadzone w sposób zorganizowany, co nie zawsze jest przestrzegane[21]. W dalszej części artykułu zostaną przedstawione najważniejsze elementy omawianej koncepcji, tj. pozyskiwanie istotnych danych ze źródeł jawnych. Po pierwsze konieczne jest bliższe określenie sposobu, w jaki może być prowadzone sprawdzanie mediów społecznościowych przez służby migracyjne. Po drugie równie istotne jest zidentyfikowanie konkretnych problemów i ograniczeń wynikających ze stosowania takiej metody.

Dane wejściowe

Oczywiste może się wydać porównanie poszukiwania w Internecie potencjalnych sprawców ataków terrorystycznych z szukaniem igły w stogu siana. Częstym problemem z technikami opartymi na narzędziach SOCMINT jest konieczność przebrnięcia przez ogromną liczbę danych, aby podczas ich analizy móc wyodrębnić informacje nadające się do wykorzystania[22]. Osoby zatrudnione do obsługi procesów migracyjnych (m.in. do decydowania o wydaniu wizy) mają jednak w tym zakresie ogromną przewagę w postaci dostępu do pewnych, weryfikowalnych i relatywnie kompletnych danych na temat osoby starającej się o wjazd (podanych przez nią osobiście w urzędowych formularzach). Takie informacje można wykorzystać jako dane wstępne w celu stworzenia „filtra" danych służących de facto odwróceniu procesu monitoringu Internetu – zamiast poszukiwania „niebezpiecznych" treści w celu ich przypisania do konkretnego autora, przeszukiwanie zasobów otwartych może polegać na poszukiwaniu treści związanych z konkretnymi i znanymi osobami w celu ich sprawdzenia. W ten sposób proces wykrywczy ulega transformacji – zamiast poszukiwania informacji o charakterze zmiennej „nieznanej nieznanej" (tj. o zagrożeniach nieznanych pochodzących od osób nieznanych) poszukuje się informacji o cechach „znanej nieznanej" (tj. o zagrożeniach nieznanych, ale pochodzących od osób znanych), co jest relatywnie skuteczniejsze i prostsze w wykonaniu[23].

[21] Część funkcjonariuszy australijskich służb granicznych podczas poufnych wywiadów badawczych przyznaje, że chociaż nie istnieje tam oficjalna procedura korzystania z informacji pochodzących z mediów społecznościowych, to stosują te techniki z własnej inicjatywy, w celu zweryfikowania osób wjeżdżających do kraju.

[22] D. Omand, J. Bartlett, C. Miller, *Introducing Social Media Intelligence (SOCMINT)*, „Intelligence and National Security" 2012, nr 3, s. 6–7.

[23] Zob. N.N. Taleb, *Black Swan. The impact of the highly improbable*, New York 2007, s. 127, 272.

Konkretne dane wejściowe dostępne służbom migracyjnym różnią się w zależności od szczegółowych rozwiązań prawnych obowiązujących w różnych krajach. Przykładowo więc obywatel zachodniej Europy podróżujący do Australii w celu uzyskania tzw. wizy elektronicznej musi podać tamtejszym służbom swoje podstawowe dane osobowe (tj. imię, nazwisko, płeć, datę urodzenia, dane paszportowe i kraj zamieszkania) oraz działający adres mejlowy. Obywatel Egiptu chcący odwiedzić Polskę musi natomiast przekazać również swój wizerunek (zdjęcie) i wiele innych dokumentów, o które może go poprosić konsulat RP (np. zaświadczenie o niekaralności)[24]. W przypadku wiz na pobyty długoterminowe wymogi we wszystkich krajach są zwykle większe. Z założenia jednak podstawowy zestaw danych na temat osoby starającej się o legalny wjazd na podstawie wizy, który może być wykorzystany przy przeszukiwaniu zasobów otwartych i który jest dostępny dla służb, obejmuje co najmniej najważniejsze dane osobowe, adres mejlowy, adres domowy, zdjęcie itp. Często są to wystarczające dane, aby skutecznie zidentyfikować i zweryfikować tożsamość internetową konkretnej osoby – o ile nie stara się ona aktywnie zamaskować swoich aktywności.

Dostęp

Po utworzeniu „filtra" danych wejściowych konieczne jest ustanowienie odpowiedniego dostępu do adekwatnych źródeł danych online. Jedną z możliwości jest zwrócenie się o pomoc wprost do usługodawców prowadzących media społecznościowe. Jednak zazwyczaj nie są oni otwarci na dobrowolną współpracę, zwłaszcza z zagranicznymi (z ich perspektywy) instytucjami rządowymi. Jeżeli uzyskanie danych bezpośrednio od usługodawców jest w ogóle możliwe, to zwykle jest konieczne pozyskanie odpowiednich (tj. respektowanych przez adresata) nakazów władz[25]. Niektórzy dostawcy usług aktywnie zwalczają tego rodzaju próby pozyskiwania informacji przez służby[26] lub publikują „raporty transparentności" na temat ich żądań[27]. Jakkolwiek pozytywnie można by było to oceniać z perspektywy prawa jednostek do prywatności, to faktem jest, że takie działania stanowią przeszkodę w prowadzeniu czynności wywiadowczych. Obecnie jest za wcześnie, aby ocenić, w jaki sposób w dłuższej perspektywie będzie się zmieniać podejście i usługodawców, i użytkowników do prywatności ich

[24] Ministerstwo Spraw Zagranicznych RP, system eKonsulat, https://secure.ekonsulat.gov.pl/Uslugi/RejestracjaTerminu.aspx?IDUSLUGI=1&IDPlacowki=157 [dostęp: 15 IV 2018].

[25] Zob. m.in.: Facebook, *Information for law Enforcement Authorities*, https://scontentfra31.xx.fbcdn.net/hphotosxfp1/t39.23656/12532957_530107840495531_2074830868_n.pdf [dostęp: 15 IV 2018]; Twitter, *Guidelines for law enforcement*, https://support.twitter.com/articles/41949# [dostęp: 15 IV 2018].

[26] A. Fine, *Twitter appeals ruling in bat tle over occupy Wall Street protester's information*, https://www.aclu.org/blog/twitter-appeals-ruling-battle-over-occupy-wall-street-protesters-information?redirect=blog/technology-and-liberty-national-security-free-speech/twitter-appeals-ruling-battle-over-occupy [dostęp: 15 IV 2018].

[27] Zob. *Google Transparency Report*, https://www.google.com/transparencyreport/userdatarequests/#! [dostęp: 15 IV 2018].

danych, chociażby w kontekście głośnej sprawy udostępniania informacji podmiotom trzecim przez Facebook[28].

Pozyskiwanie danych ze źródeł otwartych nie opiera się jednak na zdobywaniu dostępu do nich kanałami oficjalnymi ani na gromadzeniu informacji, do których dostęp jest przez użytkowników zastrzeżony. Opiera się na założeniu, że wiele przydatnych i znaczących informacji jest dostępnych publicznie. Podobnie rzecz się ma w odniesieniu do profili w mediach społecznościowych. Oczywiście, użytkownicy świadomi swojej prywatności i potrzeby jej ochrony nie korzystają z takich mediów ani nie publikują treści, które mogą ich w jakikolwiek sposób narazić na niebezpieczeństwo, albo korzystają z „ustawień prywatności" skonfigurowanych tak, aby osoby trzecie nie miały bezpośredniego dostępu do publikowanych informacji. Takie działanie stanowi kolejną przeszkodę w zastosowaniu technik SOCMINT. Równocześnie jednak zaskakująco wysoka liczba użytkowników mediów społecznościowych utrzymuje swoje profile w całości, lub przynajmniej częściowo, widoczne – nawet dla osób niezarejestrowanych.

Możliwości w zakresie dostępu do danych źródłowych mogą być zwiększone dzięki wykorzystaniu szczególnych metod i narzędzi oraz rozbudowanych zintegrowanych systemów pozyskiwania informacji ze źródeł otwartych. W zasadzie głównym narzędziem jest zakładanie „fałszywych kont" w mediach społecznościowych w taki sposób, aby pozyskujący dane mógł się uwierzytelnić na platformie społecznościowej jako użytkownik zarejestrowany, a tym samym – zyskać większy dostęp do przetwarzanych wiadomości. Pomimo tego, że jest to na ogół wbrew regulaminom poszczególnych usług społecznościowych[29] i wytycznym przełożonych, taka metoda jest relatywnie często wykorzystywana przez funkcjonariuszy organów ścigania[30]. Przy czym, uzyskiwanie dostępu do informacji oraz ich zdobywanie może następować kompleksowo lub częściowo, w formie procesu zautomatyzowanego, bez konieczności uciążliwego ręcznego „klikania" w treści na portalu społecznościowym. Na rynku działa już wiele systemów i programów komercyjnych wyspecjalizowanych w zbieraniu informacji z internetowych źródeł otwartych. Tego typu systemy oraz programy są w pełni dostępne także dla instytucji państwowych. Mogą one być dostosowywane na zamówienie w celu spełnienia ich określonych potrzeb i zapewnienia tym samym możliwości efektywnego kosztowo zbierania informacji wywiadowczych[31].

[28] D. Ingram, *Facebook says data leak hits 87 million sers, widening privacy skandal*, https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM [dostęp: 15 IV 2018].

[29] Teoretycznie wszyscy użytkownicy Facebooka są zobowiązani regulaminem do używania swoich prawdziwych imion i nazwisk. Zob. *Facebook community standards*, https://www.facebook.com/communitystandards [dostęp: 15 IV 2018].

[30] W początkowo niejawnych wytycznych Facebooka dla organów ścigania zawarto prośbę o niekorzystanie z fałszywych kont w celu prowadzenia postępowań. Zob. *Facebook law enforcement guidelines*, 2010, https://info.publicintelligence.net/Facebook2010-2.pdf [dostęp: 15 IV 2018].

[31] Kilku dużych dostawców oprogramowania, m.in. Symantec, Oracle czy Wynyard, oferuje „systemy pozyskiwania danych" (producenci stosują tu różną terminologię, jednak w każdym przy-

Ocena i weryfikacja

Po utworzeniu wstępnego filtra danych wejściowych i uzyskaniu dostępu do źródeł informacji o jednostce weryfikowanej najważniejszą fazą sprawdzania bezpieczeństwa jest ocena wiedzy zgromadzonej w ten sposób. Dokonując jej, należy mieć na uwadze treść i rodzaj pozyskanych informacji oraz zakładane wymogi bezpieczeństwa i kryteria przyznania prawa wjazdu do kraju.

Wiele wymogów wizowych (np. dotyczących stanu zdrowia czy niekaralności) może być weryfikowanych dzięki informacjom pozyskanym ze źródeł otwartych. Istotne jest przy tym zwracanie uwagi na to, które dane mogą być w takiej weryfikacji pomocne i gdzie ich szukać. Przede wszystkim należy zwrócić uwagę na treści zamieszczone na profilu społecznościowym przez osobę sprawdzaną. Ze względu na wspomniane wcześniej zjawisko „naddzielenia się" przez użytkowników informacjami prywatnymi treści przez nich publikowane nierzadko mogą dostarczyć wiarygodnych i rzetelnych podstaw do odmowy prawa wjazdu (na przykład, gdy są wymagane przymioty niekaralności za przestępstwa i niebycia podmiotem bieżących postępowań karnych). Niekiedy oświadczenia w tym zakresie mogą być negatywnie zweryfikowane na podstawie publikowanych treści wskazujących na przeszłe lub bieżące problemy z prawem. Wielokrotnie się zdarzało, że zdjęcie umieszczone w mediach społecznościowych, a odnalezione przez organy ścigania, stanowiło podstawę do wszczęcia stosownego postępowania[32]. Nie ma więc powodu, aby nie korzystać z tego narzędzia podczas procedur migracyjnych i wizowych.

Oprócz treści wytworzonych i publikowanych bezpośrednio przez użytkowników należy zwrócić uwagę na informacje pośrednie: treści „udostępnione", strony „polubiane", statusy, zdjęcia, grupy, do których należy użytkownik itp. (dotyczy to takich stron, jak Facebook i Twitter, ale też innych platform z mikroblogami czy mediów społecznościowych, choć szczegółowa terminologia dotycząca m.in. „udostępniania" i „polubień" będzie się różniła w odniesieniu do poszczególnych z nich). Takie treści mogą wskazywać na zainteresowania i poglądy, które mogą wywołać uzasadnione podejrzenie co do intencji danej osoby. Zwłaszcza w przypadku potencjalnych sprawców przestępstw terrorystycznych znaczenie może mieć wczesne ujawnienie oznak radykalizacji; osoba, która śledzi strony publikujące propagandę terrorystyczną, może być podejrzewana o zainteresowanie działalnością o takim charakterze[33].

Dokonując oceny i selekcji zgromadzonych informacji na podstawie analizy profili w mediach społecznościowych w kontekście zagrożenia ze strony terrorystów indywidualnych, w odpowiedni sposób należy oceniać również mniej niebezpieczne

padku chodzi o oprogramowanie wywiadowcze dostępne na rynku komercyjnym).

[32] Istnieje wiele rodzajów i przykładów takich zachowań. Zob. A. Shontell, *7 People who were arrested because of something they wrote on Facebook*, http://www.businessinsider.com/people-arrested-for-facebook-posts-2013-7?IR=T [dostęp: 15 IV 2018].

[33] Zob. J. Klausen, *Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq*, „Studies in Conflict and Terrorism" 2015, nr 38, s. 1–22.

treści. Dotychczasowe badania przeprowadzone w tym zakresie wskazują na wiele tzw. zachowań ostrzegawczych w Internecie i mediach społecznościowych, których wystąpienie może sugerować skłonność lub planowanie agresji (zostały one szczegółowo opisane)[34]. To, czy wystąpienie tego rodzaju „znaku ostrzegawczego" powinno skutkować odmową wjazdu na teren kraju (a niekiedy również innymi konsekwencjami, np. objęciem danej osoby kontrolą operacyjną), musi jednak być zależne od przyjętej polityki wewnętrznej.

Zagrożenia i przeszkody

Wykorzystywanie informacji zgromadzonych w wyniku przeszukiwania mediów społecznościowych przy ocenie aplikacji wizowych jest związane z wieloma poważnymi zagrożeniami i przeszkodami. Wiedza o nich oraz spójne zasady wewnętrzne określające metody prowadzenia działań i reagowania na poszczególne zagrożenia muszą być istotnym elementem wdrażania technik SOCMINT. Spośród najistotniejszych zagadnień należy wymienić weryfikację tożsamości online, bariery językowe i kulturowe oraz problemy organizacyjne, prawne, etyczne, a także związane z podejmowaniem decyzji ostatecznych.

Prawdziwa tożsamość

Pomimo tego, że teoretycznie dostawcy usług mediów społecznościowych wymagają od swoich użytkowników posługiwania się prawdziwymi danymi osobowymi, w praktyce jest to zasada nagminnie nieprzestrzegana[35]. Stąd wynika jeden z najpoważniejszych problemów związanych z próbą precyzyjnego zebrania informacji z tego typu źródeł. Alias może być używany ze względu na chęć ochrony prywatności – jako dokładnie przemyślana lub intuicyjna decyzja dotycząca niepublikowania w Internecie własnych danych (co skądinąd zasługuje na pochwałę z punktu widzenia indywidualnych zasad bezpieczeństwa). Niektóre fałszywe profile są tworzone celowo, aby móc podszywać się pod inną osobę albo dręczyć innych użytkowników i popełniać przestępstwa. Niezależnie od powodu używania aliasu, ogranicza on możliwość rzetelnego ustalenia tożsamości autora treści wyłącznie na podstawie danych otwartych. Osoba prowadząca czynności wywiadowcze musi brać pod uwagę, że nawet jeśli dane osobowe wskazane w profilu są prawdziwe, to nie musi to oznaczać, że ten profil należy

[34] Istotne jest to, że istnieje możliwość wykrycia niektórych rodzajów „zachowań ostrzegawczych" w Internecie dzięki szczegółowej analizie mediów społecznościowych (np. przez wykrywanie specyficznych konstrukcji językowych świadczących o poszczególnych zachowaniach). Zob. K. Cohen i in., *Detecting linguistic markers for radical violence in social media*, „Terrorism and Political Violence" 2014, nr 26/1, s. 246–256; J. Reid Meloy, *Identifying warning behaviors of the individual terrorist*, http://drreidmeloy.com/wp-content/uploads/2016/05/2016_Individual-Terrorist.pdf [dostęp: 15 IV 2018].

[35] Zob. K. Raynes-Goldie, *Aliases, creeping and wall clearing: understanding privacy in the age of Facebook,* „First Monday" 2010, nr 1–4 (sic!).

do osoby sprawdzanej. Szczególnie mylące i niepozwalające na rzetelną weryfikację są imiona i nazwiska – w takim samym zestawieniu może je bowiem nosić wiele osób. Przykładowo, wyszukanie imienia i nazwiska konkretnej osoby wśród kont na Twitterze ujawni co najmniej kilka kont, z których żadne może nie być kontem tej osoby[36].

Niestety, nie ma idealnej metody weryfikacji wątpliwych tożsamości online wyłącznie na podstawie źródeł otwartych i bez konfrontowania danej osoby z nimi (lub sięgania po dodatkowe dane spoza źródeł otwartych). Najlepsze możliwe rozwiązania tego problemu opierają się na tym, aby: 1 – zdobyte informacje weryfikować krzyżowo z posiadanymi już danymi o wyszukiwanej osobie (istotne mogą być także dane dotyczące relacji tej osoby z innymi osobami, np. z członkami rodziny, którzy również mogą mieć konta w mediach społecznościowych), 2 – być niezwykle ostrożnym przy wyciąganiu jakichkolwiek konsekwencji wyłącznie na podstawie treści odnalezionych online.

Bariery językowe i kulturowe

Istotny problem przy gromadzeniu i analizie danych publikowanych online przez służby migracyjne mogą stanowić bariery językowe i kulturowe. Z oczywistych względów użytkownicy mediów społecznościowych znajdujący się w kręgu zainteresowań pracowników i funkcjonariuszy takich służb będą się na ogół posługiwali obcymi językami narodowymi, niekoniecznie znanymi osobie, która ich weryfikuje. Ten problem można rozwiązać na poziomie organizacyjnym jedynie częściowo – przez zatrudnianie osób o wysokich kwalifikacjach językowych. Narzędziem stosowanym pomocniczo może być także tłumaczenie maszynowe (automatyczne), zwłaszcza przy uwzględnieniu stale rosnącej jakości tego typu usług. Może ono pozwolić na zredukowanie wymaganych umiejętności lingwistycznych wywiadowcy[37].

Różnice kulturowe i brak wiedzy mogą przeszkodzić służbom migracyjnym w zrozumieniu wielu informacji także ze względu na brak znajomości odpowiednich kontekstów czy znaczeń. Bez odpowiedniej wiedzy na temat chociażby bieżących trendów w światowej czy regionalnej propagandzie terrorystycznej wyłonienie treści, które się do niej odwołują, może być znacznie utrudnione. Jako przykład takiego problemu może posłużyć wykorzystywanie przez Państwo Islamskie w 2014 r. oznaczenia #Brazil2014 nawiązującego do trwających wówczas mistrzostw świata w piłce nożnej w celu propagowania materiałów ekstremistycznych[38]. Każda osoba publikująca treści

[36] Przykładowo, przeszukanie wspomnianego portalu społecznościowego pod kątem użytkowników o takim samym imieniu i nazwisku, jak autora niniejszego artykułu, ujawni kilka kont, z których żadne nie jest przez niego prowadzone. Tak prosty „eksperyment" może być powtórzony z wykorzystaniem dowolnych danych osobowych. Z przyczyn etycznych autor artykułu postanowił przedstawić problem na własnym przykładzie.

[37] K. Cohen i in., *Detecting linguistic markers*…, s. 251.

[38] C. Milmo, *Iraq crisis exclusive: Isis jihadists using World Cup and Premier League hashtags to promote extremist propaganda on Twitter*¸ http://www.independent.co.uk/news/world/middle-east/iraq-crisis-exclusive-isis-jihadists-using-world-cup-and-premier-league-hashtags-to-promo-

z tym oznaczeniem mogła więc być albo rzeczywistym fanem piłki nożnej, albo ekstremistą wspierającym terroryzm. Rozróżnienie takich osób wymagało odpowiedniej wiedzy. Podobne problemy można rozwiązać jedynie częściowo – przez prowadzenie szkoleń wewnętrznych i właściwą politykę kadrową.

Problemy prawne i etyczne

Gromadzenie informacji ze źródeł otwartych na podstawie dostarczonych formularzy wizowych może wywoływać wiele pytań o zgodność takiego działania z przepisami prawa i zasadami etyki. Dane z mediów społecznościowych na ogół będą stanowiły „dane osobowe", których gromadzenie i przetwarzanie podlega ścisłym regułom – zwłaszcza prawo obecnie obowiązujące na terenie Unii Europejskiej czyni pozyskiwanie takich informacji problematycznym[39]. Nie przekreśla to szerokiego wykorzystania opisywanych działań, ale może wymusić zmiany w obowiązującym prawie lub szczegółową analizę wymogów, które dotyczą ich legalności.

Częściowym rozwiązaniem może być pozyskanie od samych zainteresowanych zgody na przetwarzanie ich danych, w treści obejmującej zgodę na weryfikację informacji na ich temat opartą na technikach SOCMINT. Pozwoliłoby to na przesunięcie całego procesu poza prawno-etyczną „szarą strefę", ale jednocześnie niesie za sobą zagrożenie zaalarmowania sprawdzanych osób, które w związku z tym mogą starać się usunąć lub ukryć część dostępnych treści. Aby tego uniknąć, należy rozważyć, w jaki sposób można zredagować formularz zgody stanowiący część dokumentów w sprawie aplikacji wizowej i w ten sposób zmniejszyć to ryzyko bez ujawniania zbyt wielu informacji o procesie weryfikacyjnym. Podobnego typu zgody były już stosowane zarówno w sektorze publicznym, jak i prywatnym[40]. Jednak zbyt ogólnikowy formularz zgody może być niewystarczający do spełnienia wymogów prawnych, szczególnie w odniesieniu do gromadzenia danych wrażliwych. Te kwestie muszą być skrupulatnie rozważone przy wdrażaniu jakiejkolwiek polityki.

Podejmowanie decyzji

Po odnalezieniu podejrzanych treści w mediach społecznościowych niezwykle istotne jest uwzględnianie przy ocenie wszystkich ograniczeń, aby wykluczyć możliwość wystąpienia nieporozumień. Treści zamieszczane w Internecie często można źle zrozumieć, fałszywie przypisać ich autorstwo określonej osobie, błędnie uznać za prawdziwe,

te-9555167.html [dostęp: 15 IV 2018].

[39] Zob. zwłaszcza *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych)*.

[40] Zob. m.in. wzór formularza ankiety bezpieczeństwa dla kandydatów do służby cywilnej w Kanadzie, http://www.fja-cmf.gc.ca/appointments-nominations/forms-formulaires/bc-va/bc-va.pdf [dostęp: 15 IV 2018].

podczas gdy są one kłamliwe lub żartobliwe. Przykładowo, publikacja, która miała mieć charakter żartobliwy, spowodowała problemy w sprawie L. van Bryana i E. Bunting – pary podróżującej z Wielkiej Brytanii do Stanów Zjednoczonych, która przed podróżą zamieściła na Twitterze informację o tym, że jedzie „zniszczyć Amerykę". Pomimo tego, że ich zamiarem wyrażonym w ten sposób było spędzanie czasu na imprezach w klubach i barach, kontekst tej informacji nie został rzeczywiście wzięty pod uwagę przez amerykańskie służby. Parze odmówiono prawa wjazdu do Stanów Zjednoczonych i zawrócono ją z granicy USA[41]. Inny przykład dotyczy osoby, która ubiegała się o tygodniową wizę turystyczną i która bezpośrednio przed wyjazdem opublikowała długą wiadomość pożegnalną skierowaną do znajomych. Wynikało z niej, że planuje wielomiesięczną nieobecność w kraju ojczystym. Takie zachowanie mogło wskazywać na chęć przekroczenia terminu dozwolonego pobytu, ale również – na ewentualny wyjazd po jego upływie do innych państw lub nawet zmianę rodzaju wizy z turystycznej na pobytową wkrótce po przyjeździe (np. w związku z zawarciem planowanego małżeństwa)[42].

Co do zasady prawdziwe jest stwierdzenie, że skuteczne wykorzystanie informacji wywiadowczych nie polega li tylko na samym ich gromadzeniu, ale że sukces jest uzależniony od wartości, jaką takie informacje wniosą przy podejmowaniu określonych decyzji[43]. Tym samym najistotniejszą częścią całego procesu jest ocena zgromadzonych danych i odniesienie się do tej oceny przy podejmowaniu decyzji w sprawach wizowych (przy założeniu, że celem jest przestrzeganie rzetelnej i spójnej procedury migracyjnej). Przy czym jest niezbędne ustalenie odpowiedniej i sformalizowanej polityki wewnętrznej w tym zakresie. Dzięki temu osoby odpowiedzialne za przebieg procesów migracyjnych i podejmowanie wiążących decyzji nie powinny być zdane na opieranie się w tej sprawie wyłącznie na własnym przeczuciu co do tego, w jaki sposób należy reagować w konkretnych sytuacjach. Konieczne jest więc zdefiniowanie zasad stosowania technik SOCMINT obejmujących szczegółowe wytyczne i wskazówki dotyczące nie tylko technik i możliwości gromadzenia danych ze źródeł otwartych, lecz także tego, w jaki sposób należy reagować w określonych sytuacjach, jakie treści powinny być uznane za „interesujące" i kwalifikujące się do dalszego sprawdzenia, kiedy i jakie informacje należy weryfikować w innych źródłach, kiedy prosić o dodatkowe dokumenty czy też w jakim momencie i na jakich warunkach osobiście konfrontować daną osobę z pozyskanymi informacjami jeszcze przed podjęciem decyzji ostatecznej.

[41] R. Hartley-Parkinson, *I'm going to destroy America and dig up Marilyn Monroe': British pair arrested in the US on terror charges over Twitter jokes*, http://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes, html [dostęp: 15 IV 2018].

[42] Sprawa została zrelacjonowana podczas wywiadu badawczego z przedstawicielem australijskiej agencji rządowej (szczegółowe dane nie zostały ujawnione ze względu na konieczność zachowania poufności).

[43] D. Omand, J. Bartlett, C. Miller, *Introducing Social Media Intelligence (SOCMINT)*, „Intelligence and National Security" 2012, nr 1, s. 7.

Wnioski i rekomendacje

Wykorzystanie technik SOCMINT bez wątpienia stwarza wiele możliwości wszelkim podmiotom państwowym i prywatnym, w tym zwłaszcza dbającym o utrzymanie bezpieczeństwa wewnętrznego. Zastosowanie tych technik w procesie migracyjnym, przy weryfikacji osób starających się o prawo wjazdu do danego kraju czy pobytu na jego terenie, może pozwolić na uzyskanie dodatkowej warstwy ochronnej w kontekście zagrożeń terrorystycznych, jak również może służyć weryfikacji danych prawnie relewantnych (tj. wpływających na prawo do wjazdu), podawanych przez takie osoby. Służby wizowe i migracyjne dysponują kompletnymi zestawami danych osobowych, które mogą służyć za „filtr danych wejściowych" w celu przeprowadzenia sprofilowanych przeszukań źródeł otwartych. Jednocześnie przy wykorzystywaniu tego rodzaju informacji należy pamiętać o uwzględnianiu obowiązujących norm prawnych.

Dzięki ocenie treści zamieszczonych na profilu społecznościowym jest możliwe ujawnienie zagrożeń bezpieczeństwa lub informacji stanowiących podstawę do odmowy wydania decyzji dotyczącej prawa wjazdu. Skutki odmowy wjazdu lub pobytu na terytorium danego kraju mogą być dla zainteresowanego bardzo poważne na gruncie prywatnym. Z tego powodu należy ze szczególną ostrożnością uwzględniać potencjalne problemy z tym związane, a cała procedura musi być prowadzona z przestrzeganiem zasady domniemania niewinności (stosowanej tu odpowiednio i w specyficznym rozumieniu). Biorąc pod uwagę wielość możliwości i zagrożeń wynikających z wykorzystania technik SOCMINT w procesie migracyjnym, należy opowiedzieć się za każdorazowym tworzeniem wewnątrzinstytucjonalnej polityki ich stosowania. W celu ograniczenia kosztów i zminimalizowania różnych rodzajów ryzyka polityka wewnętrzna powinna odnosić się do takich spraw, jak to, kiedy przeprowadzać weryfikację (czy wszyscy kandydaci powinni być sprawdzani, czy tylko niektóre ich grupy, np. odwiedzający kraj po raz pierwszy?), jakie narzędzia powinny być wykorzystywane przy weryfikacji (czy ewentualnie planuje się wdrożenie specjalistycznego oprogramowania?), gdzie poszukiwać informacji, jak je weryfikować (czy kandydat powinien być konfrontowany z pozyskanymi informacjami?) i czym się należy kierować na ostatecznym etapie procesu decyzyjnego. Stworzenie tego rodzaju wewnętrznego regulaminu działania powinno być wsparte również przez prowadzenie adekwatnych szkoleń merytorycznych. Można założyć, że wykorzystywanie danych ze źródeł jawnych w różnych obszarach życia publicznego i procedurach bezpieczeństwa będzie się pogłębiać. Już dziś trzeba poszukiwać najefektywniejszych sposobów wykorzystania SOCMINT w celu zapewnienia bezpieczeństwa.

Bibliografia:

Arslan C., Yanuk M., *A New Discipline of Intelligence: Social Media*, Istanbul 2015, ICMSS.

Benson D.C., *Why the Internet is not increasing terrorism*, „Security Studies" 2014, nr 23/2, s. 6.

Cohen K. i in., *Detecting linguistic markers for radical violence in social media*, „Terrorism and Political Violence" 2014, nr 26/1, s. 246–256.

Dabhi M.D., *Geofencing: a generic approach to Real time location based tracking system*, „International Journal of Computer Networks and Wireless Communications" 2016, t. 6.

Hamm M., Spaaij R., *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies*, Washington 2015, US Department of Justice.

Kaplan A., Haenlein M., *Users of the world, Unite!*, „Business Horizons" 2010, nr 53/1.

Klausen J., *Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq*, „Studies in Conflict and Terrorism" 2015, nr 38.

Liaropoulos N., *The challenge of social media for the Intelligence community*, „Journal of Mediterranean and Balkan Intelligence" 2013, nr 1.

Omand D., Bartlett J., Miller C., *Introducing Social Media Intelligence (SOCMINT)*, „Intelligence and National Security" 2012, nr 1.

Paullet K., Pinchot J., *Cybercrime: the unintentional effects of oversharing information on Facebook*, Proceedings of the Conference on Information Systems Applied Research, New Orleans 2012, EDSIG-AITP.

Raynes-Goldie K., *Aliases, creeping and wall clearing: understanding privacy in the age of Facebook*, „First Monday" 2010, nr 1–4.

Taleb N.N., *Black Swan*. *The impact of the highly improbable*, New York 2007, Random House.

Apuzzo M., Schmidt M.S., Preston J., *U.S. Visa Process Missed San Bernardino Wife's Online Zealotry*, 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?_r=0 [dostęp: 15 IV 2018].

Cooke K., *US Police used Facebook, Twitter data to track protesters*, http://www.reuters.com/article/social-media-data-idUSL4N1CH4J1 [dostęp: 15 IV 2018].

Facebook community standards, https://www.facebook.com/communitystandards [dostęp: 15 IV 2018].

Facebook, *Information for law Enforcement Authorities*, https://scontentfra31.xx.fbcdn.net/hphotosxfp1/t39.23656/12532957_530107840495531_2074830868_n.pdf [dostęp: 15 IV 2018].

Facebook law enforcement guidelines, 2010, https://info.publicintelligence.net/Facebook2010-2.pdf [dostęp: 15 IV 2018].

Full text of Gym Killer's blog, http://nypost.com/2009/08/05/full-text-of-gym-killers-blog/ [dostęp: 15 IV 2018].

Google Transparency Report, https://www.google.com/transparencyreport/userdatarequests/#! [dostęp: 15 IV 2018].

Hartley-Parkinson R., *'I'm going to destroy America and dig up Marilyn Monroe': British pair arrested in the US on terror charges over Twitter jokes*, http://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes.html [dostęp: 15 IV 2018].

http://www.fp7-prime.eu/home_page [dostęp: 15 IV 2018].

Ingram D., *Facebook says data leak hits 87 million sers, widening privacy skandal*, https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM [dostęp: 15 IV 2018].

Milmo C., *Iraq crisis exclusive: Isis jihadists using World Cup and Premier League hashtags to promote extremist propaganda on Twitter*, http://www.independent.co.uk/news/world/middle-east/iraq-crisis-exclusive-isis-jihadists-using-world-cup-and-premier-league-hashtags-to-promote-9555167.html [dostęp: 15 IV 2018].

Ministerstwo Spraw Zagranicznych RP, *System eKonsulat*, https://secure.ekonsulat.gov.pl/Uslugi/RejestracjaTerminu.aspx?IDUSLUGI=1&IDPlacowki=157 [dostęp: 15 IV 2018].

O'Brien B., *U.S. visa applicants to be asked for social media history: State Department*, https://www.reuters.com/article/us-usa-immigration-visa/u-s-visa-applicants-to-be-asked-for-social-media-history-state-department-idUSKBN1H611P [dostęp: 15 IV 2018].

Reid Meloy J., *Identifying warning behaviors of the individual terrorist*, http://drreidmeloy.com/wp-content/uploads/2016/05/2016_IndividualTerrorist.pdf [dostęp: 15 IV 2018].

Ross B. i in., *Secret US Policy blocks agents from looping at social media of visa applicants, former official says*, http://abcnews.go.com/US/secret-us-policy-blocks-agents-social-media-visa/story?id=35749325 [dostęp: 15 IV 2018].

Schengen Information System, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm [dostęp: 15 IV 2018].

Serrano R.A., *FBI chief: San Bernardino shooters did not publicly promote jihad on social media*, http://www.latimes.com/nation/la-ln-fbi-san-bernardino-social-media-20151216-story.html [dostęp: 15 IV 2018].

Shontell A., *7 People who were arrested because of something they wrote on Facebook*, http://www.businessinsider.com/people-arrested-for-facebook-posts-2013-7?IR=T [dostęp: 15 IV 2018].

Social media use in law enforcement: crime prevention and investigative activities continua to driver usage, https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf [dostęp: 15 IV 2018].

Terrorist Screening Center, https://www.fbi.gov/about-us/nsb/tsc/tsc [dostęp: 15 IV 2018].

Twitter appeals ruling in bat tle over occupy Wall Street protester's information, https://www.aclu.org/blog/twitter-appeals-ruling-battle-over-occupy-wall-street-protesters-information?redirect=blog/technology-and-liberty-national-security-free-speech/twitter-appeals-ruling-battle-over-occupy [dostęp: 15 IV 2018].

Twitter, *Guidelines for law enforcement*, https://support.twitter.com/articles/41949# [dostęp: 15 IV 2018].

Abstrakt

Monitoring Internetu i analiza danych ze źródeł otwartych stanowią istotną część działań antyterrorystycznych o charakterze prewencyjnym. Bogactwo informacji i danych osobowych możliwych do odnalezienia w mediach społecznościowych jest wykorzystywane nie tylko do zwalczania zagrożeń terrorystycznych, lecz także do walki z przestępczością kryminalną. Artykuł opisuje możliwości i zagrożenia związane z potencjalnym wykorzystywaniem tzw. *Social Media Intelligence* (SOCMINT) w procedurach migracyjnych w celu zagwarantowania bezpieczeństwa wewnętrznego.

Słowa kluczowe: terroryzm, migracja, OSINT, SOCMINT, media społecznościowe.